Sicherheitskonzept für autonome Fahrzeuge

23

Andreas Reschka

Inhaltsverzeichnis

A. Reschka (✉)
Technische Universität Braunschweig, Institut für Regelungstechnik, Deutschland
reschka@ifr.ing.tu-bs.de

M. Maurer et al. (Hrsg.), *Autonomes Fahren*,
DOI 10.1007/978-3-662-45854-9_23,

23.1 Einleitung

Die Entwicklung von autonomen Fahrzeugen fokussiert sich derzeit auf die Funktionalitäten von Fahrzeugführungssystemen. In zahlreichen Demonstrationen von Versuchsfahrzeugen wurden beeindruckende Fähigkeiten gezeigt (im Folgenden werden die neuesten zuerst genannt). So z. B. bei der Fahrt auf der Bertha-Benz-Route des Karlsruher Instituts für Technologie und der Daimler AG [69], im Projekt Stadtpilot der Technischen Universität Braunschweig [41], [60] den Aktivitäten der Google Inc. [13], [59], dem Forschungsfahrzeug BRAiVE und dem VIAC Projekt des VisLab-Instituts der Università degli Studi di Parma [4], [8], den Forschungsaktivitäten des Sonderforschungsbereichs 28 der Deutschen Forschungsgemeinschaft [31], [55], [57] und den Resultaten bei der DARPA Urban Challenge [51], [52], [53]. Falls die Versuchsträger am öffentlichen Straßenverkehr teilnahmen, war immer ein Sicherheitsfahrer an Bord, der das technische System überwacht hat. Dieser musste eingreifen, falls ein technischer Defekt auftrat, die aktuelle Situation die Fähigkeiten des Fahrzeugs überforderte oder ein anderes Ereignis dies erforderlich machte. Durch diese notwendige Überwachung des technischen Systems sind die gezeigten Versuchsfahrten im öffentlichen Straßenverkehr nach der Klassifikation von Automatisierungsgraden nach [20] als *teilautomatisiert* einzustufen. Das Ziel zukünftiger Fahrzeugführungssysteme mit höheren Automatisierungsgraden ist jedoch, die Systeme selbstständig in allen Situationen auch ohne überwachende Menschen betreiben zu können.

Bei der Entwicklung von Fahrzeugführungssystemen ist daher ein Sicherheitskonzept notwendig, das die verschiedenen Schritte im Entwicklungsprozess wie z. B. die Spezifikation, den Entwurf, die Entwicklung und den Test der Funktionen abdeckt. Außerdem sind Sicherheitsfunktionen im System notwendig, die einen sogenannten *sicheren Zustand* erreichen können bzw. diesen zu erhalten versuchen.

23.2 Sicherer Zustand

Die Verwendung des Begriffs *sicherer Zustand* ist oftmals nicht eindeutig. Sicherheit als relatives Maß ist abhängig von einer individuellen Einschätzung des Betrachters. Sicherheit besteht nach der Norm ISO 26262 in einem Betriebsmodus eines Systems oder einer Anordnung von Systemen, ohne *unzumutbares* Risiko (vgl. „safe state“, ISO 26262, Part I, 1.102 [30]). Dies beinhaltet, dass Sicherheit nur dann vorliegt, wenn das aktuelle und das zukünftige Risiko unterhalb einer von einer Gesellschaft akzeptierten Schwelle liegen (vgl.

„unreasonable risk“, ISO 26262, Part I, 1.136 [30]). Diese Schwelle ist als nicht akzeptabler Wert in einem spezifischen Kontext gemäß gesellschaftlicher, moralischer und ethischer Auffassungen zu sehen (vgl. ISO 26262, Part I, 1.136 [30]). Unter Risiko wird eine Kombination aus der Auftrittswahrscheinlichkeit und der Schwere eines Personenschadens verstanden (vgl. „risk“ und „harm“, ISO 26262, Part I, 1.99 und 1.56).

Aus diesem Verständnis lässt sich ein sicherer Zustand als ein Zustand mit zumutbarem Risiko eines Systems verstehen. Der häufig verwendete Begriff *risikominimaler Zustand* (z. B. in [20]) ist missverständlich, da dieser das Risiko nicht in eine Relation zu einem akzeptierten Risiko stellt und auch keine Aussage darüber enthält, ob ein System, das risikominimal betrieben wird, auch sicher ist.

Die wesentliche Herausforderung bei der Verwendung des Begriffs *sicherer Zustand* im Sinne eines Zustands mit zumutbarem Risikos für Insassen und weitere Verkehrsteilnehmer ist die Identifikation einer Schwelle, unterhalb der ein Risiko zumutbar ist. Beim Betrieb eines automatisierten Fahrzeugs hängt das zumutbare Risiko von der aktuellen *Situation*, in der sich das Fahrzeug befindet, ab. Zur Situation gehören hier analog zu [21] und [43]

- alle für eine Fahrentscheidung relevanten stationären und dynamischen Objekte,
- die Intention der dynamischen Objekte einschließlich des autonomen Fahrzeugs,
- die geltenden rechtlichen Bedingungen,
- die Mission des autonomen Fahrzeugs,
- die aktuelle Leistungsfähigkeit des autonomen Fahrzeugs.

Für ein autonomes Fahrzeug ist daher eine kontinuierliche Ermittlung des aktuellen Risikos basierend auf der aktuellen Situation und ein Abgleich des Risikos mit dem Schwellwert, der als gerade noch zumutbar gilt, notwendig. Im Sinne der Norm ISO 26262 bedeutet dies, dass für jede Situation und ihre zukünftig möglichen Entwicklungen die Auftrittswahrscheinlichkeit für einen Personenschaden und die Schwere des Personenschadens für jeden beteiligten Verkehrsteilnehmer ermittelt und dann die Handlungsoptionen identifiziert werden müssen, die ein zumutbares Risiko ergeben. Eine technische Lösung für dieses Problem ist dem Autor bisher nicht bekannt.

23.2.1 Sicherer Zustand in Fahrerassistenzsystemen im Serieneinsatz

In Fahrerassistenzsystemen überwacht der Fahrer das technische System und muss dem Verkehrsgeschehen aufmerksam folgen. Er wird bei der Fahraufgabe unterstützt. In der aktuellen S-Klasse von Mercedes-Benz wird das „DISTRONIC PLUS mit Lenk-Assistent und Stop&Go Pilot“ genannte System angeboten, das den Fahrer sowohl bei der Längsführung als auch bei der Querführung unterstützt [49]. Der Fahrer muss jedoch weiterhin dem Verkehrsgeschehen folgen, und die Querführung deaktiviert sich nach einer gewissen Zeit, falls der Fahrer die Hände vom Lenkrad nimmt:

> Erkennt der Lenk-Assistent mit Stop&Go Pilot, dass der Fahrer während der Fahrt die Hände vom Lenkrad nimmt, wird der Fahrer intelligent in Abhängigkeit von der Fahrsituation, des Handmomentensensors, der erfassten Umgebung und der Geschwindigkeit optisch im Kombiinstrument gewarnt. Reagiert der Fahrer nicht, ertönt ein Warnton und die Querführung wird deaktiviert. [49]

Durch diese Eigenschaft ist das System als teilautomatisiert nach [20] bzw. *Partial Automation* nach [48] einzustufen. Die Längsführung kann sich ebenfalls beenden und bei geeigneter Signalisierung an den Fahrer übergeben, sobald es zu technischen Störungen kommt oder, je nach Auslegung des Systems, Systemgrenzen wie z. B. eine minimale Geschwindigkeit unterschritten werden [62].

In [25] wurde 2010 ein Sicherheitskonzept für teilautomatisierte und hochautomatisierte Fahrerassistenzsysteme vorgestellt. Jedoch wurden die Begriffe hier noch anders verwendet. In [25] bedeutete *Fully Automated DAS* (FA-DAS) eigentlich *teilautomatisiert* nach [20], da der Fahrer die Quer- und die Längsführung überwachen muss. *Autonomous DAS* (A-DAS) in [25] ist gleichbedeutend mit *vollautomatisiert* nach [20], da der Fahrer nicht dauerhaft überwachen muss und das System selbstständig einen sicheren Zustand erlangen kann. Nach [24] wird der sichere Zustand durch ein Anhalten an einem ungefährlichen Ort erreicht. Da der Fokus auf einem System zur automatisierten Staufahrt auf der Autobahn bis maximal 60 km/h liegt, erscheint das Anhalten auf einem Fahrstreifen als sicherer Zustand, bis ein Mensch die Kontrolle übernimmt. Die relativen Geschwindigkeiten werden aufgrund der Stausituation als gering angenommen [24], [25].

Zum gleichen Ergebnis kommt auch eine Studie zum Potenzial der automatisierten Fahrt auf Autobahnen [45]. Diese entstand im Rahmen der Entwicklung eines Notfallassistenzsystems, das ein Fahrzeug stoppen kann (sicherer Zustand), falls der Fahrer das Bewusstsein verliert oder aus anderen Gründen nicht mehr zur Fahrzeugführung in der Lage ist [32], [45]. Auch in [37] wird ein solches System vorgestellt. Die Sicherheitsanforderungen sind hier höher als bei einem Stauassistenzsystem, da das Fahrzeug nicht einfach anhalten, sondern den fließenden Verkehr verlassen und auf dem Seitenstreifen stoppen soll. Außerdem ist das System auch für den normalen Autobahnverkehr und nicht nur für den Stau konzipiert, sodass es zu sehr hohen relativen Geschwindigkeiten kommen kann. Daraus ergeben sich erhöhte Anforderungen an die Zuverlässigkeit der Umfeldwahrnehmung, da andere Verkehrsteilnehmer bei den Fahrstreifenwechseln auf den Seitenstreifen beachtet werden müssen [45]. Redundante Sensorik zumindest für den Bereich vor, hinter und bei Rechtsverkehr auch rechts neben dem Fahrzeug ist hier erforderlich. Der Nutzen solcher Notfallassistenzysteme ist dennoch vorhanden, auch wenn das System aufgrund technischer Probleme nicht voll einsatzfähig ist. Ein unkontrolliert fahrendes Fahrzeug auf der Autobahn ist gefährlicher als ein kontrolliert langsam fahrendes oder stehendes Fahrzeug, das durch geeignete Signalisierung auf sich aufmerksam machen kann – selbst wenn der Wechsel auf den Seitenstreifen nicht möglich ist [32], [37].

Zusammenfassend lässt sich für Fahrerassistenzsysteme sagen, dass bei Verfügbarkeit eines Fahrers im Fahrzeug ein sicherer Zustand entweder mit der Übergabe an diesen oder

mit dem Bremsen in den Stillstand erreicht werden kann. Wie bei dem vorgestellten Notfallassistenzsystem kann zwar versucht werden, den Seitenstreifen zu erreichen, jedoch sind die Anforderungen hierfür relativ hoch. Auch bei höher automatisierten Systemen stellen die Übergabe an einen möglichen Verfügbarkeitsfahrer und die Abbremsung in den Stillstand mögliche Aktionen zur Erhaltung und Erlangung eines sicheren Zustands dar.

23.2.2 Sicherer Zustand in Versuchsträgern zum autonomen Fahren

Im Fokus der im Folgenden vorgestellten Projekte steht das autonome Fahren auf allen Straßenarten und in allen Umgebungen. Die entwickelten Systeme sollen die Fahraufgabe vollständig übernehmen können und den Menschen als Überwacher nicht mehr benötigen. Über die Sicherheitsfunktionen und Sicherheitskonzepte der verschiedenen Projekte gibt es nur wenige Veröffentlichungen. Dies kann u. a. daran liegen, dass es relativ einfach ist, den Fahrer weiterhin als Überwacher einzusetzen und daher keine umfangreichen Sicherheitssysteme zu nutzen, oder auch daran, dass der funktionalen Sicherheit der Systeme für den fahrerlosen Betrieb bisher keine angemessene Aufmerksamkeit zukommt. Die betrachteten Projekte sind im Folgenden chronologisch gelistet, der erreichte Automatisierungsgrad nach [20] und die eingesetzten Sicherheitsmechanismen werden hervorgehoben.

Die Projekte der 1950er- bis in die 1990er-Jahre fokussierten sich nur auf die funktionalen Aspekte der maschinellen Fahrzeugführung wie z. B. die ersten Ansätze zur Verknüpfung von Infrastruktur und Fahrzeug in den General Motors Research Labs, wo Magnete in die Fahrbahn eingelassen wurden, die dann vom Fahrzeug erkannt werden konnten. Der Fahrer musste dabei ständig auf den Verkehr achten und das System überwachen [17]. In Japan wurde in den 1970er- und 1980er-Jahren die Fahrzeugautomatisierung durch Erkennung von Fahrstreifen mit bildgebenden Kameras erforscht. Auch hier wurde das System dauerhaft vom Fahrer überwacht [58]. Gleiches gilt für die Aktivitäten in den 1990er-Jahren, beispielsweise bei der Demonstration *No Hands Across America* 1995 der Carnegie Mellon University [50], [56]. Hier wurde nur die Querführung maschinell durchgeführt. Auf europäischer Seite ist eine Versuchsfahrt der Universität der Bundeswehr von München nach Odense mit dem Versuchsträger *VaMoRs-P* ebenfalls im Jahr 1995 hervorzuheben. Bei dieser Fahrt wurde die Längs- und Querführung maschinell durchgeführt und vom Fahrer überwacht. Zusätzlich wurden automatische Fahrstreifenwechsel vom Fahrer ausgelöst [36]. Mit dem Versuchsträger *ARGO* des VisLab-Instituts der Università degli Studi di Parma erfolgten ebenfalls Langstreckenfahrten im Jahr 1998. Die Automatisierung deckte neben der Längs- und Querführung auch Fahrstreifenwechsel ab, die vom Sicherheitsfahrer ausgelöst wurden [7]. Alle genannten Projekte sind als teilautomatisiert nach [20] einzuordnen. Der sichere Zustand wurde durch eine Übergabe an den Sicherheitsfahrer erreicht bzw. durch einen Eingriff des Sicherheitsfahrers in die Fahrzeugführung wiederhergestellt. Einen ausführlicheren Einblick in die Entwicklungen in den 1990er-Jahren gibt Dickmanns in [14] mit einem Fokus auf kamerabasierte Bildverarbeitung.

Tabelle 23.1 Fehlercodes (übersetzt aus dem Englischen, aus [6])

Fehlercode	Bedeutung	Aktion
F0	„OK!“	keine Aktion
F1	„Wartung notwendig“	notwendige Wartung berücksichtigen
F2	„Nach Hause zurückkehren“	Rückkehr zur Wartungsstation mit reduzierter Geschwindigkeit
F3	„Sicheres Parken“	auf dem nächsten verfügbaren Parkplatz anhalten
F4	„Sofortiges Anhalten“	sofortiges Anhalten des Fahrzeugs am Straßenrand ohne Gefährdung anderer Verkehrsteilnehmer
F5	„Nothalt“	sofortiges kontrolliertes Bremsen in den Stillstand (mit Lenkfunktion, falls möglich)
F6	„Notbremsung“	sofortiges Stoppen des Fahrzeugs durch Betätigung der Bremsen

Im Projekt *Autonomes Fahren* in Niedersachsen wurde 1998 ebenfalls an der Entwicklung autonomer Fahrzeuge geforscht. In [6] wird ein Sicherheitskonzept beschrieben, das verschiedene Methoden enthält, die auch für heutige Systeme denkbar und sinnvoll sind. In Tab. 23.1 sind Fehlercodes, deren Bedeutung und Aktionen enthalten, die zur Erlangung eines sicheren Zustands vom Fahrzeug ausgeführt werden können. Die gewählte Kategorisierung ist auch für hoch- und vollautomatisierte Systeme nach [20] möglich. Eine ausführlichere Diskussion der Aktionen folgt bei der Betrachtung der jeweiligen sicheren Zustände zu den Use-Cases aus Kap. 2.

In der DARPA Urban Challenge wurden alle teilnehmenden autonomen Fahrzeuge ohne Fahrer an Bord auf einem abgesperrten Militärstützpunkt betrieben. Das Sicherheitskonzept wurde von der DARPA vorgegeben und beinhaltete eine Möglichkeit zum sofortigen Anhalten der Fahrzeuge über eine Fernsteuerung und über Not/Aus-Schalter außen an den Fahrzeugen [2]. Das Sicherheitskonzept des Teams CarOLO der Technischen Universität Braunschweig nutzte die Zeit nach dem Nothalt, um Aktionen der Selbstheilung durchzuführen [19], [22], [44]. Dadurch war das autonome Fahrzeug in der Lage, fehlerhafte Komponenten des Fahrzeugführungssystems neu zu starten [2]. Ähnlich sind auch die anderen Teams im Finale der Urban Challenge vorgegangen [51], [52], [53].

Der Nothalt über eine Fernsteuerung als letzte Aktion zur Erreichung eines sicheren Zustands war nur möglich, weil die Fahrzeuge auf einem abgesperrten Gebiet fuhren, von überwachenden Fahrzeugen verfolgt wurden und die anderen Verkehrsteilnehmer entweder von professionellen Fahrern geführte Fahrzeuge oder autonome Fahrzeuge waren. Im öffentlichen Straßenverkehr wäre eine Fahrt mit den Leistungsfähigkeiten der Versuchsträger zu gefährlich gewesen.

Im Projekt Stadtpilot der Technischen Universität Braunschweig wird teilautomatisiertes Fahren seit 2010 im öffentlichen Straßenverkehr gezeigt [41], [60]. Die Forschung in diesem Projekt ist auf den vollautomatisierten Betrieb des Versuchsträgers *Leonie* ausge-

richtet. Bei der Fahrt im öffentlichen Straßenverkehr muss jedoch ein Sicherheitsfahrer den Verkehr überwachen und eingreifen, bevor es zu gefährlichen Situationen kommen kann.

Das Fahrzeugführungssystem übergibt die Kontrolle an den Sicherheitsfahrer, falls es an Systemgrenzen stößt bzw. Fehler im System auftreten. Da im öffentlichen Straßenverkehr keine anderen Sicherheitsaktionen durchgeführt werden, ist der sichere Zustand die Übergabe an den Fahrer. Da das System in Teilen in der Lage ist, die eigene Leistungsfähigkeit zu ermitteln, wie z. B. die Güte der Lokalisierung, sind auch andere Aktionen möglich. Beispielsweise ist ein Anhalten am Straßenrand oder auch auf dem aktuellen Fahrstreifen denkbar, eine Weiterfahrt mit erhöhten Sicherheitsabständen und mit reduzierter Geschwindigkeit ist ebenfalls möglich, wird bisher aber nur auf dem Testgelände durchgeführt [46], [47].

Mit dem autonomen Versuchsträger Junior 3 demonstrierten die Stanford University und das Volkswagen Electronic Research Lab 2010 automatisiertes Fahren [35], [54]. Der Aufbau des Versuchsträgers ist dem Versuchsträger Leonie aus dem Projekt Stadtpilot ähnlich. Die Aktivierung von automatisierten Fahrfunktionen wird über *silver switches* gesteuert. Diese ermöglichen eine Verbindung zwischen dem Fahrzeugführungssystem und der Aktorik des Fahrzeugs. Im *Fail-safe-* Zustand sind diese Schalter geöffnet, und es besteht keine Verbindung zwischen Fahrzeugführungssystem und Fahrzeug. Dadurch liegt die Kontrolle beim notwendigen Sicherheitsfahrer. Eine Besonderheit ist die Valet-Parken-Funktion des Fahrzeugs, die auf einem abgesperrten Gelände auch ohne Sicherheitsfahrer genutzt werden kann. Zur Sicherheit verfügt das Fahrzeug über eine *e-stop* genannte Funktion, die in ähnlicher Weise auch in der DARPA Urban Challenge genutzt wurde. Die Überwachung des Systems wird mit einem *Health Monitor* realisiert, der Fehlfunktionen von Softwaremoduln erkennt und Funktionen zur Selbstheilung auslöst. Außerdem ist das Fahrzeug selbstständig in der Lage, im Notfall die Bremsen zu betätigen und anzuhalten. Das stehende Fahrzeug ist somit der sichere Zustand, der über den e-stop und durch das Sicherheitssystem erreicht wird.

Das VisLab-Institut der Università degli Studi di Parma zeigte 2012 mit dem Versuchsträger BRAiVE teilautomatisiertes Fahren im öffentlichen Straßenverkehr auf einer teilweise gesperrten Strecke. Auf Teilstücken der Strecke war kein Fahrer auf dem Fahrersitz, und nur der Beifahrer konnte über einen Not/Aus-Schalter in die Fahrzeugführung eingreifen. Außerdem war ebenfalls eine e-stop- Funktionalität integriert [8], [23].

An der Carnegie Mellon University wurde nach der DARPA Urban Challenge weiter am Versuchsträger BOSS gearbeitet und ein Ansatz zur Überwachung und Rekonfiguration in Echtzeit entwickelt und veröffentlicht [33]. Dieser *SAFER* genannte Ansatz nutzt redundante Softwarekomponenten, die sich im Normalbetrieb im Stand-by befinden und bei Bedarf aktiviert werden können. Dadurch ist es möglich, innerhalb kürzester Zeit von einer defekten Komponente auf eine redundante Lösung umzuschalten. Da keine Hardwareüberwachung stattfindet, werden auch keine Sensoren und Aktoren überwacht, wodurch der Ansatz als Ergänzung zu Methoden der Hardwareredundanz zu nutzen ist.

Als letztes Beispiel für die derzeitige Entwicklung von autonomen Fahrzeugen soll das Projekt *Self Driving Car* der Google Inc. betrachtet werden. Zunächst wurden in diesem Projekt seriennahe Fahrzeuge mit Sensorik ausgestattet und im öffentlichen Verkehr in

Nevada und Kalifornien betrieben [13], [59]. Obwohl es nur spärliche Informationen über die genutzte Technologie in den Fahrzeugen gibt, erscheint ein Einsatz ohne Sicherheitsfahrer bisher noch nicht möglich. Wie in [13] beschrieben, gibt es zahlreiche Situationen, die die Leistungsfähigkeit des Systems übersteigen. Der sichere Zustand bei diesen Fahrzeugen ist ebenfalls die Übernahme der Kontrolle durch den Fahrer. 2014 wurde ein Prototyp vorgestellt, der nicht mehr über Bedienelemente für den Fahrer verfügt und somit auf jeden Fall als vollautomatisiert nach [20] einzustufen ist, da es keine Möglichkeit zur Übersteuerung gibt. Dieses Fahrzeug wird jedoch bisher nicht im öffentlichen Straßenverkehr eingesetzt.

23.2.3 Zusammenfassung

Wie die betrachteten Projekte zeigen, gibt es bisher noch kein durchgängiges Sicherheitskonzept, das alle Anforderungen an eine Automatisierung von Fahrzeugen ohne Sicherheitsfahrer im öffentlichen Straßenverkehr erfüllt. In einigen der Projekte wurden jedoch leistungsfähige Sicherheitsfunktionen gezeigt, die verschiedene Situationen und Ereignisse abdecken. Nimmt man an, dass der sichere Zustand zukünftig entsprechend der „Adopted Regulation of the Department of Motor Vehicles“, Abschnitt 16.2 (d) aus Nevada erreicht werden soll, muss ein autonomes Fahrzeug zu jedem Zeitpunkt der Fahrt in der Lage sein, den fließenden Verkehr zu verlassen und am Straßenrand oder auf einem Seitenstreifen anzuhalten [39]. Dies würde Fahrstreifenwechsel erfordern, die wiederum von einer zuverlässig funktionierenden Umfeldwahrnehmung, Entscheidungsfindung und deren Umsetzung abhängen. Ein einfaches Anhalten, wie es in einigen der Projekte neben der Übergabe an den Sicherheitsfahrer gemacht wird, ist nicht ausreichend. Die Nutzung von einer Kombination aus den vorgestellten Ansätzen zur funktionalen Sicherheit erscheint daher notwendig – wahrscheinlich sind jedoch noch weitere Sicherheitsmaßnahmen zu ergreifen, mit denen eine höhere Zuverlässigkeit erreicht werden kann [39].

23.3 Sicherheitskonzepte aus anderen Disziplinen

Neben autonomen Fahrzeugen und Fahrerassistenzsystemen spielt die funktionale Sicherheit auch in anderen technischen Bereichen eine wichtige Rolle. Im Folgenden werden daher Sicherheitskonzepte aus weiteren Disziplinen vorgestellt und deren Anwendbarkeit auf autonome Fahrzeuge untersucht.

23.3.1 Schienenfahrzeuge

Schienenfahrzeuge werden bereits seit einigen Jahren automatisch betrieben. Im Personenverkehr ist dabei meist ein Zugführer vorhanden, der eine überwachende Aufgabe über-

nimmt [66]. Im Gegensatz zu den hier betrachteten autonomen Fahrzeugen werden Sicherheitsfunktionen häufig in die Infrastruktur integriert, beispielsweise werden Gleisbelegungen in Steuerzentralen koordiniert, und die überwachenden Komponenten sind in die Gleise integriert. Die Steuerungssysteme haben die Aufgabe, Streckenabschnitte immer nur mit einem Zug zu belegen, um Kollisionen zu vermeiden. Dies wird durch im Gleis verbaute Sensoren und Systeme (w*aysidecentric*) wie z. B. Achszähler am Eingang und am Ausgang eines Streckenabschnitts realisiert [42]. Ist ein Abschnitt belegt, so werden die Signale entsprechend geschaltet, um eine Einfahrt zu verhindern. Die Kollisionsvermeidung ist daher vorrangig ein logistisches Problem, speziell der Verkehrsbetriebstechnologie. Die mechanische Querführung ohne Freiheitsgrad bei Schienenfahrzeugen reduziert die Komplexität der Situationen und Handlungsoptionen. Vereinfacht gesagt kommt es nur darauf an, dass Züge auf freien Gleissegmenten mit angemessener Geschwindigkeit fahren, um ein Entgleisen zu verhindern. Eine Überwachung der Strecke vor dem Zug ist aufgrund der langen Anhaltewege nicht mit Umfeldsensorik möglich. Dennoch verfügen Züge und Bahnen über Nothaltefunktionen, die von den Passagieren und dem Zugführer an Bord und in fahrerlosen Bahnen auch von extern ausgelöst werden können.

In fahrerlosen Zügen und Bahnen wird die Geschwindigkeit der Fahrt automatisch geregelt, und neben der Überwachung der Gleisbelegung durch die Infrastruktur verfügen die Systeme auch über Onboard-Mechanismen (*vehiclecentric*). Die Kommunikation zwischen Steuerzentrale und Fahrzeug erfolgt über Funktechnologien, genauso wie die Kommunikation zwischen Bahnsteigen und fahrerlosen U-Bahnen. Dadurch kann eine redundante Türüberwachung am Bahnsteig und in der Bahn genutzt werden, um Gefährdungen durch sich schließende Türen zu verhindern. Das *Communication Based Train Control* (CBTC) hat sich zu einem Standard entwickelt, der in zahlreichen Bahnsystemen weltweit eingesetzt wird [42].

In der Nürnberger U-Bahn RUBIN wird ein solches System zur automatisierten Zugführung eingesetzt. Auf den Bahnstrecken gibt es einen gemischten Verkehr von Bahnen mit und ohne Fahrer. Ein wesentlicher Bestandteil des Sicherheitskonzepts ist die Überwachung der Türen [38]. Hier werden Komponenten der automatischen Zugschutzsysteme (*Automatic Train Protection* (ATP)) und des automatischen Zugbetriebs (*Automatic Train Operation* (ATO)) eingesetzt, die in stationäre und Onboard-Komponenten unterteilt werden. Mit ATP wird die Geschwindigkeit unterhalb existierender Begrenzungen gehalten, und es werden Sicherheitsstopps und Nothalte ausgelöst. Das System muss daher die Anforderungen an das Sicherheitsintegritätslevel 4 (höchste Sicherheit) nach der europäischen Norm IEC 50128:2011 erfüllen [29]. Die dafür notwendige Hard- und Software ist in Relation zu den hohen Kosten von Schienenfahrzeugen im Vergleich zu Kraftfahrzeugen relativ günstig.

23.3.2 Rein elektrische Ansteuerung von Aktoren (X-by-Wire)

Bei autonomen Fahrzeugen erfolgt die Ansteuerung der Aktoren über elektrische Signale. Gas, Bremse, Lenkung und Sonderfunktionen werden über Steuergeräte angesteuert. Die-

se X-by-Wire-Technologie ist bisher noch nicht vollständig in Serienfahrzeugen erhältlich. Das elektronische Gaspedal, die elektromechanische Lenkung und das elektrohydraulische Bremssystem gibt es zwar schon seit einigen Jahren. Jedoch verfügen Lenkung und Bremse immer noch über einen mechanischen/hydraulischen Durchgriff, zumeist permanent und in eher seltenen Fällen als Rückfallebene, falls das elektrische System ausfällt.[1] Der Fahrer kann das Fahrzeug dadurch auch ohne Elektronik kontrollieren.

Für autonome Fahrzeuge muss die Aktorik daher mehrfach redundant angesteuert werden, wie das beispielsweise in Flugzeugen erfolgt. Sowohl die Kommunikationssysteme zwischen Bedienelementen, Steuergeräten und Aktoren als auch die Bedienelemente, Steuergeräte und Aktoren (inklusive der Energieversorgung) selbst werden hier mehrfach verbaut, sodass im Fehlerfall auf die redundanten Systeme zurückgegriffen werden kann [3]. In [67] wird ein dreifach-redundantes Steuerungssystem für ein Boeing 777-Passagierflugzeug vorgestellt. Jede sicherheitsrelevante Komponente des Flugzeugkontrollsystems wird auf drei unterschiedliche Arten redundant umgesetzt, um eine hohe Verfügbarkeit der Ansteuerung durch einen Piloten oder den Autopiloten zu realisieren. Aufgrund der Kritikalität der Flugzeugführung sind in Passagierflugzeugen neben dem Autopiloten zwei menschliche Piloten an Bord vorgeschrieben [15].

Die in Flugzeugen eingesetzten Architekturmuster und auch die Hard- und Software zur Realisierung erscheinen auch für Fahrzeuge technisch anwendbar. In Flugzeugen spielen die hohen Kosten solcher redundanter Systeme aufgrund der hohen Gesamtkosten des Flugzeugs selbst nur eine geringe Rolle. Für Fahrzeuge wären bei einer analogen Anwendung von dreifacher Redundanz jedoch der dreifache Entwicklungsaufwand und die dreifache Hardware im Vergleich zu heutigen Systemen im Fahrzeug erforderlich. Es bleibt allerdings offen, ob in Fahrzeugen tatsächlich eine dreifache Redundanz der Systeme erforderlich wäre.

Im Flugverkehr werden die Flugrouten durch eine zentrale Luftverkehrskontrolle vorgegeben, und die Autopiloten halten die Flugzeuge auf den vorgegebenen Kursen. Ein Autopilot im Flugzeug lässt sich mit einem teilautomatisierten Fahrerassistenzsystem vergleichen, da die Piloten die Aufgabe haben, das System zu überwachen. In unbemannten Flugzeugen entfällt diese Überwachung durch Piloten, und die Anforderungen an das Flugzeugführungssystem steigen. Durch Flugrouten, die nur über dünnbesiedelte Gebiete gelegt werden, sollen Risiken reduziert werden. Da keine Personen an Bord sind, ist ein Absturz im freien Feld durchaus möglich, da niemand dabei verletzt wird [34].

23.3.3 Robotik

Mobile Roboter können sich selbst und ihre Umgebung durch Kollisionen mit Objekten, Personen und weiteren Lebewesen und durch Übersehen von Absätzen, Abgründen, Stufen

1 Der Fahrzeughersteller Nissan hat 2012 eine Lenkung vorgestellt, die im Fehlerfall eine mechanische Verbindung über eine Kupplung herstellt.

etc. gefährden [1], [10], [18]. Automatisierte Manipulatoren, die entweder stationär oder auf mobilen Plattformen eingesetzt werden, können Menschen gefährden, indem sie ihre Gelenke bewegen und mit den Menschen kollidieren oder durch die Werkzeuge, die sie einsetzen, verletzen. Sowohl für mobile Roboter als auch für Manipulatoren ist der sichere Zustand ein Stopp aller Manipulatoren in der aktuellen Position bzw. ein Anhalten [5]. In den meisten Fällen gilt: Je schneller dies geschieht, umso niedriger ist die Gefährdung, die von dem Roboter für seine Umwelt ausgeht. Ausnahmen sind Werkzeuge und Manipulatoren, wie z. B. Hände und Greifer, die einen Druck ausüben können. Ein Stopp der Aktoren könnte hier einen Druck erhalten, der zu Verletzungen und Beschädigungen führen kann. Wird ein Roboter für komplexere Tätigkeiten eingesetzt, so können daraus Verletzungen und Schäden entstehen, die zwar nicht direkt durch die Bewegung des Roboters verursacht werden, aber durch die Folgen seiner Aktionen. Beispielweise kann es zu Bränden kommen, wenn ein Bügelroboter abrupt stehen bleibt oder Gefahrgut von einem mobilen Roboter transportiert wird [64].

In [64] und [65] wird eine sicherheitsgetriebene Architektur für Steuerungssysteme von Robotern vorgestellt, die eine Sicherheitsschicht enthält. Diese soll einen Roboter stets in einen sicheren Zustand überführen. Die sicheren Zustände sind abhängig von den Funktionen, die ein Roboter erfüllen soll. Diese können sehr vielfältig sein, und daher wird in [64] und [65] ein Regelsatz (*safety policies*) vorgeschlagen, der übergeordnete Regeln enthält, die einen sicheren Betrieb eines Roboters ermöglichen. Es ist vorstellbar, dass ein Roboter unerwartete Lösungswege für ein Problem abhängig von seiner Entscheidungsfreiheit und seinen grundlegenden Fähigkeiten findet und es dadurch zu gefährlichen Situationen kommen kann. Wie in [9] beschrieben, kann dies bei der häufig angewendeten Subsumptionsarchitektur erfolgen. Übertragen auf autonome Fahrzeuge bedeutet dies, dass zwar Fahrentscheidungen nach verschiedenen Kriterien wie z. B. der Straßenverkehrsordnung, effizienter Fahrweise und Komfort getroffen werden können, aber stets eine Kollisionsvermeidung aktiv wäre, die als übergeordnete Instanz eingreifen könnte.

23.3.4 Kraftwerkstechnik

Kernkraftwerke gelten weithin als besonderes Risiko, da bei Störfällen hohe Schäden für die Umwelt entstehen können. Die dort eingesetzten Steuer- und Regelungssysteme müssen daher die höchsten Sicherheitsanforderungen erfüllen, um einen Betrieb auch nach Naturkatastrophen, terroristischen Anschlägen und internen technischen Fehlern zu ermöglichen. Da bei Kernkraftwerken eine sofortige Abschaltung nicht möglich ist und die Brennelemente auch nach ihrem Einsatz im Reaktor weiterhin aktiv sind und gekühlt werden müssen, sind mehrfach redundante Systeme vor allem zur Kühlung vorgeschrieben.

Die Sicherheit eines Kernkraftwerks hängt maßgeblich davon ab, wie vollständig und fehlerfrei die Steuerungs- und Kontrollsysteme spezifiziert und entwickelt werden. Die

Einbeziehung der Menge der möglichen Situationen und Ereignisse spielt dabei eine wesentliche Rolle, da vor allem Kettenreaktionen und Mehrfachfehler zu einer Gefährdung führen können. Beispielsweise befand sich das Kernkraftwerk Fukushima Daiichi in Fukushima, Japan, nach dem Erdbeben in einem Fail-safe-Zustand und alle Sicherheitssysteme wurden automatisch korrekt aktiviert. Nach dem Auftreffen des Tsunamis wurden jedoch Teile der redundanten Sicherheitssysteme, vor allem der Notstromaggregate, beschädigt. Im Nachhinein betrachtet liegt der Fehler nicht am Versagen der Sicherheitsfunktionen, sondern an der fehlerhaften Spezifikation [63].

Für autonome Fahrzeuge lässt sich daraus folgern, dass die zahlreichen Ereignisse und Kombinationen von Ereignissen und Fehlerquellen bereits bei der Spezifikation berücksichtigt werden müssen. Möglicherweise ist daher eine Standardisierung für die Ermittlung der Anforderungen, vergleichbar mit Kernkraftwerken, notwendig. Bei deren Entwicklung spielt die Sicherheit bereits in der Designphase eine tragende Rolle und steht im Mittelpunkt des Entwicklungsprozesses (*safety by design*, [26]).

23.4 Sichere Zustände in den Use-Cases

Ein wichtiges Kriterium beim Betrieb eines autonomen Fahrzeugs ist, ob sich Passagiere an Bord des autonomen Fahrzeugs befinden oder nicht. So muss beispielsweise bei der Wahl des Abstellorts nicht auf das sicher mögliche Verlassen des Fahrzeugs von Passagieren, wohl aber auf die anderen Verkehrsteilnehmer geachtet werden. Außerdem spielt der Fahrkomfort keine Rolle, wodurch eine andere Fahrweise möglich wird, die den Komfort ignoriert. Sind jedoch Passagiere an Bord, so muss das Fahrzeugführungssystem die Aufgaben eines menschlichen Fahrers übernehmen. Dazu gehört auch die Überwachung der Passagiere, beispielweise, ob diese angegurtet auf den Passagierplätzen sitzen oder sich riskant verhalten. Es kann immer zu Kollisionen mit anderen Verkehrsteilnehmern kommen, und so sind Mechanismen der passiven Sicherheit wie z. B. Sicherheitsgurte und Airbags auch in autonomen Fahrzeugen erforderlich. Gleiches gilt für die Sicherung von Ladung, besonders für Gefahrgut.

Im folgenden Abschnitt werden die vier für das Projekt definierten Use-Cases untersucht und jeweils die Eigenschaften des sicheren Zustands herausgearbeitet.

23.4.1 Use-Case 1: Autobahnautomat mit Verfügbarkeitsfahrer – Autobahnpilot

Durch die Beschränkung des Einsatzes auf Autobahnen ist auch die Anzahl der möglichen und wahrscheinlichen Situationen im Vergleich zum städtischen Straßenverkehr geringer. Der Verfügbarkeitsfahrer steht grundsätzlich als Rückfallebene zur Verfügung, und er ist in der Lage, die Kontrolle jederzeit nach eigenem Ermessen zu übernehmen. Das Fahrzeug ist in den folgenden Situationen in einem sicheren Zustand:

1. Das Fahrzeug steht still. Von einem stehenden Fahrzeug geht aktiv keine unmittelbare Gefahr aus (vgl. [6] und [27]). Die Sicherheit für Passagiere und andere Verkehrsteilnehmer hängt jedoch vom Standort des Fahrzeugs ab:
   - *Fahrstreifen auf einer Autobahn*: Aufgrund des Verfügbarkeitsfahrers ist eine manuelle Weiterfahrt mit hoher Wahrscheinlichkeit möglich. Falls eine manuelle Weiterfahrt nicht mehr möglich ist, kann ein stehendes Fahrzeug wie in den Fehlercodes F5 und F6 nach [6] (s. Tab. 23.1) auf einem Fahrstreifen einer Autobahn zu gefährlichen Situationen führen. Einerseits weil das Fahrzeug übersehen oder zu spät gesehen werden könnte, andererseits weil die Passagiere das Fahrzeug eventuell verlassen müssen. Eine weitere Gefährdung kann entstehen, falls das automatisierte Fahrzeug beispielsweise eine Rettungsgasse im Stau blockiert. Ist eine manuelle Fahrt nicht mehr möglich, so obliegt es dem Verfügbarkeitsfahrer, das Fahrzeug entsprechend den geltenden Gesetze abzusichern, z. B. nach §15 StVO [11].
   - *Seitenstreifen auf einer Autobahn oder Fahrbahnrand einer Autobahn bei fehlendem Seitenstreifen oder Parkplatz, Nothaltebucht oder ähnlicher Standort*: Bleibt ein automatisiertes Fahrzeug auf dem Seitenstreifen einer Autobahn, am Fahrbahnrand oder an einem ähnlichen Standort liegen, kann der Verfügbarkeitsfahrer das Fahrzeug möglicherweise manuell weiterfahren, oder er muss das Fahrzeug entsprechend den geltenden Gesetze absichern (vgl. Fehlercodes F2, F3 und F4 in [6]).
2. Das Fahrzeug fährt auf einem Fahrstreifen mit den vorgeschriebenen oder aufgrund der Leistungsfähigkeit des Fahrzeugs auch größeren Sicherheitsabständen zu anderen Verkehrsteilnehmern und mindestens mit der minimal vorgeschriebenen Geschwindigkeit bzw. höchstens mit der maximal erlaubten oder aufgrund der Leistungsfähigkeit des Fahrzeugs auch maximal möglichen Geschwindigkeit. Das Fahrzeug kennt seine eigene Leistungsfähigkeit und kann daher Systemgrenzen selbstständig erkennen.
3. Das Fahrzeugführungssystem reagiert mit einer Aktion (s. Abschn. 23.5) auf ein Ereignis (s. Abschn. 23.4), um das aktuelle Risiko zu verringern. Dadurch soll ein sicherer Zustand erreicht oder der sichere Zustand erhalten werden – beispielsweise durch eine Übergabe an den Verfügbarkeitsfahrer.

23.4.2 Use-Case 2: Autonomes Valet-Parken

In diesem Use-Case ist die Maximalgeschwindigkeit des Fahrzeugs nur gering (ca. 30 km/h). Dadurch ist die resultierende Energie, die im Notfall abgebremst werden muss, deutlich geringer als die üblicherweise erlaubten 50 km/h in deutschen Städten. Eine Übergabe an einen Verfügbarkeitsfahrer ist in diesem Use-Case nicht möglich, da das Fahrzeug fahrerlos betrieben werden kann. Die Sicherheit von Passagieren spielt keine Rolle, da das Fahrzeug ohne Passagiere fährt. Die Fahrtroute muss so geplant werden, dass keine Straßen befahren werden, die das Fahrzeug nicht beherrscht, beispielsweise Straßen mit Bahnübergängen.

In folgenden Situationen ist das Fahrzeug in einem sicheren Betriebszustand:

1. Das Fahrzeug steht still: Der Standort des liegen gebliebenen Fahrzeugs ist relevant, da das Fahrzeug ein gefährliches Hindernis für andere Fahrzeuge sein kann und Rettungsfahrzeuge und Rettungswege blockieren könnte. Die Absicherung des liegengebliebenen Fahrzeugs ist erschwert, da kein Mensch an Bord ist, der dies übernehmen kann. Nur die am Fahrzeug angebrachte Beleuchtung erscheint zur Absicherung nutzbar. In vielen Ländern gibt es spezielle Vorschriften zur Absicherung eines liegen gebliebenen Fahrzeugs, beispielweise durch ein Warndreieck, das einige Meter hinter dem Fahrzeug aufgestellt werden muss. Es ist schwer vorstellbar, dass dies von einem autonomen Fahrzeug selbstständig erledigt wird. Daraus folgt, dass eine oder mehrere Personen dafür verantwortlich sind. Das Fahrzeug muss also entweder ständig überwacht werden oder von sich aus Hilfe anfordern, falls es zum Anhalten gezwungen ist.
2. Das Fahrzeug fährt auf einem Fahrstreifen, wie in Use-Case 1 beschrieben. Es ist jedoch nicht möglich, an einen Verfügbarkeitsfahrer zu übergeben, da keiner an Bord ist. Eine Möglichkeit besteht, dass das Fahrzeug anhält und so einen sicheren Zustand erreicht. Es ist auch vorstellbar, dass im Fehlerfall während der Fahrt an einen Teleoperator übergeben wird, der das Fahrzeug ferngesteuert an einen sicheren Standort fahren kann.
3. Das Fahrzeug durchfährt eine Kreuzung oder einen Kreisverkehr, oder es biegt ab. Beherrscht das Fahrzeug die Situation und die aktuell geltenden Vorfahrtregeln, so sind diese Manöver sicher. Erreicht das Fahrzeug dabei seine Systemgrenzen, so kann es mit reduzierter Geschwindigkeit und Signalisierung für die anderen Verkehrsteilnehmer weiterfahren.
4. Das Fahrzeug befindet sich auf einem Parkplatz. Durch die geringen Relativgeschwindigkeiten und den verhältnismäßig geringen Verkehrsfluss sind die Anforderungen hier niedriger und das Betriebsrisiko ist geringer.

Die wesentliche Herausforderung ist der fehlende Verfügbarkeitsfahrer. Bei Ereignissen, die das Risiko erhöhen, kann nicht an den Verfügbarkeitsfahrer übergeben werden, und der Stillstand birgt in vielen Situationen ein hohes Risiko, da das Fahrzeug nicht sofort manuell bewegt werden kann. Eine Lösung könnte das teleoperierte Fahren sein, bei dem eine Kommunikationsverbindung zum Fahrzeug besteht, die zur Meldung eines Problems des Fahrzeugs und zur Fernsteuerung des Fahrzeugs genutzt wird. Ist ein Anhalten erforderlich, so muss dies den anderen Verkehrsteilnehmern entsprechend signalisiert werden. Eine Absicherung des Fahrzeugs durch den Verfügbarkeitsfahrer ist hier nicht möglich.

Das Blockieren von Rettungsfahrzeugen und Rettungswegen auf einstreifigen Straßen und bei Zufahrten für Rettungsfahrzeuge vor Gebäuden und anderen Einrichtungen, wie z. B. öffentliche Plätze, stellt einen Sonderfall dar. Das Blockieren kann dazu führen, dass Rettungsaktionen verzögert und erschwert werden. Dies ist einerseits gesetzlich verboten, andererseits ein wesentlicher ethischer Aspekt. Untersuchungen, die die Häufigkeit solcher Situationen belegen, sind dem Autor nicht bekannt. Daher kann hier keine Aussage getrof-

fen werden, ob dieser Fall explizit berücksichtigt werden muss oder nicht. Nicht automatisierte Fahrzeuge können zwar ebenfalls liegen bleiben, es ist durch den vorhandenen Fahrer jedoch einfacher, das Fahrzeug schnell und unkompliziert aus dem Weg zu fahren oder zu schieben.

23.4.3 Use-Case 3: Vollautomat mit Verfügbarkeitsfahrer

Sicherheit und Risiko dieses Use-Case sind einer Kombination der Use-Cases 1 und 2 sehr ähnlich. Durch den vorhandenen Verfügbarkeitsfahrer ist es möglich, die Kontrolle an diesen abzugeben. Er kann auch die Absicherung des Fahrzeugs übernehmen, falls dieses liegen bleibt.

Auch die notwendigen Fahrmanöver und die Situationen decken sich mit den Use-Cases 1 und 2. Zusätzlich wird das Fahrzeug auch auf Überlandverbindungen eingesetzt. Die maximale Geschwindigkeit ist in diesem Use-Case auf 240 km/h beschränkt. Dadurch sind praktisch alle Geschwindigkeiten denkbar, jedoch muss die Maximalgeschwindigkeit immer so gewählt werden, dass diese innerhalb der Leistungsfähigkeit des Fahrzeugführungssystems liegt und das Risiko entsprechend reduziert ist.

Für den sicheren Zustand gelten die gleichen Bedingungen wie in den Use-Cases 1 und 2.

23.4.4 Use-Case 4: Vehicle-on-Demand

(Sicherheits-)Technisch ist dieser Use-Case der anspruchsvollste. Das Fahrzeug muss mit allen Situationen zurechtkommen, mit denen auch ein Mensch zurechtkommen muss. Das Risiko muss stets unterhalb einer für Passagiere und andere Verkehrsteilnehmer zumutbaren Schwelle liegen. Sowohl die Fahrmanöver als auch die Bedingungen für den sicheren Zustand können unter Berücksichtigung des fehlenden Verfügbarkeitsfahrers aus den Use-Cases 1, 2 und 3 übernommen werden.

Das Fahrzeug befindet sich unter den folgenden Bedingungen in einem sicheren Zustand:

1. Das Fahrzeug steht still wie in den Use-Cases 1, 2 und 3. In jeder Situation ist das Fahrzeug auf Hilfe von außen angewiesen. Neben möglichen Passagieren sind weitere Personen involviert, die über den Zustand des Fahrzeugs informiert sein und auf Probleme des Fahrzeugs reagieren müssen.
2. Das Fahrzeug fährt auf einem Fahrstreifen wie in den Use-Cases 1, 2 und 3. Aus der Fahrt heraus muss bei einem risikoerhöhenden Ereignis selbstständig ein sicherer Zustand erhalten bzw. erreicht werden.

Durch die Verfügbarkeit auf Abruf und die universelle Nutzbarkeit muss das Vehicle-on-Demand mit allen Situationen im Straßenverkehr zurechtkommen. Die sicherheitsrelevan-

ten Ereignisse, die eine Reaktion des Fahrzeugs erfordern, werden in Abschn. 23.5 näher beschrieben.

23.4.5 Zusammenfassung

Die Betrachtung der vier Use-Cases hat ergeben, dass die größten Herausforderungen für den sicheren Zustand durch hohe Relativgeschwindigkeiten, das Fehlen eines Verfügbarkeitsfahrers und das Blockieren von Rettungsfahrzeugen und -wegen entstehen. Aus ihrer Betrachtung lassen sich folgende Sicherheitsanforderungen an das Fahrzeug ableiten:

- Ein autonomes Fahrzeug muss seine eigene aktuelle Leistungsfähigkeit kennen.
- Ein autonomes Fahrzeug muss seine eigenen aktuellen funktionalen Grenzen abhängig von der aktuellen Situation kennen.
- Ein autonomes Fahrzeug muss stets in einem Zustand betrieben werden, in dem das Risiko für Passagiere und weitere Verkehrsteilnehmer zumutbar ist.
- Ein Fahrzeug, das auf einem Seitenstreifen oder am Fahrbahnrand steht und den Verkehr nicht blockiert, ist in einem sicheren Zustand.
- Ein Fahrzeug, das auf einem Fahrstreifen steht, ist nur in einem sicheren Zustand, falls alle folgenden Bedingungen zutreffen:
  - Die Relativgeschwindigkeit zu weiteren Verkehrsteilnehmern ist unterhalb eines noch zu definierenden Maximums.
  - Das stehende Fahrzeug blockiert keine Rettungsfahrzeuge oder Rettungswege.
  - Ein Verfügbarkeitsfahrer oder ein Teleoperator kann das Fahrzeug in kurzer Zeit von diesem Standort entfernen.
  - Ein Verfügbarkeitsfahrer kann das Fahrzeug absichern.
- Ein Fahrzeug, das sich mit hohem Risiko bewegt oder an einer gefährlichen Stelle stehen geblieben ist, muss einen Notruf absetzen und Hilfe anfordern können.

23.5 Sicherheitsrelevante Ereignisse

Im Straßenverkehr können verschiedene Ereignisse auftreten, die das Risiko in der aktuellen Situation und in der zukünftigen Entwicklung der Situation beeinflussen. Einerseits verringern technische Defekte und Fehler im Fahrzeugführungssystem die eigene Leistungsfähigkeit, andererseits erhöhen Veränderungen der Umweltbedingungen, Situationen, die das Fahrzeugführungssystem überfordern, fehlerhaftes Verhalten der anderen Verkehrsteilnehmer und Ereignisse der höheren Gewalt die Anforderungen an das Fahrzeugführungssystem. Besonders eine Kombination aus reduzierten Fähigkeiten und erhöhten Anforderungen führt zu einem größeren Risiko.

Defekte und technische Fehler am Fahrzeug und am Fahrzeugführungssystem können unvermittelt auftreten und sind daher schwer vorherzusehen. Neben mechanischen Defek-

ten am Fahrzeug können Defekte und Entwicklungsfehler im Fahrzeugführungssystem zu einer verringerten Leistungsfähigkeit führen (vgl. [16]). Ungünstige Licht- und Wetterverhältnisse erhöhen die Anforderungen an die Robustheit der eingesetzten Sensorik zur Umfeldwahrnehmung. Außerdem führen ungünstige Wetterbedingungen zu schlechteren Straßenverhältnissen. Diese wirken sich direkt auf die Fahrdynamik aus. Aufgrund der Komplexität des Straßenverkehrs und der offenen Menge an möglichen Situationen ist es wahrscheinlich, dass bei der Entwicklung eines Fahrzeugführungssystems nicht alle Situationen berücksichtigt werden können. Gerät das Fahrzeug in eine Situation, die mit der bestehenden Software nicht gelöst werden kann, hat dies einen direkten Einfluss auf das Risiko.

Eine große Herausforderung ist das Erkennen der eigenen Leistungsfähigkeit und der Systemgrenzen in solchen Situationen. Das Verhalten der anderen Verkehrsteilnehmer ist nicht immer regelkonform, und so kann es vorkommen, dass sich diese gefährdend verhalten. In manchen Situationen könnte der Betrieb eines automatisierten Fahrzeugs nicht sicher sein, weil sich andere Verkehrsteilnehmer gefährlich verhalten. Denkbar ist sogar, dass dies mutwillig geschieht, falls das automatisierte Fahrzeug als solches erkannt wird. Auch durch höhere Gewalt kann das Risiko des Betriebs zunehmen, beispielsweise durch Erdbeben und Flutwellen oder durch Sonnenstürme, die zu einer Störung von genutzten Systemen wie eines globalen Navigationssatellitensystems oder der Fahrzeug-zu-Fahrzeug-Kommunikation führen [12]. Bei der Entwicklung von Fahrerassistenzsystemen nach ISO 26262 wurden solche Ereignisse nicht berücksichtigt [30]. Wie dies bei autonomen Fahrzeugen gehandhabt wird, ist bisher noch offen [61].

23.6 Aktionen zur Reduzierung des Risikos

Unter der Annahme, dass ein automatisiertes Fahrzeug stets mit einem zumutbaren Risiko betrieben werden und gleichzeitig einen möglichst hohen Funktionsumfang bereitstellen soll, sind als Reaktion auf sicherheitsrelevante Ereignisse Aktionen auszuführen, die das Risiko auf einen zumutbaren Wert senken oder diesen erhalten und gleichzeitig einen hohen Funktionsumfang ermöglichen. Eine Reduzierung der Fahrgeschwindigkeit, eine Erhöhung der Sicherheitsabstände, eine sicherheitsoptimierte Planung von Fahrmanövern, das Verbot bestimmter Fahrmanöver und die Ausführung von Sicherheitsfahrmanövern sind möglich. Das zugrundeliegende Prinzip der funktionalen Degradation (*graceful degradation*) stammt aus der Biologie und wurde beispielsweise in [40] vorgestellt. In [68] wird u. a. ein Überblick über die Anwendungen der funktionalen Degradation in der Luft- und Raumfahrt, der Kraftwerkstechnologie und weiteren Forschungsbereichen gegeben. Treten Fehler in einem System auf oder sind die Ressourcen eingeschränkt, so werden die „lebenswichtigen“ Prozesse erhalten und weniger wichtige Prozesse reduziert oder beendet. Beispielsweise kann bei einem eingeschränkten Sichtfeld die Geschwindigkeit des Fahrzeugs reduziert werden. Unter bestimmten Bedingungen können jedoch auch diese Aktionen nicht zu einer Reduzierung des Risikos auf einen zumutbaren Wert führen, sodass ein An-

halten des Fahrzeugs [25], [46] oder, falls dies ebenso zu riskant ist, ein Verlassen des Straßenverkehrs notwendig werden.

Bei der funktionalen Degradation ist es nicht nur notwendig, einen sicheren Zustand zu erreichen bzw. zu erhalten, sondern auch die Leistungsfähigkeit zu erhöhen, indem Mechanismen zur Selbstheilung und Rekonfiguration angewendet werden. In technischen Systemen ist der Neustart von Komponenten eine weitverbreitete Aktion zur Wiederherstellung der Leistungsfähigkeit [22], [44]. Ein Neustart benötigt in der Regel einige Zeit, und es kann je nach Systemstruktur vorkommen, dass ein Neustart einer Komponente auch den Neustart oder zumindest eine erneute Initialisierung anderer Komponenten nach sich zieht. Daher werden sicherheitskritische Komponenten häufig (diversitär) redundant ausgelegt (vgl. [3], [28]).

Neben der Redundanz gibt es auch für einzelne Komponenten Möglichkeiten zur Wiederherstellung der Funktionalität. Für Sensoren und Aktoren bietet sich die Rekalibrierung an, mit deren Hilfe Messwerte bzw. die Umsetzung von Stellwerten abhängig von der aktuellen Situation verbessert werden können. Für das Gesamtsystem können zudem Rekonfigurationsmechanismen genutzt werden, die einen sicheren Betrieb auch nach risikoerhöhenden Ereignissen erlauben [33].

Eine Herausforderung stellt das Erkennen von riskanten Situationen dar. Externe Ereignisse müssen über die Umfeldwahrnehmung erfasst und richtig interpretiert werden. Technische Fehler am Fahrzeug und im Fahrzeugführungssystem müssen jedoch ebenfalls erkannt werden. Ein Fahrer beobachtet Warn- und Kontrollleuchten und nimmt Veränderungen am Fahrzeug, beispielsweise durch technische Defekte, über seine Sinne wahr. In ein autonomes Fahrzeug müssen daher Sensoren und Funktionen integriert werden, die Defekte und Fehler erkennen und anhand ihrer Schwere die aktuelle und zukünftige Leistungsfähigkeit und den möglichen Funktionsumfang ermitteln. Die zu erwartende Komplexität eines Fahrzeugs mit Fahrzeugführungssystem führt zu einer hohen Anzahl an Messwerten. Als Ergebnis wird eine Selbstrepräsentation des Fahrzeugs erstellt, die genutzt wird, um abhängig von der Situation und der Leistungsfähigkeit zu einer Bewertung des aktuellen Risikos zu gelangen. Darauf basieren dann die o. g. Sicherheitsaktionen [46].

23.7 Antizipation von Degradationssituationen

Aufgrund der hohen Dynamik des Straßenverkehrs und der Eigenschaften von elektrischen und elektronischen Systemen können sicherheitsrelevante Ereignisse in Sekundenbruchteilen auftreten und erfordern daher eine schnelle Reaktion des Systems. Besser ist es jedoch, wenn sich Situationen, die ein erhöhtes Risiko aufweisen, vorhersehen lassen oder zumindest bei der Planung von Fahrmanövern berücksichtigt werden. Das *vorausschauende Fahren* des Menschen kann in einem Fahrzeugführungssystem noch umfangreicher implementiert werden, da beispielsweise die Überwachung und Nutzung von zahlreichen Messwerten aus dem Fahrzeug direkt erfolgen.

Die gesammelten Messwerte müssen für eine Vorhersage der Entwicklung der Situation überwacht und gespeichert werden. Anhand von umfangreichen Datenanalysen könnten sich anbahnende Fehler erkannt werden. Bereits eine Erkennung von Schwierigkeiten einige Zehntelsekunden vor einem Ereignis kann zu einer sichereren Reaktion führen. Ein notwendiges Bremsmanöver, das beispielweise 0,3 Sekunden eher erkannt und ausgelöst wird, kann den Anhalteweg bei einer Fahrt mit 50 km/h um 4,2 Meter verkürzen.

Weiteres Potenzial zur Erhöhung der Sicherheit liefern Kommunikationsmöglichkeiten mit der Infrastruktur und weiteren Fahrzeugen. Je eher Informationen über Gefahren vorliegen, umso eher kann auf diese reagiert werden, beispielweise bei Straßenschäden, Verschmutzung und Glätte, bei vorausliegenden Stauenden oder bei Notbremsmanövern von vorausfahrenden Fahrzeugen.

23.8 Dilemma-Situationen

In manchen Fällen kann eine Verkettung von Ereignissen zu einer Situation führen, die nicht ohne Personenschaden lösbar ist. Ein automatisiertes Fahrzeug muss in diesen Dilemma-Situationen innerhalb kürzester Zeit eine mögliche Handlungsoption auswählen, die zwar zu einem Personenschaden führt, jedoch den minimalen Schaden hervorruft. Mögliche Sachschäden und Verstöße gegen geltende Gesetze sind dabei ebenfalls denkbar, haben aber eine geringere Priorität. Die Anzahl der eigenen Passagiere und die Art und Dynamik der anderen Verkehrsteilnehmer müssen unter möglichen Unsicherheiten berücksichtigt werden. Die Kommunikation mit anderen Verkehrsteilnehmern ist hier besonders wichtig und kann helfen, solche Situationen mit dem minimalen Personenschaden zu lösen.[2] Eine detaillierte ethische Diskussion zu Dilemma-Situationen findet sich in Kap. 4 dieses Buches. Im Folgenden werden daher nur technische Aspekte betrachtet.

Abbildung 23.1 zeigt zwei Situationen. Die erste ist kollisionsfrei lösbar. Die zweite kann zu einem Dilemma führen. Zu Beginn der ersten Situation fährt das Fahrzeug auf einem Fahrstreifen, und am Straßenrand sind weitere Fahrzeuge geparkt. Zwischen diesen tritt unerwartet und schwer zu erkennen eine Person auf den Fahrstreifen. Es gibt nun mehrere Möglichkeiten, wie das Fahrzeug reagieren kann, um eine Kollision mit dem Fußgänger zu vermeiden. In Option 1 kann das Fahrzeug bremsen und vor dem Fußgänger anhalten. In Option 2 kann das Fahrzeug auf den Nachbar-Fahrstreifen ausweichen und eine Kollision verhindern. Dabei ist ein Überfahren der durchgehenden Linie zwischen den Fahrstreifen erforderlich. Dies ist ein Verstoß gegen die StVO.

In der zweiten Situation fährt ein entgegenkommendes Fahrzeug auf dem zweiten Fahrstreifen. Nimmt man an, dass ein Bremsmanöver nicht mehr zu einer Verhinderung der Kollision mit dem Fußgänger führt, befindet sich das autonome Fahrzeug in einem Dilemma:

2 Das DFG-Schwerpunktprogramm „Kooperativ interagierende Fahrzeuge“ wird dieses Thema in den nächsten Jahren ebenfalls untersuchen.

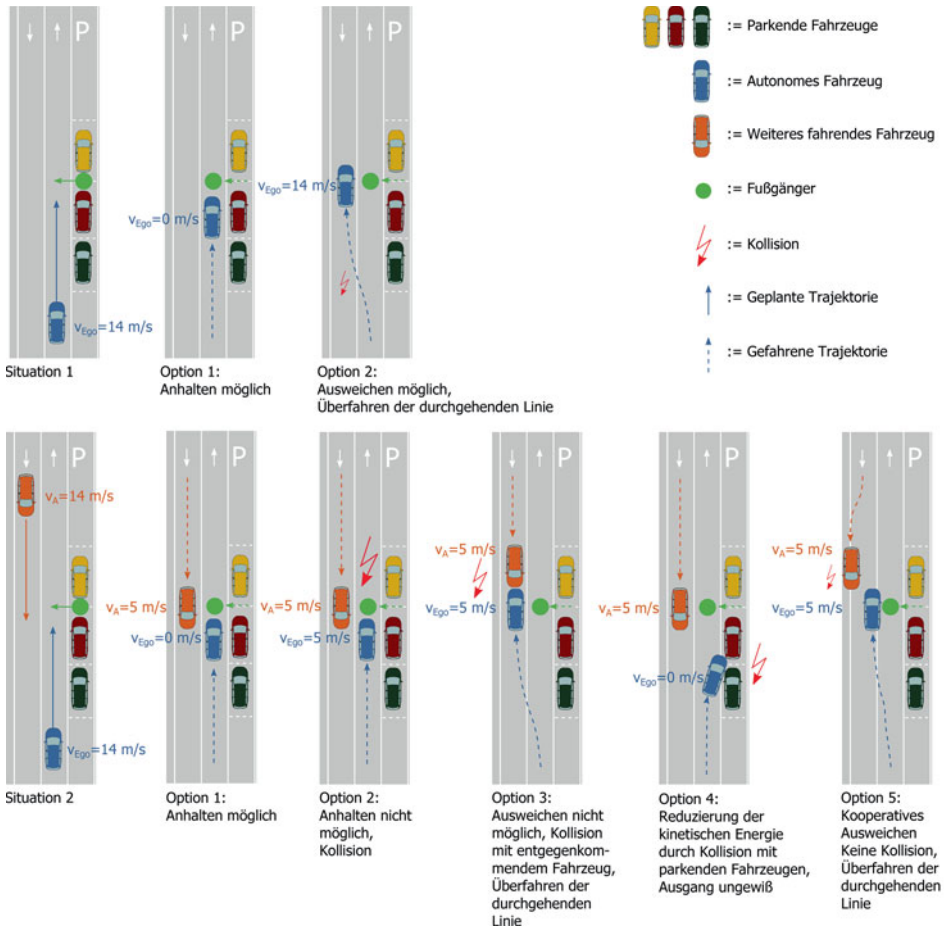

Abb. 23.1 Zwei Situationen, die zu einem Dilemma führen können

Mit dem Fußgänger zu kollidieren, kann schwere Verletzungen bei diesem hervorrufen (Option 2). Ausweichen auf den Nachbar-Fahrstreifen führt zu einer Kollision mit dem entgegenkommenden Fahrzeug, und möglicherweise kann dadurch auch der Fußgänger verletzt werden (Option 3). Eine Kollision mit den parkenden Fahrzeugen zur Reduzierung der eigenen Geschwindigkeit ist ebenfalls denkbar (Option 4), jedoch ist die Unsicherheit, ob dadurch der Fußgänger verschont bleibt, sehr groß. Für solche Situationen ist daher auch die Implementierung von ethischen Grundsätzen in der Software zur Entscheidungsfindung innerhalb des Fahrzeugführungssystems erforderlich.

Eine Lösung zumindest dieses Problems könnte die Anwendung von Fahrzeug-zu-Fahrzeug-Kommunikation zwischen dem autonomen und dem entgegenkommenden Fahrzeug sein. Die beiden Fahrzeuge könnten gemeinsam eine Lösung finden, die dazu führt, dass das entgegenkommende Fahrzeug an den Fahrbahnrand ausweicht und das autonome

Fahrzeug zwischen entgegenkommendem Fahrzeug und Fußgänger kollisionsfrei passieren kann (Option 5). Beide Fahrzeuge würden dabei gegen die StVO verstoßen, da beide eine durchgehende Linie überfahren müssen.

Dennoch muss auch der Betrieb ohne Kommunikation mit anderen Verkehrsteilnehmern und der Infrastruktur möglich sein, da es unwahrscheinlich ist, dass diese Kommunikationsmöglichkeiten flächendeckend und mit allen Verkehrsteilnehmern zur Verfügung stehen.

Die Fahrzeugführung muss daher auf der bordeigenen Sensorik möglich sein. Dieser *bordautonome Betrieb* (vgl. [36]) stellt einerseits die höchsten Anforderungen an das Fahrzeugführungssystem, andererseits aktuell die einzige Möglichkeit zu einem Einsatz im Straßenverkehr dar. Dies schränkt besonders die Möglichkeiten in gefährlichen Situationen und Dilemma-Situationen ein und erhöht die Unsicherheit bei der Wahrnehmung von Situationen. Auch die Signalisierung anderer Verkehrsteilnehmer ist nur durch optische und akustische Signale möglich.

23.9 Zusammenfassung

Bei den aktuellen Entwicklungen von Fahrerassistenzsystemen und in verwandten Entwicklungs- und Forschungsbereichen gibt es eine Vielzahl von Methoden, die auch bei der Entwicklung autonomer Fahrzeuge eingesetzt werden können und möglicherweise müssen. Aufgrund der Vielfalt der Technologien greifen diese an verschiedenen Stellen im Entwicklungsprozess und im zu entwickelnden System an und können zur Sicherheit autonomer Fahrzeuge beitragen.

Zunächst muss eine Metrik gefunden werden, mit der das Betriebsrisiko von autonomen Fahrzeugen bewertet werden kann, und dann muss eine allgemein zumutbare Schwelle definiert werden. Die Vorgehensweise bei der Ermittlung der Sicherheitsanforderungen und der Integration der funktionalen Sicherheit in das Gesamtsystem aus der Kraftwerksentwicklung kann dabei hilfreich sein.

Bei der funktionalen Sicherheit der Regelung und Aktorik können Vorbilder in der Luft- und Raumfahrt, teilweise im Bahnbereich und in der aktuellen Forschung und Entwicklung der Fahrzeugtechnik angewendet werden. Mehrfache, diversitäre funktionale Redundanz ist eines der erfolgversprechenden Mittel. Gleiches gilt auch für die Softwarekomponenten in der Situationsanalyse, Entscheidungsfindung und Bewegungsplanung, wobei bisher nur in der Robotik ähnlich komplexe Situationen beherrscht werden müssen. Das Risiko dort ist jedoch meist geringer.

Eine der größten Herausforderungen liegt in der Zuverlässigkeit und Verlässlichkeit der Umfeldwahrnehmung, die auch die Selbstwahrnehmung und Situationswahrnehmung mit einschließt. Aufgrund der offenen Menge an möglichen Situationen ist es nach Kenntnisstand des Autors bisher nicht gelungen, komplexe Anwendungen, wie in den Use-Cases beschrieben, sicher umzusetzen. Auch hier sind Hardware- und Softwareredundanz sowie funktionale Redundanz notwendig, beispielsweise bei der Zusammensetzung der das Umfeld wahrnehmenden Sensoren.

In den Forschungsprojekten zu autonomen Fahrzeugen ist weiterhin ein Sicherheitsfahrer notwendig, der das System überwacht – zum einen durch direkte Eingriffe, zum anderen durch Notstoppfunktionen per Funk oder durch Not/Aus-Schalter. Die betrachteten Forschungsprojekte fokussieren sich derzeit noch stark auf die Funktionen und weniger auf deren funktionale Sicherheit.

Die Sicherheit autonomer Fahrzeuge ist eine der wesentlichen Herausforderungen in der zukünftigen Forschung. Für die Entwicklung der Technologie sind aber nicht nur technische, sondern auch juristische und gesellschaftliche Probleme zu lösen.

Literatur

1. Albers, A., Brudniok, S., Ottnad, J., Sauter, C., Sedchaicharn, K. (2006). Upper Body of a new Humanoid Robot – the Design of ARMAR III. 6th IEEE-RAS International Conference on Humanoid Robots, S 308–313. Genua, Italien
2. Basarke, C., Berger, C., Rumpe, B. (2007). Software & Systems Engineering Process and Tools for the Development of Autonomous Driving Intelligence. Journal of Aerospace Computing, Information, and Communication (JACIC), 4(12), S 1158–1174
3. Bergmiller, P., Maurer, M., Lichte, B. (2011). Probabilistic fault detection and handling algorithm for testing stability control systems with a drive-by-wire vehicle. 2011 IEEE International Symposium on Intelligent Control (ISIC), S 601–606. Denver, CO, USA
4. Bertozzi, M., Broggi, A., Coati, A., Fedriga, R. I. (2013). A 13,000 km Intercontinental Trip with Driverless Vehicles: The VIAC Experiment. Intelligent Transportation Systems Magazine, 5(1), S 28–41
5. Bicchi, A., Peshkin, M. A., Colgate, J. E. (2008). Safety for Physical Human-Robot Interaction. In B. Siciliano, O. Khatib (Hrsg), Springer Handbook of Robotics, S 1335–1346. Springer-Verlag Berlin Heidelberg
6. Binfet-Kull, M., Heitmann, P., Ameling, C. (1998). System safety for an autonomous vehicle. 1998 IEEE Intelligent Vehicles Symposium (IV), Stuttgart, Deutschland
7. Broggi, A., Bertozzi, M., Fascioli, A. (1999). ARGO and the MilleMiglia in Automatico Tour. Intelligent Systems and their Applications, 14(1), S 55–64
8. Broggi, A., Buzzoni, M., Debattisti, S., Grisleri, P., Laghi, M. C., Medici, P., Versari, P. (2013). Extensive Tests of Autonomous Driving Technologies. IEEE Transactions on Intelligent Transportation Systems, 14(3), S 1403–1415
9. Brooks, R. A. (1986). A robust layered control system for a mobile robot. IEEE Journal of Robotics and Automation, 2(1), S 14–23
10. Bubeck, A., Weisshardt, F., Sing, T., Reiser, U., Hägele, M., Verl, A. (2012). Implementing best practices for systems integration and distributed software development in service robotics – the Care-O-bot® robot family. IEEE/SICE International Symposium on System Integration (SII), S 609–614. Fukuoka, Japan
11. Bundesministerium der Justiz, für Verbraucherschutz. (2013). Straßenverkehrs-Ordnung. Bonn, Deutschland
12. Carrano, C. S., Bridgwood, C. T., Groves, K. M. (2009). Impacts of the December 2006 solar radio bursts on the performance of GPS. Radio Science, 44 (RS0A25)
13. Chatham, A. (2013). Google's Self Driving Cars: The Technology, Capabilities, Challenges. Embedded Linux Conference. San Francisco, CA, USA
14. Dickmanns, E. D. (2002). The development of machine vision for road vehicles in the last decade. 2002 IEEE Intelligent Vehicles Symposium (IV). Versailles, Frankreich

15. EASA. (2013). EASA LIST OF CLASS OR TYPE RATINGS AEROPLANES. Köln, Deutschland
16. Echtle, K. (1990). Fehlertoleranzverfahren. Springer-Verlag Berlin Heidelberg
17. Fenton, R. (1970). Automatic vehicle guidance and control – A state of the art survey. Transactions on Vehicular Technology, 19(1), S 153–161
18. Fischer, H., Voges, U. (2011). Medizinische Robotersysteme. In R. Kramme (Hrsg), Medizintechnik, S 915–926. Springer-Verlag Berlin Heidelberg
19. Ganek, A., Corbi, T. (2003). The Dawning of the Autonomic Computing Era. IBM Syst. J., 42(1), S 5–18
20. Gasser, T. M., Arzt, C., Ayoubi, M., Bartels, A., Bürkle, L., Eier, J., Flemisch, F., Häcker, D., Hesse, T., Huber, W., Lotz, C., Maurer, M., Ruth-Schumacher, S., Schwarz, J., Vogt, W. (2012). Rechtsfolgen zunehmender Fahrzeugautomatisierung : gemeinsamer Schlussbericht der Projektgruppe. Wirtschaftsverlag NW, Verlag für neue Wissenschaft
21. Geyer, S. (2013). Entwicklung, Evaluierung eines kooperativen Interaktionskonzepts an Entscheidungspunkten für die teilautomatisierte, manöverbasierte Fahrzeugführung. Dissertation, Technische Universität Darmstadt, VDI Reihe 12 Band 770
22. Ghosh, D., Sharman, R., Raghav Rao, H., Upadhyaya, S. (2007). Self-healing systems – survey and synthesis. Decision Support Systems in Emerging Economies, 42(4), S 2164–2185
23. Grisleri, P., Fedriga, I. (2010). The Braive Autonomous Ground Vehicle Platform. IFAC Symposium on intelligent autonomous vehicles, 7. Lecce, Italien
24. Hörwick, M. (2011). Sicherheitskonzept für hochautmatisierte Fahrerassistenzsysteme. Dissertation, Technische Universität München
25. Hörwick, M., Siedersberger, K.-H. (2010). Strategy and architecture of a safety concept for fully automatic and autonomous driving assistance systems. 2010 IEEE Intelligent Vehicles Symposium (IV), S 955–960. San Diego, CA, USA
26. IAEA. (2012). Safety of Nuclear Power Plants: Design – Specific Safety Requirements No. SSR-2/1. Wien, Österreich
27. Isermann, R. (2006). Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance. Springer-Verlag Berlin Heidelberg
28. Isermann, R., Schwarz, R., Stölzl, S. (2002). Fault-tolerant drive-by-wire systems. IEEE Control Systems, 22(5), S 64–81
29. ISO. (2011). EN 50128:2011 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. Genf, Schweiz
30. ISO. (2011). ISO 26262:2011 Road vehicles – Functional safety. Genf, Schweiz
31. Kammel, S., Ziegler, J., Pitzer, B., Werling, M., Gindele, T., Jagzent, D., Schröder, J., Thuy, M., Goebl, M., von Hundelshausen, F., Pink, O., Frese, C., Stiller, C. (2008). Team AnnieWAY's autonomous system for the 2007 DARPA Urban Challenge. Journal of Field Robotics, 25(9), S 615–639
32. Kämpchen, N., Waldmann, P., Homm, F., Ardelt, M. (2010). Umfelderfassung für den Nothalteassistenten – ein System zum automatischen Anhalten bei plötzlich reduzierter Fahrfähigkeit des Fahrers. AAET 2010, Braunschweig, Deutschland
33. Kim, J., Rajkumar, R., Jochim, M. (2013). Towards Dependable Autonomous Driving Vehicles: A System-level Approach. SIGBED, 10(1), S 29–32
34. Korn, B., Tittel, S., Edinger, C. (2012). Stepwise integration of UAS in non-segregated airspace-The potential of tailored uas atm procedures. Integrated Communications, Navigation and Surveillance Conference (ICNS), S 1–8. Herndon, VA, USA
35. Levinson, J., Askeland, J., Becker, J., Dolson, J., Held, D., Kammel, Kolter, J. Z., Langer, D., Pink, O., Pratt, V., Sokolsky, M., Stanek, G., Stavens, D., Teichman, A., Werling, M., Thrun, S. (2011). Towards fully autonomous driving: Systems and algorithms. 2011 IEEE Intelligent Vehicles Symposium (IV), S 163–168. Baden-Baden, Deutschland

36. Maurer, M. (2000). Flexible Automatisierung von Straßenfahrzeugen mit Rechnersehen. VDI-Verlag
37. Mirwaldt, P., Bartels, A., Lemmer, K. (2012). Gestaltung eines Notfallassistenzsystems bei medizinisch bedingter Fahrunfähigkeit. 5. Tagung Fahrerassistenz. München, Deutschland
38. Müller, R. (2003). Das Projekt RUBIN – Automatische U-Bahnen ab 2006 in Nürnberg: Mehr Service, niedrigere Kosten im Nahverkehr. 19th Dresden Conference on Traffic and Transportation Science. Dresden, Deutschland
39. NDMV. (2012). Adopted Regulation of the Department of Motor Vehicles LCB File No. R084-11. Carson City, NV, USA
40. Norman, D. A., Bobrow, D. G. (1975). On data-limited and resource-limited processes. Cognitive Psychology, 7(1), S 44–64
41. Nothdurft, T., Hecker, P., Ohl, S., Saust, F., Maurer, M., Reschka, A., Böhmer, J. R. (2011). Stadtpilot: First fully autonomous test drives in urban traffic. 2011 IEEE International Annual Conference on Intelligent Transportation Systems (ITSC), S 919–924. Washington DC, USA
42. Pascoe, R. D., Eichorn, T. N. (2009). What is communication-based train control? IEEE Vehicular Technology Magazine, 4(4), S 16–21
43. Pellkofer, M. (2003). Verhaltensentscheidung für autonome Fahrzeuge mit Blickrichtungssteuerung. Dissertation, Universität der Bundeswehr München
44. Psaier, H., Sustdar, S. (2011). A survey on self-healing systems: approaches and systems. Computing, 91(1), S 43–73
45. Rauch, S., Aeberhard, M., Ardelt, M., Kämpchen, N. (2012). Autonomes Fahren auf der Autobahn – eine Potentialstudie für zukünftige Fahrerassistenzsysteme. 5. Tagung Fahrerassistenz. München, Deutschland
46. Reschka, A., Böhmer, J. R., Nothdurft, T., Hecker, P., Lichte, B., Maurer, M. (2012). A Surveillance and Safety System based on Performance Criteria and Functional Degradation for an Autonomous Vehicle. 2012 IEEE International Conference on Intelligent Transportation Systems (ITSC), S 237–242. Anchorage, AK, USA
47. Reschka, A., Böhmer, J. R., Saust, F., Lichte, B., Maurer, M. (2012). Safe, Dynamic and Comfortable Longitudinal Control for an Autonomous Vehicle. 2012 IEEE Intelligent Vehicles Symposium (IV), S 346–351. Alcalá des Henares, Spanien
48. SAE International. (2014). Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (J3016). SAE International
49. Schopper, M., Henle, L., Wohland, T. (2013). Intelligent Drive – Vernetzte Intelligenz für mehr Sicherheit. ATZextra, 18(5), S 106–114.
50. Shladover, S. (2007). PATH at 20 – History and Major Milestones. Transactions on Intelligent Transportation Systems, 8(4), S 584–592
51. Singh, S. (2008). Special Issue on the 2007 DARPA Urban Challenge Part I (Vol. 25). Wiley Subscription Services, Inc.
52. Singh, S. (2008). Special Issue on the 2007 DARPA Urban Challenge Part II (Vol. 25). Wiley Subscription Services, Inc.
53. Singh, S. (2008). Special Issue on the 2007 DARPA Urban Challenge Part III (Vol. 25). Wiley Subscription Services, Inc.
54. Stanek, G., Langer, D., Müller-Bessler, B., Huhnke, B. (2010). Junior 3: A test platform for Advanced Driver Assistance Systems. 2010 IEEE Intelligent Vehicles Symposium (IV), S 143–149. San Diego, CA, USA
55. Stiller, C., Färber, G., Kammel, S. (2007). Coooperative Cognitive Automobiles. 2007 IEEE Intelligent Vehicles Symposium (IV). Istanbul, Türkei
56. Thorpe, C., Jochem, T., Pomerleau, D. (1997). The 1997 automated highway free agent demonstration. 1997 IEEE Conference on Intelligent Transportation Systems (ITSC). Boston, MA, USA

57. Thuy, M., Goebl, M., Rattei, F., Althoff, M., Obermeier, F., Hawe, S., Nagel, R., Kraus, S., Wang, C., Hecker, F., Russ, M., Schweitzer, M., Leon, F.P., Färber, G., Buss, M., Diepold, K., Eberspächer, J., Heißing, B., Wünsche, H.-J. (2008). Kognitive Automobile – Neue Konzepte und Ideen des Sonderforschungsbereichs/TR28. 3. Tagung Aktive Sicherheit durch Fahrerassistenz. Garching b. München, Deutschland
58. Tsugawa, S. (1994). Vision-based vehicles in Japan: machine vision systems and driving control systems. Transactions on Industrial Electronics, 41(32), S 398–405
59. Urmson, C. (2012). Realizing Self-Driving Vehicles. 2012 IEEE Intelligent Vehicles Symposium (IV). Alcalá des Henares, Spanien
60. Wille, J. M., Saust, F., Maurer, M. (2010). Stadtpilot: Driving autonomously on Braunschweig's inner ring road. 2010 IEEE Intelligent Vehicles Symposium (IV), S 506–511. San Diego, CA, USA
61. Winkle, T., Gasser, T. M. (2014). E-Mail Kommunikation
62. Winner, H., Danner, B., Steinle, J. (2009). Adaptive Cruise Control. In: Winner, H., Hakuli, S., Wolf, G. (Hrsg.), Handbuch Fahrerassistenzsysteme, S 478–521. Wiesbaden: Vieweg Teubner | GWV Fachverlage GmbH
63. WNA. (2014). Fukushima Accident. Tech. rep., World Nuclear Association
64. Woodman, R., Winfield, A. F., Harper, C., Fraser, M. (2010). Safety control architecture for personal robots: Behavioural suppression with deliberative control. The Seventh IARP Workshop on Technical Challenges for Dependable Robots in Human Environments. Toulouse, Frankreich
65. Woodman, R., Winfield, A. F., Harper, C., Fraser, M. (2012). Building safer robots: Safety driven control. The International Journal of Robotics Research, 31(13), S 1603–1626
66. Yasunobu, S., Miyamoto, S. (1985). Automatic Train Operation System by Predictive Fuzzy Control. In M. Sugeno (Hrsg), Industrial Applications of Fuzzy Control, S 12–29. Elsevier Science Publishers B.V. (North-Holland)
67. Yeh, Y. (1996). Triple-triple redundant 777 primary flight computer. 1996 IEEE Aerospace Applications Conference,S 293–307. Aspen, CO, USA
68. Zhang, Y., Jiang, J. (2008). Bibliographical review on reconfigurable fault-tolerant control systems. Annual Reviews in Control, 32(2), S 229–252
69. Ziegler, J., Bender, P., Lategahn, H., Schreiber, M., Strauß, T., Stiller, C. (2014). Kartengestütztes automatisiertes Fahren auf der Bertha-Benz-Route von Mannheim nach Pforzheim. Workshop Fahrerassistenzsysteme. Walting, Deutschland