Eignung und Anwendung der Gefahrenanalyse STPA zur Erarbeitung eines umfassenden Sicherheitsnachweises für automatisierte Fahrzeuge SAE Level vier und fünf

Dissertation

zur Erlangung des akademischen Grades

Doktoringenieurin / Doktoringenieur

(Dr.-Ing.)

von M. Sc. Greta Carlotta Kölln
geb. am 19.06.1992 in Oldenburg in Holstein
genehmigt durch die Fakultät Maschinenbau
der Otto-von-Guericke-Universität Magdeburg

Gutachter:
Prof. Dr.-Ing. Stephan Schmidt
Prof. Dr.-Ing. Stefan Wagner

Promotionskolloquium am 22.06.2023

Kurzfassung

Softwareanteile in Fahrzeugen nehmen stetig zu, die Komplexität steigt weiter an. Mit der Möglichkeit des automatisierten Fahrens gehen neue Sicherheitsrisiken einher, welche zukünftig beherrscht werden müssen. Damit verknüpft könnte sich potenziell in den nächsten Jahren ein Wandel in den Mobilitätskonzepten und Betriebsorganisationen vollziehen, der ebenfalls untersucht werden muss, um das Gesamtsystem *automatisiertes Fahren* hinreichend abzusichern. Die in der ISO 26262 vorgeschlagenen Gefahrenanalysen zur funktionalen Absicherung von E/E Komponenten im Fahrzeug sind allein nicht mehr ausreichend, um autonome Fahrzeuge hinreichend sicherheitskritisch zu analysieren. Es gilt neue Gefahrenanalysemethoden anzuwenden, welche den Kanon bereits bestehender Gefahrenanalysen erweitern, um auch zukünftig Fahrzeuge und mögliche Umstrukturierungen in der Mobilität abzusichern. Im Rahmen dieser Arbeit wird die Gefahrenanalyse STPA (System Theoretic Process Analysis) auf ein autonomes Fahrzeug SAE Level vier und fünf angewendet. STPA ist noch keine in den Standards der Automobilindustrie etablierte Analyse. Ziel ist es, Sicherheitsanforderungen zu identifizieren und zu formulieren, diese dann mit bereits bestehenden Anforderungen traditioneller Methoden der Automobilindustrie abzugleichen und zu validieren, sowie Anforderungen zu identifizieren, die mit den traditionellen Methoden noch nicht hinreichend adressiert wurden. Weiter wird die Anwendungsfähigkeit der Analyse im Hinblick der Serienproduktion automatisierter Fahrzeuge untersucht.

Abstract

The complexity of Software in vehicles are increasing. The possibility of automated driving brings with it new safety risks, which must be controlled in the future. Linked to this, there could potentially be a change in mobility concepts and operational organisations in the coming years, which also needs to be analyzed in order to adequately safeguard the overall system *autonomous driving*. The hazard analyses proposed in ISO 26262 for the functional safety of E/E components in the vehicle are no longer sufficient on their own to analyse autonomous vehicles safety-critical. It is important to apply new hazard analysis methods that extend the canon of existing hazard analyses in order to safeguard vehicles and possible restructuring in mobility in the future. In this work, the hazard analysis STPA (System Theoretic Process Analysis) is applied to an autonomous vehicle SAE level four and five. STPA is not yet an established analysis in the standards of the automotive industry. The aim is to identify and formulate safety requirements, to compare and validate them with existing requirements of traditional methods of the automotive industry, and to identify requirements that have not yet been sufficiently addressed by traditional methods. Furthermore, the applicability of the analysis regarding the series development of automated vehicles is investigated.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

A	Anforderungen
ACC	Adaptive Cruise Control
ARP	Aerospace Recommended Practice
ASIL	Automotive Safety Integrity Level
BaST	Bundesanstalt für Straßenwesen
CCF	Common cause failures
CMF	Common mode failures
EPS	Electric Power Steering
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
G	Gefahr
GPS	Global Positioning System
GuR	Gefahren und Risikoanalyse
HAZOP	Hazard and Operability
HMI	Human Machine Interface
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
MIL	United States Military Standard
MRM	Minimum Risk Maneuver
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
PHA	Preliminary Hazard and Risk Analysis
PRA	Probabilistische Risikoanalyse
RPZ	Risikopräferenzzahl
SAE	Society of Automotive Engineers

SC	Sicherheitsanforderungen
SOTIF	Safety Of The Intended Functionality
SRC	Safety Requirements
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
TO	Teleoperation
UCA	Unsichere Kontrollaktion
WHO	World Health Organization

1. Einleitung und Motivation

Autonome Fahrzeuge sind potentiell in der Lage die Automobilbranche, Mobilität und die Gesellschaft grundlegend zu verändern [1]. In der medialen, politischen und wissenschaftlichen Öffentlichkeit wird im Zusammenhang mit der Markteinführung autonomer bzw. automatisierter Fahrzeuge über einen „disruptiven Technologiewandel“ [1], „einer weiteren mobilen Revolution“ [2], oder bspw. „einer neuen Ära“ [1] diskutiert. Erwartete Vorteile autonomer bzw. hochautomatisierter Fahrzeuge sind unter anderem die Erhöhung des Komforts, der Sicherheit, Effizienzgewinne und die Entlastung des Fahrers im Verkehrssystem [3]. Eine der notwendigen Voraussetzungen für die Markteinführung autonomer bzw. hochautomatisierter Fahrzeuge ist die Garantie hinreichender Betriebssicherheit. Dieses Ziel wurde unter anderem von der Deutschen Ethikkommission im Juni 2017 [4] gefordert. In dieser Arbeit soll ein Beitrag zur Sicherheit automatisierter bzw. autonomer Fahrzeuge geleistet werden, um das Ziel einer positiven Risikobilanz im Vergleich zu konventionellen Fahrzeugen zu erreichen.

Sicherheitsrelevante elektrische/ bzw. elektronische Systeme in Kraftfahrzeugen werden nach den Richtlinien der ISO 26262:2018 [5] abgesichert. In der Anwendung der Norm sind zwei grundlegende Problemstellungen zu lösen: Es müssen Konzepte entwickelt werden, um Gefahrenpotentiale zu minimieren und Systemgefahren zu identifizieren. Donald Rumsfeld, der damalige US- Verteidigungsminister, sagte auf einer Pressekonferenz am 12. Februar 2002: „There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – there are things we do not know we don't know.“

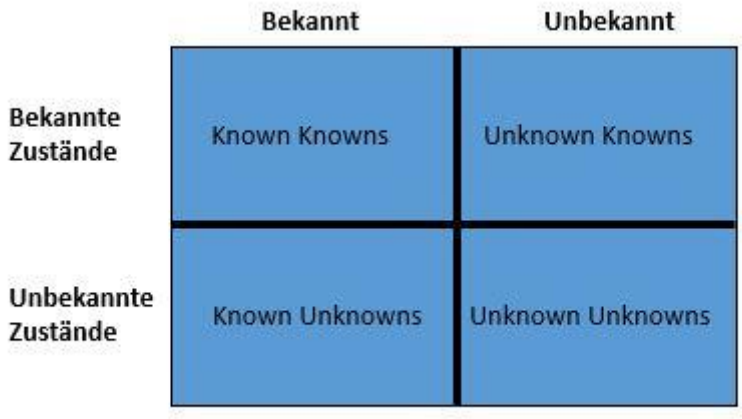

Abbildung 1: Zustände nach Nicholas Talebs

Diese Annahme ist auf verschiedenste Sektoren übertragbar und wurde beispielsweise vom Finanzmathematiker Nassim Nicholas Taleb aufgegriffen. Der *Schwarze Schwan* ist in der Wirtschaft das Synonym für unerwartete unwahrscheinliche Ereignisse. Bis ins 18. Jahrhundert war ein schwarzer Schwan etwas Unvorstellbares, denn die Annahme war, dass Schwäne ausschließlich ein weißes Federkleid hatten. 1790 wurde der erste schwarze Schwan entdeckt und die These, dass Schwäne ausschließlich weiß waren, musste widerlegt werden. Dieses Ereignis war nicht prognostizierbar und ist ein Beispiel für ein zufälliges unerwartetes Ereignis, was die Menschheit dazu zwingt ein neues Modell der Vererbung von Farben des Federkleids anzunehmen. Nach der Aussage von Rumsfeld basierend auf Nassim Nicholas Talebs, werden, übertragen auf den Automobilsektor, somit zwangsläufig Unfälle entstehen, die sich aus den „Known Unknowns“, aber auch aus den „Unknown Unknowns“ ergeben. Es gilt die „Known Unknown“ und die „Unknown Unknowns“ durch adäquate Absicherung zu reduzieren und die Anzahl der „Known Knowns“ zu vergrößern. Wobei sich die Identifizierung der „Unknowns Unknowns“ als besonders problematisch darstellt, da auf etwas Unbekanntes kaum zielgerichtet reagiert werden kann. Basierend auf dieser Theorie kann geschlussfolgert werden, dass einzelne schwerwiegende Schadensereignisse auch in Zukunft existieren werden und nicht verhindert werden können. [6] [7] [8]

Folgende Beispiele veranschaulichen Herausforderungen, denen Gefahrenanalysen speziell in der Absicherung autonomer und hochautomatisierter Fahrzeuge gegenüberstehen. Gefahrenanalysen sind Methoden zur Identifizierung und Kategorisierung ungewünschter Ereignisse sowie zur Identifizierung von Sicherheitszielen und ASILs im Zusammenhang mit der Minderung und Vorbeugung der damit verbundenen Gefahren in Systemen. Im automatisierten Fahrzeug nimmt der Aktionsraum des Menschen mit steigenden Automatisierungsgraden ab. Ziel vollautonomer Fahrzeuge ist, dass komplexe Verkehrssituationen fahrerlos bewältigt werden können, da der Mensch nicht mehr als Rückfallebene fungiert. In der Absicherung muss somit zukünftig ein Schwerpunkt auf die Mensch-Maschine-Interaktionen von Fahrer bzw. Passagier und Fahrzeug gelegt werden. Infolge von Urbanisierung und steigender Fahrzeugbetriebskosten könnten sich Fahrzeuge tendenziell von Konsumgütern zu reinen Investitionsgütern wandeln. Mobilitätskonzepte und somit die Rolle von Betreibern, Herstellern und Nutzern würden sich grundlegend verändern. Daraus ergeben sich vermehrt fahrzeugsystemübergreifende Schnittstellen, die auf Gefahrenpotentiale untersucht werden müssen. Nach einer Studie des Center of Automotive Management wurden im ersten Halbjahr 2014, 4,5-mal mehr Fahrzeuge zurückgerufen, als auf dem US-Markt verkauft. Dies stellt eine Verdreifachung der Zahlen gegenüber dem Vorjahr dar. Davon waren 50 Prozent der Rückrufe softwarebedingt, Tendenz steigend. Fehlerarten softwareintensiv geprägter Systeme unterscheiden sich im Vergleich zu mechanisch geprägten Systemen. Mögliche Fehlerursachen sind aufgrund der Komplexität und des

Umfangs in Software komplex zu identifizieren. Weiter steigt die Komplexität und Unüberschaubarkeit von Software mit Implementierung von Softwareupdates, die eine gesamtheitliche Absicherung erschweren. Eine adäquate Vorgehensweise zur Identifizierung dieser Fehlerarten muss zukünftig erarbeitet werden. [9]

Dieser Entwicklung gegenüber stehen Gefahrenanalysen zur Absicherung von Systemen, die vor über 30 Jahren entwickelt wurden. Es ist fraglich, ob eine adäquate Absicherung moderner, softwareintensiver Systeme ausschließlich mit den traditionellen Methoden möglich ist. Die FTA (Fault Tree Analysis) beschreibt Unfälle beispielsweise als lineare Abfolge von Ereignissen, wobei jedes Ereignis direkt mit dem vorhergehenden verknüpft ist. Aufgrund der wachsenden Komplexität des Gesamtsystems sind diese Ereignisketten allerdings nicht mehr stringent linear und erfordern daher ein Umdenken in der Herangehensweise zur Analyse dieser Systeme. [10]

STPA (System Theoretic Process Analysis) ist eine von Nancy Leveson entwickelte Gefahrenanalyse, deren Ansatz sich im Vergleich zu traditionell genutzten Gefahrenanalysen der Automobilindustrie grundlegend unterscheidet. Sicherheit wird als Kontrollproblem behandelt. Die Methode basiert auf einem systemtheoretischen Ansatz. STPA betrachtet ungewollte Ereignisse als Ergebnis unerwarteter, unkontrollierter Beziehungen zwischen den Komponenten. Diese Komponenten umfassen technische und soziale Elemente, die miteinander und mit der Umgebung interagieren. Die systemtheoretische Betrachtungsweise bedingt die Untersuchung des Systems als Ganzes und nicht als eine isolierte Betrachtung einzelner Elemente. [10] [11] [12]

STPA ist bis zum heutigen Zeitpunkt keine etablierte Methode in internationalen Standards der Automobilindustrie. Die Automobilindustrie ist eine traditionsgeprägte Branche. Neue Methoden und Konzepte müssen zunächst als Bestandteil der Absicherung akzeptiert werden. Weiter müssen die Ergebnisse adäquat in die bestehenden Entwicklungsprozesse integrierbar sein. Maßgebliche Ursache in der STPA ist jedoch fehlendes verfügbares Personal mit erforderlichem Know-How. In dieser Arbeit wird die STPA auf ein vollautomatisiertes Fahrzeug SAE[1] Level vier und ein autonomes Fahrzeug Level fünf angewendet und die Ergebnisse quantitativ und qualitativ mit den Ergebnissen der Automobilindustrie verglichen. Es wird untersucht, ob mit STPA Gefahrenpotentiale aufgedeckt werden können, die mit traditionellen Methoden der Automobilindustrie nicht identifiziert wurden. Ein Sicherheitsnachweis für ein Fahrzeug Level vier und fünf wird auf Basis der Vorgehensweise der STPA ermöglicht. Weiter

[1] SAE (International`s Levels of Driving Automation for On-Road Vehicles) als Begriffsdefinition des Automatisierungslevels im Sinne der Norm SAE J3016. Zur Vereinfachung soll in dieser Arbeit der gängige Begriff Level vier und Level fünf anstelle des fachlich korrekten Begriffs SAE Level vier und SAE Level fünf verwendet werden.

wird in dieser Arbeit die Anwendbarkeit der Methode in der Serienproduktion von Fahrzeugen untersucht. [12]

1.1. Definitionen

Zu Beginn dieser Arbeit werden einschlägige Begriffsdefinitionen auf Basis der STPA vorgestellt. Diese auch meist im Alltag verwendeten Termini sind teilweise mit feinsinnigen Bedeutungsunterschieden versehen. Die Definitionen orientieren sich an [13] und [14] und schaffen eine gemeinsame Sprachbasis bzw. Betrachtungsweise, die zur Beschreibung der Methode und anschließenden Diskussion der Ergebnisse notwendig ist. Sie geben einen Überblick über die Bedeutung und Zusammenhänge der im Folgenden angewendeten Termini.

Unfall: Ein unerwünschtes oder ungeplantes Ereignis, das zu einem Schaden führt, einschließlich Verlust von Menschenleben oder Personenschäden, Sachschäden, Umweltverschmutzung, Missionsverlust usw. [14]

Gefahr: Ein Systemzustand oder eine Reihe von Bedingungen, die zusammen mit einer bestimmten Reihe von ungünstigsten Umgebungsbedingungen zu einem Unfall führen. [14]

Systembeschränkungen: Eine Beschränkung auf Systemebene spezifiziert Systembedingungen oder Verhaltensweisen, die erfüllt werden müssen, um Gefahren zu verhindern. [13]

Kontrollstruktur: Eine Kontrollstruktur ist ein Systemmodell, das aus Regelkreisen besteht. Eine wirksame Kontrollstruktur erzwingt Einschränkungen für das Verhalten des Gesamtsystems. [13]

Unsichere Kontrollaktion (UCA): Eine unsichere Kontrollaktion kann in einem bestimmten Kontext zu einer Gefahr führen. [13]

1.2. Problemstellung und Forschungsfrage

Ein bedeutendes Ziel der Automobilbranche ist es, hinreichend sichere autonome bzw. vollautomatisierte Fahrzeuge zu entwickeln. Die Verantwortung liegt beim Hersteller der die Sicherheit seiner Fahrzeuge hinreichend garantieren muss. Insgesamt soll das System entsprechend sicher sein, sodass eine positive Risikobalance im Vergleich zur Leistung des menschlichen Fahrers erreicht wird. Obgleich die einschlägigen Normen eingehalten werden, entstehen ungewollte Ereignisse, die Menschen innerhalb und im Umkreis des Fahrzeugs

gefährden. 2018 verunfallte im US-Bundesstaat Arizona der erste Mensch aufgrund eines Zusammenpralls eines vom Transportdienstleister Uber umgebauten Volvo XC 90 im automatisierten Fahrmodus tödlich. Ursächlich für diesen Zusammenprall waren keine Komponentenausfälle im Fahrzeug. Nach NTSB (National Transportation Safety Board) hat das Fahrzeug sechs Sekunden vor dem Aufprall ein Objekt im Propagationspfad sensorisch detektieren können, konnte es jedoch im Zeitpunkt der Erfassung nicht adäquat klassifizieren. Eine Fahrradfahrerin wurde von der Software zunächst als unbekanntes Objekt, als Fahrzeug und anschließend als Fahrrad identifiziert. Potenzielle Bewegungsrichtungen des Objektes waren nicht vorhersehbar. 1,3 Sekunden vor dem Aufprall erkannte die Software die Notwendigkeit einer Notbremsung. Vor dem Unfall wurde von Ubers Entwicklern festgelegt, dass Fahrzeuge im autonomen Fahrmodus zu keinem Zeitpunkt befugt sind, Notbremsungen einzuleiten. Ziel dieser Entscheidung war die Vermeidung von sprunghaftem Fahrverhalten. Stattdessen wurde vorgesehen, dass der Fahrer in kritischen Situationen als Rückfallebene einschreitet. Faktoren, die zu diesem Unfall führten, waren unter anderem fehlerhafte Software sowie das Anforderungsmanagement, speziell im Hinblick der Anforderungsspezifikationen der HMI (Human Machine Interface) Schnittstelle. In diesem Fahrzeug fungierte der Fahrer als Rückfallebene. Vom Fahrzeug selbst wurden hingegen keine Warnsignale an den Fahrer ausgegeben, die auf eine kritische Verkehrssituation aufmerksam machten. [4]

Daraus ergibt sich die Fragestellung bezüglich der Ursachen von Unfällen in modernen Fahrzeugen und warum diese auf Basis einschlägiger Vorgehensweisen und Normen nicht identifiziert bzw. adäquat eliminiert werden. Die Entwicklung von größtenteils mechanisch geprägten Systemen unterliegt physikalischen Restriktionen. Entwicklungsmöglichkeiten werden beispielsweise durch Bauart, Bauraum oder die Belastungsgrenzen von Werkstoffen limitiert. Die Entwicklungsfreiheiten in der Softwareentwicklung sind hingegen weitreichender. Das kann beispielsweise zu komplexen, nicht vollständig erfassbaren Interaktionen innerhalb der Software führen. In der Fahrzeugentwicklung steigen die Softwareanteile, deren Vernetzung sowie Funktionsumfänge weiter an und damit einhergehend die Systemkomplexität. Von 1970 bis 2005 ist diese von 5% auf ca. 15% angestiegen. In Hybrid- und Elektrofahrzeugen liegt der Anteil der Kosten für Elektronik bei etwa 80% des Gesamtsystems. [16]

Weiter erschweren steigende Softwarekomplexität eine hinreichend sichere Installation und Entwicklung von Softwareupdates. Eine hinreichend sichere Implementierung setzt zunächst eine vollumfängliche Erfassung des Systems voraus. Zudem ist die Lebensdauer von Software im Vergleich zu mechanischen Systemen tendenziell geringer. Mit steigender Komplexität wächst die Herausforderung der Absicherung. Herr Prof. Dr. Markus Maurer von der TU Braunschweig sagte dazu: „Komplexe Softwaresysteme können heute nicht vollständig

getestet werden. Selbst die vollständige Spezifikation der Anforderung gelingt heute bei der Fahrzeugführungsaufgabe im allgemeinen Fall nicht. Es wird also immer ungetestete Softwareteile geben, die zu ungewünschten Reaktionen führen können“. Wie sollen Softwareaktualisierungen adäquat entwickelt und implementiert werden, wenn die zugrundeliegende Struktur und Interaktionen nicht vollständig erfasst sind? [14] [17] [18]

Zusammenfassend kann festgestellt werden, dass sowohl intrinsische Gefahren, also beispielsweise die Softwareprogrammierung des Fahrzeugs selbst, als auch fahrzeugsystemübergreifende Gefahren, durch die Interaktion in und mit der Umwelt Anknüpfungspunkte für Unfallursachen sein können. Letztgenannte befinden sich darüber hinaus in einem Wandel: Moderne Mobilitätskonzepte und Betriebsorganisationen lassen den Schluss zu, dass Interaktionen des technischen Systems mit fahrzeugübergreifenden Instanzen zunehmen. Dazu zählt beispielsweise die veränderte Rolle des Menschen hinsichtlich der zunehmenden Automatisierungsgrade des Fahrzeugs. Auch diese Interaktionen begründen wiederum neue Gefahrenpotentiale.

Traditionelle Gefahrenanalysen zur Absicherung von Kraftfahrzeugen stammen aus einer Zeit, in der der Softwareanteil von Fahrzeugen gering war. Der Schwerpunkt zu identifizierender Fehler mit traditionellen Methoden liegt somit auf Komponentenfehlern. Ein System ist nicht ausschließlich der Zusammenschluss von Komponenten, sondern definiert sich ebenfalls aus deren Interaktionen untereinander. Nach Nancy Leveson werden hoch vernetzte Einheiten, softwareintensive Funktionalitäten, nicht lineare Interaktionen und die daraus resultierenden Gefahrenpotentiale mit traditionellen Methoden nicht adäquat adressiert werden. In der Gefahrenidentifikation müssen Methoden bzw. Methodenkombinationen eingesetzt werden, die diesen neuen Herausforderungen angepasst sind.

Eine neue Gefahrenanalyse ist die von Nancy Leveson 2004 entwickelte STPA/STAMP (Systems-Theoretic Accident Model and Processes). [14]

Forschungsfrage dieser Arbeit ist zu analysieren, ob STPA diese neuen Herausforderungen in der Absicherung autonomer und hochautomatisierter Fahrzeuge angemessen adressieren kann. Ziel dieser Arbeit ist einen Sicherheitsnachweis für vollautomatisierte und autonome Fahrzeuge mittels des systemtheoretischen Ansatzes auf Basis von STPA/STAMP zu erarbeiten. Im Folgenden werden Fragestellungen dieser Arbeit vorgestellt.

1. Welche Eigenschaften der STPA sind besonders vorteilhaft bezüglich der Anwendung im Entwicklungszyklus eines automatisierten Fahrzeugs.
2. Wurden Gefahrenpotentiale mit STPA identifiziert, die mit etablierten Methoden der Automobilindustrie nicht bestimmt wurden?

3. Ist eine Kombination traditioneller Methoden der Automobilindustrie und der STPA notwendig, um eine hinreichende Gesamtabsicherung durchzuführen?
4. Wie unterscheiden sich die Anforderungen hinsichtlich der Komplexität eines automatisierten Fahrzeugs Level vier und fünf?
5. Welcher Zeitaufwand wird für die Durchführung der STPA für ein Fahrzeug Level vier und fünf benötigt?

Im nächsten Unterkapitel wird zunächst auf die Struktur der Arbeit eingegangen, um in den darauffolgenden Kapiteln die Forschungsfragen einzuleiten und zu beantworten.

1.3. Struktur der Arbeit

Im ersten Abschnitt werden Zielsetzungen und Problemstellungen der Arbeit erläutert.

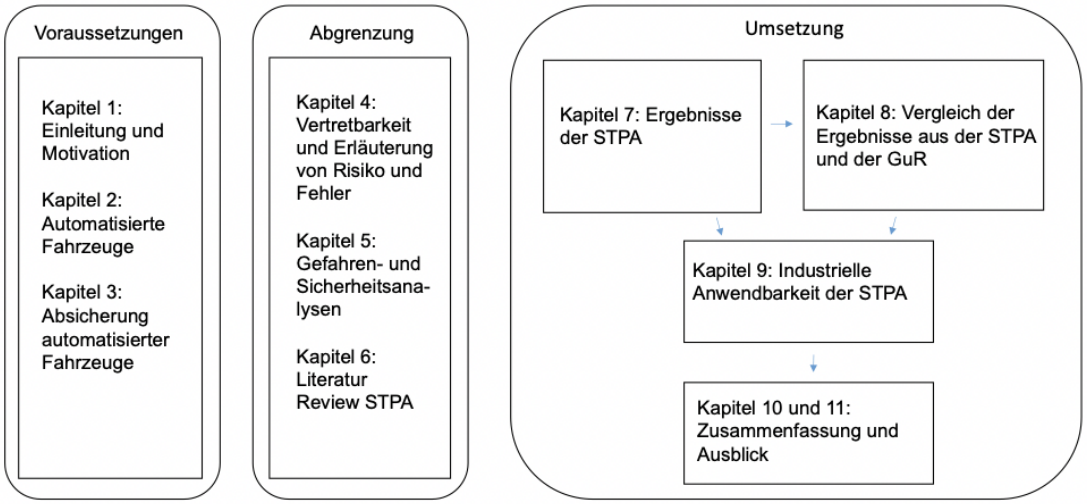

Abbildung 2: Vorgehensweise der Arbeit

Im zweiten Kapitel werden autonome Fahrzeuge und die damit einhergehenden Herausforderungen mit Schwerpunkt des Sicherheitsaspektes formuliert. Anschließend wird in Kapitel drei auf die Vorgehensweise der Absicherung von vollautomatisierten und autonomen Fahrzeugen sowie auf aktuelle Regularien eingegangen. Im vierten Kapitel werden Erläuterungen und Definitionen zum *Risiko* und *Fehler* gegeben. Im fünften Kapitel werden Gefahrenanalysen zur Gefahrenidentifikation vorgestellt. Ausführlich wird auf Gefahrenanalysen eingegangen, welche in der Automobilindustrie aktuell am häufigsten angewendet werden. Anschließend wird die Vorgehensweise der STPA dargelegt. Zum Abschluss des fünften Kapitels werden Anforderungen an Gefahrenanalysen in der

Serienentwicklung von Fahrzeugen vorgestellt, die maßgebend sind, um eine Gefahrenanalyse kosten- bzw. nutzeneffizient in der Automobilindustrie durchzuführen. Im sechsten Kapitel wird ein Literaturreview durchgeführt. Im siebten Kapitel werden Ergebnisse der STPA angewendet auf ein Fahrzeug Level vier und Level fünf ausgewertet. Dazu werden im achten Kapitel die Anforderungen der Automobilindustrie, basierend auf Anforderungen aus der Gefahren- und Risikoanalyse (GuR) der BMW Group, mit den Ergebnissen der STPA quantitativ und qualitativ verglichen. Im neunten Kapitel wird auf die Anwendbarkeit der STPA in der Serienproduktion eingegangen. Dazu werden die Vorteile und die Nachteile der STPA dargelegt. In Kapitel zehn und elf folgt eine Zusammenfassung und ein Ausblick.

2. Automatisierte Fahrzeuge

Um die Produktion eines automatisierten sowie autonomen Fahrens möglich zu machen, wird ein erheblicher Aufwand, sowohl von privaten Unternehmen, als auch von öffentlichen Organisationen betrieben [20]. Aus diesen Anstrengungen werden weitere vielfältige positive Effekte, bspw. in Bereichen der Infrastruktur, dem Modal Split[2], der Verkehrssicherheit sowie in der Beschäftigung und Wertschöpfung erwartet [21].

Im folgenden Kapitel wird auf diese Effekte eingegangen und grundlegende Motivationen und Herausforderungen in der Entwicklung automatisierter Fahrzeuge vorgestellt. Im zweiten Teil des Kapitels werden die Automatisierungsgrade erläutert sowie voneinander abgegrenzt, um den Referenzrahmen der STPA, vorgestellt in Kapitel fünf, definieren zu können.

2.1. Motivationen Entwicklung automatisierter Fahrzeuge

Die Anzahl im Straßenverkehr verunglückter Personen lag 2016 in Deutschland bei ca. 400.000, darunter 3206 tödlich verletzte Personen [21]. Die weltweit geschätzten Unfalltoten steigen jährlich stetig weiter an. 2010 starben laut WHO ca. 1,24 Millionen Menschen bei Verkehrsunfällen [7]. Der Bedarf und die Notwendigkeit die Sicherheit im Straßenverkehr zu erhöhen besteht.

Die Möglichkeit des automatisierten Fahrens eröffnet Fragestellungen einerseits in fahrzeugspezifischen andererseits in automobilübergreifenden Sektoren. Abbildung 3 zeigt einen Überblick über Sektoren, die vom autonomen Fahren beeinflusst werden können wie beispielsweise Verkehrs-, Komfort- sowie Umwelteffekte.

[2] Die Begrifflichkeit Modal Split beschreibt in der Verkehrstechnik das Transportaufkommen von Verkehrsmitteln unterschiedlicher Art.

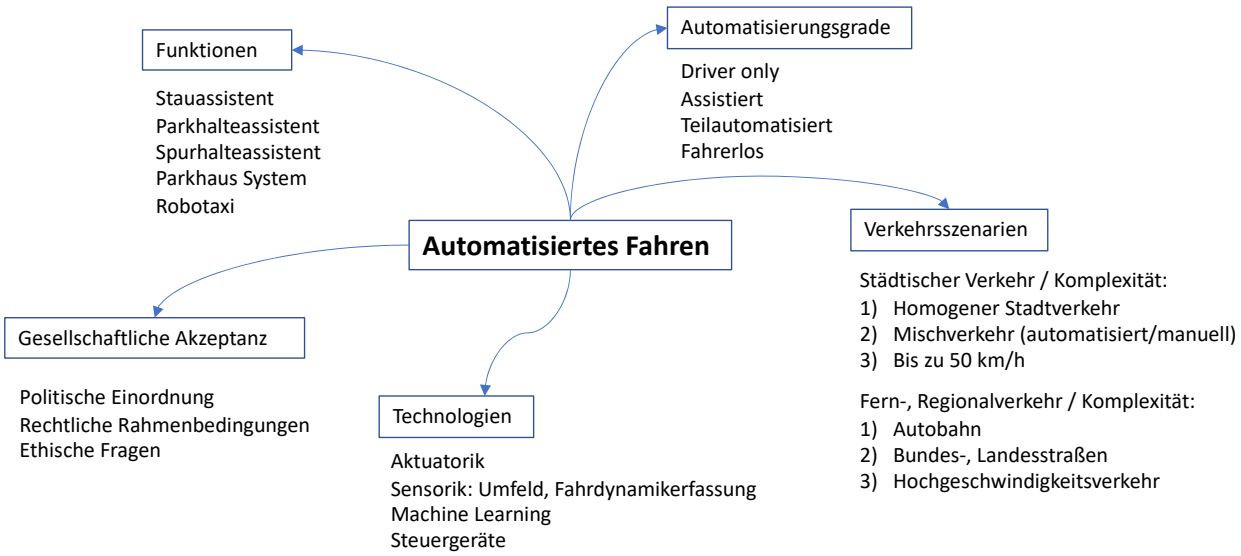

Abbildung 3: Autonomes Fahren Untersuchungsgegenstände unterschiedlicher Sektoren in Anlehnung an [21]

Mit der Zulassung automatisierter Fahrzeuge unterschiedlicher Automatisierungsgrade werden weiter im Bereich der Verkehrssicherheit Entwicklungspotentiale erwartet. Mittels autonomer bzw. automatisierter Fahrzeuge können, auf Basis der Ergebnisse unterschiedlicher Studien wie beispielsweise der Robert Bosch GmbH [22] und von PwC [23], unfallvermeidende Wirkungen erzielt werden. Die Autoren aus [22] erwarten, dass insgesamt 11.000 Menschen in den Ländern Deutschland, USA und China durch vernetzte Assistenzsysteme gerettet werden können. Ebenfalls wurden in einer Studie vom Fraunhofer Institut Effekte des automatisierten Fahrens auf die Unfallstatistik untersucht. Allgemein wird angenommen, dass menschliches Fehlverhalten einen Großteil der Unfälle verursachen. Hinreichend sichere autonome bzw. automatisierte Fahrzeuge sind daher potenzielle Teillösungen zur Erhöhung der Sicherheit im Straßenverkehr.

Eine weitere Chance ist die Optimierung des Verkehrsflusses, der Fahrzeugeffizienz und der Umweltverträglichkeit im Straßenverkehr [7]. Grundlagen dafür legte das bisher umfangreichste europäische Programm zur Fahrzeugautomatisierung „Programme for European traffic with highest efficiency and unprecedented safety (Prometheus)“. Studien über Kraftstoffeinsparpotentiale im Straßengüterverkehr wurden beispielsweise von Roland Berger [24] für das Truck Platooning und vollautomatisiertes Fahren in den USA untersucht. Die Autoren kamen zu dem Schluss, dass zunehmende Automatisierung im Schwerlastverkehr den Kraftstoffverbrauch in den USA im Jahr 2020 um 5% und im Jahr 2040 um 10% verringert. PwC ermittelte durch Platooning im Straßengüterverkehr ein Kraftstoffeinsparpotential von 7%

[23]. Das Kraftstoffeinsparpotential im Personenverkehr wurde unter anderem vom Fraunhofer Institut in [25] mit einem automatisierten Fahrzeug Level drei untersucht. Weitere internationale Studien kamen im städtischen Umfeld zu den Ergebnissen von Kraftstoffeinsparpotentialen von bis zu 31% [26]. Rahmenbedingung der Untersuchungen waren Simulations- und Modellrechnungen sowie das zugrunde legen unterschiedlicher Automatisierungsstufen.

Weiter eröffnen automatisierte Fahrzeuge die Möglichkeit einer Umgestaltung des Verkehrssystems. Besondere Beachtung haben autonome Fahrzeuge im Sektor des Güterverkehrs, durch die Ermöglichung neuer, effizienter Konzepte im Bereich des Warentransportes. [7]

Besteht erhöhter Assistenzbedarf beim Fahrer beziehungsweise bei potenziellen Nutzern, dann bieten automatisierte Fahrzeuge Potentiale zur Komforterhöhung. Sind die Fahrer physisch und/oder psychisch nicht in der Lage das Fahrzeug manuell zu führen, oder müssen bspw. ermüdende Tätigkeiten während der Fahrt ausgeführt werden, dann können automatisierte Fahrzeuge neue Möglichkeiten im Bereich des Komforts und der individuellen Fortbewegung ermöglichen. [7]

Zuoberst wird eine Manifestierung der Innovationskraft in den Sektoren der Fahrzeug- und Systemtechnologien sowie der Technologieführerschaft im Bereich automatisierter Fahrzeuge angestrebt. [21]

2.2. Klassifizierung der Automatisierungsstufen automatisierter Fahrzeuge

Die Automatisierungsstufen von Fahrzeugen wurden von der Bundesanstalt für Straßenwesen (BASt), der National Highway Traffic Safety Administration (NHTSA) und der SAE definiert.[3] In Abbildung 4 ist die Klassifizierung automatisierter Fahrzeuge nach SAEJ 3016 erläutert, da sich die folgenden Definitionen dieser Arbeit auf den SAEJ 3016 Standard beziehen[4].

[3] Neben den Definitionen der SAE und der BASt werden im deutschen sowie im englischen Sprachgebrauch weitere Termini verwendet, um die Fahrzeugautomatisierung zu klassifizieren [1]. Diese Termini unterscheiden sich nicht wesentlich von den Definitionen genannter Institutionen, andererseits ergibt sich durch die Nennung dieser Unterschiede kein Zugewinn für die vorliegende Arbeit. Auf diese Unterscheidung wird daher im Folgenden nicht näher eingegangen.

[4] Ist ein anderer Klassifizierungsstandard gemeint, dann wird diese Information beigefügt.

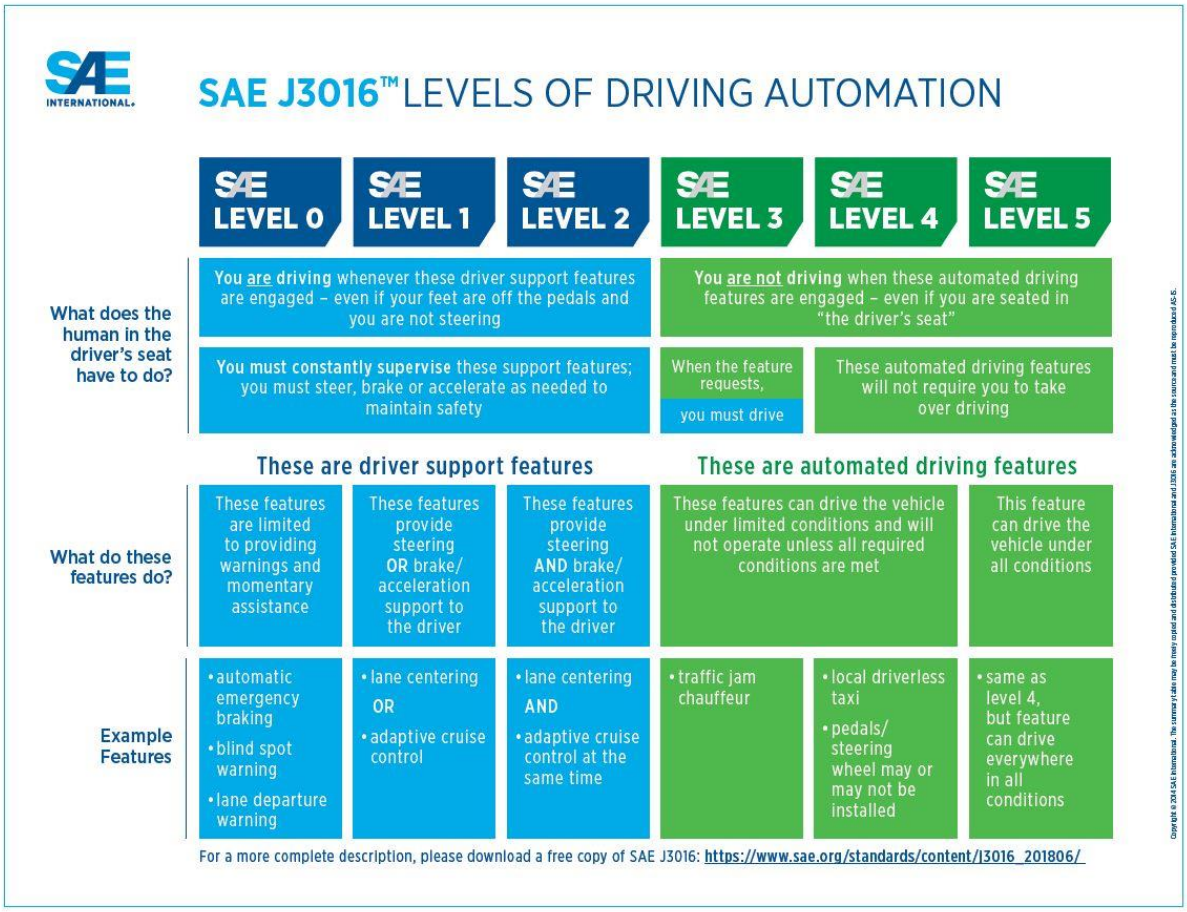

Abbildung 4: Stufen automatisierten Fahrens nach SAEJ 3016 [28]

Im Folgenden werden die Zeiträume der Einführung von Fahrzeugen unterschiedlicher Automatisierungsstufen mit beispielhaften Funktionen vorgestellt.

- Automatisierungsstufe Level eins[5]: Fahrerassistenzsysteme, beispielsweise ACC (Adaptive Cruise Control) oder Spurhalteassistent, werden aktuell in Serienfahrzeugen angeboten. [21] [27]
- Automatisierungsstufe Level zwei: Teilautomatisierte Systeme, wie beispielsweise Spurhalteassistent oder automatische Notbremsung, wurden ab 2015 eingeführt. [21] [27]
- Automatisierungsstufe Level drei: Bedingte Automatisierung beschreibt das selbstständig automatisierte Führen des Fahrzeugs für einen begrenzten Zeitraum, wie beispielsweise der Stauassistent. Unter entsprechenden rechtlichen Voraussetzungen wird diese Automatisierungsstufe voraussichtlich in den 2020er-Jahren prognostiziert. [20] [21] [27]

[5] Zur Vereinfachung soll in dieser Arbeit der Begriff Fahrzeug Level vier bzw. fünf anstelle des fachlich korrekten Begriffs: Fahrzeug SAE Level vier bzw. fünf verwendet werden.

- Automatisierungsstufe Level vier: Dies ist die Vorstufe des autonomen Fahrens. Das System übernimmt nach Aktivierung die Längs- und Querführung und kann hochkomplexe Fahrsituationen selbstständig bewältigen, wie beispielsweise das fahrerlose Parken. Das Fahrzeug wird in einen sicheren Zustand überführt, wenn Warnhinweise bezüglich einer Übernahme vom Fahrer ignoriert werden. Der Sichere Zustand ist beispielsweise das Verzögern in den Stillstand. Diese Systeme sind deutlich nach 2024 zu erwarten. [18] [27]
- Automatisierungsstufe Level fünf: Im vollautonomen Fahrzeug muss der Nutzer weder eine Fahrerlaubnis besitzen, noch muss er fahrtüchtig sein. Das Fahrzeug übernimmt die Fahraufgabe von Start bis Ziel vollständig. Die Markteinführung wird nach 2030 erwartet. [21] [27]

Aufgrund vielfältiger Herausforderungen unterschiedlicher Bereiche sind die Automatisierungsstufen drei, vier und fünf am Markt nicht verfügbar[6]. Auf diese Herausforderungen werden im folgenden Kapitel eingegangen.

2.3. Herausforderungen

Entwicklungen automatisierter Fahrzeuge vollziehen sich auf unterschiedlichen Ebenen. Eine interdisziplinäre Betrachtung ist zur Lösung übergeordneter Problemstellungen zwingend erforderlich. Nicht ausschließlich technische Bereiche, sondern ebenfalls die rechtlichen und politischen Rahmenbedingungen, der Markt an sich und gesellschaftliche Herausforderungen müssen in Kombination mit dem Ziel einer erfolgreichen Einführung automatisierter Fahrzeuge berücksichtigt werden. Besonders die gesellschaftliche Akzeptanz von disruptiven Technologien ist ein wesentlicher Einflussfaktor und tangiert vielfältige Sektoren unterschiedlicher Ebenen. Im Folgenden werden wesentliche Herausforderungen vorgestellt. [29]

2.3.1. Gesellschaftliche Akzeptanz

Technische und rechtliche Problemstellungen, aber auch die Frage was potenzielle Nutzer für Erwartungen und Einstellungen bezüglich neuer Technologien haben, gilt es für die Markteinführung automatisierter Fahrzeuge zu analysieren. Nach [30] werden sich neue Technologien langfristig etablieren, wenn der gesamtgesellschaftliche Vorteil den möglichen Schaden überwiegt. Der Wandel von konventionellen Fahrzeugen zum autonomen bzw.

[6] Stand 09/2020.

vollautomatisierten Fahrzeug bietet für die Gesellschaft und das Individuum neue Nutzerperspektiven. Ausgehend von diesen Veränderungen stellt sich damit die Frage, inwieweit der Einzelne und die Gesellschaft als Ganzes bereit sind, autonome Fahrzeuge im Straßenverkehr zu akzeptieren. [7]

Unter Akzeptanz wird allgemein folgendes verstanden: „annehmen, hinnehmen, billigen, anerkennen, mit jemanden oder etwas einverstanden sein“. Akzeptanz ist etwas Aktives, kann sich zeitlich stark verändern und vollzieht sich in sozialen und technischen Konstruktionsprozessen. Das bedeutet, sie ist abhängig von den Menschen, deren Einstellungen, Wahrnehmungen, Erwartungen, ihrer Umwelt, etc. Akzeptanz unterscheidet sich somit grundlegend von den Begriffen Duldung und Toleranz und kann im Verlauf der Zeit stark variieren. Mit der Akzeptanzforschung soll ermöglicht werden, spezifische Technologien so zu entwickeln, dass diesen eine hohe Akzeptanz zu Teil wird. Unterschiedliche Institutionen haben sich gebildet, die sich mit dem Thema Akzeptanz im gesellschaftlichen Kontext beschäftigen. Diesen liegt die Annahme zugrunde, dass Technik im Kontext gesellschaftlicher, wirtschaftlicher und nutzenbezogener Bereiche betrachtet werden muss. Fahrzeughersteller, die automatisierte Fahrzeuge mit noch nicht ausgereifter Technologie verkaufen, gehen das *Risiko* nicht hinreichend sicher entwickelter Fahrzeuge ein. Ergeben sich vermehrt Unfälle, dann hat dies Auswirkungen auf die gesellschaftliche Akzeptanz dieser Fahrzeuge. Solche Auswirkungen beziehen sich jedoch regelmäßig nicht ausschließlich auf den betroffenen bzw. verursachenden Fahrzeughersteller, sondern auf die gesamte Automobilbranche. Notwendige Bedingung bei der Einführung neuer Technologien wie dem automatisierten bzw. autonomen Fahren ist folglich die Akzeptanz so früh wie möglich zu adressieren und in die Diskussionen unternehmens- und branchenübergreifend einzubinden. Wesentliche Einflussfaktoren können somit frühzeitig erkannt werden und der Wandel gegebenenfalls aktiv gesteuert werden. [7] [31]

2.3.2. Rechtliche, politische Herausforderungen

Rechtliche Rahmenbedingungen, die es ermöglichen autonome Fahrzeuge anzubieten, müssen vorliegen, bevor diese zugelassen werden. Derzeit sind diese Rahmenbedingungen nicht eindeutig formuliert bzw. geregelt. Es wird hierbei grundlegend auf das amerikanische und deutsche Recht Bezug genommen.

Annahme nach [7] ist, dass das was gesellschaftlich als konsensfähig erachtet wird, sich auf rechtlicher Ebene widerspiegelt. Beim Abgleich des möglichen Betriebs autonomer Fahrzeuge mit geltendem Recht, lässt sich derzeit zusammenfassen, dass dem Sinn und Zweck der Gesetze entsprechend, eigenständiges Wirken von Maschinen noch nicht berücksichtigt ist.

Ziel der Gesetze bzw. des Straßenverkehrsrechts, ist die Möglichkeit, diese auf jegliche Lebenssachverhalte anwenden zu können. Wenn die Wirklichkeit sich jedoch so grundlegend verändert, kann dies nur durch eine Aktualisierung des Rechts erfolgen. Diese verändernden Lebenssachverhalte könnten eintreten, wenn sich vollautomatisierte bzw. autonome Fahrzeuge im Verkehrssystem etablieren würden. Als Rahmen für diese Veränderungen müssten übergeordnete Werte der Gesellschaft, bis auf Ebene der Grundrechte hinzugezogen werden, um auf Basis dieser Anpassungen an die neuen Lebensumstände zu führen. [7]

Wird dieser Annahme entsprochen, steht die Frage des Automatisierungsrisikos bezüglich der Grundrechte im Raum. Vollzieht sich der Wandel von menschlich kontrollierter zu eigenständig, maschineller Fahrzeugsteuerung, dann rückt unter anderem die Entscheidungsqualität dieser Steuerung in den Mittelpunkt gesellschaftlicher Akzeptanz. Die Entscheidungen des automatisierten Fahrzeugs können das Recht auf Leben und der körperlichen Unversehrtheit tangieren und sind somit wie grundrechtsrelevante Gefahren im Straßenverkehr einzuordnen. Der Mensch hat ein Grundrecht auf Leben und körperliche Unversehrtheit, geschützt durch Art. 2 Abs. 2 Satz 1 Grundgesetz. Dieser Artikel umfasst den Schutz des Menschen sowohl vor gezielter Tötung als auch vor Verhaltensweisen, die ungewollt den Tod verursachen. Die Schutzpflicht des Staates greift auch und gerade bei rechtswidrigen Eingriffen Dritter. Sind diese Eingriffe nicht zu rechtfertigen, dann ist es die staatliche Pflicht diese mit beispielsweise Normen und Gesetzen zu verbieten. Die verfassungsmäßigen Dogmatiken des Schutzes von Leben und Gesundheit unterscheiden sich teilweise stark zwischen Nationalstaaten, was eine internationale Vereinheitlichung erschwert. Neben der Diskussion der Grundrechte ergeben sich weitere Unklarheiten aus bspw. dem Bereich des Zivilrechts über Haftungsfragen oder dem länderübergreifenden Schutz persönlicher Daten. [7]

2.3.3. Technische Herausforderungen

Die Fähigkeit autonom in komplexen Situationen zu agieren bedarf unterschiedlicher Technologien verschiedenster Disziplinen wie beispielsweise Informatik, Robotik, Elektrotechnik und Steuerung [31]. Die Fahraufgabe eines automatisierten und autonomen Fahrzeugs unterteilt sich in Umfelderfassung, Planung und Umsetzung der Strategie. Im Folgenden werden Problemstellungen domänenspezifisch erläutert.

Wahrnehmung, Modellierung und Interpretation der Umgebung

Zur Identifizierung der Position des Fahrzeugs werden GPS (Global Positioning System), Odometrie[7] sowie Radar und Lidar[8] eingesetzt [32] [33]. Kamerasysteme werden zur Lokalisierung von Hindernissen, Verkehrszeichen und Verkehrsteilnehmern sowie zur Positionierung des Fahrzeugs genutzt [34] [35] [36]. Ultraschallsensoren fungieren zur Entfernungsmessung reflektierender Objekte im unmittelbaren Fahrzeugumfeld [19]. Gespeicherte digitale Karten und Ortungssystem sowie Car-to-Car Kommunikation übermitteln weitere Umfeldinformationen [33].

Grundlage für die Planung einer hinreichend sicheren Referenztrajektorie[9] sind umfassende Umfeldinformationen, die jederzeit verfügbar sind. Diese Sensoren werden eingesetzt, um das Fahrzeug in der Fahrbahn, Verkehrsteilnehmer, stationäre Hindernisse sowie Verkehrszeichen und akustische Signale zu lokalisieren [19] [37].

Einzelne Sensoren bzw. Technologien sind nicht in der Lage zuverlässig und präzise zu erkennen, zu klassifizieren und robust während widriger Umweltbedingungen zu arbeiten.[10] Ein multimodaler Ansatz wird gewählt, um positive Eigenschaften jeweiliger Technologien zu kombinieren. Sensorfusionsalgorithmen fusionieren die Daten zu einem Umweldmodell [19]. Sensordegradation mehrerer Sensoren und/oder Softwarefehler der Sensorfusionsalgorithmen führen zu Fehlinformationen [19]. Diese Problemstellungen müssen zukünftig adressiert werden, um hinreichend sichere Umfeldinformationen bereitstellen zu können.

Planung von Manövern und Trajektorien

Algorithmen automatisierter Fahrzeuge basieren unter anderem auf Machinelearning. In sicherheitsbezogenen Komponenten konventioneller Fahrzeuge wird diese Technologie seltener eingesetzt. Machinelearning jedoch wird als entscheidende Technologie im Bereich des automatisierten Fahrens angesehen [38]. Algorithmen leiten auf Basis von Daten die Identifizierung von Mustern bzw. Strukturen ab [32]. Es folgt eine Mustererkennung. Die Lösungsstrategien sind keine durch menschlich verständliche programmierte Algorithmen, sondern sind datengetrieben.

[7] Odometrie ist eine Methode zur Schätzung von Position und Orientierung eines Fahrzeugs auf Basis von Gierraten, Längsbeschleunigung, Querbeschleunigung, Fahrzeuggeschwindigkeit, Schlupfwinkel und weitere Vortriebssystemparameter. [19]
[8] Lidar: Light detection and ranging; Radar: Radio detection and ranging.
[9] Eine Fahrtrajektorie beschreibt den Bewegungspfad eines Fahrzeugs in Abhängigkeit von Zeit und Ort.
[10] Stand 09/2021

Die Bahnplanung, Trajektorienplanung und Optimierung in einem automatisierten bzw. autonomen Fahrzeug werden derzeit hauptsächlich mit deterministischen Planungsalgorithmen durchgeführt. Machinelearningalgorithmen stellen unter Anderem interpretierte Ergebnisse für die Bahnplanung bereit. Hochautomatisierte Fahrzeuge sind mit zahlreichen Sensoren ausgestattet. Aufkommende Datenmengen erhöhen sich stetig und müssen verarbeitet werden. Neuronale Netze können in der Umfelderkennung einen Beitrag leisten. Verkehrsobjekte und Fahrbahnmarkierungen können beispielsweise erkannt werden und stellen Daten für die Manöverplanung bereit [39].

Aktuelle Sicherheitsstandards sind nicht auf die Besonderheiten der Machinelearningalgorithmen angepasst. Allgemeine Standards zur Erfassung von Datensätzen liegen nicht vor und es wurden noch keine Leistungsbewertungsmetriken definiert. Die Vorgehensweise mit auftretenden Unsicherheiten ist nicht eindeutig festgelegt [32]. Um die Gesamtsicherheit des Systems zu gewährleisten, ist eine gesamtheitliche Betrachtung notwendige Bedingung für hinreichende Sicherheit. Validierungsmethoden und Sicherheitsstandards von Machinelearningalgorithmen müssen zukünftig an diese Herausforderungen angepasst werden, um hinreichend sichere Fahrzeuge zu ermöglichen. [19]

Umsetzung

Die Aktuatorik wird eingesetzt um Trajektorien, vorgegeben von den Steuerungs- und Regelungssystemen, zu realisieren. Die technische Umsetzung der Anforderungen durch die Regelungssysteme in einem autonomen bzw. automatisierten Fahrzeug unterscheidet sich nicht wesentlich von der Umsetzung in einem konventionellen Fahrzeug. Die Aktuatorik stellt somit weitestgehend keine Herausforderung dar, da wesentliche Elemente aus dem konventionellen Fahrzeug verfügbar sind. Stellglieder und insbesondere Stellgrößenbegrenzungen müssen hingegen in der Analyse der Gesamtstrategie berücksichtigt werden. [37]

3. Absicherung automatisierter Fahrzeuge

Einheitliche Standards und Normen dienen zur Rationalisierung und Qualitätssicherung eines Produktes. In der Entwicklung von sicherheitskritischen Systemen können somit Vorgehen zur Qualitätssicherung festgelegt werden. Dadurch können sicherheitsrelevante Bereiche auf einheitliche Weise standardisiert und überprüft werden. Sie sind notwendige Voraussetzung für eine automobilherstellerübergreifende Entwicklung.

Im folgenden Kapitel werden zunächst Standards vorgestellt, auf deren Basis die Automobilindustrie hochautomatisierte bzw. autonome Fahrzeuge entwickelt bzw. entwickeln wird. Die *Wiener Straßenverkehrskonventionen* [40], die ISO 26262, die ISO 21448 [41] und die ISO/SAE CD 21434 [42] sind die im Folgenden erläuterte Normen. Anschließend wird auf branchenübergreifende Standards eingegangen, die auch die Normen der Automobilindustrie prägen bzw. geprägt haben.

3.1. Wiener Straßenverkehrskonventionen

1968 wurden die *Wiener Straßenverkehrskonventionen* über den Straßenverkehr mit Bezug zur Sicherheit im Straßenverkehr ratifiziert. Grundgedanke zur Schaffung der Norm ist die weltweite Standardisierung von Verkehrsregeln. Das Übereinkommen wurde von 80 Ländern einschließlich Deutschland ratifiziert[11]. In der Norm wurde seit 1968 festgehalten, dass ein Fahrzeug jederzeit vom Fahrer manövriert werden muss. Es soll sichergestellt werden, dass der Fahrer die Möglichkeit hat Fahrbewegungen durchzuführen. 2014 wurde der Vertrag überarbeitet. Seit 2016 sind automatisierte Fahrzeuge im Straßenverkehr zulässig, wenn sie vom Fahrer übersteuerbar sind bzw. der autonome Fahrmodus jederzeit deaktiviert werden kann.

Ein vollautonomes Fahrzeug ist nach aktueller Gesetzgebung in Deutschland nach wie vor nicht zulassungsfähig[12]. Derzeit wird der Vertrag überarbeitet, um die Richtlinien auf hochautomatisierte sowie autonome Fahrzeuge weiter anzupassen. Unter anderem haben die USA die *Wiener Straßenverkehrskonventionen* nicht ratifiziert. Dort dient das „Automated Driving System *A Vision for Safety* als Regelwerk des Rechtsrahmens für automatisiertes Fahren. In China wurden vom Ministerium für Industrie und Informationstechnologie im Bereich automatisierter bzw. autonomer Fahrzeuge 2018 Leitlinien für den Aufbau des nationalen Internet-Standardsystems der Fahrzeugindustrie bekannt gegeben, um Forschung und

[11] Stand 11/2021.
[12] Stand 11/2021.

Entwicklung vernetzter Fahrzeuge zu fördern. Weitere Standards werden entwickelt. [43] [44][45]

3.2. Funktionale Sicherheit IEC 61508 und ISO 26262

Die Normenreihe IEC 61508 [46] –Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbar elektronischer Systeme- wurde 1998 veröffentlicht. Die funktionale Sicherheit ist ein Teilgebiet der Gesamtsicherheit und adressiert die adäquate Funktionsfähigkeit des sicherheitsbezogenen Systems[13] sowie Maßnahmen zur Identifikation systemtheoretischer Fehler und zufälliger Ausfälle. Die IEC 61508 ist eine branchenübergreifende Grundnorm aus der domänenspezifische Normen jeweiliger Anwendungsfelder abgeleitet wurden, beispielsweise die ISO 26262 als Standard für die Automobilindustrie (siehe Abbildung 5). Die IEC 61508 ist aus dem Bewusstsein entstanden, dass restriktive Entwicklungsprozesse notwendig sind, um systematische Fehler einzugrenzen. [47] [48]

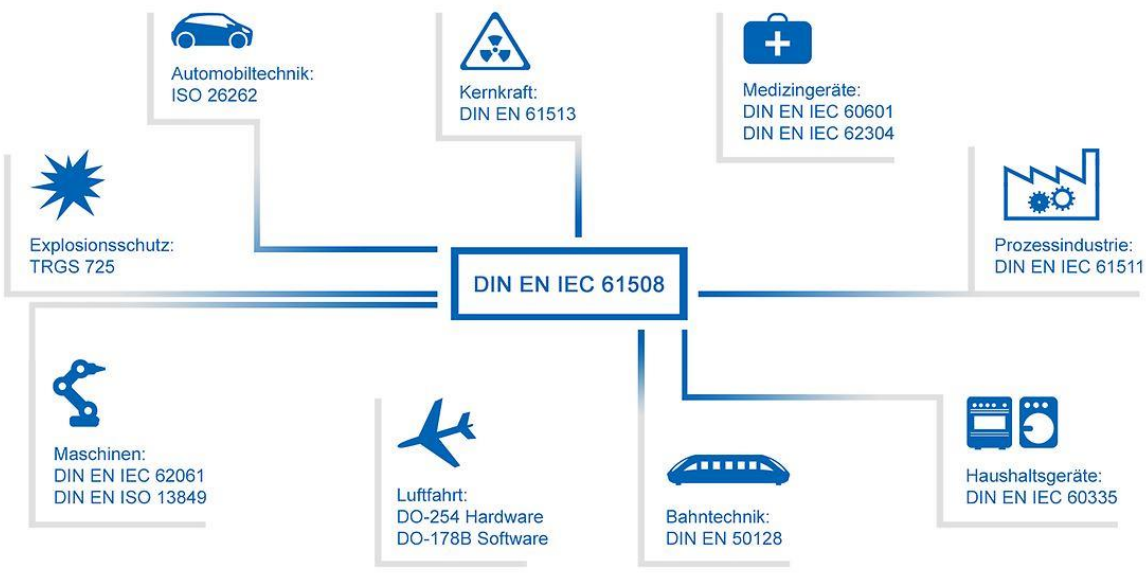

Abbildung 5: Branchenspezifische Normen abgeleitet aus der Grundnorm IEC 61508 [44]

Im November 2011 wurde die ISO 26262:2011 veröffentlicht, um die funktionale Sicherheit von sicherheitskritischen E/E Komponenten und Systemen im Fahrzeug zu adressieren. Sie

[13] Das sicherheitsbezogene System hat eine oder mehrere Funktionen, um die Anforderungen der funktionalen Sicherheit zu erfüllen. Fällt eine Funktion aus, dann wären unerwünschte Zustände das Resultat. [48]

wurde unter anderem auf Basis von state-of-the-art Systemen und branchenübergreifenden Standards abgeleitet. Die ISO 26262:2018[14] ist die zweite, aktualisierte Version der ISO 26262:2011. Die Norm ist aktueller Standard zur funktionalen Sicherheit im Automobilsektor. [47] [49] [50]

Die ISO 26262 unterteilt sich in zehn Bereiche mit Teilgebieten zu Sicherheitsmanagement, Produktlebenszyklus, Analysemethoden und Sicherheitsrichtlinien. Sie gibt ein spezifisches Vorgehensmodell zur Absicherung vor und beschreibt einerseits die gesamtheitlichen Anforderungen an E/E Systeme und andererseits die Normanforderungen an den gesamten Produktlebenszyklus, siehe Abbildung 6.

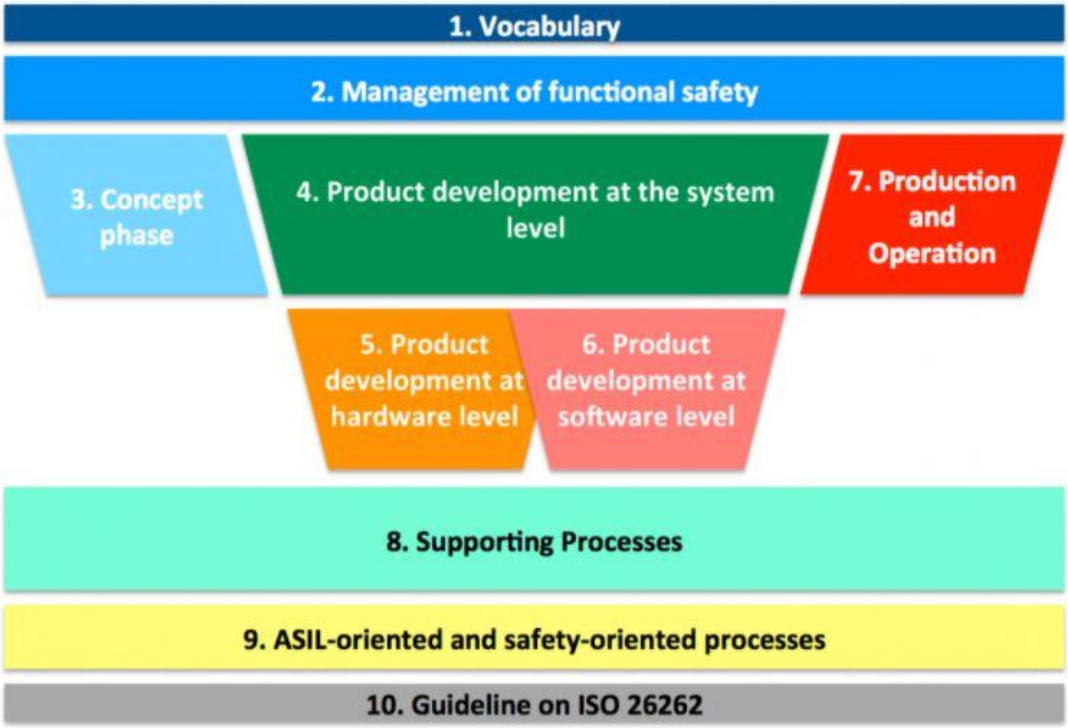

Abbildung 6: ISO 26262 schematische Vorgehensweise [51]

Im ersten Teil der Norm wird das Vokabular als Grundlage für nachfolgende Kapitel definiert. Teil zwei adressiert das Management der Funktionssicherheit im Allgemeinen. Teil drei bis sieben gehen auf den Produktentwicklungslebenszyklus näher ein. Die ISO 26262 definiert darin zunächst das zu untersuchende System und die Funktion, das sogenannte Item. Ein Item definiert ein System oder Array von Systemen. Im Item müssen die Funktionen und die Abhängigkeiten mit Umwelt- bzw. weiteren Elementen definiert sein. Mittels Gefahrenanalysen werden mögliche Gefahrenzustände des Systems identifiziert. FTA, FMEA (Failure Mode and

[14] Zur Vereinfachung soll in dieser Arbeit fortan der Begriff ISO 26262 anstelle des fachlich korrekten Begriffs ISO 26262:2018 verwendet werden.

Effects Analysis), PHA (Preliminary Hazard Analysis) und die HAZOP-Analyse (Hazard and Operability) sind unter anderem die dafür vorgesehenen Gefahrenanalysemethoden. Im achten Teil werden die unterstützenden Prozesse und Tools aufgelistet. Im neunten Teil wird das ASIL (Automotive Safety Integrity Level) definiert. Die Fehler werden in Risikoklassifizierungsschemata eingeteilt. Das ASIL kategorisiert Elemente, gibt durch die Clusterung vor wie sicher diese sein müssen und definiert Richtlinien über bestimmte Vorgehensweisen in den Prozessschritten. Die Norm macht Vorgaben zu Sicherheitsmaßnahmen, beispielsweise Kategorisierungen der Notwendigkeit von Modellierungs- und Codierungsrichtlinien in Abhängigkeit des jeweiligen ASILs. [19] [49] [52]

3.3. Gebrauchssicherheit

Die 2019 veröffentlichte Norm ISO/PAS 21448, kurz SOTIF (Safety of the Intended Functionality) geht auf die Gebrauchssicherheit der beabsichtigten Funktionalität bzw. Sollfunktion ein. Der Funktionsentwicklungs- und Funktionsdesignprozess wird iterativ durchgeführt. Dieser umfasst sowohl die Validierung und die Verifikation. Im Vergleich zur ISO 26262 werden keine grundlegenden neuen Vorgehensweisen angewendet, hingegen steht die beabsichtigte Funktionalität des zu untersuchenden Systems im Zentrum der Analyse. Bei bestimmungsgemäßem Gebrauch oder zu erwartetem Fehlgebrauch dürfen keine personengefährdenden Schäden auftreten. Um dieses Ziel zu erreichen, werden auf Basis der Norm Eigenschaften des Produktes, des Produktentwicklungsprozesses und geeignete Tests formuliert. In der funktionalen Sicherheit werden hingegen Gefährdungen analysiert, die durch eine Fehlfunktion verursacht werden. Im Folgenden werden Beispiele für Fehlerursachen, die der Gebrauchssicherheit zugeordnet werden, aufgelistet. [19] [47]

1. Vorhersehbarer Missbrauch einer Funktion.
2. Fehler, die sich aufgrund eines Überschreitens vordefinierter Rahmenbedingungen ergeben.
3. Fehler, die aufgrund limitierter technischer Gegebenheiten entstehen.

Grundgedanke dieses Ansatzes in der Klassifizierung der Risiken ist die Unterteilung von Szenarien in Bekannte und Unbekannte. Es wird angenommen, dass in bekannten Szenarien einerseits ein sicheres Systemverhalten, andererseits ein potenziell nicht vorhersehbares und somit gefährdendes Systemverhalten vorliegt. Ebenfalls können Szenarien definiert werden die unbekannt und für Mensch und Umwelt gefährdend sind, siehe Abbildung 7. [19] [47]

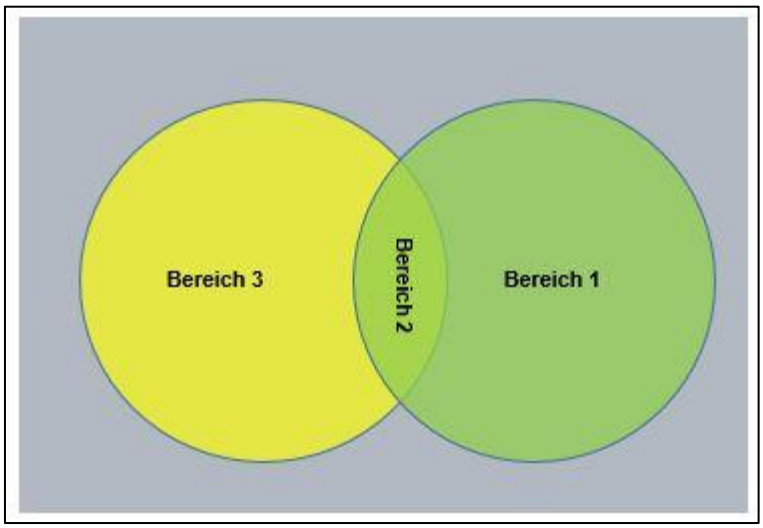

Abbildung 7: Klassifizierung der Szenarien nach SOTIF in Anlehnung an [19]

1. Bereich (grün gefärbt): Bekanntes sicheres Systemverhalten.
2. Bereich (grün/gelb gefärbt): Bekanntes Systemverhalten, welches potenziell gefährdend bzw. nicht vorhersehbar ist.
3. Bereich (gelb gefärbt): Unbekanntes potenziell gefährdendes Systemverhalten.
4. Umgebender Bereich (grau gefärbt): Sicherer Bereich.

Ziel der SOTIF ist es, den Bereich eins zu maximieren und den Bereich zwei und drei zu minimieren. Bekanntes bzw. unbekanntes gefährdendes Systemverhalten[15] muss eliminiert werden, sodass die Systemsicherheit auf ein akzeptables Risikoniveau gehoben werden kann. Zusammenfassend ist die ISO 21448 eine Ergänzung zur ISO 26262, um die Sicherheit von Systemen hinsichtlich ihres vorgesehenen Systemverhaltens zu analysieren. In vollautonomen Fahrzeugen ist aufgrund des Fehlens einer Rückfallebene durch den Fahrer die Gebrauchssicherheit von entscheidender Bedeutung. [19]

3.4. Cybersecurity

Die Cybersecurity ist ein Teilgebiet der Absicherung, die das System befähigt, sich gegenüber absichtlich, böswilligen Akteuren zu schützen. Gefahren aus der Systemumwelt werden analysiert. Mutwillige Angriffe von Akteuren außerhalb können Sicherheitsfunktionen außer Kraft setzen und somit die funktionale Sicherheit beeinflussen. Diese Angriffe können ein unerwartetes Systemverhalten verursachen und die Gebrauchssicherheit beeinflussen. Ungewollte Ereignisse in der Security werden von aktiven Gegnern verursacht. Sicherheit

[15] Auf etwas Unbekanntes kann nicht zielgerichtet reagiert werden, siehe Kapitel 1.

konzentriert sich hingegen auf die adäquate Funktionsweise des Systems. Gefahrenpotentiale des letztgenannten Bereichs gehen von passiven Gegnern aus, bspw. aufgrund von Zufälligkeiten in der Natur bzw. vom menschlichen Handeln. [19] [47]

Aufgrund der zunehmenden Konnektivität innerhalb des Fahrzeugs sowie mit der Betriebsumgebung und weiteren Verkehrsteilnehmern, nehmen Schnittstellen zwischen Steuerungsfunktionen, den IT-Backend Systemen und anderen Informationsquellen zu. Diese Schnittstellen sind mögliche Angriffspunkte böswilliger Akteure. Es müssen Cybersecurityprinzipien und -praktiken angewendet werden, sodass ungewollte willkürliche Einflussnahme von Angreifern verhindert werden. Ist die Integrität der Daten beeinträchtigt, werden fehlerhafte Daten verarbeitet, die zu Kollisionen bzw. unerwünschten Ereignissen führen können. Derzeit steht ein Standard, der Cybersecurity adressiert, zur Verfügung. Die ISO/SAE CD 21434, welche auf die vorsätzliche Manipulation von Akteuren erstmalig Bezug nimmt, wurde im August 2021 veröffentlicht. [19]

3.5. Funktionale Absicherung mit Fokus auf Avionik und Automobilindustrie

Auf Sicherheitsnormen im Bereich der funktionalen Sicherheit in Branchen mit Automationsbezug außerhalb der Automobilindustrie wird im Folgenden eingegangen. Die Luftfahrt hat im Verhältnis zu Industrien wie beispielsweise der Medizintechnik oder der Automobilindustrie frühzeitig begonnen, systematisch funktionale Sicherheit zu standardisieren. Die Herausforderung der Luftfahrt bestand darin, ein Fail-Operational-Verhalten zu entwickeln. Die Anforderungen in der Automobilbranche liegen hingegen in der Entwicklung eines Fail-Safe-Verhaltens. Insbesondere Anforderungen im Bereich der Avioniksoftwareentwicklung sind von der Luftfahrthistorie geprägt. In den 1980er[16] Jahren wurden die ersten Softwaresicherheitsstandards in der Luft- und Raumfahrt eingeführt. 1982 wurde die erste Version der RTCA DO-178 [20] zur Zertifizierung von Software veröffentlicht. Sie gibt ein praxisorientiertes Verfahren zur Entwicklung sicherheitskritischer Software vor. Die ARP 4754 [53] gibt einen Prozess zur Entwicklung ziviler Luftfahrsysteme vor und wurde 1996 verabschiedet. Diese Normen bestimmen bis heute die System- und Softwareentwicklung in der Luftfahrt. Diese Erfahrungswerte haben die Entwicklung des ISO 26262 Standards in der Automobilindustrie im Jahr 2011 maßgeblich beeinflusst. Sie bildet das Pendant zu den Avionikstandards. In der Medizintechnik wurden im Vergleich zur Automobilindustrie funktionale Sicherheitsstandards später eingeführt. [54] [55]

[16] 1982 wurde die Norm DO-178 ratifiziert.

3.6. Überarbeitung von Standards in der Absicherung

In der Automobilindustrie wird großer Aufwand betrieben, um die Entwicklung hochautomatisierter und autonomer Fahrzeuge voranzutreiben. Die ISO 26262 und die ISO/PAS 21448 [41] sind nicht ausreichend, um komplexe, softwareintensive automatisierte Fahrzeuge hinreichend sicher zu entwickeln. In der ISO 26262:2018 wird beispielsweise keine konkrete Methode vorgegeben, welche das *Risiko* eines unerwünschten Ereignisses und die Sicherheit in einem optimalen Trade-off definiert. Wird die Entwicklung risikoreich ausgelegt, dann sind Systeme nicht hinreichend sicher, hingegen jederzeit verfügbar. Werden sie konservativ ausgelegt, dann ist die Systemverfügbarkeit gering, aber dementsprechend erhöht sich die Sicherheit. Weiter können Informationen aus Erfahrungen von vollautonomen Fahrzeugen nach Markteinführung nicht abgeleitet werden, da die Markteinführung noch nicht stattgefunden hat. Darüber hinaus sind keine Fahrzeugarchitekturmodelle für die Abschätzung von Ausfallraten vorgegeben. Auf Basis von Erfahrungen, Studien, der Literatur und Standards aus anderen Branchen, wie bspw. der Luftfahrtindustrie, müssen die Standards weiter überarbeitet werden. Problemstellungen ergeben sich in der Absicherung künstlicher Intelligenz, der Interaktion von Fahrzeug und Mensch sowie der Leistungsfähigkeit der Sensorik. Normen und Standards für autonome bzw. hochautomatisierte Fahrzeuge müssen weiterhin überarbeitet und international standardisiert werden, um der Entwicklung dieser Technologie weltweit einheitliche, hinreichende Rahmenbedingungen vorzugeben. [19] [49] [52]

4. Vertretbarkeit und Erläuterung von Risiko und Fehler

Im folgenden Kapitel werden auf die Begriffe Risiko und Fehler eingegangen, einschließlich der Bewertung und Einordnung in den Kontext des Automobilbaus. Diese Begrifflichkeiten sind Grundlage folgender Kapitel mit Fokus auf Sicherheitsanalysen und Gefahrenidentifikation.

4.1. Risiko allgemein

In der ISO 26262 wird *Risiko* als Kombination von Schadensschwere und der Auftretenswahrscheinlichkeit definiert. Technische Systeme und Umwelt stehen direkt bzw. indirekt in Interaktion. Ziel ist ein positiver Nutzen für die Umwelt bzw. für den Menschen zu schaffen. Sicherheitsrelevante technische Systeme ohne *Risiko* zu entwickeln ist aufgrund der Unmöglichkeit einer vollständigen Abbildung der Realität in Modellen und endlicher Komponentenzuverlässigkeit nicht realisierbar. International wurden quantitative Vorgaben zur Vertretbarkeit von Grenzrisiken in domänenspezifischen Standards formuliert. Das akzeptierte Grenzrisiko ist das größte noch akzeptierbare *Risiko* eines technischen Systems. In Abbildung 8 sind die unterschiedlichen Begrifflichkeiten veranschaulicht. Bei der Nutzung von Atomkraft wurden beispielsweise folgende Werte festgelegt: Das Ereignis einer Kernschmelze in einem Kraftwerksbetriebsjahr soll kleiner sein als 10^{-5}. Die Freisetzung größerer Radioaktivitätsmengen soll pro Jahr kleiner sein als 10^{-6}. In der Luftfahrt gilt für Mehrfachfehler eine Auftrittsrate von 10^{-9} pro Stunde. Im Schienenverkehr wurde die Versagenswahrscheinlichkeit pro Einstellung einer Fahrstraße bei 10^{-9} innerhalb eines Jahres formuliert. In der Automobilindustrie werden derzeit vertretbare Risikowerte für bspw. das Drive-by-Wire und andere Systeme diskutiert. Von technischen Systemen wird somit stetig ein *Risiko* ausgehen. Eines der Ziele aus technischer Sicht ist das *Risiko*, welchem der Mensch durch die technische Komponente ausgesetzt ist, zu vermindern. Gefahren für den Menschen werden allerdings nicht ausschließlich durch technische Systeme verursacht, sondern können auch durch andere, nicht beeinflussbare Faktoren wie beispielsweise Krankheiten ausgelöst werden. Der Mensch lebt somit naturgemäß unsicher und bewegt sich in einer risikoreichen Umwelt. Das oberste Ziel ist das Gesamtrisiko so gering wie möglich zu halten, um die Wahrscheinlichkeit des Eintritts eines gefährdenden Ereignisses und dessen Konsequenzen zu verringern. In diesem Zusammenhang stellt sich die grundlegende Frage der Definition nach hinreichender Sicherheit technischer Systeme. Wie sicher ist sicher genug? [56]

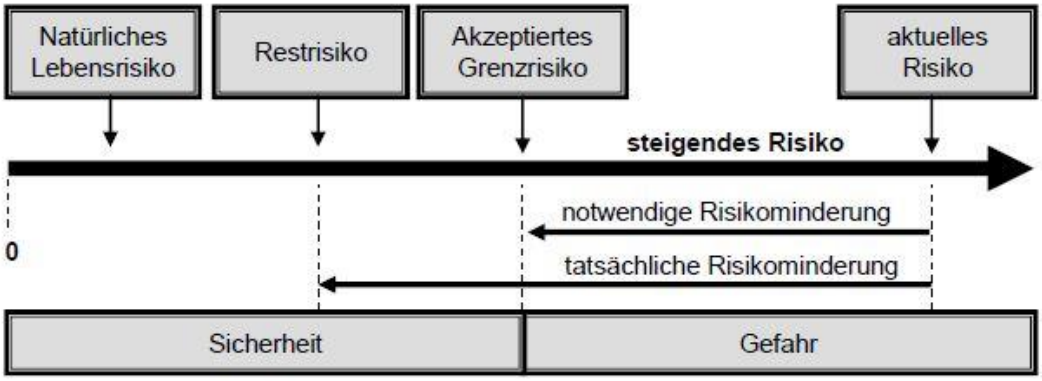

Abbildung 8: Arten des Risikos [56]

Die Risikoakzeptanz der Gesellschaft, siehe Kapitel 2.3.1., ist ein Einflussfaktor, um diese Frage zu beantworten. Bezugnehmend auf die automobilspezifische Sicherheitsnorm ISO 26262 wird ein System als sicher bezeichnet, wenn das Restrisiko geringer ist, im Vergleich zu einem, nach gesellschaftlichen und moralischen Konzepten, akzeptierten Grenzrisiko. [56]

4.2. Fehler

Unter Anderem hat Laprie [57] Begriffsdefinitionen für die im deutschen meist vielseitig verwendete Begrifflichkeit *Fehler* eingeführt. Eines der Ziele von Laprie ist die Formulierung einer Basisterminologie zur Vereinheitlichung des Sprachgebrauchs. Laprie unterscheidet zwischen den Begriffen Ausfall (*failure*), Fehler (*error*) und der Fehlerursache (*fault*). [57]

- Ein *failure* ist eine unzulässige Veränderung eines Systemmerkmals, welche zu einem nicht zu erwarteten Systemverhalten führt.
- Ein *error* kann hingegen verschiedene Zustände einnehmen. Das System fällt auf gesamtheitlicher Ebene aus oder Funktionalitäten fallen auf hierarchieniedrigerer Ebenen aus (Degradation). Diese führen zu einem Zustand eingeschränkter Funktionserfüllung.
- Ein *fault* ist die Ursache eines *errors*.

Die ISO 26262 weist dem Begriff *fault* im Vergleich zu Laprie eine deutlich spezifischere Bedeutung zu. Ein *fault* wird durch eine beliebige fehlerauslösende Ursache erzeugt. Es wird als „abnormal condition“ bezeichnet, wobei dieser Begriff im Standard nicht weiter definiert ist. Die Abweichung von der angestrebten Funktionalität bietet sich folglich als mögliche Interpretation an. Bei der Gefahrenidentifikation werden jedoch auch Ursachen betrachtet, die nicht ausschließlich durch Abweichungen der vorhergesehenen Funktionalität ausgelöst werden. Daher erscheint die Definition von Laprie in dieser Arbeit geeigneter. [58]

Abbildung 9 stellt eine mögliche Unterteilung der Fehlerarten dar. Diese Klassifizierung ist für die Bewertung der Gefahrenanalysen der Systemtheorie sowie der Zuverlässigkeitstheorie von Relevanz und wird in der STPA Auswertung *(Kapitel 7)* erneut aufgegriffen. Im Folgenden wird konkret auf die Unterteilung in systematische Fehler, zufällige Fehler und Gebrauchsfehler eingegangen und diese erläutert. [56]

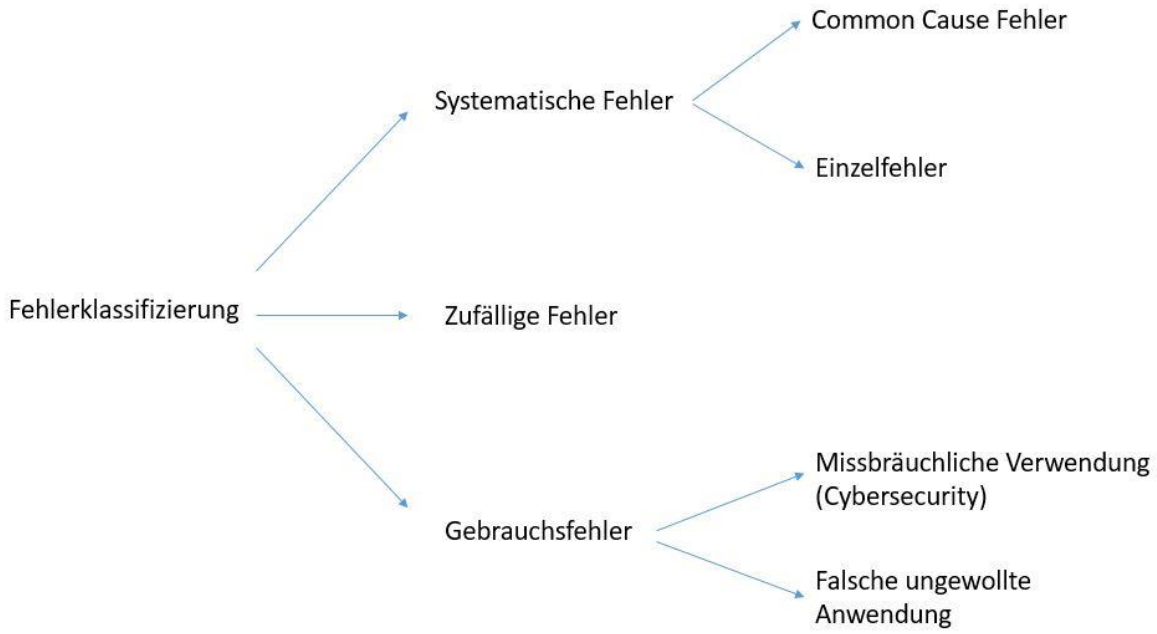

Abbildung 9: Klassifizierung der Fehlerarten in Anlehnung an [56]

Systematische Fehler

Systematische Fehler liegen bei inadäquaten Anforderungsspezifikationen an das System bzw. einer inadäquaten Umsetzung der Anforderungen vor. Systematische Fehler prägen sich unter spezifischen Umständen in Interaktion mit internen Systemeinheiten bzw. systemübergreifenden Elementen aus. Zum Zeitpunkt der Inbetriebnahme des Systems sind diese Fehler integriert. Die spezifischen Umstände, beziehungsweise den Einfluss auf tangierende Teilsysteme sind naturgemäß nicht bekannt, andernfalls würden diese Fehler nicht auftreten. Ursachen für systematische Fehler sind unter anderem komplexe Systeme, die nicht ganzheitlich erfasst werden können sowie nicht sicherheitsgerichtete Entwicklungsprozesse, welche die Ausprägung dieser Fehlerart fördern. [56]

Zufällige Fehler

Im Vergleich zu den systematischen Fehlern liegen zum Zeitpunkt der Inbetriebnahme des Systems keine zufälligen Fehler vor. Sie werden ausgelöst durch spontane nicht vorhersehbare Prozesse und werden mittels statistischer Methoden abgeschätzt. Die spezifischen Ursachen für das Auftreten zufälliger Fehler können in der Fehleranalyse nicht eindeutig identifiziert werden. [59]

Common Cause Fehler

Eine Untergruppe der systematischen Fehler bilden die Common Cause Fehler (CCF). CCF beschreiben Mehrfachausfälle in redundanten Systemen, die durch eine gemeinsame Ursache ausgelöst werden. Dabei müssen die Mehrfachausfälle der Teilsysteme nicht zwangsläufig zu einem Ausfall des Gesamtsystems führen. Ausfälle unterschiedlicher Art werden als CCF bezeichnet, Mehrfachausfälle gleicher Art als „Common Mode Fehler“ (CMF). [56]

Ausfälle bzw. Fehler θ_1, $\theta_2 \ldots \theta_n$, die nicht durch eine gemeinsame Ursache ausgelöst werden sind stochastisch unabhängig, wenn folgende Gleichung zur Berechnung der Verbundwahrscheinlichkeit gilt, wobei $\{k_1, k_2, \ldots, k_n\} \subset \{1,2,\ldots,n\}$

$$P\left(\theta_{k_1} \cap \theta_{k_2} \cap \ldots \theta_{k_n}\right) = P\left(\theta_{k_1}\right) \cdot P\left(\theta_{k_2}\right) \cdot \ldots \cdot \theta_{k_n} \qquad \text{(Gl. 1)}$$

Bei abhängigen Fehlern, den CCF und den CMF, wird die Verbundwahrscheinlichkeit über die bedingte Wahrscheinlichkeit berechnet, siehe Gleichung 2.

$$P(\theta_2|\theta_1) = \frac{P(\theta_1 \cap \theta_2)}{P(\theta_1)} \quad \text{für } P(\theta_1) \neq 0 \qquad \text{(Gl. 2)}$$

Handhabungs-, Bedien-, und Wartungsfehler

Dieser Kategorie werden Fehler zugeordnet, die während des bestimmungsgemäßen Gebrauchs, des nicht bestimmungsgemäßen Gebrauchs und des erwarteten Fehlgebrauchs des Systems ausgelöst werden (siehe Kapitel 3.3.). Sie können beispielsweise durch Handhabungs-, Bedien- und Wartungsfehler verursacht werden. Mutwillig ausgelöste Fehler durch böswillige Akteure werden hingegen nicht dieser Art zugeordnet. [59]

Ursächlich für den nicht bestimmungsgemäßen Gebrauch des technischen Systems ist beispielsweise Mode Confusion[17]. Das Prozessmodell des Menschen vom technischen

[17] Als Mode Confusion wird bezeichnet, wenn das Verhalten eines technischen Systems nicht mit dem mentalen Prozessmodell des Nutzers vom technischen System übereinstimmt. [14]

System ist nicht deckungsgleich mit dem tatsächlichen Prozessmodell des technischen Systems. Mode Confusion lässt sich unter anderem durch geeignete Ausbildungsmaßnahmen oder adäquate Spezifikationen der Mensch-Maschine Schnittstelle vermeiden. [14] [56]

Probabilistische Analysen können zufällige Fehler mittels Kenngrößen identifizieren. Systematische Fehler bzw. Bedienfehler sind mit diesen Analysen nur eingeschränkt adressierbar. Um ein hinreichend sicheres System zu entwickeln, müssen die diskutierten Fehlerarten bestimmt und Maßnahmen eingeleitet werden, um das Gesamtrisiko für ungewünschte Ereignisse zu minimieren.

- Verminderung von systematischen Fehlern im System durch beispielsweise Nutzung diversitärer Redundanz in der Auslegung von Systemen [56] sowie geeigneter sicherheitsbezogener Entwicklung [57]
- Adäquate Sicherheitskonzepte unter Berücksichtigung des Auftretens zufälliger Fehler [57]
- Erhöhung der Zuverlässigkeit der Komponenten
- Schutz des technischen Systems gegenüber böswilligen Akteuren [56]

Die diskutierten Normen in Kapitel 3 greifen diese Anforderungen auf.

5. Gefahrenanalysen und Sicherheitsanalysen

Geeignete Sicherheitskonzepte, Standards und Vorgehensweisen müssen definiert werden, um hinreichend Sicherheit in automatisierten Fahrzeugen zu gewährleisten. Im Folgenden werden Herausforderungen vorgestellt, die sich speziell auf die Anwendung der GuR sowie auf das funktionale Sicherheitskonzept aus der ISO 26262 für die Absicherung automatisierter Fahrzeuge beziehen. Allgemeine Herausforderungen automatisierter Fahrzeuge werden in Kapitel 2.3 vorgestellt.

5.1. Herausforderungen im Hinblick der GuR

Im Entwicklungsprozess nach ISO 26262 ist die Durchführung von Sicherheitsanalysen sowie das Testen von Systemen existenzieller Bestandteil in der Absicherung von Fahrzeugen. Auf Basis der Sicherheitsanalysen werden in der GuR die Sicherheitsziele abgeleitet, die für die Tests und die Identifikation von Anforderungen für das funktionale Sicherheitskonzept maßgeblich sind.

Die Identifikation von Systemgefahren, stellt eine eigene Forschungsfrage dar. Es ist möglich Gefahren auf Basis der „Known Knowns“ und „Known Unknowns“ zu identifizieren. Es ist hingegen herausfordernd die „Unknowns Knowns“ und die „Unknowns Unknowns“ methodisch vorherzusehen. [58] [60]

Gefährdungen für automatisierte Fahrzeuge können andererseits nicht ausschließlich aus Daten gefahrener Kilometer konventioneller Fahrzeuge abgeleitet werden. Fehlerhafte Erkennung der Umwelt durch Radarsensoren bei ungünstigen Wetterbedingungen sind bspw. keine Unfallursachen manueller Fahrten. Datenbanken, angepasst auf automatisierte Fahrzeuge zur Identifikation von Gefährdungen haben derzeit noch aufgrund geringer Qualität und Quantität wenig Aussagekraft [61]. Es ist darauf hinzuweisen, dass sich das Pegasus-Projekt ausführlich mit dieser Thematik beschäftigt.

Des Weiteren sind Parameter der Umgebungsmodellierung automatisierter Fahrzeuge und die daraus bestimmte Kritikalität hochgradig unstetig. Algorithmenprozesse resultieren in Endergebnissen, in denen die Grenzwerte bezüglich korrekter bzw. fehlerhafter Entscheidungen aufgrund von Machine-Learning nicht exakt bekannt sind. [58]

Derzeit werden Fahrzeuge hergestellt, die automatisierte Teilaufgaben während der Fahrzeugnutzung übernehmen. Der Fahrer muss auf Basis rechtlicher Rahmenbedingungen jederzeit manövrierfähig sein (Level zwei). Es ergeben sich Risiken durch inkorrektes Eingreifen von Assistenzsystemen (false positive). In hochautomatisierten Fahrzeugen (Level drei bis fünf) fungiert der Fahrer nicht als Rückfallebene. Zusätzlich zu den false positives

können in diesen Systemen fehlende Reaktionen (false negatives) zu Gefährdungen führen. Diese neue Fehlerart muss in der Gefahrenidentifikation berücksichtigt werden. [58]

In den folgenden Kapiteln wird zunächst auf Grundlagen der Zuverlässigkeitstheorien und anschließend auf etablierte Gefahrenanalysen, die FMEA, FTA, PRA (Probabilistische Risikoanalyse), PHA, HAZOP sowie auf die von Leveson entwickelte Methode STPA eingegangen.

5.2. Zuverlässigkeitstheorie und endliche Zuverlässigkeit

Ein technisches System definiert sich aus einer endlichen Menge von Elementen bestimmter Eigenschaften und aus den strukturgebenden Interaktionen und Verbindungen. Unter Zuverlässigkeit wird die Eigenschaft eines Systems verstanden innerhalb einer definierten Zeitdauer [0, t] unter vorgegebenen Rahmenbedingungen die erwartete(n) Funktion(en) zu erfüllen. Eine Kenngröße ist die Überlebenswahrscheinlichkeit K(t)=P(T>t). Die Zuverlässigkeit eines Elementes in einem technischen System ist endlich. Daraus folgt, dass die Zuverlässigkeit bezogen auf das Gesamtsystems, welches aus diesen Elementen besteht, ebenfalls endlich ist. Die Zuverlässigkeitstheorie befasst sich mit der Messung, Vorhersage, Erhaltung und Optimierung der Zuverlässigkeit mit dem theoretischen Fundament technischer Systeme [62]. Die Grundlage der Zuverlässigkeitstheorie ist die Wahrscheinlichkeitstheorie, da Zuverlässigkeit demgemäß etwas Zufälliges ist [62]. Der Ausfallzustand wird sich in Abhängigkeit der Ausfallwahrscheinlichkeit X(t) und der voranschreitenden Zeit einstellen. Die Verteilungsfunktion von K(t) ist streng monoton fallend basierend auf folgenden Randbedingungen: [14] [56]

$$K(t)\begin{cases} K(t=0)=1 \\ K(t\to\infty)=0 \\ X(t)=1-K(t) \end{cases} \qquad \text{(Gl. 1)}$$

Im folgenden Kapitel werden die Gefahrenanalysen basierend auf der Zuverlässigkeitstheorie und dem Brainstorming vorgestellt.

5.3. Etablierte Gefahrenanalysemethoden

In personen-, sach-, sowie aufgaben- und projektbezogenen Bereichen müssen Gefahrenanalysen nach spezifischen Eigenschaften ausgewählt werden, um je nach Industrie und Anwendungsfall unterschiedlichen Anforderungen zu entsprechen. [58]

Etablierte Methoden zur Gefahrenidentifikation und Entwicklung des Sicherheitskonzeptes sind die FTA, FMEA und die HAZOP. Diese Methoden wurden in der Zeit in der analoge Informationsflüsse vorherrschten entwickelt. Die Anwendung dieser Methoden in der hochkomplexen technischen Moderne führt zu unzureichenden Absicherungen. [63]

5.3.1. FMEA

Die Standard-FMEA wurde in den 60-er Jahren erstmals im Apollo-Projekt der NASA eingesetzt und ist eine systematische, halbquantitative Risikoanalysemethode [62] [64]. In der Praxis werden FMEAs in verschiedene Arten unterteilt, die Prozess-FMEA, Software-FMEA, Hardware-FMEA, System-FMEA und Design-FMEA. Ergebnisse der Analyse sind bottom-up generierte Aussagen. Die Methode untersucht präventiv Ursache-Wirkungsprinzipien und bewertet Risiken hinsichtlich ihres Auftretens und der Bedeutung.

In der FMEA wird zunächst das Gesamtsystem in einzelne Komponenten bzw. Teilsysteme aufgeteilt und das Zusammenwirken bzw. die Interaktionen der Elemente untersucht. Ungewollte Ereignisse werden beispielsweise mit Ursachen- und Wirkungsdiagrammen bestimmt. In der FMEA wird die Auftrittswahrscheinlichkeit der identifizierten Gefahren mit einer Risikopräferenzzahl (RPZ) bewertet. Daraus wird die Priorität für Maßnahmen definiert. In Abbildung 10 wird die grobe Vorgehensweise der Analyse vorgestellt. Für eine ausführliche Beschreibung der FMEA wird vollständigkeitshalber auf den IEC Standard [65] verwiesen. [62] [64] [66]

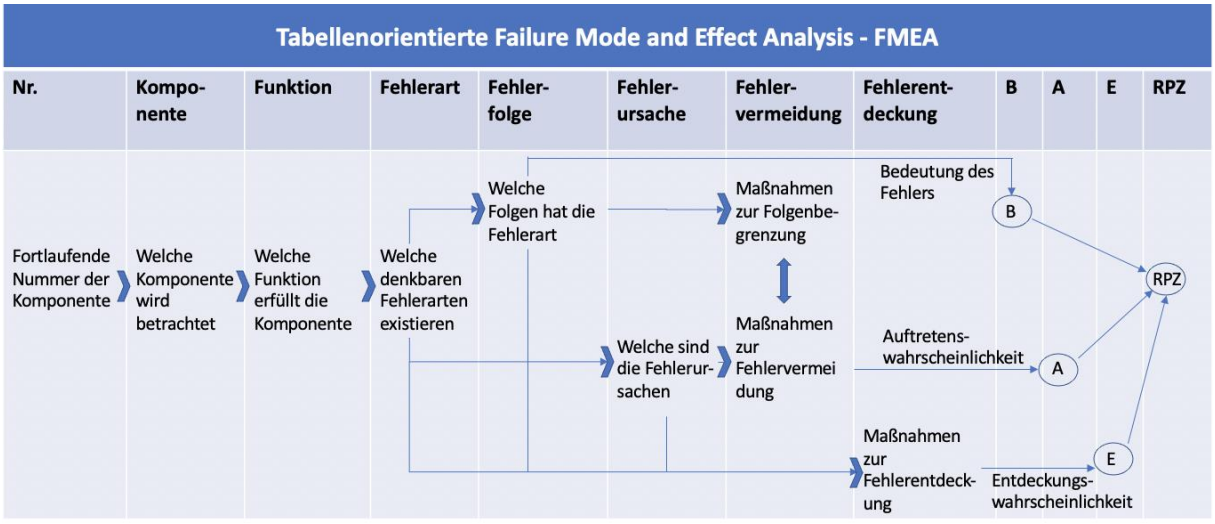

Abbildung 10: Vorgehensweise der Standard-FMEA in Anlehnung an [56]

Voraussetzung zur Durchführung der Analyse ist, dass das System entsprechend entwickelt ist, um es im Zuge der bottom up Analyse in einzelne Elemente aufzuteilen. Die FMEA gibt kein konkretes Analyseabbruchkriterium vor. Es kann somit nicht sichergestellt werden, dass alle Pfade und Kombinationen bestimmt wurden. Ein Vollständigkeitskriterium ist somit nicht gegeben. Mit FMEA wird geprüft, ob bestehende Designs sicher sind, anstelle Designs zu entwickeln die von Beginn an sicher sind. Die FMEA ist Nachweisinstrument und grundsätzlich keine Methode mit Schwerpunkt auf präventiver Gefahrenidentifikation. Erfahrene Analytiker können CCF mit der FMEA eingeschränkt aufdecken. Die Analyse ist zeitaufwendig, da nicht jeder Fehler zu einem Systemausfall bzw. Degradation führen muss. Hauptproblematik der FMEA ist, dass ausschließlich einzelne Fehler bzw. Ursachen untersucht werden können. Die Analyse der Kombination mehrerer Fehler und deren Auswirkungen sind nicht möglich. [1] [67] [68] [69] [70] [71] [72]

5.3.2. FTA

Die FTA ist eine systematische, deduktive Gefahrenanalyse. Das Konzept wurde 1961 von Bell Telephone Laboratories entwickelt. Mit der FTA wird die Wahrscheinlichkeit eines Systemausfalls bestimmt. Die FTA basiert auf dem Konzept der boolschen Algebra. Mit der FTA werden logische Verknüpfungen potenzieller Teilsystemausfälle in potenziell möglichen Pfaden ermittelt. Ausgangsbasis der FTA ist keine Systemkomponente wie in der FMEA, sondern ein Schaden auf oberster Untersuchungsebene.

Im ersten Vorgehensschritt wird das Gesamtsystem beschrieben. Anschließend wird das Fehlerereignis (Top Level Event) mittels logischer Verknüpfung in hierarchieniedrigere Elemente zerteilt. Der Fehlerbaum repräsentiert die Basisergebnisse, die zu dem Ausgangspunkt, dem Top Level Ereignis führen. Die Verknüpfungen lassen sich in Oder-Verknüpfung bzw. Und- Verknüpfung klassifizieren. Nach Erstellung des Fehlerbaums wird jedem Element eine Ereigniswahrscheinlichkeit zugeteilt, auf deren Basis die Gesamtwahrscheinlichkeit des Systemausfalls bestimmt wird. Die spezifische Vorgehensweise der Methode ist ausführlich in [65] beschrieben.

Die Durchführung der Analyse ist stark abhängig von Erfahrungswerten des Durchführenden. Während der Durchführung der FTA werden weniger Ressourcen benötigt im Vergleich zur FMEA. Ein Vollständigkeitskriterium hat die Methode nicht. Die FTA kann hingegen entwicklungsbegleitend durchgeführt werden. Weiterer Vorteil der FTA ist die Vorgabe einer Grundstruktur durch den Fehlerbaum (Minimal Cut Sets). Die zeitliche Abfolge des Auftretens von Ursachen kann in einem beschränkten Umfang berücksichtigt werden, diese Ansätze werden in der Automobilindustrie normalerweise nicht verwendet. Mit der FTA können

hingegen Common Cause Fehler adressiert werden. Die Methode ist nicht ausschließlich zur Gefährdungsidentifikation geeignet, da ein Top Level Event vorgegeben sein muss. [17] [64] [72] [73]

5.3.3. PRA

Mit der PRA wird eine probabilistische Risikobewertung durchgeführt. Die Folgen möglicher Unfälle werden bspw. in Form physikalischer Parameter quantifiziert. Die PRA besteht aus einer Ursache-Konsequenz-Logik, zusammengesetzt aus Fehler- und Ereignisbäumen. Diese sind wiederum zu einem übergeordneten Modell zusammengefügt. Die Ereignisbäume beschreiben eine Erfolg-Misserfolg-Logik. Die Kombination aller Ereignisse und Fehlerbäume resultiert im probabilistischen Modell. Folgen werden durch quantifizierte Wahrscheinlichkeiten charakterisiert. [74]

In Abbildung 11 sind die Vorgehensschritte der PRA dargestellt.

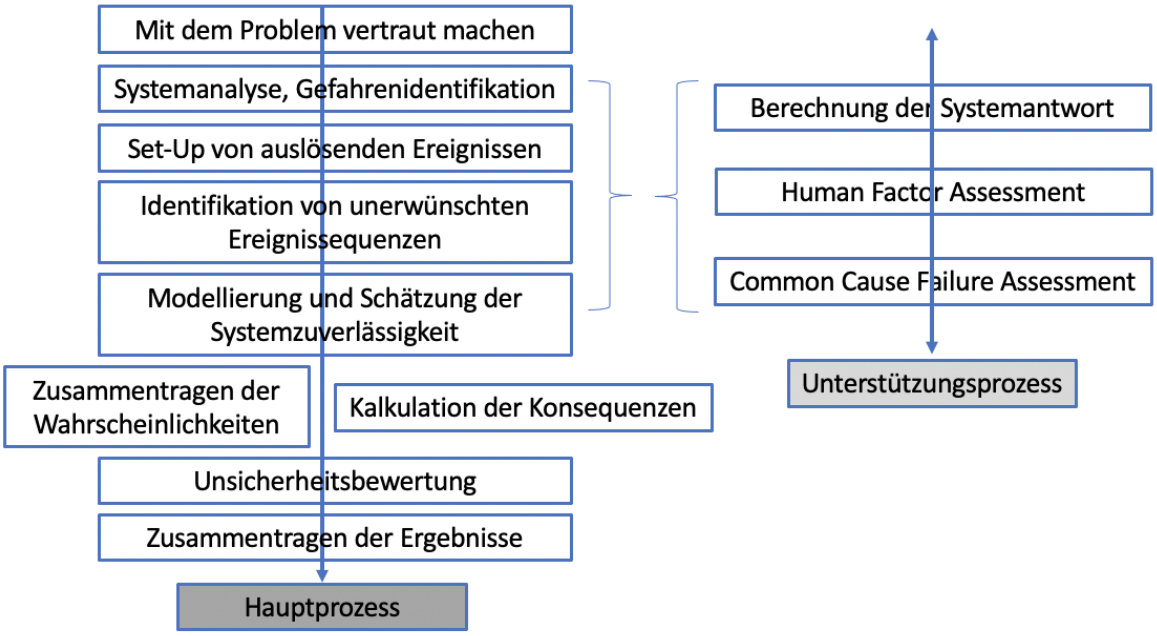

Abbildung 11: Vorgehensschritte der PRA in Anlehnung an [74]

Mit der PRA können folgende drei Fragestellungen beantwortet werden:

- Was können innerhalb des untersuchten Systems für Gefahrenpotentiale auftreten?
- Was sind die Folgen ungewollter Ereignisse?
- Mit welcher Wahrscheinlichkeit kann das Auftreten dieser Folgen bewertet werden?

Vorteil der PRA ist die Möglichkeit einer relativen Risikoaussage des untersuchten Systems. Mit PRA wird innerhalb der Systemgrenze (Modellierungsumfang oder Detaillierungsgrad) die Sicherheit des Systems quantifiziert. Einflussfaktoren außerhalb des Modellierungsumfanges fließen naturgemäß nicht in die Bewertung ein. Die absoluten Werte sind daher fraglich. Maßgeblich für die Aussagekraft ist die Datenqualität, die bei disruptiven Technologien meist nicht existiert. [74] [75]

5.3.4. HAZOP

Die HAZOP wurde in den 1970er Jahren in der chemischen Prozessindustrie entwickelt. Die Gefahrenanalyse wird auf sprachlicher Ebene mit Schwerpunkt der Gefahrenidentifikation durchgeführt. Die HAZOP wird weder den top-down-, noch den bottom-up-Analysen zugeordnet, da sowohl Gefahrenursachen als auch Auswirkungen bestimmt werden können. [74] [76] [58]

Im ersten Schritt wird der zu untersuchende Prozess bzw. das System grob in Funktionseinheiten aufgeteilt. Im nächsten Schritt werden Sollfunktionen definiert. Den Sollfunktionen werden Attribute wie beispielsweise Kraft oder Spannung zugewiesen. Die Auswahl der Leitworte kann durch Listen erfolgen. Diese Attribute werden mit Leitworten verknüpft, wie beispielsweise „kein“, „weniger“ usw. In einem anschließenden Brainstorming werden die Sätze auf Kritikalität hinsichtlich ausgehender Gefahren des Systems untersucht. Im letzten Schritt werden mögliche Ursachen und Folgen analysiert, um daraus Maßnahmen abzuleiten, um die zuvor definierten kritischen Umstände zu minimieren. Voraussetzung für eine gewinnbringende Analyse ist ein interdisziplinär aufgestelltes Untersuchungsteam. Eine besondere Rolle kommt dem Moderator zu, der die Teammitglieder motiviert und in Diskussionen leitet. Zur spezifischen Beschreibung der HAZOP wird vollständigkeitshalber auf [65] verwiesen. [74] [76]

Die HAZOP liefert den Input wie beispielsweise das Top Level Event in der FTA. Diese Methodenkombination ist sinnvoll, da mit der HAZOP keine aufeinanderfolgenden Abweichungen identifiziert werden, sondern ausschließlich ein Schadensereignis bestimmt wird. Die HAZOP kann auf bestehende Systeme bzw. sich in der Entwicklung befindende Systeme angewendet werden. Erfahrungen im Umgang der Methode sind maßgeblich für eine gewinnbringende Auswertung. Nachteile der HAZOP liegen in der Risikobewertung, die mit der Methode nicht quantifizierbar ist. Die Systematik der Analyse bleibt beschränkt und untersucht keine Fehlerkonsequenzen bzw. -ursachen. Die lebhafte Interaktion der Teammitglieder im Brainstormingprozess ist maßgeblicher Faktor für eine erfolgreiche Durchführung. Die HAZOP konzentriert sich stärker auf die Folgen von Abweichungen

bezüglich Prozessparametern, Softwarefunktionen und Softwareverfahren. Hauptanwendungsgebiet der HAZOP sind weniger hochkomplexe Systeme. [77] [72]

5.3.5. PHA

Die PHA ist eine semi-quantitative Gefahrenanalyse, die in frühen Entwicklungszyklen von Systemen eingesetzt wird. Mit den Ergebnissen der PHA können Konzepte verglichen, ein Fokus auf Risikofragen gesetzt und ein Beitrag zur Gefahrenidentifikation geleistet werden. Drüber hinaus dient sie auch als Input für detailliertere kausale Analysen.

In der PHA werden zunächst die Systemgrenzen festgelegt, auf deren Basis die Analyse durchgeführt wird. Anschließend wird ein Team mit Mitgliedern unterschiedlichster Bereiche zusammengestellt. Gefahren werden mittels Brainstorming identifiziert. Checklisten (zum Beispiel aus der EN 1050) können dazu genutzt werden. Des Weiteren können beispielsweise Erfahrungen aus anderen Bereichen abgeleitet werden. Auf der Basis von Daten wie bspw. Unfallstatistiken, Unfalldaten oder Unfallreports können weitere Gefahren abgeleitet werden. Die PHA bedarf folglich keiner systematischen Vorgehensweise. Im letzten Schritt wird die Häufigkeit und Schwere des identifizierten Ereignisses geschätzt. Anschließend wird eine Reihenfolge der identifizierten Gefahren auf Basis der Häufigkeit und Schwere bestimmt. [72] [76]

5.4. Systemtheorie und Kybernetik als Grundlage der STPA

Die Systemtheorie ist eine Herangehensweise zur analytischen Betrachtung der Welt und ist grundlegendes Ordnungsschema allen Seins. Systemtheorie ist ein Wissenschaftsansatz, der versucht, Systeme unterschiedlicher Arten und Klassen mit gleicher theoretischer Basis zu beschreiben, mathematisch zu interpretieren, einzuordnen und in strukturierte Beziehungen zueinander zu setzen. Spezifische Bereiche ähnlicher Zusammenhänge abzugrenzen sowie gleichermaßen das gesamtheitliche Zusammenwirken zu berücksichtigen, nutzte bereits der griechische Philosoph Platon im Höhlengleichnis (427-347 v. d. Z). [78]

Ludwig von Bertalanffy prägte die Systemtheorie als Reaktion auf den Reduktionismus: 1946 formulierte er die ersten Grundbausteine des heutigen Begriffs der allgemeinen Systemtheorie. Bertalanffy versuchte auf Basis des methodischen Holismus Gemeinsamkeiten in physikalischen, biologischen und sozialen Systemen aufzudecken. Grundannahme war, dass reale Systeme mit der Umwelt interagieren und Informationen austauschen. Durch Interkationen verändern sich die Systemeigenschaften. Unerwünschte

Ereignisse sind auf Fehlfunktionen in Regelkreisen zurückzuführen. In Abbildung 12 ist das Prinzip eines Systems nach Bertalanffys Systemtheorie dargestellt. Ein Regelkreis besteht aus den typischen regelungstechnischen Bestandteilen. Ein Zielzustand wird mit dem tatsächlichen Zustand des Prozesses abgeglichen. Differenzen werden durch Eingabe oder/und Ausgabe angeglichen. Dadurch nähert sich der Prozesszustand dem Zielzustand an. [63] [78] [79] [80] [81]

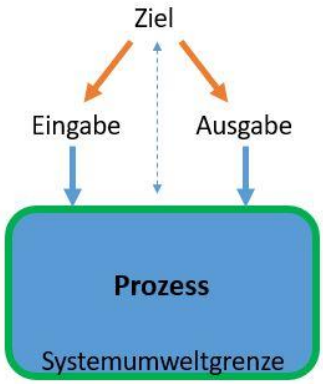

Abbildung 12: Prinzipdarstellung der Funktionsweise eines Systems nach Bertalanffy

Norbert Wiener formulierte ebenfalls eine Theorie für Regelung und Kommunikation. Wiener und Bertalanffy prägen die heutige Systemtheorie maßgeblich. Unter dem Begriff Kybernetik wird heutzutage die Steuerung und Regelung von technischen-, organisatorischen-, und sozialen Prozessen auf Basis mathematischer Systemtheorie zusammengefasst. [78]

Die Systemtheorie steht für eine ganzheitliche Betrachtungsweise, entgegen der Fokussierung auf einzelnen Systembausteinen. Mittels der Systemtheorie konnten Vorgänge in organischen, technischen und soziologischen Systemen zusammengefasst beschrieben werden und folgende Gedankenansätze verfolgt werden:

- Alles Sein ist auf bestimmte Prinzipien bzw. Strukturen zurückzuführen. [78]
- Dem Bewusstsein eines zusammenhängenden Gebildes bzw. Seins, in dem die einzelnen Teildisziplinen nicht isoliert betrachtet werden dürfen. [78]
- Weitere Erkenntnisse systematisch und analytisch zu generieren, mit der Annahme, dass sich das zu Erklärende in das bisher Bekannte einfügen lässt. [78]
- Verschiedene Sektoren interdisziplinär betrachten zu können, damit eine höhere Allgemeingültigkeit erreicht wird, sodass beispielsweise hochspezifische Gültigkeitsbereiche in einzelnen disziplinspezifischen Modellen an Bedeutung verlieren. [78]

Es ist wahrscheinlich, dass es eine von den einzelnen Teildisziplinen unabhängige Theorie geben muss, welche Prinzipien allgemeingültig disziplinübergreifend beschreiben kann. [78]

Gültigkeit der Systemtheorie

Die Allgemeingültigkeit und Vollständigkeit der Systemtheorie ist gegeben, wenn sie vollumfänglich anwendbar ist[18]. Gibt es Entitäten, die dem Prinzip nicht zuordenbar sind, dann ist die Theorie nicht mehr allgemeingültig, folglich auch nicht vollständig, jedoch nicht falsch. Die Theorie ist wiederum für einen bestimmten Bereich formuliert, gilt jedoch nicht bereichsübergreifend, ähnlich wie die Systeme, die wiederum von der betrachteten Theorie zusammengefasst wurden. Um eine allgemeingültige Theorie zu formulieren, ist die Vollständigkeit notwendige Bedingung. Die absolute Vollständigkeit ist in Systemen aus systemischer Argumentation hingegen nicht erreichbar. Der Mathematiker Kurt Göbel konnte in bestimmten Teilgebieten nachweisen, dass Systeme in sich nicht absolut vollständig sind. Der erste und zweite Unvollständigkeitssatz besagt unter anderem, dass Systeme ihre eigene Widerspruchsfreiheit nicht beweisen können und dass Systeme entweder unvollständig oder widersprüchlich sind. Kann die Systemtheorie jedoch alle derzeitigen Systeme beschreiben, dann ist sie die bislang allgemeingültigste Theorie. [78]

5.5. Gefahrenanalysen auf Basis der Systemtheorie

Im Folgenden wird eine auf dem systemtheoretischen Ansatz basierende Gefahrenanalyse vorgestellt. Der Ansatz ist gegensätzlich zu den zufallsbasiert geprägten Methoden, genutzt in der Automobilindustrie. STPA wurde 2004 von Nancy Leveson entwickelt und ist Hauptuntersuchungsgegenstand dieser Arbeit. STPA basiert auf dem Unfallkausalmodell STAMP. STPA und STAMP werden im Folgenden vorgestellt. Zunächst werden Grundlagen erläutert, um anschließend konkret auf die Durchführung der Analyse einzugehen. Für weitere Informationen bezüglich der Durchführung wird auf [14] verwiesen.

5.5.1. STAMP

STAMP ist ein Unfallkausalmodell entwickelt auf Basis der System-, und Kontrolltheorie. STAMP betrachtet Systeme als zusammenhängende Einheiten, die durch Kontrollaktionen und Feedbacks im Gleichgewicht gehalten werden. Daten von übergeordneten Kontrolleinheiten die vom untersuchten System genutzt sowie Daten, die vom System an die Umwelt abgegeben werden, beeinflussen den internen Systemzustand, da Umwelt und das

[18] Die Anwendbarkeit geht über menschlich wahrnehmbare Prozesse hinaus.

untersuchte System in Interaktion stehen. Daten werden an die Umwelt abgegeben, dort verarbeitet und haben wiederrum indirekte Auswirkung auf das untersuchte System. In STAMP wird ein Modell vom System auf funktionaler Ebene erstellt. Die Funktionsweise des Systems wird mittels Regelkreise beschrieben. Die Regelkreise sind hierarchisch miteinander vernetzt. In Abbildung 13 ist ein Beispiel eines Regelkreises nach STAMP abgebildet. [63] [79] [80]

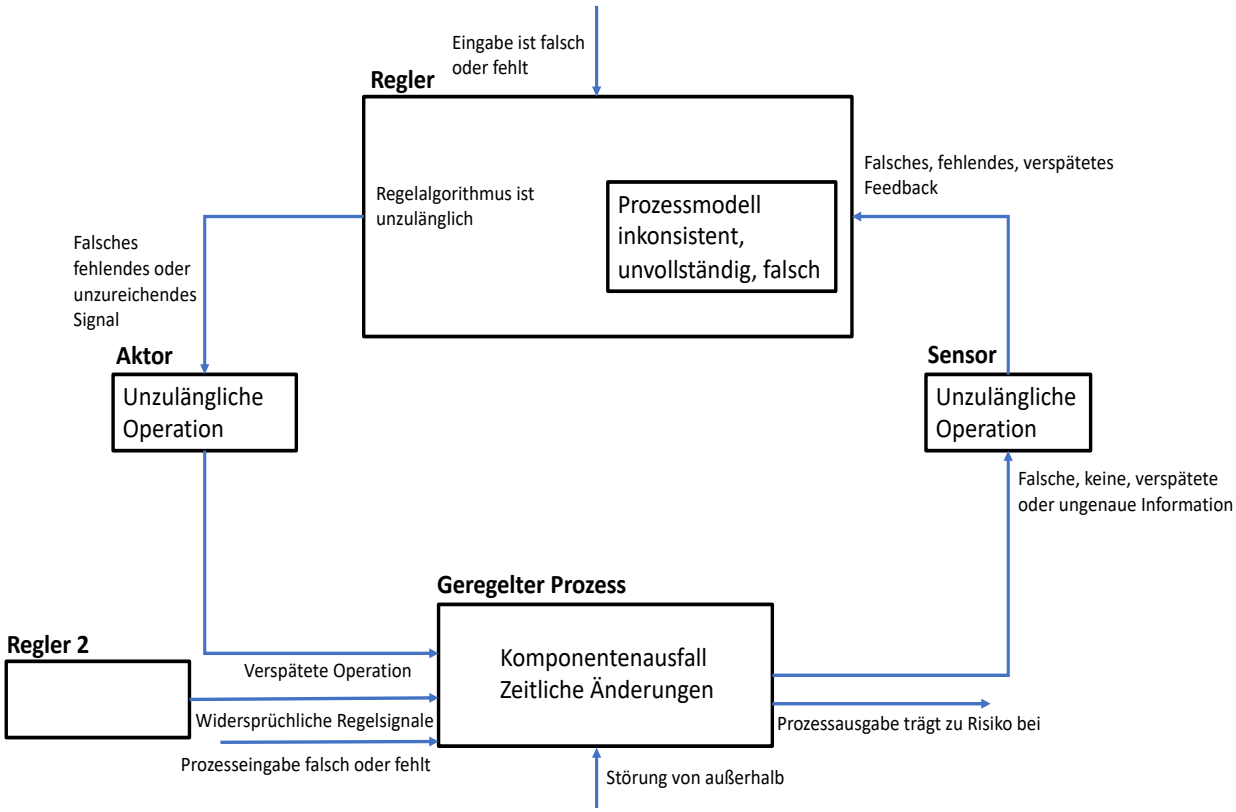

Abbildung 13: Beispiel eines Regelkreises nach STAMP in Anlehnung an [63]

Grundannahme zur Vermeidung von Unfällen in STAMP liegt auf der Identifikation geeigneter Sicherheitsbeschränkungen (SC) im Regelprozess. Ein System ist sicher, wenn adäquate Kontrollmaßnahmen bzw. Restriktionen definiert und erfüllt werden, sodass sich das System jederzeit im sicheren Zustand befindet. Nicht hinreichend sichere Systeme sind nicht ausreichend reguliert. Unsichere Systeme entstehen, wenn Restriktionen nicht vorhanden bzw. adäquat sind, um die unischeren Zustände bzw. Interkationen von menschlichen, organisatorischen und technischen Einheiten zu eliminieren. Tritt ein ungewollter Zustand ein, dann sind folgende Bedingungen erfüllt:

1. Inadäquate Sicherheitsanforderungen (SC) werden formuliert und umgesetzt.
2. Hinreichend adäquate Sicherheitsanforderungen werden an den Empfänger übertragen. Anforderungen werden nicht bzw. nicht adäquat umgesetzt.

Die Ursache für eine nicht hinreichende Regelung kann drei Kategorien zugeordnet werden: Die Art und Weise des Betriebs des Reglers, das Verhalten der Aktuatoren und des geregelten Prozesses sowie die Kommunikation und Koordination zwischen den Reglern. [63]

Durch die systemische Herangehensweise in STAMP können Komponentenausfälle sowie Ursachen wie bspw. fehlender bzw. inadäquater Informationsaustausch, ein inadäquater Systementwurf sowie die Interaktion von Mensch und technischem System untersucht werden. Auf Basis dieser Herangehensweise können potenziell komplexe Systeme in STAMP zusammengefasst werden. [81] [14]

5.5.2. STPA

Konfrontiert mit den Problemstellungen und den daraus resultierenden Herausforderungen hat Leveson 2004 die Gefahrenanalyse STPA entwickelt. Im Folgenden Abschnitt werden zunächst grundlegende Denkmuster der STPA erläutert, um anschließend auf die Vorgehensweise einzugehen und zum Abschluss des Kapitels grundlegende Anforderungen an die Nutzung von Gefahrenanalysen vorzustellen. In den folgenden Kapiteln werden anschließend die Ergebnisse der STPA sowie Vorteile und Nachteile in der Anwendung im Hinblick der Serienentwicklung diskutiert.

Allgemein

STPA ist eine deduktive Gefahrenanalysetechnik auf Basis der Systemtheorie. Ziel sind Systemgefahren, deren Ursachen sowie mögliche Auslöser zu identifizieren. Mit STPA können kausale Zusammenhänge systemübergreifend erfasst werden, was dazu befähigt, Gefahren aufgrund von funktionalen Unzulänglichkeiten, Mode Confusion, Modellierung und der Interpretation der Umgebung zu bestimmen. Etablierte Methoden der Automobilindustrie basieren auf der Zuverlässigkeitstheorie und auf Brainstormingprozessen. STPA unterscheidet sich durch den systemtheoretischen Ansatz fundamental. [1] [14] [63] [82] [18]

Nach Leveson sind unerwünschte Ereignisse Folge eines dynamischen Kontrollproblems. Unfälle ergeben sich laut STPA aufgrund unzureichender Regelung bzw. mangelnder Durchführung von Regelungen im Systemdesign. Nach Leveson besteht das Gesamtsystem aus mehr als der Summe einzelner Komponenten. Eine Minderheit einer Vielzahl von Unfällen in komplexen Systemen sind Komponentenausfälle. Vielmehr ergeben sich Unfälle aufgrund inadäquater Anforderungsspezifikationen. Verhalten sich Komponenten nach vorgesehenem Prinzip, dann sind Unfälle nicht ausgeschlossen. Treten zum Beispiel unerwartete Interaktionen zwischen Komponenten bzw. funktionalen Einheiten auf, die in der Entwicklung

nicht berücksichtigt wurden, dann könnten diese zu unerwünschten Ereignissen führen, obgleich sie den in der Entwicklung definierten Anforderungsspezifikationen genügen. Wird folglich der Fokus auf die Reduzierung der Komponentenausfallquote gelegt, resultiert daraus eine höhere Systemzuverlässigkeit, jedoch nicht zwingend eine Erhöhung der Sicherheit. Mit Erhöhung der Zuverlässigkeit lässt sich die Sicherheit stets nur bis zu einem definierten Level erhöhen, und zwar bis zur Absicherung der „Known Knowns“. Leveson beschreibt die Zuverlässigkeit als Komponenteneigenschaft. Sicherheit im weiteren Sinne ist hingegen eine Systemeigenschaften. Safety and Security sind damit komponentenübergreifende Eigenschaften. In STPA wird analysiert, unter welchen Bedingungen eine Regelung auftritt, die zu Gefährdungen führt. In softwareintensiven Systemen steigen Interaktionen zwischen Komponenten, infolgedessen steigt das Gefahrenpotential, wenn keine adäquaten Gefahrenanalysen eingesetzt werden, die diese Interaktionsfehler adressieren. [14] [18] [63] [82] [18]

Vorgehensweise STPA

In Abbildung 14 ist das Vorgehen der STPA dargestellt. Im ersten Schritt werden Unfälle auf oberen Systemebenen definiert. Auf Basis der Unfälle werden Gefahren und Anforderungen abgeleitet. Danach wird das System funktional aufgegliedert. Es wird eine Kontrollstruktur erstellt. Im nächsten Schritt werden unsichere Kontrollaktionen aus der Kontrollstruktur identifiziert, um anschließend Maßnahmen zur Vermeidung der zuvor identifizierten unsicheren Ereignisse zu formulieren. Die einzelnen Schritte werden im Folgenden detailliert erläutert.

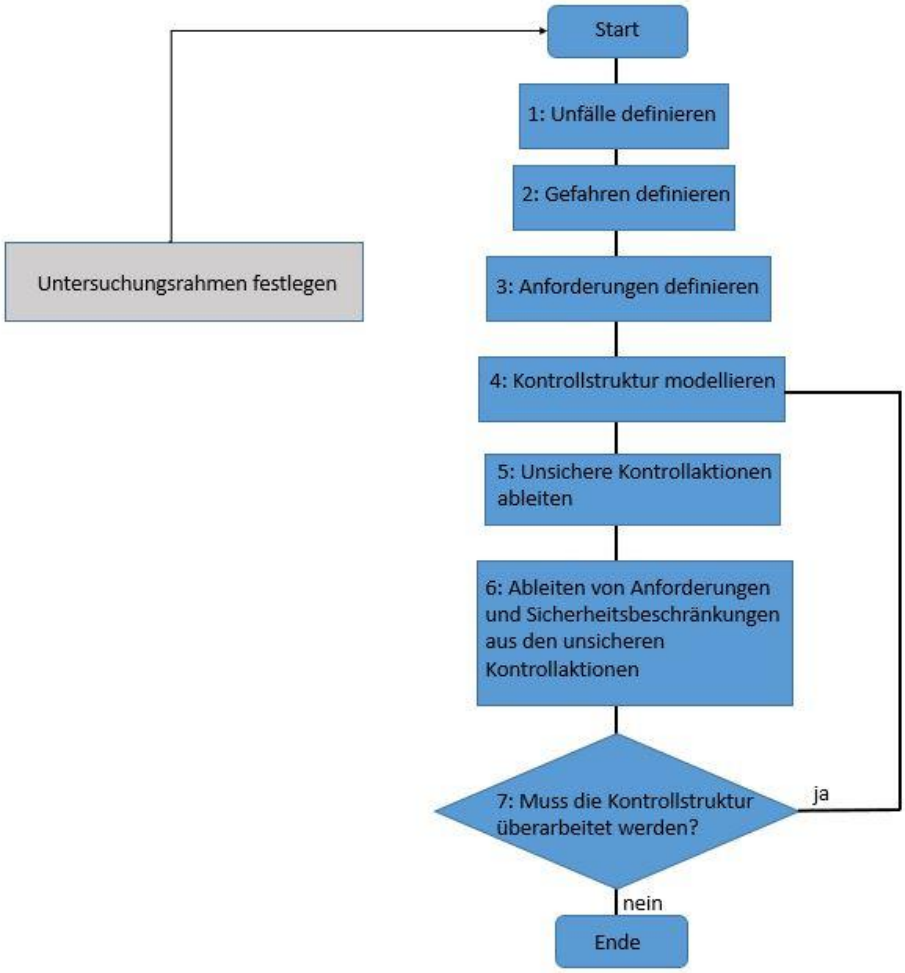

Abbildung 14: Vorgehensweise der STPA

Um die *Unfälle* im ersten Schritt zu formulieren, werden Ziele und Interessen von Interessengruppen wie beispielsweise Anwender, Hersteller oder Käufer in einem Brainstormingprozess definiert. Die Ziele werden negiert, um daraus die *Unfälle* auf obersten Systemebenen abzuleiten. Die Formulierung wird allgemein gehalten, es werden bspw. keine Komponentenausfälle oder menschliches Versagen beschrieben. [14]

Beispiel eines unerwünschten Ereignisses*: Verlust der Mission.*

Im zweiten Schritt werden aus den *Unfällen* hierarchiehohe Systemgefahren abgeleitet. Jede Systemgefahr muss eine Referenzierung zum jeweiligen *Unfall* aufweisen. Eine Eins-zu-Eins-Referenzierung muss nicht erfolgen. Potenziell können mehrere *Gefahren* einen Schaden auslösen. *Gefahren* beschreiben Systemzustände oder Bedingungen, die in Kombination mit spezifischen Umweltbedingungen zu unerwünschten Ereignissen bzw. *Unfällen* führen. Sie sind nicht zwangsläufig Auslöser eines ungewollten Ereignisses. Die Nutzung eines autonomen Fahrzeugs wird beispielsweise nicht als Gefährdung angesehen, da die Nutzung

für das Zielerreichen der Produktion eines automatisierten Fahrzeugs notwendig ist. *Gefahren* werden auf oberen Systemebenen formuliert und dürfen keine spezifischen Zustände wie Komponentenausfall oder menschliches Versagen referenzieren. Je spezifischer die Formulierung, desto höher ist die Wahrscheinlichkeit Gefährdungen zu übersehen. Ist die Gefährdung hingegen zu allgemein definiert, dann sinkt der Mehrwert. [14]

Im Folgenden ein Beispiel für eine *Gefahr: Das Fahrzeug hält den Mindestabstand zu anderen Objekten und/oder Personen während der Fahrt nicht ein.*

Im dritten Schritt werden Anforderungen bzw. Restriktionen formuliert, um das Eintreten der *Gefahren* zu verhindern. Potenziell können mehrere Anforderungen aus einer *Gefahr* abgeleitet werden. Die Sicherheitsanforderung gibt keine spezifische Problemlösung vor. [14]

Im Folgenden ein Beispiel für eine Sicherheitsanforderung: *Das Fahrzeug muss jederzeit einen Mindestabstand zu anderen Objekten und/oder Personen außerhalb des Fahrzeugs einhalten.*

Im vierten Schritt wird auf Basis der Sicherheitsanforderungen eine Kontrollstruktur abgeleitet. Das Modell wird mit STAMP entwickelt[19] und iterativ präzisiert. Es besteht unter anderem aus Kontrollern und zu kontrollierenden Prozessen. In Abbildung 15 ist ein Beispiel für eine Kontrollstruktur aus dem Automobilsektor dargestellt. Eines der zu kontrollierenden Prozesse ist beispielsweise die Plattform des vollautomatisierten Fahrsystems, in der Abbildung blau markiert. Der Kontroller ist die HMI, in der Abbildung orange umrandet, welche wiederrum ein zu kontrollierender Prozess für Regelkreise auf höheren Hierarchieebenen ist. Zwischen den funktionalen Einheiten werden Kontrollaktionen und Feedbacks versendet. Jeder Kontrollaktion folgt ein Feedback. Die Verantwortlichkeiten werden aus dem Portfolio der Sicherheitsanforderungen bestimmt. Eine Kontrollstruktur kann aus mehreren Regelkreisen unterschiedlicher Hierarchieebenen bestehen. Ziel ist eine funktional-, jedoch nicht komponentenbasierte Aufgliederung. [14]

[19] Ausführlich beschrieben in Kapitel 5.5.1.

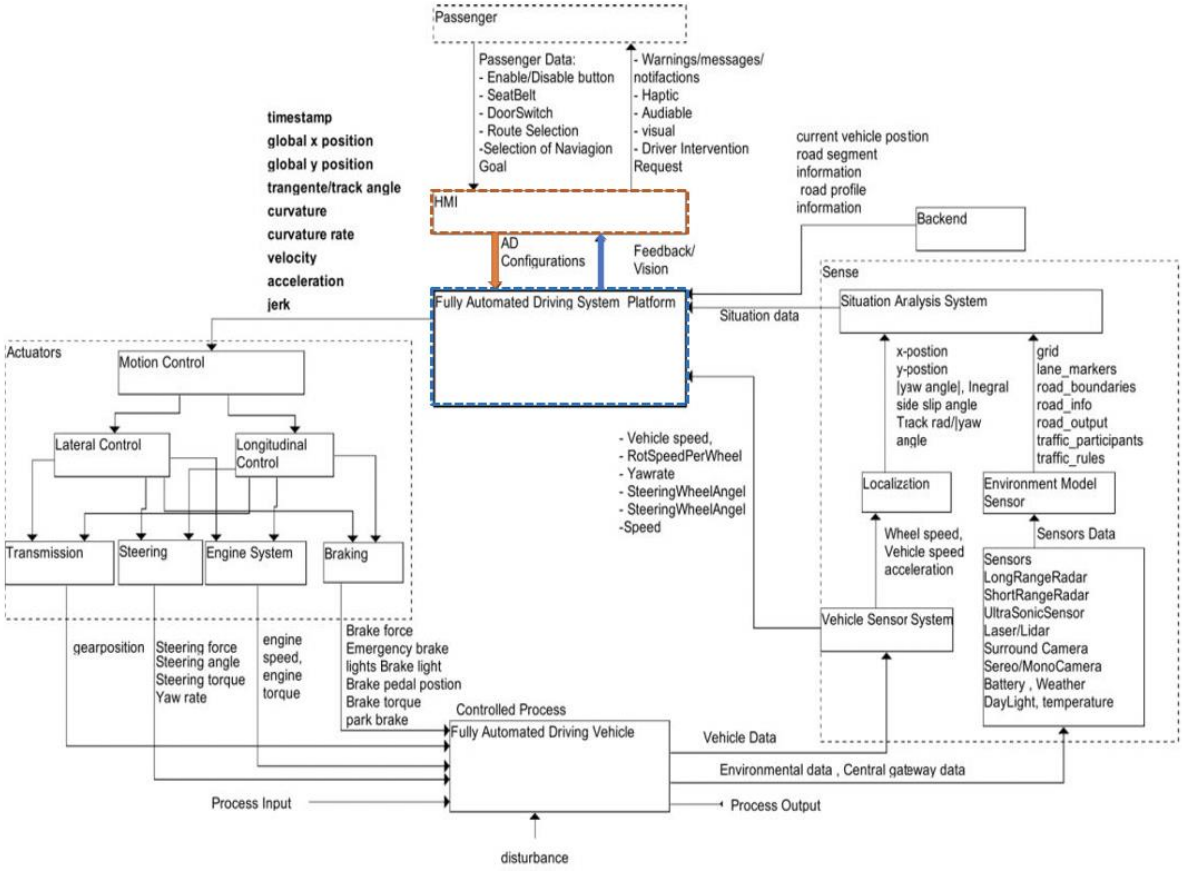

Abbildung 15: Beispiel einer Kontrollstruktur aus dem Automobilsektor in Anlehnung an [16]

Im nächsten Schritt werden unsichere Kontrollaktionen aus der Kontrollstruktur abgeleitet. Unsichere Kontrollaktionen in Verbindung mit spezifischen Umweltbedingungen können zu Schaden führen. Es muss untersucht werden in welchem Maß und Kontext Kontrollaktionen unsicher sind. Unsichere Kontrollaktionen werden mit folgenden Leitsätzen bestimmt:

1. Eine Kontrollaktion wird *nicht bereitgestellt*.
2. Eine inadäquate Kontrollaktion *wird bereitgestellt.*
3. Eine Kontrollaktion wird *zu früh oder zu spät bereitgestellt*.
4. Eine Kontrollaktion wird *zu früh beendet oder zu lange angewendet*.

Die Zusammensetzung der unsicheren Kontrollaktion ist stringent vorgegeben und muss Quelle, Typ, Kontrollaktion und Kontext enthalten. Die Quelle bezeichnet die funktionale Einheit des Regelkreises. Darauf folgt die eigentliche Kontrollaktion, die dem Typ eins bis vier zugeordnet wird (*bereitgestellt, nicht bereitgestellt usw.*). Im letzten Teil des Satzes folgt der Kontext, dem eine entscheidende Bedeutung zukommt. Eine Kontrollaktion ist ausschließlich unter bestimmten Umständen unsicher. Diese Umstände werden im letzten Teil des Satzes näher bestimmt. [14]

Unsichere Kontrollaktion: *Das hochautomatisierte Fahrzeug stellt die Übernahmeanforderung bereit, wenn der Fahrer physisch und oder psychisch nicht in der Lage ist das Fahrzeug hinreichend sicher zu führen.*

Grundsätzlich können vier übergeordnete Kategorien unterteilt werden, die zu unsicheren Zuständen führen, siehe Abbildung 16.

1. Inadäquate Reglerentscheidungen
2. Inadäquate Ausführung der Kontrollaktionen
3. Das Prozessverhalten wird inadäquat geregelt
4. Inadäquates Feedback und weitere Inputs

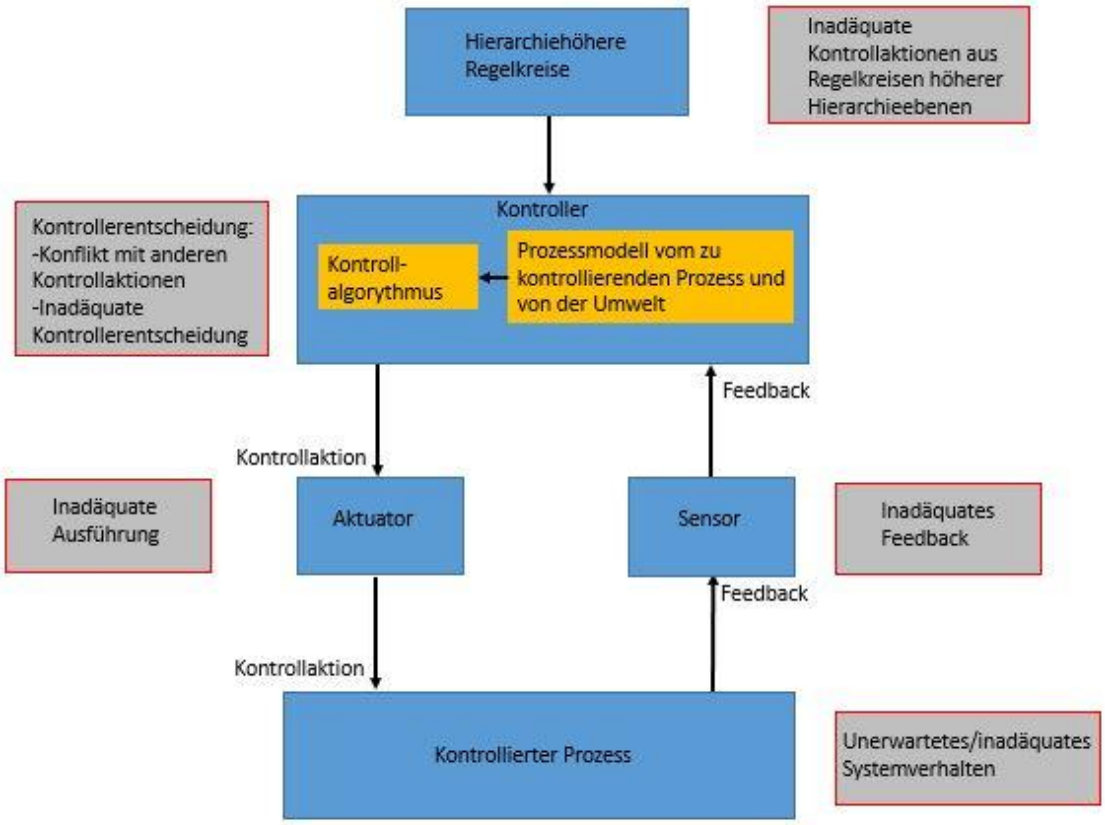

Abbildung 16: Möglichkeiten von Einflüssen die zu unsicherer Zuständen im Regelkreis führen in Anlehnung an [83]

Im letzten Schritt werden aus den unsicheren Kontrollaktionen Anforderungen, Feedback und Kontrollaktionen abgeleitet.

Im Folgenden ein Beispiel für eine modellierte Anforderung im sechsten Schritt: *Es muss sichergestellt werden, dass vor der manuellen Übernahme des Fahrzeugs ein Zeitraum x implementiert wird, in dem sich der Fahrer auf die aktuelle Fahrsituation/Fahrzustand*

einstellen kann, so dass die Verkehrssituation zum Zeitpunkt der Übernahme vollständig erfasst wurde.

Werden unangemessene Regulierungen in der Kontrollstruktur bestimmt, folgt eine Überarbeitung der Kontrollstruktur und die Schritte vier bis sechs werden erneut durchgeführt. [14]

In Abbildung 17 sind die Kausalitäten von unsicheren Ereignissen auf unterschiedlichen Hierarchieebenen aufgezeigt.

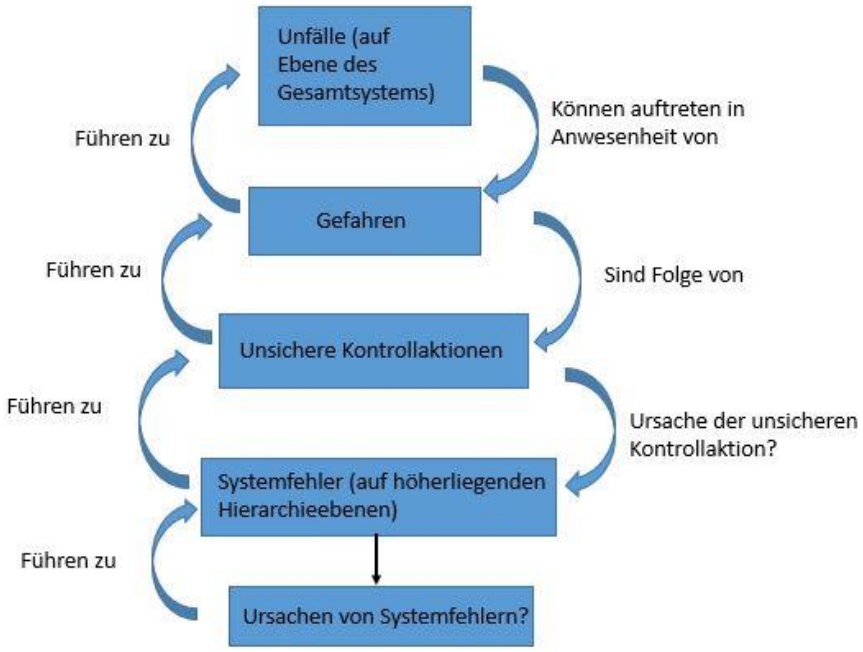

Abbildung 17: STPA Kausalität in Anlehnung an [83]

5.6. Anforderungen an Risikoanalysemethoden in der Automobilindustrie

Um eine Gefahrenanalysemethode effizient anzuwenden, müssen in den personenbezogenen, sachbezogenen, sowie aufgaben- und projektbezogen Bereichen verschiedene Charakteristika der Gefahrenanalysen erfüllt sein. Im Folgenden werden Eigenschaften von Gefahrenanalysen aufgezählt, die in der Entwicklung sicherheitsrelevanter Systeme und speziell in der Serienentwicklung autonomer Fahrzeuge entscheidend sind. Die Anforderungen wurden abgeleitet aus Expertengesprächen und Beobachtungen aus den Entwicklungsprozessen. Die Anforderungen (A) werden diskutiert, um anschließend die PRA, FTA, FMEA, PHA, HAZOP und STPA in den Kontext definierter Anforderungen einzuordnen.

A 1: Ein spezifisches Verständnis des zu untersuchenden Systems sollte keine notwendige Voraussetzung sein, um Methoden gewinnbringend anzuwenden.

Unterliegen Systeme einem ständigen technischen Wandel, bspw. in der Serienproduktion automatisierter Fahrzeuge, ist es ressourceneffizient Methoden anzuwenden, die kein detailliertes technisch-fachliches Verständnis des Systems voraussetzen. Es ist ein Vorteil, wenn nicht ausschließlich technische Systemexperten in der Lage sind die Analyse durchzuführen. Ein Methodenexperte könnte somit unmittelbar in neuentwickelten technologischen Bereichen eingesetzt werden. Diese Eigenschaft fördert kosten- und nutzenoptimale Arbeitsweisen. [14] [84] [85]

A 2: Die Gefahrenanalyse kann in frühen Entwicklungsstadien eingesetzt werden.

Es ist sinnvoll sicherheitsrelevante Entscheidungen parallel zum Entwicklungsprozess zu treffen. Sind sicherheitsbedingte Umstrukturierungen frühzeitig ein Teil der Entwicklung, dann sind kosten- und nutzeneffiziente Prozesse wahrscheinlicher. Werden Analysen erst zum Ende des Entwicklungsprozesses eingesetzt, dann sind Systeme oft unnötig komplex, da sicherheitsbedingte Veränderungen im Design erst nachträglich umgesetzt werden können. Analysemethoden sollten somit in komplexen Systemen frühzeitig anwendbar sein. [14] [82] [86] [87]

A 3: Methoden können Softwarefehler und Kommunikationsinteraktionsfehler identifizieren.

Hardwarefehler sind nicht ausschließlich Ursache von unerwünschten Ereignissen. Unfallursachen, bspw. durch inadäquate Komponenteninteraktion und Softwarefehler, sind Fehlerarten, die mit Nutzung softwareintensiver Systeme und ansteigender Vernetzung an Bedeutung gewinnen werden. Analysen müssen in der Lage sein, eine Vielzahl von Fehlerarten zu identifizieren, um die Gesamtheit der Fehlerursachen zu erfassen. [14] [82] [86] [88]

A 4: Die Methode integriert menschliche Interaktionen.

Aktives Eingreifen eines Menschen während automatisierter Fahrten bietet Gefahrenpotential. Entspricht bspw. die Fahrweise eines automatisierten Fahrzeugs Level vier nicht dem Fahrzeugprozessmodell des Fahrers, greift dieser unnötig in das Geschehen ein. Folglich steigt das Gefahrenpotential abhängig von der Komplexität der Fahrsituation in der sich Fahrer und Fahrzeug befinden. In Gefahrenanalysen, die auf autonome bzw. automatisierte

Fahrzeuge angewendet werden, besteht die Notwendigkeit menschliche Operatoren in die Analyse einzubeziehen. [86] [88] [89]

A 5: Die Methode sollte weitere fahrzeugsystemübergreifende Einflüsse einbeziehen.

Ein technisches System wird unter anderem durch systemübergreifende Institutionen beeinflusst, beispielsweise durch die Gesetzgebung. Fahrzeugübergreifende Einflüsse müssen in Analysen berücksichtigt werden können, um die Gesamtheit potenzieller Fehlerursachen zu identifizieren. Durch die zunehmende Vernetzung des Fahrzeugs nimmt die Bedeutung fahrzeugübergreifender Einflüsse zu. [14] [86] [89] [90]

A 6: Es sollte möglich sein, die identifizierten Fehler hinsichtlich ihrer Kritikalität für das Gesamtsystem zu klassifizieren, um Ressourcen effektiv einsetzen zu können.

Eine Klassifizierung der Fehlerursachen hinsichtlich der Auftretenswahrscheinlichkeit, der Entdeckungswahrscheinlichkeit und den Auswirkungen, erlaubt eine Priorisierung der Maßnahmen zur Bekämpfung der Fehlerursachen. Begrenzte Ressourcen können somit effizient eingesetzt werden. [67] [84] [92]

A 7: Ein Endkriterium in der Methode wird vorgegeben.

Ist ein eindeutiges Abbruchkriterium in der Gefahrenanalyse vorgesehen, steigt die Wahrscheinlichkeit der Vollständigkeit der Analyse. Andernfalls ist nicht eindeutig, ob alle Fehlerursachen identifiziert sind und somit die Gefahrenanalyse beendet werden kann. [14] [18] [67]

A 8: Eine restriktive Vorgehensweise der Analyse sollte gegeben sein.

Je konkreter die Anweisungen der Vorgehensschritte der Gefahrenanalyse, desto praktikabler und vielseitig einsetzbar ist diese. [67]

A 9: Common Cause Fehler sind systematisch identifizierbar.

Um ein hinreichend sicheres System zu entwickeln, müssen Common Cause Fehler untersucht werden. Zwischen Folgefehlern und der Ursache eines Ursprungfehlers muss unterschieden werden können, um unsichere Zustände adäquat zu eliminieren.

Die in Kapitel 5 beschriebenen Gefahren- und Sicherheitsanalysen werden auf Basis diskutierter Anforderungen eingeordnet, siehe Tabelle 1. Grün markierte Felder bilden eine positive, rot markierte Felder eine negative Zuordnung zwischen den Anforderungen und der Methode ab. Orange markierte Felder entsprechen einer indifferenten Zuordnung.

Tabelle 1: Gefahrenanalysen im Vergleich

Anforderung	PRA	FTA	FMEA	STPA	PHA	HAZOP
Die Analyse kann eine nicht technische Ebene des Systems unabhängig von menschlichen Fehlern untersuchen.						
Die Analyse ist in Entwicklungsstadien, in denen Detailfragen auf technischer Basis nicht geklärt sind, einsetzbar.						
Die Analyse kann komplexe Systeme (Softwarefehler, Interaktionen) adäquat untersuchen.						
Die Analyse kann menschliche Interaktionen mit dem technischen System untersuchen.						
Möglichkeit der Gefahrenidentifikation beispielsweise hinsichtlich Fehlerschwere.						
Ein intrinsisches Endkriterium/Abbruchkriterium der Analyse liegt vor.						
Es wird ein restriktiver Rahmen in Bezug auf die Durchführung der Analyse vorgegeben.						
Möglichkeit der systematischen Identifizierung von Common Cause Fehler ist gegeben.						

Die in Tabelle 1 aufgelisteten Methoden haben unterschiedliche Stärken und Schwächen in der Anwendung bzw. Anwendungsfelder, in denen sie effizient eingesetzt werden können. Eine spezifische Analyse wird nicht in der Lage sein, alle sicherheitsrelevanten Fragen eines

Systems vollumfänglich zu lösen. Die Kenntnisse ihrer Vorteile und Nachteile ermöglichen jedoch einen zielgerichteten Einsatz. HAZOP und STPA sind Gefahrenanalysen mit systematischem Hintergrund. Entscheidender Nachteil in der HAZOP ist gegenüber der STPA, dass Systemexperten notwendig sind, um eine gewinnbringende Analyse durchzuführen. Die PRA ist eine effiziente systematische Sicherheitsanalyse, jedoch aufgrund benötigter bzw. fehlender Datenmengen in der Automobilindustrie noch nicht praktikabel. Die FMEA dient als Nachweisinstrument eines hinreichenden Sicherheitskonzeptes. Entscheidender Nachteil in der FMEA und FTA ist der Fokus auf Komponentenfehlern. Weitreichende Interaktionen in komplexen Systemen können nicht hinreichend erfasst werden.

5.7. Zusammenfassung

Eine systematische Vorgehensweise von Risikoanalysen dient der Vervollständigung und Optimierung von Sicherheitskonzepten. Verfahren zur Risikoanalyse[20] können in zwei verschiedene Kategorien unterteilt werden: Einerseits die identifizierenden, qualitativen, deterministischen Methoden und andererseits bewertende, quantitative, probabilistische Methoden. Die Analysen basieren auf zwei grundlegenden Arbeitsweisen, einer induktiven Vorgehensweise bei quantitativen und einer deduktiven Vorgehensweise bei qualitativen Methoden. Darauf aufbauend wird in dieser Arbeit zwischen Gefahrenanalysen und Sicherheitsanalysen unterschieden[21]. STPA, HAZOP und PHA werden den Gefahrenanalysen zugeordnet, da deren Schwerpunkt auf der Gefahrenidentifikation liegt. FMEA, FTA und PRA sind Sicherheitsanalysen in der Modellierung hinreichender Sicherheitskonzepte.

Ergebnisse von Gefahrenanalysen und Sicherheitsanalysen können aufeinander aufbauen bzw. bedingen sich. Der FTA muss beispielsweise ein Top Level Event vorliegen, welches durch eine STPA oder eine HAZOP gestellt werden kann. Die FMEA kann hingegen ein Nachweisinstrument eines Designkonzeptes sein. Es sind folgende Zwischenziele in der Gesamtabsicherung zu unterscheiden: Die Gefahrenidentifikation, die Risikobewertung, die Maßnahmenplanung, der Nachweis des Sicherheitskonzeptes sowie die Erstellung eines adäquaten Sicherheitskonzeptes. Alle Teilgebiete mit einer spezifischen Analyse abzudecken ist mit bisher in der Literatur bekannten Methoden nicht möglich. Es ist fraglich, ob ausgehend von diesen Zielstellungen, Methoden mit entsprechenden Schwerpunkten kombiniert werden können. STPA ist bislang keine etablierte Methode in der Automobilindustrie, obgleich STPA im Vergleich zu anderen Gefahrenanalysen eine spezifische systematische Vorgehensweise zur Gefahrenidentifikation bereitstellt. [93]

[20] Siehe ausführlich Kapitel 5.1 bis 5.5
[21] In der Literatur werden Gefahrenanalysen und Sicherheitsanalysen unterschiedlich definiert.

Es ist fraglich, ob STPA als Gefahrenanalyse den Absicherungsprozess unterstützen kann. Im Folgenden Kapitel wird zunächst ein Literaturreview und anschließend die Durchführung einer STPA auf ein Fahrzeug Level vier und fünf vorgestellt.

6. Literatur Review STPA

Im Folgenden wird ein Überblick über die Anwendung der STPA in unterschiedlichen Themenkomplexen explizit mit Fokus auf die Automobilbranche gegeben. STPA wurde bisher in den Bereichen Automobil, Eisenbahn, Luftfahrt, Raumfahrt, Schifffahrt, Gesundheitswesen, Medizintechnik, Verteidigung, Kernkraft und Infrastruktur durchgeführt.

Die ersten hochautomatisierten bzw. komplex vernetzten Systeme wurden in der Luft- und Raumfahrtindustrie entwickelt. STPA wurde erfolgreich eingesetzt, wie bspw. in [94] auf ATSA-ITP und in [95] auf TCAS II. TCAS II ist ein Kollisionswarnsystem, um Flugzeugkollisionen in der Luft zu vermeiden. ATSA-ITP ist eine Funktion, um die Möglichkeit von Flughöhenveränderungen bereit zu stellen und damit Kraftstoffeinsparungen zu ermöglichen.

In der Automobilindustrie wurde STPA auf Fahrzeugfunktionen wie Adaptive Cruise Control (ACC) in [96], Cruising Chauffeur System («Lane Change») in [97], Spurhalteassistenzsystem [52], Collision Avoidance System [98], Electric Power Steering (EPS) [99] und auf die HMI-Schnittstelle eines automatisierten Fahrzeugs [100] angewendet. Schwerpunkt der Analysen lag auf unterschiedlichen Untersuchungseinheiten im Kontext des Gesamtfahrzeugs. Zusammenfassend werden von den Autoren grundsätzlich positive Erfahrungen hinsichtlich des Einsatzes von STPA postuliert.

In [101] wird das Zusammenspiel von drei unabhängig entwickelten Funktionen, Auto-Hold, Motor Start Stopp, und ACC mit Stopp and Go Funktion mit STPA untersucht. Fokus lag auf der Identifizierung von unischeren Kontrollaktionen in der Interaktion der drei Funktionen. Placke fand heraus, dass speziell die Interaktionen der drei Funktionen mit STPA gewinnbringend analysiert werden konnten.

Hosse hat in [102] STPA auf ein Unfallszenario mit einem Tesla Model S mit aktiviertem Highway Assistent angewendet und Ursachen für den Unfall in Florida 2016 unter anderem auf fahrzeugsystemübergreifenden Ebenen identifiziert. STPA wurde in [103] im Bereich der Cybersecurity mit Fokus auf das autonome Fahrzeug eingesetzt.

In [104] wurde STPA auf ein automatisiertes Fahrzeug angewendet. Schwerpunkt lag auf der Handhabbarkeit der Methode, hingegen nicht auf der Absicherung. Abdulkhaleq hat STPA auf ein vollautonomes Fahrzeug angewendet [105] und die Betriebssicherheit der autonomen Fahrzeugarchitektur auf höherliegenden Hierarchieebene analysiert. Die Kontrollstrukturen des autonomen Fahrzeugs der vorliegenden Dissertation und Abdulkhaleqs unterscheiden sich aufgrund unterschiedlicher Schwerpunktsetzung. Ebenfalls werden in der vorliegenden Arbeit die Gesamtheit der Anforderungsspezifikationen explizit vorgestellt. Alvarez hat STPA im Kontext eines automatisierten Fahrzeugs in [18] angewendet. Fokus waren

fahrzeugsystemübergreifende Organisationseinheiten in Interaktion mit dem automatisierten Fahrzeug.

Im Mittelpunkt der vorliegenden Dissertation steht nicht ausschließlich die Praktikabilität der Analyse, sondern die Identifikation von Anforderungsspezifikationen für ein Fahrzeug Level vier und fünf, mit dem Ziel, Gefährdungen zu identifizieren, die mit etablierten Methoden der Automobilindustrie noch nicht bzw. nur mit unverhältnismäßigem Aufwand bestimmt werden können.

7. Ergebnisse der STPA

STPA wird auf ein Fahrzeug Level vier und fünf angewendet. Es werden zunächst die Rahmenbedingungen vorgestellt, auf Basis derer die Analyse durchgeführt wird. Anschließend werden die Teilergebnisse erläutert. Um die Analyse in den Kontext der Risikoanalysen der Automobilindustrie einzuordnen, wird im nächsten Schritt der Zeitbedarf für die Durchführung der Analyse vorgestellt. Im Anschluss dieses Kapitels erfolgt eine Zusammenfassung bezüglich einer möglichen Anwendung in der Automobilindustrie.

7.1. Prämissen und Rahmenbedingungen

Im folgenden Abschnitt werden die Prämissen und Grundlagen zur Durchführung der STPA vorgestellt. Die STPA wurde nach den Richtlinien relevanter Literatur durchgeführt. Es wurde eine Einarbeitungsphase eingeplant, um die Validität der Vorgehensweise sicher zu stellen. Die Ergebnisse sind ausschließlich Resultate der Anwendung der STPA und wurden ohne Informationen spezifischer Problemstellungen und Lösungsansätze aus der Automobilindustrie erstellt. Aus diesem Grund wurde die Analyse organisatorisch von allen konkreten Entwicklungszyklen der BMW Group getrennt durchgeführt. Während der STPA wurden regelmäßig Feedbackgespräche mit Methodenexperten sowohl von akademischer-, als auch von Unternehmensseite durchgeführt.

Im Rahmen dieser Arbeit wurde das Fahrzeug Level vier bzw. Level fünf auf denen in Abbildung C.1 und Abbildung C.2 abgebildeten Hierarchielevel untersucht. Zunächst wurde der Abstraktionsgrad der Analyse festgelegt. Untersuchungsgegenstand der Arbeit war das technische System mit besonderem Fokus auf Interaktionen mit der HMI und der Umwelt. Um Gefahrenpotentiale in diesen Schnittstellen sowie auf technischer Ebene adressieren zu können, wurden die folgenden Abstraktionsgrade gewählt. Die STPA sollte auf einem Hierarchielevel so grob wie möglich und so spezifisch wie nötig angewendet werden. Ist die Kontrollstruktur zu detailliert, könnten Gefahrenpotentiale aufgrund eines enger vorgegeben Rahmens in der Kontrollstruktur nicht identifiziert werden. Ist die Kontrollstruktur hingegen zu grob formuliert, dann sind Ergebnisse nicht aussagefähig. Es gilt somit einen optimalen Trade off zu definieren.

In der Automobilindustrie gilt auf Basis der ISO 26262:2018 [5] Band zehn die Vorgabe, das technische System bis zum ersten Unfallszenario zu untersuchen. In der Luftfahrt hingegen muss über das erste Szenario hinaus analysiert werden, siehe die Richtlinien ARP4761 und ARP4754 [53]. In dieser STPA werden, abhängig vom Erkenntnisgewinn, unsichere Kontrollaktionen bis zum zweiten Unfallszenario untersucht.

Hauptaugenmerk liegt auf dem technischen System, der Interaktion mit hierarchiehöheren Organisationseinheiten sowie der Mensch Maschine Interaktion. Gefahrenpotentiale innerhalb von Organisationsstrukturen werden nicht untersucht.

Weiterhin wird festgelegt, dass keine Fahreranforderungen modelliert werden. Es ist nicht sinnvoll diese in der STPA zu formulieren, da die Umsetzung der Anforderungen von Fahrern nicht hinreichend garantiert werden kann. Es ist sinnvoller Gefahrenpotentiale ausgehend vom Fahrer durch regulative beziehungsweise technische Anforderungen einzugrenzen.

Während der Analyse ergeben sich Anforderungsspezifikationen, welche gegensätzlicher Maßnahmen bedürfen: So ergab sich die Frage, ob ein hochautomatisiertes Fahrzeug Level vier jederzeit vom Fahrer manuell überstimmbar sein sollte. Mode Confusion und ein daraus resultierendes inadäquates Eingreifen in die Fahrzeuglängs- und querführung könnte im Vergleich zu einem inadäquat agierenden Fahrzeug ebenfalls zu Unfällen führen. In der STPA wurden weitere Anforderungen modelliert, die den derzeitigen gesetzlichen Bestimmungen entgegen sprachen. So wird bspw. auf Basis der identifizierten Anforderungen durch STPA abgeleitet, dass das Fahrzeug nicht jederzeit vom Fahrer überstimmbar sein darf.

Weiter hatte der Durchführende im Bereich der Gefahren- und Sicherheitsanalysen keine Erfahrungen. Dadurch konnte die Analyse ohne Einfluss von Prozessmodellen anderer Gefahrenanalysen durchgeführt werden.

7.2. STPA Ergebnisse Fahrzeug Level vier und Level fünf

Im folgenden Unterkapitel werden die Ergebnisse gemäß der jeweiligen Vorgehensschritte der STPA für ein Fahrzeug Level vier und fünf vorgestellt. Die vollständigen Ergebnisse der STPA sowie die Kontrollstruktur sind im Anhang A hinterlegt. Im ersten Teil des Anhangs A werden die Systemunfälle, die Gefahren und die daraus abgeleiteten Anforderungen dargelegt. Im zweiten Teil werden die Kontrollstrukturen für ein Fahrzeug Level vier und fünf vorgestellt, um anschließend auf das Teilergebnis der Anforderungsspezifikationen der Automatisierungsstufen einzugehen. Teilweise sind unsichere Kontrollaktionen während der Untersuchung eines Regelkreises bestimmt worden, die nicht in den Kontext dieses spezifischen Regelkreises einzuordnen waren, durch bestimmte Verbindungswörter des untersuchten Regelkreises jedoch bestimmt werden konnten. Diese Kontrollaktionen sind daher in den Ergebnissen der untersuchten Regelkreise, in denen sie identifiziert wurden, aufgeführt, jedoch nicht in den regelkreisspezifischen Tabellen. Weiter wurden den Ergebnissen Notizen, die während der Bearbeitung zu den jeweiligen Anforderungen erstellt wurden, der Ergebnisliste hinzugefügt.

7.3. Anforderungen im Vergleich

In Tabelle 2 sind die Regelkreise, aus denen Anforderungen für ein Fahrzeug Level vier und fünf extrahiert wurden, in Kategorien a bis f eingeordnet. Es wurden Regelkreise einer Kategorie zugeordnet, die sich auf ähnlichen Hierarchieebenen befinden. Die Regelkreise der übergeordneten Institutionen unabhängig vom technischen System wurden einer Kategorie zugeordnet, da das Hauptaugenmerk dieser Arbeit auf Interaktionen mit dem Fahrzeug liegt.

Tabelle 2: Clusterung der Regelkreise

Kat.	Regelkreise Fahrzeug Level vier	Regelkreise Fahrzeug Level fünf
a	Legislative-Hersteller; Legislative-Ausführende Behörde; Ausführende Behörde-Fahrer; Hersteller-Fahrer; Hersteller-Steuerungs- und Regelungssysteme; Hersteller-Ausführende Behörde; Ausführende Behörde-Umwelt	Ausführende Behörde-Passagier; Hersteller-Passagier; Legislative-Hersteller, Legislative-Ausführende Behörde; Hersteller-Steuerungs- und Regelungssysteme; Hersteller-Ausführende Behörde; Ausführende Behörde-Umwelt
b	Fahrer-HMI; Fahrer-Physikalischer Fahrzeugzustand	Passagier-HMI; Teleoperator-HMI Teleoperator
c	Steuerungs- und Regelungssysteme-HMI	Steuerungs- und Regelungssysteme-HMI; HMI Teleoperator-Sensorische Schnittstelle
d	Physikalischer Fahrzeugzustand-Steuerungs- und Regelungssysteme-Fahrzeugsensoren	Physikalischer Fahrzeugzustand-Steuerungs- und Regelungssysteme-Fahrzeugsensoren
e	Sensorische Schnittstelle-Steuerungs- und Regelungssysteme; Umwelt-Physikalischer Fahrzeugzustand; Umwelt-Fahrer; Umwelt-Fahrzeugsensoren-Steuerungs- und Regelungssysteme	Sensorische Schnittstelle-Steuerungs- und Regelungssysteme; Umwelt-Physikalischer Fahrzeugzustand; Umwelt-Passagier; Umwelt-Fahrzeugsensoren-Steuerungs- und Regelungssysteme
f	Allgemeingültige Anforderungen an Feedbacks und Kontrollaktionen unabhängig vom jeweiligen Regelkreis und der Automatisierungsebene	

Abbildung 18 zeigt alle Anforderungen quantitativ, identifiziert durch STPA für ein Fahrzeug Level vier und fünf. Die Anzahl identischer Anforderungen an ein Fahrzeug Level vier und Level fünf sind im Balkendiagramm blau dargestellt und werden daher für beide Automatisierungsstufen einmalig gezählt. Die Anzahl der Anforderungen, die ausschließlich für Level vier und nicht für das Fahrzeug Level fünf gelten, sind im grünen Balken hinterlegt. Anforderungen, die ausschließlich für das vollautonome Fahrzeug gelten, sind gelb markiert. Diese Systematik wurde für die Anforderungen, die aus den Regelkreisen, eingeordnet in Kategorien der Tabelle 2, identifiziert wurden, durchgeführt.

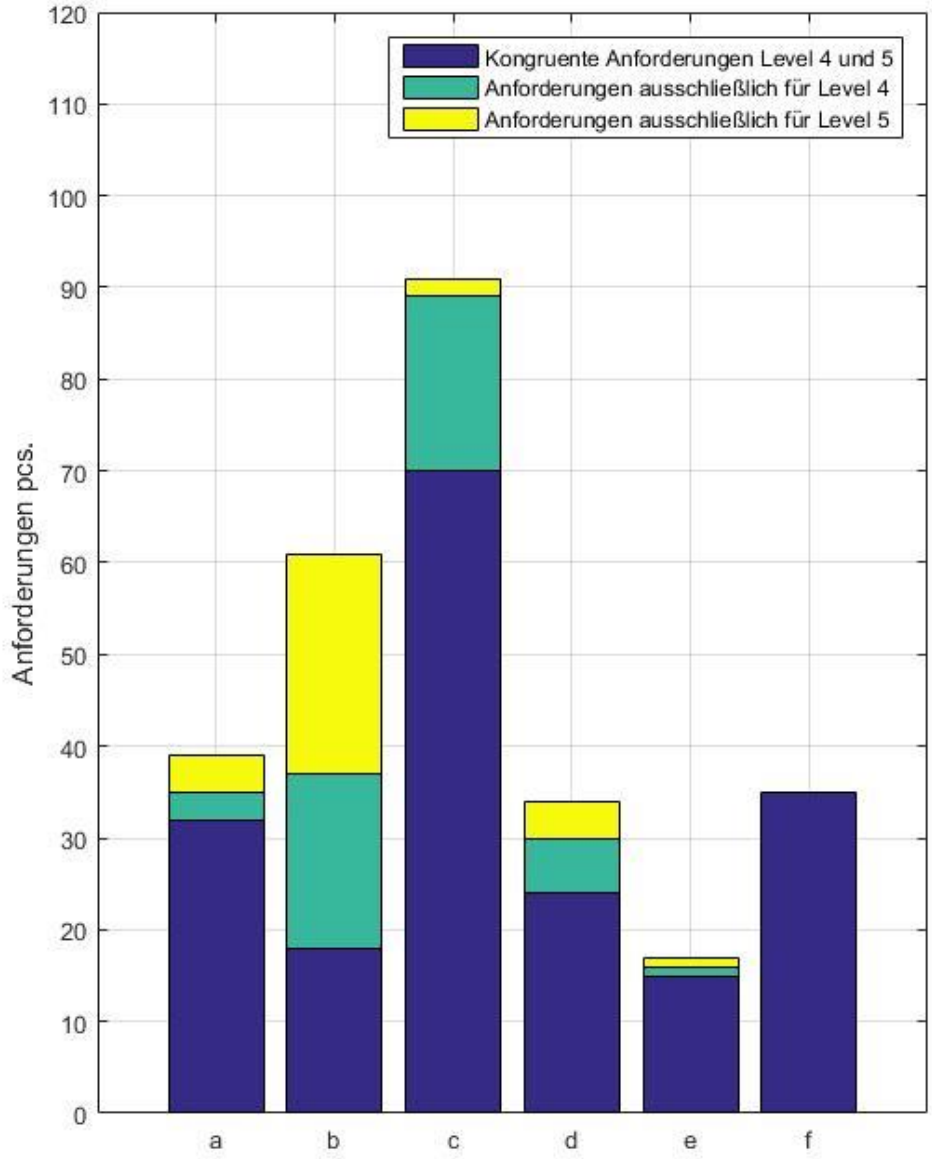

Abbildung 18: Vergleich Anforderungen quantitativ Level vier und fünf

Da das hochautomatisierte Fahrzeug Level fünf keine direkte Interaktion zwischen Fahrzeug und Insassen hinsichtlich der Fahrzeugsteuerung vorsieht, entfallen die Schnittstellenprobleme bei der Übergabe der Verantwortung sowohl nominell als auch im Fehlerfall. Das vereinfacht die Regelkreise und Anforderungen entfallen. Neue Regelkreise hingegen kommen ausschließlich für die Teleoperation hinzu, nicht aber auf anderen Hierarchieebenen, denn das vollautomatisierte Fahren ist bereits in Stufe vier vollständig als Nutzfunktion definiert. Mit STPA lässt sich diese Betrachtung systematisch durch die Anzahl der Anforderungen an die jeweilige Automatisierungsebene in den modellierten Regelkreisen manifestieren.

7.4. Einzelne Anforderungen spezifisch diskutiert

Die Anforderungen aus der STPA sind keine im technischen Sinne ausformulierten Anforderungen, sondern anforderungsartige Formulierungen. Nach STPA müssen diese Anforderungen erfüllt werden, damit das Fahrzeug hinreichend sicher agiert. Als Ergebnis der Analyse konnten Anforderungen formuliert werden, deren Umsetzung im Kontext derzeitiger regulativer Gegebenheiten und technischer Möglichkeiten unklar ist. Diese mit STPA identifizierten Anforderungen werden in diesem Kapitel aufgrund ihrer Bedeutung für die Entwicklung automatisierter Fahrzeuge noch einmal explizit vorgestellt und diskutiert. Die Gesamtheit der Anforderungen sind im Anhang hinterlegt. Weiter wird beschrieben, aus welchen Regelkreisen und unsicheren Kontrollaktionen diese Anforderungen abgeleitet werden konnten.

R 1: Es muss sichergestellt werden, dass das hochautomatisierte Fahrzeug Level vier im automatisierten Betriebsmodus innerhalb von x m an einer Unfallstelle entfernt in adäquater Art und Weise in den Stillstand verzögert hat, wenn Personen an der Unfallstelle in Not sind.

Regelkreis:

1. Steuerungs- und Regelungssysteme-Umwelt-Fahrzeugsensoren
2. Steuerungs- und Regelungssysteme-Fahrzeugsensoren-physikalischer Fahrzeugzustand

UCA:

-Das hochautomatisierte Fahrzeug Level vier stellt die Abnahme der Fahrparameter im automatisierten Fahrmodus nicht, bzw. zu spät, bzw. zu früh bereit, wenn Menschen außerhalb des Fahrzeugs in Not sind.

-Das hochautomatisierte Fahrzeug Level vier stoppt die Abnahme der Fahrparameter im automatisierten Fahrmodus zu früh bzw. zu spät, wenn Menschen außerhalb des Fahrzeugs in Not sind.

Fraglich ist, wenn innerhalb von x m nicht automatisiert hinreichend sicher gehalten werden kann bspw. auf der Autobahn/Baustelle. Abhängig von den Umgebungsbedingungen könnte ein sicherer Halt erst möglich sein, wenn aufgrund der Distanz zur Person in Not keine adäquate Hilfe mehr geleistet werden kann.

Sollte ein Fahrzeug innerhalb von x m hinreichend sicher parken/halten können, beispielsweise an einer Bushaltestelle, müsste ein automatisiertes Fahrzeug in Abhängigkeit der Situation in der Lage sein, Verkehrsregeln zu überstimmen. Die technische Umsetzung dieser Anforderung ist zu diskutieren.

Fraglich ist, wie das automatisierte Fahrzeug detektieren bzw. einschätzen soll, ob am Unfallort helfende Personen vor Ort sind. Nicht jedes vorbeifahrende Fahrzeug sollte am Unfallort halten.

Wie sollen die Steuerungs- und Regelungssysteme zwischen einer Person in Not im Vergleich zu keiner hilfsbedürftigen Person adäquat differenzieren.

Sollte das automatisierte Fahrzeug Personen in Not erkennen können, muss detektiert werden, ob sich im eigenen Fahrzeug Menschen befinden, die körperlich in der Lage sind Hilfe zu leisten.

R 2: Das hochautomatisierte Fahrzeug Level vier muss Objekte zwischen überfahrbaren und nichtüberfahrbar unterscheiden können.

Regelkreis:

1. Physikalischer Fahrzeugzustand-Fahrzeugsensorik-Steuerungs- und Regelungssysteme
2. Steuerungs- und Regelungssysteme-Fahrzeugsensorik-Umwelt

UCA:

-Die Fahrzeugsensorik stellt den Steuerungs- und Regelungssystemen des automatisierten Fahrzeugs bei einer Fahrzeuggeschwindigkeit >0km/h inadäquate Feedbackinformationen der Umgebungsbedingungen zur Verfügung.

-Die Steuerungs- und Regelungssysteme des automatisierten Fahrzeugs stellen eine Veränderung der Fahrparameter bereit, wenn Objekte im Propagationspfad des Fahrzeugs detektiert werden, mit denen in Kontakt getreten werden darf.

-Die Steuerungs- und Regelungssysteme des automatisierten Fahrzeugs stellen eine Veränderung der Fahrparameter nicht bereit, wenn Objekte im Propagationspfad des Fahrzeugs detektiert werden, mit denen nicht in Kontakt getreten werden darf.

Wie sollen Gegenstände im Propagationspfad in Bezug auf eine hinreichend sichere Überfahrt korrekt eingeordnet werden. Das Gefährdungspotential einer Vollbremsung, ausgelöst durch eine Plastikplane im Propagationspfad, ist potenziell höher, als diese zu überfahren. Es sollte hingegen vermieden werden über nicht überfahrbare Objekte, bspw. Ziegelsteine, zu fahren.

R 3: Es muss sichergestellt werden, dass das hochautomatisierte Fahrzeug Level vier nach Kontakt mit einem nicht überfahrbaren Objekt und/oder Person innerhalb von x m hinreichend sicher in den Stillstand verzögert.

Regelkreis:

1. Steuerungs- und Regelungssysteme-Physikalischer Fahrzeugzustand-Fahrzeugsensorik
2. Steuerungs-und Regelungssysteme-Fahrzeugsensorik-Umwelt

UCA:

-Die Steuerungs- und Regelungssysteme stellen die Abnahme der Fahrparameter im automatisierten Fahrmodus zu spät bereit, wenn nicht überfahrbare Objekte bzw. Personen überfahren werden.

Ist das Fahrzeug aufgrund einer Kollision dermaßen beschädigt, dass eine hinreichend sichere Fahrt nicht gewährleistet werden kann, dann wird ein MRM eingeleitet. Problematisch sind Kollisionen mit Objekten/Personen, welche das Fahrzeug marginal beschädigen. Ein Beispielszenario ist ein Fußgänger, welcher gegen ein Fahrzeug prallt. Die Krafteinwirkung auf die Außenhaut des Fahrzeugs ist verhältnismäßig gering. Fußgänger könnten durch diesen Aufprall schwer verletzt sein. Es ist zunächst zu diskutieren wie diese Kräfte am Fahrzeug sicher detektiert werden können. Falls der Kontakt zukünftig detektiert werden kann, ist fraglich, ob bei jedem Kontakt mit einem Objekt ein Notfallszenario eingeleitet werden sollte. Äste könnten während der Fahrt auf ein Fahrzeug hinabfallen, woraufhin fälschlicherweise Notfallszenarien eingeleitet werden.

R 4: Es muss sichergestellt werden, dass autorisierte Sicherheitskräfte (bspw. Polizei, Feuerwehr, Rettungsdienst) die hochautomatisierten Fahrzeuge Level vier bezüglich der Längs-, und Querregelung anweisen können.

Regelkreis:

1. Sensorische Schnittstelle-Steuerungs- und Regelungssysteme

2. Fahrzeugsensoren-Steuerungs- und Regelungssysteme-physikalischer Fahrzeugzustand

UCA:

-Die sensorische Schnittstelle stellt den Zugriff auf die Steuerungs- und Regelungssysteme des hochautomatisierten Fahrzeugs nicht bereit, wenn Personen außerhalb des hochautomatisierten Fahrzeugs in Not sind und die Steuerungs- und Regelungssysteme keine Veränderung der Fahrparameter vorsehen.

-Die Steuerungs- und Regelungssysteme stellen eine Veränderung der Fahrparameter bereit, wenn nicht autorisierte Personen Zugriff auf die Steuerungs- und Regelungssysteme haben wollen.

Das hochautomatisierte Fahrzeug sollte Sicherheitskräfte, im Vergleich zu Personen, die diesen ähnlich sehen und nicht autorisiert sind, unterscheiden können. Nicht autorisierte Personen sollten nicht in der Lage sein das Fahrzeug anzuweisen.

R 5: Es muss sichergestellt werden, dass das hochautomatisierte Fahrzeug Level vier mit Personen außerhalb des Fahrzeugs, im Propagationspfad des Fahrzeugs von x m, kommunizieren kann.

Regelkreis:

1. Steuerungs- und Regelungssysteme-Umwelt-Fahrzeugsensorik

Auf Basis der STPA müssen in den Regelkreisen Kontrollaktionen und Feedbacks definiert werden. Die Umwelt übergibt der Fahrzeugsensorik Informationen. Die Steuerungs- und Regelungssysteme müssen hingegen ebenfalls Feedback an die Umwelt übergeben, damit der Regelkreis vollständig ist.

Es muss sichergestellt werden, dass das automatisierte Fahrzeug Feedback an Personen außerhalb des Fahrzeugs übermitteln kann, bspw. an einem Zebrastreifenübergang. Fraglich ist derzeit die technische Umsetzung und Reglementierung dieser Anforderung.

R 6: Es muss sichergestellt werden, dass die Zunahme/Abnahme der Fahrparameter eines hochautomatisierten Fahrzeugs Level vier durchgeführt wird, bevor das Fahrzeug aufgrund von inadäquat prädizierten Umweltbedingungen im Propagationspfad des Fahrzeugs bzw. Fahrzeugparametern in einen instabilen Fahrzustand gelangt.

Regelkreis:

1. Steuerungs- und Regelungssysteme-Umwelt-Fahrzeugsensorik

2. Steuerungs- und Regelungssysteme- physikalischer Fahrzeugzustand- Fahrzeugsensorik

UCA:

-Die Zunahme/Abnahme der Fahrparameter, vorgegeben von den Steuerungs- und Regelungssystemen des automatisierten Fahrzeugs, wird zu spät bereitgestellt, wenn das Fahrzeug sich aufgrund von Umweltbedingungen in einem instabilen Fahrzustand befindet.

-Die Fahrzeugsensorik stellt den Steuerungs- und Regelungssystemen die physikalischen Fahrzeugparameter für eine hinreichend sichere Fahrt nicht bzw. zu spät bereit, wenn Umgebungsbedingungen diese erfordern.

-Die Steuerungs- und Regelungssysteme stellen eine Zunahme der Fahrparameter bereit, während das Fahrzeug manövrierunfähig ist.

Fraglich ist die technische Umsetzung frühzeitiger Prädizierung von Umweltbedingungen und deren Auswirkungen auf den Propagationspfad des Fahrzeugs.

Es muss sichergestellt werden, dass im automatisierten Fahrmodus die Fahrmanöver ausgehend vom aktuellen, physikalischen Fahrzeugzustand berechnet werden. Die Vorausschau bzw. Messungen von verschleißenden Fahrzeugteilen, bspw. Reifenabrieb, ist während der Fahrt technisch noch nicht möglich.

R 7: Es muss sichergestellt werden, dass bei Nichtbestätigung des Fahrers einer automatisierten Fahrt Level vier am Zielort nach x min eine Notfallkette eingeleitet wird.

Regelkreis:

1. Fahrer-HMI

UCA:

-Das hochautomatisierte Fahrzeug hat die Stillstandssicherung zu früh bereitgestellt, wenn eine Person bzw. Personen im Fahrzeug in Not sind.

Der Fahrer wird während der Fahrt fahruntauglich. Er kann die Fahrt nach Abschluss nicht bestätigen und eine Notfallkette wird eingeleitet. Fraglich ist, ob Fahrzeughersteller dazu verpflichtet sind Menschen im automatisierten Fahrzeug zu helfen, wenn diese ohne jegliche äußere Einwirkung Hilfe benötigen.

Sollte sich die Betriebsorganisation verändern, beispielsweise Nutzer der Fahrzeuge sind nicht mehr die Besitzer, dann müsste unter dieser Annahme das Ende der Fahrt bestätigt werden. Das Fahrzeug kann erneut angefordert werden.

Die Fahrt wird x min nach Fahrzeugstillstand nicht bestätigt, da der Nutzer sich noch darin aufhalten möchte. Infolgedessen sollte hingegen keine Notfallkette eingeleitet werden.

R 8: Es muss sichergestellt werden, dass ein Risikomanagement/Einrichtung geschaffen wird, die sicherheitskritische Prozesse im Straßenverkehr regelt.

Regelkreis:

1. Hersteller-Steuerungs- und Regelungssysteme

UCA:

-Die Steuerungs- und Regelungssysteme stellen dem Hersteller inadäquate Feedbackinformationen bereit.

-Die Steuerungs- und Regelungssysteme stellen eine inadäquate Zunahme/Abnahme der Fahrparameter bereit, wenn eine normale Fahrsituation vorliegt.

Eine Organisationseinheit muss die Feedbackprozesse des automatisierten Fahrzeugs adäquat auswerten und das automatisierte Fahrzeug auf Basis der Daten sicherheitskritisch überwachen. Fraglich ist derzeit die Umsetzung dieser Überwachung.

R 9: Es muss sichergestellt werden, dass das hochautomatisierte Fahrzeug Level vier hinreichend sicher manuell geführt wird, wenn die Fahrerübernahme erfolgt.

Regelkreis:

1. HMI-Fahrer

UCA:

-Das Fahrzeug stellt dem Fahrer nach Fahrerübernahmeaufforderung die manuelle Fahrfunktion bereit, wenn der Fahrer nicht in der Lage ist, das Fahrzeug hinreichend sicher zu bedienen.

Es ist nicht sinnvoll dem Fahrer das Fahrzeug manuell zu übergeben, sollte dieser keine Fahrroutine mehr haben. Der Nachweis einer Fahrerlaubnis ist keine hinreichende Bedingung für Fahrroutine. Es ist eine Nachregulierung notwendig.

R 10: Es muss sichergestellt werden, dass das hochautomatisierte Fahrzeug Level vier verlassen wird, wenn Personen innerhalb des Fahrzeugs schädlichen- und außerhalb des Fahrzeugs keinen schädlichen Bedingungen ausgesetzt werden.

Regelkreis:

1. Steuerungs- und Regelungssysteme-physikalischer Fahrzeugzustand-Fahrzeugsensoren

UCA:

-Die Steuerungs- und Regelungssysteme stellen das Öffnen des Fahrzeugs bereit, wenn Personen außerhalb des Fahrzeugs schädlichen Bedingungen ausgesetzt sind.

-Die Steuerungs- und Regelungssysteme stellen das Öffnen des Fahrzeugs bereit, während das physikalische Fahrzeug diese Kontrollaktion nicht umsetzt.

-Die Steuerungs- und Regelungssysteme stellen das Schließen des Fahrzeugs bereit, wenn Personen im Fahrzeug schädlichen Bedingungen ausgesetzt sind.

Als Ergebnis der Anforderungsliste der STPA muss sich im hochautomatisierten Fahrzeug Level vier mindestens ein Fahrer mit Fahrerlaubnis befinden. Der Person im Fahrzeug sind auf Basis dieser modellierten Anforderung die Verkehrsregeln bekannt. Dieser Fahrer sollte die Fahrsituation hinsichtlich eines hinreichend sicheren Ausstiegs aus dem bspw. kollidierten Fahrzeug adäquat einschätzen können. Problematisch sind Personen im Schockzustand. Diese könnten nach einem Crash nicht mehr psychisch in der Lage sein das Fahrzeug hinreichend sicher zu verlassen.

R 11: Es muss sichergestellt werden, dass sicherheitskritische Aktuatoren nach einem Crash entsprechend aktiviert/deaktiviert werden, sodass Personen in und am Fahrzeug keinen schädlichen Bedingungen ausgesetzt werden.

Regelkreis:

1. Steuerungs- und Regelungssysteme-Physikalischer Fahrzeugzustand (sicherheitskritische Aktuatorik)-Fahrzeugsensorik

UCA:

-Sicherheitskritische Aktuatorik des Fahrzeugs wird zu spät deaktiviert, wenn Umweltbedingungen diese erfordern.

-Sicherheitskritische Aktuatorik des Fahrzeugs wird zu spät aktiviert, wenn Umweltbedingungen diese erfordern.

Fraglich ist, welche Aktuatoren nach einem Crash aktiviert/deaktiviert werden sollen. Die Aktivierung und Deaktivierung der Aktuatoren hängt mit der Kritikalität des Unfalls zusammen. Entstehen im Motorraum giftige Gase, dann sollte die Klimaanlage kein Rauch in die Fahrgastzelle strömen lassen und folglich deaktiviert werden. Bei lebensfeindlichen Außentemperaturen sollte nach einem Crash die Klimaautomatik hingegen aktiviert sein. Welche Arten von Anforderungen an Post-Crash-Szenarien sind zukünftig zu bewältigen?

Mit STPA konnten unklare regulative Gesetzeslagen sowie technisch unklar durchsetzbare Anforderungen aufgedeckt werden, die von Automobilherstellern und der Gesetzgebung zukünftig adressiert werden müssen. In diesem Abschnitt wurden diese Anforderungen aufgezählt und die Herleitung in STPA aufgezeigt.

7.5. Zeitaufwand STPA

Es wurden insgesamt ca. 560 Arbeitsstunden für die Durchführung der STPA aufgewendet. Für die Orientierungs- und Einarbeitungsphase wurden ca. 593 Stunden benötigt. In der Einarbeitungsphase hat sich der Durchführende die Vorgehensweise der STPA angeeignet, die STPA in den Kontext der Gefahrenanalysen eingeordnet sowie STPA in Anwendungsbeispielen für verschiedene sicherheitskritische und soziotechnische Systeme im Bereich der Luft- und Raumfahrt, Automobilindustrie, Medizintechnik, Verteidigung, Infrastruktur, Eisenbahn und Nukleartechnik angewandt. Der Schwerpunkt lag auf technisch geprägten Übungsbeispielen.

In Abbildung 19 ist die benötigte Arbeitszeit für die Durchführung der STPA für ein Fahrzeug Level vier und fünf dargestellt. Insgesamt wurden fünf Iterationsschritte der STPA durchgeführt, da der Erkenntnisgewinn nach dem fünften Iterationsschritt verhältnismäßig gering war. In Abbildung 20 ist die prozentuale Arbeitszeit dargestellt, um die STPA unter definierten Rahmenbedingungen anzuwenden. Differenziert wird in der Auswertung zwischen den einzelnen Vorgehensschritten der STPA[22] ins Verhältnis gesetzt zur Gesamtarbeitszeit. Indirekte Denkprozesse sind nicht direkt quantifizierbar und sind somit kein Teil der Aufstellung.

[22] Siehe Abbildung 14.

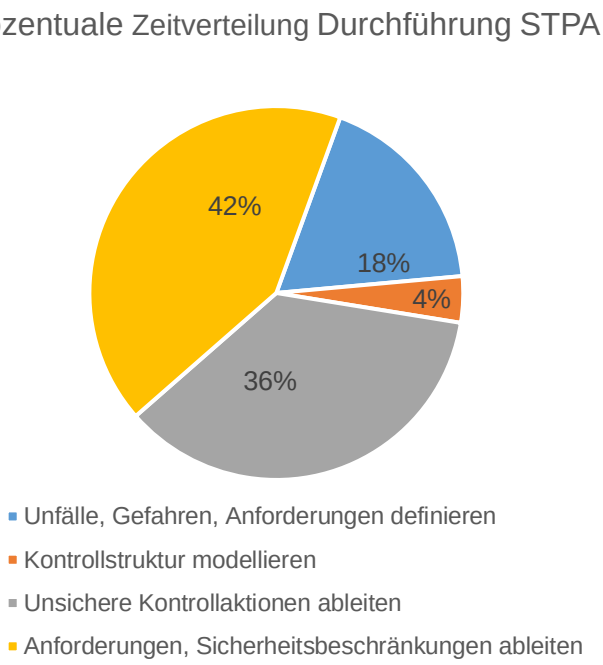

Abbildung 19: Benötigte Zeit zur Durchführung der STPA unter gegebenen Rahmenbedingungen unterteilt in einzelne Arbeitsschritte

In Abbildung 20 wird hingegen differenziert zwischen der Einarbeitungsphase und der Durchführung, welche erneut in die Kategorie der Kausalanalyse und der Bewertung von unerwünschtem Systemverhalten klassifiziert wird.

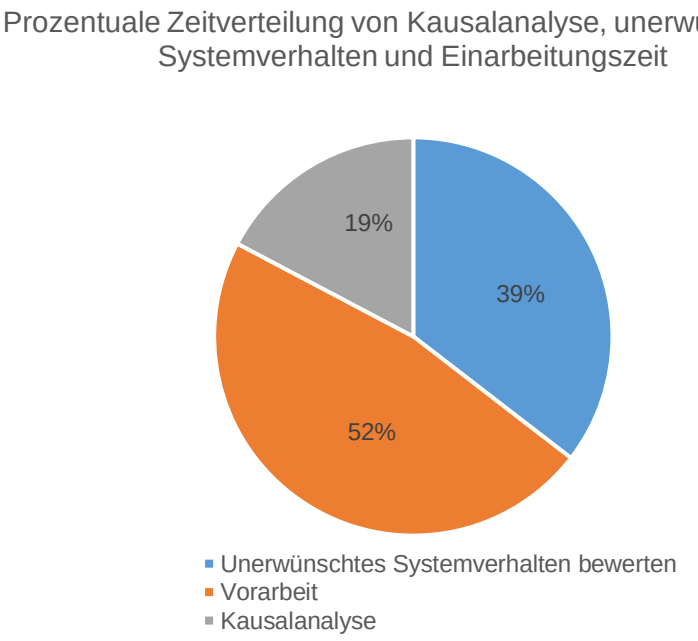

Abbildung 20: Prozentuale Zeitverteilung Durchführung und Vorarbeit STPA

Der größte Zeitbedarf wird zur Identifizierung der unsicheren Kontrollaktionen und der Anforderungen aufgewendet. Die Modellierung der Kontrollstruktur nimmt im Vergleich zur Gesamtarbeitszeit den geringsten Aufwand ein. Der Aufwand zur Identifikation der Gefahren, Unfälle und die Bestimmung der Sicherheitsanforderung ist hingegen insgesamt geringer als die Identifikation der unsicheren Kontrollaktionen und das Ableiten der Sicherheitsanforderungen. Die aufgewendeten Arbeitsstunden sind abhängig vom untersuchten System, den getroffenen Rahmenbedingungen, dem Wissensstand und individuellen Voraussetzungen der Durchführenden. Die Werte unterliegen somit keiner Allgemeingültigkeit, sondern sind vielmehr als Richtwerte für den spezifischen Anwendungsfall zu verstehen. Dennoch können aus dieser Dokumentation grobe Einschätzungen weiterer Anwendungsbeispiele abgeleitet werden. Der benötigte Zeitaufwand der GuR der BMW Group wurde von Experten deutlich höher eingeschätzt im Vergleich zur STPA.

7.6. Diskussion und Zusammenfassung

Es kann bestätigt werden, dass mittels STPA Anforderungen für ein Fahrzeug Level vier und fünf bestimmt werden konnten. Es wurden explizit Unfallursachen im fahrzeugsystemübergreifenden Kontext sowie die Mensch-Maschine Schnittstelle analysiert. Insgesamt wurden Anforderungen für ein Fahrzeug Level vier und Level fünf bestimmt. Es konnten schwerpunktmäßig unsichere Kontrollaktionen durch inadäquate Prozessmodelle, inadäquatem Feedback und Kontrollaktionen identifiziert werden. Inadäquate Feedbacks, Kontrollaktionen, Prozessmodelle entstanden unter anderem aufgrund nicht oder inadäquat identifizierter Umweltzustände, die im System unzureichend verarbeitet wurden und in unsicheren Aktionen resultierten. Da das Fahrzeug Level fünf keine direkte Interaktion zwischen Fahrzeug und Insassen im Hinblick auf die Fahrzeugführung vorsieht, fallen Schnittstellenprobleme sowohl nominal als auch im Fehlerfall weg. Damit vereinfachen sich die Regelkreise und entsprechende Anforderungen fallen weg. Neue Regelkreise kommen hingegen ausschließlich für die Teleoperation hinzu, auf anderen Hierarchieebenen hingegen nicht, da das vollautomatisierte Fahren als Nutzfunktion im Level vier vollständig definiert ist.

8. Vergleich der Ergebnisse aus STPA und GuR

Im folgenden Kapitel werden Anforderungen der vorliegenden STPA mit den Safety Goals einer GuR verglichen. Eine GuR ist ein formaler Prozess der Risikobewertung (ASIL) der ISO 26262. In dieser Arbeit wird analysiert, ob Anforderungen mittels STPA bestimmt werden konnten, die in der GuR nicht identifiziert wurden. In der Vergleichs-GuR wurden Gefahren mittels Brainstormingprozessen, Experteneinschätzungen und der HAZOP bestimmt. Ziel dieses Kapitels sind Aussagen bezüglich der Ergebnisse der STPA, im Vergleich zum Output der GuR.

Im ersten Teil des Kapitels werden Prämissen und Rahmenbedingungen des Vergleichs formuliert. Im zweiten Teil des Kapitels werden Anforderung verglichen und Themengebiete aufgelistet, die in der STPA bzw. in der GuR aufgedeckt wurden, hingegen kein Teilergebnis der jeweiligen Referenzmethode waren.

8.1. Rahmenbedingungen bzw. Problemstellungen Durchführung

Der Vergleich wird unter definierten Rahmenbedingungen durchgeführt, die im Folgenden erläutert werden. Basis des Vergleichs sind die Ergebnisse aus der STPA (siehe Kapitel 7) und die Safety Goals einer GuR. Die GuR wird von der BMW Group zur Verfügung gestellt und wurde als Beitrag zur funktionalen Absicherung einer hochautomatisierten bzw. autonomen Fahrfunktion, dem Urban Pilot[23], erstellt. Zum Zeitpunkt des Vergleichs ist die GuR der BMW Group Vorentwicklungsstand, hingegen kein vollständig ausgereiftes Endprodukt.

Im Folgenden werden Problemstellungen des Vergleichs erläutert. Anforderungen der GuR und der STPA unterscheiden sich im Detailgrad und Wortgebung, was einen direkten Vergleich der Anforderungen erschwert. In der ISO 26262 werden aus der GuR Safety Goals abgeleitet, aus denen anschließend Anforderungen mit vergleichsweise hohem Detailgrad für die Sicherheitskonzepte bestimmt werden, siehe Abbildung 21. Ergebnis der STPA sind Anforderungen mit höherem Detailgrad im Vergleich zu den Safety Goals, hingegen mit niedrigerer Granularität im Vergleich zu den Anforderungen der Sicherheitskonzepte. Je allgemeiner Anforderungen formuliert werden, desto mehr Aspekte werden abgedeckt, hingegen desto geringer ist die Aussagekraft der jeweiligen Anforderung. Weiter lagen zum Zeitpunkt des Vergleichs ausschließlich die Safety Goals der GuR vollständig vor, welche daher die Grundlage der Auswertungen sind. Weiter sind Anforderungen aus GuR und STPA in Wortgebung nicht deckungsgleich, hingegen in Sinnhaftigkeit. Zusammenfassend werden

[23] Urban Pilot ist eine entwickelte Funktion der BMW Group für eine Fahrt im Level vier bzw. fünf.

Anforderungen, die in einem bestimmten Interpretationsspielraum zuordenbar waren, als deckungleich klassifiziert.

Abbildung 21: Granularität der Anforderungen aus der GuR, STPA und Sicherheitsanforderungen

Potenziell können aufgrund der Granularität mehrere Anforderungen aus der STPA von einem Safety Goal abgedeckt werden. Ob das Safety Goal mit den Anforderungen vollumfänglich beschrieben wurde, muss grundsätzlich aufgrund der „Unknowns Unknowns“[24] verneint werden. Daher wird in der Auswertung ausschließlich angegeben, ob eine Anforderung aus der STPA zuordenbar war, hingegen nicht, ob das Safety Goal ganzheitlich beschrieben ist.

Mittels STPA können Anforderungen in der Gebrauchssicherheit, der funktionalen Sicherheit und der Cybersecurity modelliert werden, obgleich das Augenmerk in der vorliegenden STPA auf funktionaler Sicherheit liegt. Die GuR adressiert hingegen ausschließlich die funktionale Sicherheit. Daher werden Themengebiete, die nicht in der GuR, hingegen in der STPA bestimmt wurden, in funktionale Sicherheit, Gebrauchssicherheit und Cybersecurity unterteilt, um Vergleichbarkeit zu schaffen. Weiter werden keine Zahlenwerte hinsichtlich übereinstimmender bzw. ungleicher Anforderungen angegeben, da Zahlenwerte aufgrund genannter Rahmenbedingungen das Ergebnis nicht vollumfänglich erfassen würden. Vielmehr liegt der Mehrwert in der Zusammenfassung und Diskussion nicht identifizierter Themengebiete und der Einordnung der Anforderungen der STPA im Gesamtkontext.

8.2. Inhaltlicher Vergleich der Anforderungen aus GuR und STPA

Im folgenden Kapitel werden Anforderungen der GuR und der STPA verglichen. In diesem Kapitel wird die Forschungsfrage beantwortet, ob mittels STPA Gefahrenpotentiale aufgedeckt

[24] Siehe Kapitel 1

wurden, die mit traditionellen Methoden nicht identifiziert wurden. Es kann zusammengefasst werden, dass Safety Goals aus der Vergleichs-GuR mit der STPA identifiziert werden konnten. Weiter wurden in der STPA Anforderungen bestimmt, die keinem Safety Goal der GuR zuordenbar waren. Im Folgenden werden zusammenfassend Themenkomplexe aufgelistet, die in der STPA bestimmt bzw. ausführlicher untersucht wurden, hingegen nicht in der GuR identifiziert wurden. Hierbei wird erneut in die Sektoren der funktionalen Sicherheit, Gebrauchssicherheit, Cybersecurity sowie nicht sicherheitskritischer Aspekte differenziert. Weiter wird die Anforderung vorgestellt, die von der STPA nicht identifiziert wurde, hingegen von der GuR.

Funktionale Sicherheit:

- Informationsweitergabe zwischen regelkreisspezifischen Elementen im Fahrzeug und in fahrzeugübergreifenden Strukturen speziell hinsichtlich Kompatibilität, Abweichungen vom Erwartungsbereich, zeitliche Reihenfolge, Protokollierung, Datenlogging, Manipulation von Daten, Feedbacks, Priorisierung, Erkennen fehlerhafter Informationen, Verschlüsselung.
- Möglichkeit der Kommunikation (länderübergreifend) des Fahrzeugs mit Menschen im und im Umkreis des Fahrzeugs mit Fokus auf funktionaler Sicherheit.
- Updates (Reihenfolge, Empfängerfahrzeug) mit Fokus auf funktionaler Sicherheit.
- Auswirkung von Umweltbedingungen auf das Fahrzeug speziell im Hinblick auf „andere Aktuatorik“ mit Fokus auf funktionale Sicherheit.
- Übergangszustände Fahrmoduswechsel, mit Fokus auf die HMI Schnittstelle.
- Mögliche Umstrukturierung hinsichtlich des Risikomanagements im Sektor Mobilität mit Fokus auf funktionaler Sicherheit.

Gebrauchssicherheit:

- Möglichkeit der Kommunikation (länderübergreifend) des Fahrzeugs mit Menschen im und im Umkreis des Fahrzeugs mit Fokus auf Gebrauchssicherheit.
- Wartung bzw. Service des Fahrzeugs.
- Updates (Autorisierung, Reihenfolge, Empfängerfahrzeug) mit Fokus auf Gebrauchssicherheit.
- Übergangszustände Fahrmoduswechsel, mit Fokus auf der HMI Schnittstelle.
- Auswirkung von Umweltbedingungen auf das Fahrzeug speziell im Hinblick auf „andere Aktuatorik“ mit Fokus auf Gebrauchssicherheit.

- Unfälle mit und ohne Eigenbeteiligung des automatisierten Fahrzeugs (Detektion/Identifikation von Unfällen im automatisierten Fahrzeug, Einleitung von Maßnahmen, Hilfeleistung).

Cybersecurity:

- Updates (Autorisierung, Reihenfolge, Empfängerfahrzeug) mit Fokus auf Cybersecurity.
- Übergangszustände Fahrmoduswechsel, mit Fokus auf der HMI Schnittstelle.
- Zugriffsberechtigte und Zugriffsrechte auf das Fahrzeug (Zugriff nicht autorisierter Personen bzw. Zugriff autorisierter Personen zum falschen Zeitpunkt).
- Mögliche Umstrukturierung hinsichtlich des Risikomanagements im Sektor Mobilität mit Fokus auf Cybersecurity.
- Unfälle mit und ohne Eigenbeteiligung (Detektion/Identifikation von Unfällen im vollautonomen Fahrzeug, Einleitung von Maßnahmen, Hilfeleistung) mit Fokus auf Cybersecurity.

Nicht sicherheitskritische Faktoren:

- Schädigung des Rufes des Herstellers bzw. der Technologie durch beispielsweise unzureichende Verfügbarkeitsanforderungen des autonomen bzw. hochautomatisierten Fahrmodus.

Folgendes Safety Goal wurde in der STPA nicht identifiziert, hingegen in der GuR:

„During Teleoperation a vehicle speed above the specified max. TO speed shall be avoided“

In der STPA ergab sich aus den unsicheren Kontrollaktionen keine Anforderung für eine maximale Geschwindigkeitsbegrenzung während der Teleoperation.

8.3. Zusammenfassung

Mit STPA konnten Anforderungen für ein Fahrzeug Level vier und fünf bestimmt werden. Weiter wurden auf Basis des Vergleichs Ergebnisse erzielt, die über die GuR hinausgehen. Unter definierten Rahmenbedingungen hat die STPA Anforderungen bestimmt, die in der GuR nicht enthalten waren. Ein Großteil der Anforderungen aus der GuR konnten hingegen von der STPA identifiziert werden. In der STPA sind aufgrund der systemtheoretischen

Vorgehensweise, identifizierte Gefahren durch regelkreisspezifische Elemente geprägt. In der GuR liegt in diesem Bereich keine systematische Untersuchung vor, was potenziell Ursachen für nicht erkannte Themenfelder sind. Durch die konsequente Durchpermutation der unsicheren Kontrollaktionen im Kontext des Regelkreises wurden Faktoren in der STPA identifiziert, die in der GuR nicht vorhanden waren. Es wurden in STPA ebenfalls Gefahren auf fahrzeugsystemübergreifenden Ebenen formuliert, die in der GuR nicht bestimmt wurden, obgleich die Gefahren der funktionalen Sicherheit zugeordnet werden können wie beispielsweise die Car-to-X Kommunikation. Mit STPA konnten Gefahren in den Bereichen der funktionalen Sicherheit, Gebrauchssicherheit, Cybersecurity und in Bereichen nicht sicherheitskritischer Faktoren identifiziert werden. Es ist zu berücksichtigen, dass aufgrund der unterschiedlichen Detailgrade und der sprachlichen Ausführung der Anforderungen keine exakte Vergleichbarkeit der Anforderungen, wie beispielsweise mit numerischen Daten, aus STPA und GuR gegeben ist. Die Vergleichbarkeit basiert auf einem Interpretationsspielraum und wurde nach bestem Wissen und Gewissen im Untersuchungsrahmen durchgeführt.

9. Industrielle Anwendbarkeit der STPA

Im folgenden Kapitel werden die in dieser Analyse identifizierten Stärken und Schwächen in der Anwendung der STPA zusammengefasst. Die nachfolgenden Aufzählungen nehmen konkret Bezug auf die Anwendung von STPA in der Serienproduktion von Fahrzeugen.

9.1. Stärken STPA

In STPA werden Anforderungen formuliert, deren Hintergründe bzw. Gedankengänge als Methodenbestandteil beschrieben werden müssen. Zusätzliche Erklärungen reduzieren Fehlinterpretationen und wirken dem Informationsverlust durch Verknappung der Informationen entgegen. Auswirkungen durch Verknappung von Informationen bzw. einem fehlenden Kontext wird unter anderem in Unternehmen wie Amazone thematisiert [106]. Weiter gibt eine Dokumentation als Methodenbestandteil Haftungssicherheit für die Anwender der Analyse.

In STPA wird im Vergleich zur FTA nicht mit einem unsicheren Zustand begonnen. Die Gesamtheit der Kontrollaktionen wird in den Regelkreisen analysiert. Diese können sowohl unsicher als auch sicher sein. Fragewörter zielen in STPA nicht auf bestimmte Fehler ab. Der Weitblick für unsichere Zustände wird nicht eingeschränkt.

Mit STPA können Anforderungen für Gebrauchssicherheit, funktionale Sicherheit sowie Cybersecurity bestimmt werden. Gebrauchssicherheit, funktionale Sicherheit und Cybersecurity werden derzeit in der Automobilindustrie unabhängig voneinander geprüft. Eine gesamtheitliche Betrachtungsweise aller drei Bereiche würde Überschneidungen bzw. komplexe Systemstrukturen oder Widersprüche reduzieren und das gesamtheitliche Systemdesign fördern.

In STPA sind Überscheidungen von gegensätzlichen Anforderungen unvermeidbar, da Anforderungen regelkreisspezifisch formuliert werden. Durch das einheitliche Regelwerk der STPA und einer ganzheitlichen Betrachtungsweise durch eine einzelne Analyse ist die Vorgehensweise vorteilhaft im Vergleich zu einer bereichsspezifischen Durchführung mit mehreren Analysen. Weiter ist durch die restriktive Vorgehensweise der STPA die Häufigkeit von Überschneidungen reduziert.

Die Qualität von Ergebnissen bei Anwendung von traditionellen Methoden ist bedeutend abhängig vom Analytiker. Auf Basis von Expertenwissen und Erfahrungswerten werden unterschiedlich relevante Ergebnisse erzielt. STPA hingegen zwingt zu einer systematischen Vorgehensweise beispielsweise durch eine stringente Durchpermutation von Kontrollaktionen. Die Qualität der Ergebnisse ist weniger beeinflusst durch langjährige Erfahrungen.

Systemfremde Personen mit technischem Grund- und Methodenverständnis können eine STPA gewinnbringend durchführen. Explizit in der Absicherung von disruptiven Technologien bzw. grundlegenden Veränderungen in Mobilitätskonzepten liegen keine langjährigen Erfahrungswerte vor. Es ist vorteilhaft, wenn Analysen angewendet werden können, die neue Konzepte hinreichend absichern können.

Eigenschaften von Systemen[25] mit Perspektive auf unterschiedliche Hierarchieebenen unterscheiden sich. Das Gesamtsystem besteht aus der Summe der Eigenschaften aller Ebenen. Schlussfolgernd ist es ungeeignet ausschließlich auf Komponentenebene abzusichern, hingegen übergeordnete Ebenen zu vernachlässigen. Eine Absicherung auf immer detaillierteren Ebenen führt nicht zwangsläufig zu sicheren Systemen. Es gibt Fehler, die in tieferen Hierarchieebenen eliminiert werden können, hingegen Fehler die ausschließlich auf höherliegenden Ebenen gelöst werden. Mit STPA wird aufgrund der systemtheoretischen Vorgehensweise und der Kontrollstruktur der Fokus auf das Gesamtsystem gelegt und somit eine objektive Sichtweise protegiert. Mittels STPA können dadurch fahrzeugsystemübergreifende Ebenen untersucht werden.

Mit STPA können durch den systemtheoretischen Ansatz Interaktionen außerhalb des technischen Systems untersucht werden. Dieser Vorteil gewinnt maßgeblich an Bedeutung, wenn nicht nur das technische System Fahrzeug, sondern ebenfalls die Betriebsorganisation der Mobilität grundlegenden Veränderungen unterliegt. Interaktionen zwischen dem technischen System und hierarchiehöheren Strukturen gewinnen dadurch zunehmend an Bedeutung. Daher ist es notwendig Methoden bzw. Methodenkombinationen anzuwenden, die diese Schnittstellen adäquat untersuchen können.

Mit STPA kann aufgrund des Top-down Prinzips das zu untersuchende technische Design frühzeitig im Entwicklungsprozess optimiert werden. Ein detailliertes Systemdesign ist keine notwendige Voraussetzung für eine Durchführung. Der formale Rahmen und die frühe Anwendbarkeit im Entwicklungszyklus eines Fahrzeugs erhöhen die Praktikabilität der Analyse und bieten damit die Möglichkeit einer breiten Anwendung. Voraussetzung für die STPA ist kein spezifisches Systemdesign. Sicherheit muss somit nicht als Gegensatz zur Performance gesehen werden, sondern kann als Ergänzung klassifiziert werden.

Mit STPA kann die Mensch Maschine Interaktion durch den systemtheoretischen Ansatz im Vergleich zur FMEA und FTA umfangreich untersucht werden. Diese Fokussierung ist konkret für hochautomatisierte und autonome Fahrzeuge von besonderer Bedeutung. Die Analyse bedarf im Vergleich beispielsweise zur GuR einen verhältnismäßig geringen Zeitaufwand.

[25] Mit *System* ist in diesem Fall nicht ausschließlich ein technisches System gemeint. Das technische System kann beispielsweise eine Komponente eines Systems sein.

9.2. Schwächen STPA

Durch Ausbildung und Erfahrungen in teilweise vordefinierten Mustern, werden Denkweisen von Durchführenden geprägt beispielsweise durch eine komponentenorientierte Sichtweise. Um die STPA gewinnbringend durchzuführen, muss hingegen eine funktionale Denkweise eingenommen werden. Sind Problemstellungen des zu untersuchenden Systems bekannt, ist eine objektive Herangehensweise zunehmend problematisch. Zusammenfassend sind die Ergebnisse der STPA stark abhängig vom mentalen Prozessmodell des Durchführenden. Die Auswahl geeigneter Analysten mit geeignetem Verhältnis an Hintergrundwissen ist entscheidend für eine gewinnbringende Analyse.

In der STPA können aus den Regelkreisen potenziell Anforderungen modelliert werden, die jeweils gegensätzliche Aussagen präsentieren. Zum Zeitpunkt der Modellierung der einzelnen Anforderung ist die Inkonsistenz meist nicht bestimmbar. Erst nach einer Gesamtsichtung der Ergebnisse kann die Gesamtheit der Ergebnisse auf Konsistenz überprüft werden.

Einen angemessenen Zeitrahmen zur Durchführung der Analyse ist für den Erfolg der Analyse entscheidend. Die Identifikation der unsicheren Kontrollaktionen und Sicherheitsanforderungen bedarf ein hohes Maß an Kreativität. Kreativität wird durch Zeitdruck gemindert [106]. Denkprozesse können nicht beschleunigt werden. Die Automobilindustrie befindet sich in einem dynamischen Wettbewerbsumfeld. Die durch Zeitdruck geprägte Arbeitsweise in Unternehmensstrukturen hemmt eine gewinnbringende STPA.

Die Vorteile der STPA liegen in der Identifizierung von Gefahrenpotentialen auf höherliegenden Hierarchieebenen, hingegen weniger auf detaillierteren wie beispielsweise auf Bit und Byte Ebene. Je präziser das System aufgespalten wird, desto weniger können die Stärken der Analyse genutzt werden. Die Analyse verliert an Schärfe.

Die Priorisierung identifizierter Anforderungen ist kein Methodenbestandteil der STPA. Ressourcen könnten aufgrund fehlender Klassifizierung ineffizient eingesetzt werden. Weiter ist eine Strukturierung der Anforderungen aufgrund fehlender Priorisierung zeitaufwendig. Ein Großteil der Zeit zur Durchführung der Analyse wird benötigt Ergebnisse und Teilergebnisse zu ordnen und widersprüchliche Anforderungen zu eliminieren.

Weiter sind identifizierte Verfügbarkeitsanforderungen hinsichtlich einer Umsetzung kritisch zu diskutieren. Muss beispielsweise eine Landstraße in Westafrika vermessen werden, um autonom fahren zu können? STPA kann hinsichtlich Häufigkeit und Fehlerschwere nicht klassifizieren. Tritt ein Ereignis nur sehr selten auf, ist es fraglich, wie aufwendig es ist, dieses unerwünschte Ereignis zu verhindern. In der vorliegenden Untersuchung ergab sich, dass der Schwerpunkt der Analyse auf der Identifizierung von Gefahren liegt, hingegen weniger auf der Lösung identifizierter Problemstellungen im detaillierten Systemdesign.

Weiter sind Common Cause Fehler mit der STPA sowie mit traditionellen Analysemethoden nicht systematisch identifizierbar bzw. nur mit hohem Aufwand identifizierbar. Diese Problematik besteht in der Automobilindustrie sowie in anderen Industrien wie beispielsweise Luftfahrt, Medizintechnik. Die Identifizierung von Common Cause Fehlern basiert hauptsächlich auf Zufall bzw. Erfahrungen des Analytikers.

Weiter muss eine geeignete Abstraktionsebene für die STPA ausgewählt werden. Die Abstraktionsebene ist abhängig vom zu untersuchenden System und der Zielstellung. Erfahrungen in der Durchführung der STPA müssen vorhanden sein, um die Stärken der Analyse nutzen zu können.

9.3. Effektivität der Maßnahmen in der Durchführung der STPA

Im folgenden Kapitel werden Maßnahmen, die vor Durchführung der STPA ergriffen wurden, aufgelistet, um den Erfolg in der Anwendung der STPA zu erhöhen. In Tabelle 3 sind die Maßnahmen sowie der jeweilige Effekt auf den Übungsstatus aufgelistet. Diese Einordnung basiert ausschließlich auf Basis der Erfahrungswerte der vorliegenden STPA.

Tabelle 3: Maßnahmen vor Durchführung der STPA in Bezug zum Lerneffekt

Beschreibung	**Aufwand**	**Effekt**
Anwendung der STPA auf ausgesuchte Systeme unterschiedlicher Themengebiete im kleineren Untersuchungsrahmen im Vergleich zur Durchführung in dieser Arbeit.	Mittel	Hoch
Durcharbeiten des STPA Handbooks [13] sowie Engineering a Safer World [14].	Hoch	Mittel
Anwendungsbeispiele der STPA aus Veröffentlichungen eigenständig durchführen und Ergebnisse der Veröffentlichung sowie der eigenen Durchführung vergleichen.	Mittel	Hoch
Dokumentation von Gedankengängen explizit hinsichtlich Interaktionen und Verknüpfungen auf Metaebenen während der Durchführung der STPA in technisch fremden Themengebieten.	Niedrig	Hoch
STPA Tutorial Videos durcharbeiten.	Niedrig	Niedrig
Durchführung eines umfangreichen STPA Projektes.	Hoch	Hoch
Durchführung mehrerer Iterationsschritte der STPA.	Hoch	Hoch

Zu den effektiven Maßnahmen zählt die Durchführung von STPA-Übungsprojekten in technisch übergreifenden Themengebieten. Weiter ist eine Dokumentation von

Gedankengängen explizit mit Fokus auf Interaktionen und Verknüpfungen sinnvoll. Einer technisch geprägten Sichtweise wird entsprechend entgegengewirkt, die funktionsorientierte Sichtweise hingegen protegiert. Der Aufwand für die Durchführung der Maßnahmen ist jeweils durchschnittlich bis gering einzuordnen, der Nutzen hingegen hoch. Weiter ist vorteilhaft, STPA in mehreren Reviewzyklen auf das System anzuwenden. Die STPA wurde beispielsweise im vorliegenden Anwendungsbeispiel insgesamt fünf Mal iteriert. Die Iteration wurde beendet, sobald kein relevanter Mehrwert geschaffen wurde. Nutzen und Aufwand sind hoch. Weiter wurden zu Übungszwecken Veröffentlichungen mit Anwendung von STPA auf vordefinierte Beispiele durchgearbeitet. Der Aufwand die Maßnahme durchzuführen ist durchschnittlich, hat hingegen einen großen Lerneffekt. Nutzen und Effekt waren von STPA Tutorial Videos verhältnismäßig gering. Die Maßnahme *Engineering a Safer World* sowie das *STPA Handbook* durchzuarbeiten hatte einen mittleren Effekt, hingegen einen hohen Aufwand.

10. Beantwortung der Forschungsfragen

Im folgenden Kapitel werden die Forschungsfragen beantwortet. Es wurden folgende Zielstellungen definiert:

1. Welche Eigenschaften der STPA sind besonders vorteilhaft bezüglich der Anwendung im Entwicklungszyklus eines automatisierten Fahrzeugs.

STPA hat verschiedene Stärken und Schwächen und ist als alleinige Methode keine vollumfängliche Lösung in der Absicherung von automatisierten Fahrzeugen. Bestimmte Eigenschaften der STPA sind für zukünftige Entwicklungen in hochautomatisierten Fahrzeugen hingegen von entscheidendem Vorteil. STPA fördert das Zusammenspiel der Analyse von Gebrauchssicherheit, funktionaler Sicherheit, Cybersecurity und nicht sicherheitsbezogener Bereiche im Unternehmen. Durch die gesamtheitliche Betrachtung können Problemstellungen bereichsübergreifend gelöst bzw. untersucht werden. Eine gesamtheitliche Analyse unterstützt einerseits kostensparende Entwicklungen andererseits die Sicherheit.

Es kann auf Basis der vorliegenden Untersuchung zusammengefasst werden, dass die industrielle Anwendbarkeit von STPA gegeben ist. Nicht die notwendigen Ressourcen, sondern das erforderliche Know- How sind limitierende Faktoren. STPA hat Stärken auf Untersuchungsebenen, die in den traditionellen Methoden nur mit großem Aufwand bzw. nicht untersucht werden können. Um ein Gesamtsystem hinreichend abzusichern, müssen unterschiedliche Ebenen analysiert werden. Eine Absicherung ausschließlich im Bereich von Software bzw. auf Komponentenebene ist nicht zielführend.

Vernetzungen fahrzeugsystemübergreifender Bereiche steigen zukünftig weiter an. Die Relevanz von Methoden, die in der Lage sind, diese Interaktionen zu berücksichtigen steigt. Mit STPA können Interaktionen von Gefahrenpotentialen untersucht werden, speziell in Bezug menschlicher Interaktionen im Fahrzeug. STPA könnte den Absicherungsprozess zusammen mit traditionellen Methoden ergänzen. Vorteile der STPA liegen in der Durchführung auf hierarchiehöheren Ebenen, hingegen nicht auf Softwareebene.

2. Wurden Gefahrenpotentiale mit STPA identifiziert, die mit etablierten Methoden der Automobilindustrie nicht bestimmt wurden?

Es kann zunächst zusammengefasst werden, dass mittels STPA Gefahrenpotentiale identifiziert werden konnten. Die meisten Problemschwerpunkte, die mit der GuR bestimmt wurden, wurden ebenfalls in der STPA identifiziert. Die GuR basiert auf Brainstormingprozessen, Experteneinschätzungen und der HAZOP. Eine der Rahmenbedingungen war, dass die Vergleichs-GuR Vorserienstand war und kein ausgereiftes

Endprodukt. Weiter war der erforderliche Zeitaufwand für die STPA geringer im Vergleich zur GuR, die Ergebnisse waren hingegen vergleichbar und in einzelnen Schwerpunkten gehaltvoller.

3. Ist eine Kombination traditioneller Methoden der Automobilindustrie und der STPA notwendig, um eine hinreichende Gesamtabsicherung durchzuführen?

Potenziell ist es sinnvoll eine Methodenkombination zur gesamtheitlichen Absicherung fahrzeugspezifischer und fahrzeugsystemübergreifender Ebenen anzuwenden, um die jeweiligen Methodenstärken zu kombinieren und einen einheitlichen Entwicklungsprozess zu ermöglichen. Eine STPA beispielsweise mit einer FMEA oder mit einer PRA zu kombinieren, unterstützt den Absicherungsprozess, da Stärken von Analysemethoden kombiniert werden können. Eine Absicherung ausschließlich auf Fahrzeugsystemebene, spezifisch im Hinblick zukünftiger Herausforderungen, ohne Berücksichtigung der Einbettung ins Gesamtsystem *Mobilität* wird allein nicht gelingen.

Nicht ausschließlich die Identifikation von Gefahren mit STPA im systemtheoretischen Kontext, sondern ebenfalls die Art und Weise Anforderungen zu formulieren und einzubetten fördert das Lösen speziell im Hinblick zukünftiger Herausforderungen wie beispielsweise neuer Mobilitätskonzepte oder dem Wandel von Konsumgütern zu Investitionsgütern. Methoden müssen entsprechend in der Lage sein, Schnittstellen zwischen einem technischen System und übergeordneten Strukturen hinreichend zu untersuchen. STPA unterstützt diesen Prozess.

4. Wie unterscheiden sich die Anforderungen hinsichtlich der Komplexität eines automatisierten Fahrzeugs Level vier und fünf?

Da das hochautomatisierte Fahrzeug Level fünf keine direkte Interaktion zwischen Fahrzeug und Insassen hinsichtlich der Fahrzeugsteuerung vorsieht, entfallen die Schnittstellenprobleme bei der Übergabe der Verantwortung sowohl nominell als auch im Fehlerfall. Das vereinfacht die Regelkreise und Anforderungen entfallen. Neue Regelkreise hingegen kommen ausschließlich für die Teleoperation hinzu, nicht aber auf anderen Hierarchieebenen, denn das vollautomatisierte Fahren ist bereits in Stufe vier vollständig als Nutzfunktion definiert.

5. Welcher Zeitaufwand wird für die Durchführung der STPA für ein Fahrzeug Level vier und fünf benötigt?

Der Zeitaufwand der Durchführung der vorliegenden STPA im Verhältnis zur GuR, bereit gestellt von der BMW Group, ist geringer, hingegen sind die Ergebnisse vergleichbar.

STPA kann Systemingenieure in der Absicherung automatisierter Fahrzeuge unterstützen.

11. Zusammenfassung und Ausblick

Unsichere Zustände sind inhärenter Bestandteil eines Systems. Risiken in von Menschen geschaffenen technischen Systemen zu kontrollieren ist fundamentale Aufgabe, um nachhaltiges Wohlergehen von Umwelt und Lebewesen, Wettbewerbsfähigkeit sowie industriellen Fortschritt zu erhalten. Im folgenden Kapitel wird eine Zusammenfassung der im Rahmen dieser Arbeit ermittelten Ergebnisse zum Beitrag der Sicherheit autonomer bzw. automatisierter Fahrzeuge gegeben.

In der Automobilindustrie vollzieht sich ein grundlegender Wandel der Mobilität. Fahrzeuge könnten sich zukünftig von Konsumgütern zu Investitionsgütern wandeln. Damit einhergehende Veränderungen in Mobilitätskonzepten, der Rolle des Menschen im Fahrzeug sowie zunehmende Softwarekomplexität im Fahrzeug müssen sicherheitskritisch untersucht werden. Methoden, die eine Sicherheits- und Gefahrenanalyse auf unterschiedlichen Hierarchieebenen des Gesamtsystems *Mobilität* durchführen, sind für ein hinreichend sicheres System von essentieller Bedeutung. Weiter ist zwischen einem Trade off in der Auslegung hochautomatisierter Fahrzeuge zu differenzieren. Ist die Auslegung eines autonomen Fahrzeugs bezüglich des Sicherheitsaspektes zu restriktiv, dann könnten die Systemverfügbarkeitsanforderungen des automatisierten Fahrzeugs nicht eingehalten werden. Wird hingegen die Auslegung der Systemsicherheit zu großzügig durchgeführt, dann wird das Fahrzeug nicht hinreichend sicher sein, aber jederzeit verfügbar, das führt potenziell dazu, dass die Akzeptanz für diese Technologie sinkt. Es gilt eine bestimmte Ausfallsicherheit bei einer bestimmten Verfügbarkeit zu erreichen, die mit adäquatem Sicherheitsmanagement ermöglicht werden kann. Einen wesentlichen Beitrag dazu leistet das Requirement Engineering. Geschickte Formulierungen von Anforderungen an das System können sicherheitsbezogene Entwicklungsprozesse fördern. Es gilt den optimalen Trade off zwischen Detaillierungsebene der Anforderungen in Bezug auf die jeweiligen Empfänger der Anforderungen zu formulieren.

Diese Arbeit schafft einen Mehrwert im Requirement Engineering in der Absicherung eines Fahrzeugs Level vier und Level fünf, indem Anforderungen mit Fokus von Interaktionen auf hierarchiehöheren Instanzen mittels STPA identifiziert werden. Die Analyse erzielte Ergebnisse, mit einem für das Ziel der Analyse ausreichenden Detaillierungsgrad, nämlich dem Fokus auf dem technischen System, dem technischen System in Interaktion mit fahrzeugsystemübergreifenden Strukturen sowie der Menschen-Maschine Schnittstelle. Die Anforderungen wurden mit der in einer von BMW zur Verfügung gestellten GuR verglichen. Es kann zusammengefasst werden, dass die Ergebnisse der STPA im Wesentlichen die Ergebnisse der GuR abdeckten, hingegen in einer geringeren Zeitdauer identifiziert wurden. Weiter konnten in der STPA Themen identifiziert werden, die in der GuR nicht identifiziert

wurden. Weiter kann zusammengefasst werden, dass STPA speziell für die Serienentwicklung von Fahrzeugen vorteilhafte Charakteristika aufweist, beispielsweise mit der Möglichkeit des Fokus der Untersuchung von fahrzeugsystemübergreifenden Schnittstellen sowie dem Fokus auf die HMI Schnittstelle, die zukünftig an Bedeutung gewinnen wird. Weiter werden in der STPA Gefahren im Bereich der Cybersecurity, Gebrauchssicherheit und funktionellen Sicherheit bestimmt, was eine ganzheitliche Entwicklung in allen drei Bereichen, entgegen heutiger Entwicklungsvorgänge, fördert. Maßgeblicher Nachteil traditionellen Methoden und auch der STPA ist die fehlende Möglichkeit der systematischen Identifizierung von Common Cause Fehlern. Die Identifizierung dieser Fehlerart ist abhängig von erfahrenen Analytikern. In der Automobilindustrie, sowie ebenfalls in anderen Sektoren wie Medizintechnik, Luftfahrt befinden sich in einem technologischen Wandel. Mensch Maschine Interaktionen werden beispielsweise zukünftig in der Medizintechnik hohe Gewichtung haben. STPA kann aufgrund seiner Charakteristika universell in verschiedenen Sektoren angewendet werden.

Gefahrenanalysen haben unterschiedliche Zielstellungen und Vorgehensweisen. Die FTA benötigt ein Top Level Event, um eine Analyse durchzuführen. STPA könnte dieses Top Level Event in Form einer Anforderung zur Verfügung stellen. In der Entwicklung müsste ein Nachweiskonzept erstellt werden, um einen Nachweis zur Erreichung der Anforderungen zu liefern. Anforderungen der STPA könnten mit einer FMEA quergeprüft werden, sofern die Anforderungen aus der STPA auf detaillierteren technischen Ebenen formuliert wurden. FMEA könnte die STPA quantitativ, die FTA die STPA qualitativ ergänzen. Es ist sinnvoll die FMEA auf niedrigeren Ebenen einzusetzen und durch die STPA auf groben Ebenen als Ergänzung zu unterstützen. Die Analysen könnten als Nachweiswerkzeuge der Erreichung der Anforderungen aus der STPA bzw. als Ergänzung fungieren.

Zusammenfassend besteht die Einschätzung, dass STPA potenziell in der Lage Systemingenieure in der Entwicklung eines funktionalen Sicherheitskonzeptes hochautomatisierter Fahrzeuge zu unterstützen. Mit den Ergebnissen dieser Arbeit wird ein erster Einstieg geschaffen, um in folgenden Schritten die unsicheren Kontrollaktionen und Anforderungen aus der vorliegenden STPA weiter zu analysieren und in das Sicherheitskonzept einfließen zu lassen. Die Ergebnisse der Analyse sind stark abhängig von den Rahmenbedingungen und den Regelkreisen, die in der Kontrollstruktur definiert werden. Zukünftig könnten daher weitere unabhängige Analysen auf Basis unterschiedlicher Schwerpunkte durchgeführt werden, um unterschiedliche Ergebnisse zu erzielen. Zukünftig ist die Untersuchung einer Methodenkombination sinnvoll, mit denen in Kombination eine adäquate Absicherung eines hochautomatisierten Fahrzeugs im Kontext des Gesamtsystems Mobilität durchgeführt werden kann. Außerdem ist zu analysieren, ob formale Methoden mit Gefahren- und Sicherheitsanalysen sinnvoll kombiniert werden können. Es sollten zukünftig

STPAs mit variierenden Fokussen durchgeführt werden, um Anforderungsspezifikationen für ein hochautomatisiertes Fahrzeug zu ergänzen. Weiter gilt es zu untersuchen, ob eine toolgestützte Anwendung der STPA beispielsweise mit SysML sinnvoll ist.

Mit den Ergebnissen der STPA kann mit dieser Arbeit bestätigt werden, dass STPA potenziell eine gewinnbringende Gefahrenanalysemethode ist, mit der in den Bereichen funktionaler Sicherheit, Cybersecurity und Gebrauchssicherheit, Anforderungen für das autonome Fahrzeug Level vier und fünf bestimmt werden konnten.

12. Glossar

Automatisiertes Fahren: In dieser Begriffsdefinition sind alle Begriffe der Automatisierung enthalten

Autorisierung: Erlaubnis des Zugriffs auf das Fahrzeug

Autonomes Fahren: Höchste Stufe des automatisierten Fahrens

Bedienkonzept: Konzept bezüglich der Bedienung des Fahrzeugs für Menschen bzw. fahrzeugsystemübergreifende Einheiten

Car to X Kommunikation: Kommunikationen des Fahrzeugs mit externen Systemen zum Informationsaustausch

Datenlogging: Daten werden in einem bestimmten Rhythmus aufgezeichnet

Fachexperten: Fokus auf das Verständnis des Systemverhaltens und der Wechselwirkungen mit der Systemumgebung

Fahrparameter: Wird als kennzeichnende Größe verwendet, mit deren Hilfe Aussagen über die Leistungsfähigkeit des Fahrzeuges beziehungsweise den Fahrzustand gewonnen werden

Fahrzeugzustand: Beschreibt den physikalischen Fahrzeugzustand

Fahrzustand: Art und Weise des Vorhandenseins des Fahrzeugs in Interaktion mit dem Straßenverkehr

Gefahrenanalyse: Methode zur Identifizierung und Kategorisierung ungewünschter Ereignisse und zur Identifizierung von Sicherheitszielen und ASILs im Zusammenhang mit der Minderung und Vorbeugung der damit verbundenen Gefahren, um ein Risiko zu vermeiden

Kritische Updates: Updates, welche die Sicherheit des Fahrzeugs im Straßenverkehr erhöhen

Kritischer Unfall: Unfall mit geschädigten Personen

Minimum Risk Maneuver: Manöver, welches den Fahrzustand mit dem geringsten Sicherheitsrisiko für die spezifische Fahrsituation einnimmt

Mischverkehr: Verkehr mit unterschiedlichen Fahrzeugen und Betriebsweisen, welche denselben Verkehrsweg nutzen

Notfallszenario: Einleiten von unfallschweremindernden Maßnahmen

Out of Range: Daten die sich in einem Wertebereich außerhalb der Verarbeitung befinden

Postcrashsequence: Abfolge von Ereignissen die nach einem Unfall eingeleitet werden

Senderate: Maximale Informationsdichte pro Zeiteinheit

Standbymodus: Modus in dem das Fahrzeug keine Anforderungen erfüllen kann

Technische Systemexperten: Diese Experten verstehen die Aspekte der technischen Umsetzungsmöglichkeiten in detaillierten Ebenen eines technischen Modells

Teleoperator: Ein Mensch, der das Fahrzeug fernsteuert.

Einweisungen: Schulung des mentalen Prozessmodells vom Fahrer im Level vier Fahrzeug bzw. vom Passagier im Level fünf Fahrzeug.

Unkritische Beschädigung: Beschädigung am Fahrzeug, die eine hinreichend sichere Fahrt nicht beeinträchtigt.

Unkritische Updates: Updates, welche die Sicherheit des Fahrzeugs im Straßenverkehr nicht erhöhen

Verfügbarkeitsanforderung: Anforderung bezüglich der Verfügbarkeit des Systems.

Zwischenzustände: Dauer der Zustände während eines Betriebsmoduswechsels

Übernahmebedingungen: Notwendige Bedingungen, die in einem Betriebsmoduswechsel erfüllt werden müssen

Literaturverzeichnis

[1] B. Primer, “Neue Alternativen und stärkere Verzahnung,” auto, motor und sport., 2014. [Online]. Available: http://www.auto-motor-undsport.de/news/mobilitaet-von-morgen-neue-alternativen-und-staerkereverzahnung-8913944. [Accessed: 10-Oct-2021].

[2] H. (Hrsg.). Minx, E. und Dietrich, R.: Foreword. In: Maurer, M., Gerdes, J.C., Lenz, B. und Winner, Autonomous Driving. Technical, Legal and Social Aspects. Heidelberg: Springer Open, 2016.

[3] S. Beiker, Legal Aspects of Autonomous Driving. In: Chen, L.K.; Quigley, S.K.; Felton, P.L.; Roberts, C.; Laidlaw, P. (Hrsg.): Driving the Future: The Legal Implications of Autonomous Vehicles. Santa Clara, 2012.

[4] “NHTSA‘S National Center for Statistics and Analysis (NCSA). Trafic Safety Facts. Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey.,” 2015. [Online]. Available: https://www.nhtsa.gov/research-data/national-center-statistics-and-analysis-ncsa. [Accessed: 10-Oct-2021].

[5] ISO (International Standard of Organization, Road vehicles Functional safety) 26262. 2018.

[6] J. Zhang, H. Kim, Y. Liu, and M. A. Lundteigen, “Combining System-Theoretic Process Analysis and availability assessment: A subsea case study,” Proc. Inst. Mech. Eng. Part O J. Risk Reliab., 2019.

[7] M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Autonomes Fahren. Springer, Berlin, Heidelberg, 2015.

[8] N. Taleb, Der Schwarze Schwan, Albrecht Knaus Verlag, München 2010

[9] D. Faragó, “Zwischenbericht und Beteiligungsaufruf zur Studie über die Wertschöpfungskette und QA sicherheitskritischer Software in der Automobil - Branche,” 2015.

[10] G. Koelln, M. Klicker, and S. Schmidt, “Comparison of hazard analysis methods with regard to the series development of autonomous vehicles,” IEEE ITSC, New Zealand, 2019.

[11] B. Antoine, “Systems Theoretic Hazard Analysis (Stpa) Applied To the Risk Review of Complex Systems: An Example From Medical Device Industry,” Massachusetts Institute of Technologie, 2013.

[12] P. Underwood and P. Waterson, “A critical review of the stamp, fram and accimap

systemic accident analysis models," Adv. Hum. Asp. Road Rail Transp., pp. 385–394, 2012.

[13] N. Leveson and J. Thomas, STPA Handbook. 2018.

[14] N. Leveson, Engineering a Safer World, vol. 560. MIT Press Ltd, 2016.

[15] "Preliminary Report Highway: HWY18MH010," National Transportation Safety Board, 2018. [Online]. Available: https://ntsb.gov/investigations/AccidentReports/Pages/HWY18MH010-prelim.aspx. [Accessed: 04-Feb-2019].

[16] A. Abdulkhaleq et al., "A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles," Procedia Eng., vol. 179, pp. 41–51, 2017.

[17] Q. V. E. Hommes, "Applying System Theoretical Hazard Analysis Method To Complex Automotive Cyber Physical Systems," in ASME 2012 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference, 2012.

[18] S. Alvarez, "Safety benfit assessment, vehicle trial safety and crash analysis of automated driving : a Systems Theoretic approach. Business administration," PSL Research University, 2017.

[19] BMW et al., "Safety first for automated driving," White Pap., pp. 1–157, 2019.

[20] ACX GmbH, "DO-178C (Software Considerations in Airborne Systems and Equipment Certfication): Eine Einführung." [Online]. Available: https://docplayer.org/18634906-Acx-gmbh-do-178c-eine-einfuehrung.html. [Accessed: 10-Oct-2021].

[21] K. Esser and J. Kurte, "Autonomes Fahren, Aktueller Stand, Potentiale und Auswirkungsanalyse Studie für den Deutschen Industrie- und Handelskammertag e.V. Köln," 2018.

[22] R. B. GmbH, "Connected Car Effect 2025,Bosch-Studie zeigt: Mehr Sicherheit, mehr Effizienz, mehr freie Zeit durch vernetzte Mobilität, Pressemitteilung Dezember 2016.," 2016.

[23] H. Jahn, M. Heyen, and J. Wälder, The Insurance Monitor : To Be or Not to Be – the Future of Motor Insurance, no. 3. Frankfurt am Main: PricewaterhouseCoopers Aktiengesellschaft Wirtschaftsprüfungsgesellschaft, 2015.

[24] Roland Berger, "Automated Trucks, The next big disruptor in the automotive industry?," Chicago/Munich, 2016.

[25] A. Cacilo et al., “Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen,” Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, 2015.

[26] B. Milakis, D., van Arem, B., van Wee, “Policy and society related implications of automated driving: A review of literature and directions for future research,” J. Intell. Transp. Syst. Technol. Planning, Oper., pp. 1–25, 2017.

[27] J. Ahlgrimm, “Lexikon: Automatisiertes Fahren,” Deutscher Verkehrssicherheitsrat e.V., 2018.

[28] H. Bardt, “Autonomes Fahren: Eine Herausforderung für die deutsche Autoindustrie,” IW-Trends, vol. 43, no. 2, p. 55, 2016.

[29] Eva Fraedrich, “Autonomes Fahren. Individuelle und gesellschaftliche Aspekte der Akzeptanz,” Humboldt-Universität zu Berlin, 2017.

[30] K. Homann, “Wirtschaft und gesellschaftliche Akzeptanz: Fahrerassistenzsysteme auf dem Prüfstand. In Maurer, M.; Stiller, C. (Hrsg.), Fahrerassistenzsysteme mit maschineller Wahrnehmung.,” 2005. .

[31] T. Petermann and C. Scherz, “TA und (Technik-)Akzeptanz(-forschung),” TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, 2005. [Online]. Available: https://tatup.de/index.php/tatup/article/view/3569. [Accessed: 10-Oct-2021].

[32] R. Salay and K. Czarnecki, “Using Machine Learning Safely in Automotive Software: An Assessment and Adaption of Software Process Requirements in ISO 26262,” University of Waterloo, 2018.

[33] G. Lu and M. Tomizuka, “LIDAR Sensing for Vehicle Lateral Guidance: Algorithm and Experimental Study.,” IEEE/ASME Transactions on Mechatroniks 11, 2006.

[34] U. Hofmann, “Zur visuellen Umfeldwahrnehmung autonomer Fahrzeuge.,” Universität der Bundeswehr, München, 2004.

[35] C. Stiller, J. Hipp, C. Rössig, and A. Ewald, “Multisensor obstacle detection and tracking,” Image and Vision Computing 18, 2000.

[36] U. Iqbal, J. Georgy, M. Korenberg, and A. Noureldin, “Nonlinear Modeling of Azimuth Error for 2D Car Navigation Using Parallel Cascade Identification Augmented with Kalman Filtering.,” Int. J. Navig. Obs., 2010.

[37] S. Schmidt, “Ein optimales Steuerungs- und Regelungskonzept für autonome Elektrofahrzeuge,” Otto von Guericke Universität Magdeburg, 2013.

[38] M. Bansal, A. Krizhevsky, and A. Ogale, “ChauffeurNet: Learning to Drive by Imitating the Best and Synthesizing the Worst,” Freiburg im Breisgau, 2018.

[39] E. Kromer and S. Gerstl, “Deep Learning im Fahrzeug.” [Online]. Available: https://www.embedded-software-engineering.de/deep-learning-im-fahrzeug-a-810616/. [Accessed: 10-Oct-2021].

[40] Übereinkommen über den Strassenverkehr. Wien, 1968.

[41] ISO (International Standard of Organisation)/ PAS 21448: Safety of the intended functionality. 2019.

[42] ISO (International Standard of Organisation)/SAE (Society of Automotive Engineers) 21434. 2021.

[43] Guideline for Developing National Internet of Vehicles Industry Standard System (Intelligent & Connected Vehicle) Released by Ministry of Industry and Information Technology of the People ’ s Republic of China and Standardizatio. Ministry of Industry and Information Technology of the Peoples/ Republic of China and Standardization Administration of the Peoples/ Republic of China, 2018.

[44] “Funktionale Sicherheit: Der Schutz des Menschen vor der Maschine.” [Online]. Available: https://www.dke.de/de/arbeitsfelder/core-safety/funktionale-sicherheit. [Accessed: 20-Dec-2019].

[45] D. M. Li et al., “Abundance of toxic and non-toxic microcystis sp. in Lake Hongze and its correlation with environmental factors,” Huanjing Kexue/Environmental Sci., 2016.

[46] IEC (Elektrotechnische Kommission) 61508. 1998.

[47] L. Schnieder and R. Hosse, Safety of the Intended Functionality. Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2019.

[48] M. Hillenbrand, “Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen,” Institut für Technik der Informationsverarbeitung, 2012.

[49] J. Oscarsson, “Functional Safety in Co-operative Driving using Systems-Theoretic Process Analysis,” KTH Royal Intitute of Technology, 2016.

[50] A. Mallya, V. Pantelic, M. Adejouma, M. Lawford, and A. Wassyng, “Using STPA in an ISO 26262 Compliant Process,” in Computer Science, 2016.

[51] “ISO26262, flow of workproducts visualized.” [Online]. Available: https://icomod.com/ressources/aux-and-goodies/iso26262-flow-of-workproducts-

visualized/. [Accessed: 11-Oct-2021].

[52] H. S. Mahajan, T. Bradley, and S. Pasricha, “Application of Systems Theoretic Process Analysis to a Lane Keeping Assist System,” Reliab. Eng. Syst. Saf., 2017.

[53] Aerospace recommended Practice ARP4754. 1996.

[54] A. Schwierz, G. Seifert, and S. Hiergeist, “Funktionale sicherheit in Automotive und Avionik: Ein Staffellauf,” in Automotive Safety and Security 2017, 2017.

[55] M. Heininger and H. Hammerer, “Leistungselektronik nach ISO 26262 prüfen,” ATZelektronik, pp. 46–51, 2015.

[56] M. Abele, “Modellierung und Bewertung hochzuverlässiger Energiebordnetz-Architekturen für sicherheitsrelevante Verbraucher in Kraftfahrzeugen,” Universität Kassel, 2008.

[57] A. Avizienis, J.-C. Laprie, and B. Randell, “Fundamental Concepts of Dependability,” 2001. [Online]. Available: https://people.cs.rutgers.edu/~rmartin/teaching/spring03/cs553/readings/avizienis00.pdf. [Accessed: 11-Oct-2021].

[58] E. Böde et al., “Identifikation und Quantifizierung von Automationsrisiken für hochautomatisierte Fahrfunktionen Technical Report,” 2019.

[59] P. Leon and Kiencke, Messtechnik. Springer-Verlag Berlin Heidelberg, 2011.

[60] S. Khastgir, S. Birrell, G. Dhadyalla, H. Sivencrona, and P. Jennings, “Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems,” Saf. Sci., vol. 99, pp. 166–177, 2017.

[61] Handelsblatt GmbH, “Warum die Autobauer neue Partner brauchen.” [Online]. Available: https://www.wiwo.de/unternehmen/auto/autonomes-fahren-qualitaet-der-ki-entscheidet/20474922-3.html. [Accessed: 11-Oct-2021].

[62] B. Klamann, M. Lippert, C. Amersbach, and H. Winner, “Defining Pass-/Fail-Criteria for Particular Tests of Automated Driving Functions,” 2019.

[63] T. Heck, “Entwicklung eines Konzeptes zur Implementierung von Regelalgorithmen im Rahmen einer STPA und dessen Umsetzung in,” Universität Stuttgart, 2019.

[64] F. Romeike and P. Hager, “Risiko-Management in der Produktion.” [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7278271/. [Accessed: 11-Oct-2021].

[65] Analysis techniques for system reliability - Procedure for failure mode and effects

analysis (FMEA) (IEC 60812:2006). 2006.

[66] M. Xie and T. N. Goh, “FMEA: Failure mode and effects analysis,” 2012.

[67] S. M. Sulaman, A. Beer, M. Felderer, and M. Höst, “Comparison of the FMEA and STPA safety analysis methods–a case study,” Softw. Qual. J., 2017.

[68] T. Kurtoglu and I. Y. Tumer, “A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems,” J. Mech. Des., 2008.

[69] G. Menkhaus and B. Andrich, “Metric Suite for Directing the Failure Mode Analysis of Embedded Software Systems,” 2005.

[70] B. D. Owens, M. Stringfellow Herring, N. Dulac, N. G. Leveson, M. D. Ingham, and K. A. Weiss, “Application of a Safety-Driven Design Methodology to an Outer Planet Exploration Mission,” in IEEE Aerospace Conference, 2008.

[71] Harald Altinger et.al, “Testing Methods Used in the Automotive Industry: Results from a Survey,” Jamaica Workshop, 2014.

[72] “Sicherheitsanalyse - Kombination der Techniken.” [Online]. Available: https://uol.de/f/2/dept/informatik/ag/lks/download/abteilung/sicherheitsanalyse-tutorial.pdf. [Accessed: 11-Oct-2021].

[73] H. Nakao, M. Katahira, Y. Miyamoto, and N. Leveson, “SAFETY GUIDED DESIGN OF CREW RETURN VEHICLE IN CONCEPT DESIGN PHASE USING STAMP / STPA,” in 5th IAASS Conference A Safer Space for Safer World, 2012.

[74] P. Kafka, Probabilistic Risk Assessment for Nuclear Power Plants. London: Springer, 2008.

[75] C. Wassilew, “Workshop – Risikomanagement,” Bonn, 2005.

[76] VDI, “Systematische Methoden zur Gefährdungsbeurteilung Inhaltsübersicht,” in Ratgeber Anlagensicherheit 12/04, .

[77] J. Zhang, H. Kim, Y. Liu, and M. A. Lundteigen, “Combining system-theoretic process analysis and availability assessment: A subsea case study,” Proc. Inst. Mech. Eng. Part O J. Risk Reliab., 2019.

[78] M. Luft, “Einführung in die Systemtheorie (Systematik).” [Online]. Available: http://www.philoreal.de/websystem/systemtheorie.html. [Accessed: 11-Oct-2021].

[79] L. von Bertalanffy, General System Theory (Foundation, Development, Applications). New York: George Braziller, 1976.

[80] D. H. Meadows, Thinking in Syatems. Earthscan: TJ International Ltd, 2009.

[81] P. Checkland, Systems Thinking, Systems Practice. New York: John Wiley & Sons Ltd, 1981.

[82] T. Ishimatsu, N. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, and H. Nakao, “Modeling and Hazard Analysis Using STPA,” in Proceedings of the 4th IAASS Conference, Making Safety Matter, 2010.

[83] R. Hegde, K. Post, S. Nuesch, and S. Yako, Systems Theoretic Process Analysis for Layers of System Safety. Orlando: Annual INCOSE international symposium, 2019.

[84] N. G. Leveson et al., “Accessed Hazard Analysis of Complex Spacecraft using Systems-Theoretic Process Analysis,” J. Spacecr. Rockets, 2014.

[85] VDA, Präventive Qualitätsmanagement-Methoden in der Prozesslandschaft, Auswahl – Anwendung – Nutzen Band 14. Springer Professional, 2008.

[86] J. Thomas, “Extending and automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis,” Massachusitts Institute of Technologie, 2013.

[87] A. Abdulkhaleq and S. Wagner, “A Software Safety Verification Method Based on System-Theoretic Process Analysis,” in SAFECOMP 2014, 2015.

[88] A. Abdulkhaleq and D. Lammering, Using STPA in Compliance with ISO 26262. Automotive -Safety and Security 2017, 2017.

[89] F. Yan, T. Tang, and H. Yan, “Scenario based STPA analysis in Automated Urban Guided Transport system,” 2016 IEEE Int. Conf. Intell. Rail Transp. ICIRT 2016, pp. 425–431, 2016.

[90] P. Sundaram and D. Hartfelder, “Compatibility of STPA with GM System Safety Engineering Process,” 2013. [Online]. Available: http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/04_Sundaram_GM_STPA_Study_Presentation_MIT.pdf. [Accessed: 11-Oct-2021].

[91] N. Leveson, “A new accident model for engineering safer systems,” Saf. Sci., vol. 42, no. 4, pp. 237–270, 2004.

[92] The International Marine Contractors Association, “Failure Modes & Effects Analyses (FMEAs),” 2002. [Online]. Available: http://dp-courses.am.szczecin.pl/userfiles/IMCA_circulars/IMCA_M_166.pdf. [Accessed: 11-Oct-2021].

[93] I. Teßmer, “Qualitative und quantitative Methoden zur systematischen Risikoanalyse

von verfahrenstechnischen Anlagen," Neuruppin: TK Verlag Karl Thomé-Kozmiensky, 2012, pp. 139–152.

[94] C. H. Fleming, M. Spencer, N. Leveson, and C. Wilkinson, Safety Assurance in NextGen. NASA, 2012.

[95] N. Leveson, A new approach to hazard analysis for complex systems. Ottawa: International Conference of the System Safety Society, 2003.

[96] A. Abdulkhaleq, S. Wagner, and N. Leveson, "A comprehensive safety engineering approach for software-intensive systems Based on STPA," Elsevier B.V., Tokyo, 2015.

[97] A. Abdulkhaleq, M. Baumeister, H. Böhmert, and S. Wagner, "Missing no Interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems," Int. J. Saf. Sci., vol. 02, no. 01, pp. 115–124, 2018.

[98] S. M. Sulaman, T. . Abbas, K. . Wnuk, M. Höst, and K. Wnuk, Hazard analysis of collision avoidance system using STPA. Pennsylvania: ISCRAM 2014, 2014.

[99] R. S. Martinez, "System Theoretic Process Analysis of Electric Power Steering for Automotive Applications," Massachusetts Institute of Technology, 2015.

[100] L. Balzer, "Human Factor Analyse eines zukünftigen Systems zum automatisierten Fahren mittels STPA und Evaluation des Mehrwerts ggü. traditionellen Verfahren," University Stuttgart, 2018.

[101] S. Placke, J. Thomas, and D. Suo, Integration of Multiple Active Safety Systems using STPA Systems Theoretic Process Analysis (STPA). SAE Technical Paper, 2015.

[102] R. Hosse, G. Bagschik, M. Marer, K. Bengler, and U. Becker, Evolution Issues of Automated Driving Functions by Application of Systemic Accident Analysis. STAMP Workshop 2017, 2017.

[103] L. C. Wei and S. E. Madnick, "A System Theoretic Approach to Cybersecurity Risk Analysis and Mitigation for Autonomous Passenger Vehicles," SSRN Electron. J., 2019.

[104] S. Sharma, A. Flores, C. Hobbs, J. Stafford, and S. Fischmeister, Safety and security analysis of AEB for L4 autonomous vehicle using STPA. Workshop on Autonomous Systems Design (ASD), 2019.

[105] S. Wagner, D. Lammering, and H. Boehmert, "Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehiclesm," in Automotive - Safety & Security 2017, 2017.

[106] C.V.A., "Ist kreatives Arbeiten unter zeitdruck möglich?," 2014. [Online]. Available:

https://uni.de/redaktion/kreatives-arbeiten-unter-zeitdruck. [Accessed: 11-Oct-2021].

[107] A. Pütz, A. Zlocki, and L. Eckstein, “Absicherung hochautomatisierter Fahrfunktionen mithilfe einer Datenbank relevanter Szenarien,” 11. Work. Fahrerassistenzsysteme und Autom. Fahr., pp. 161–168, 2017.

A Anhang: STPA Ergebnisse Systemunfälle, Systemgefahren, Anforderungen, Kontrollstrukturen

A.1 Systemunfälle

Im ersten Schritt der STPA müssen die systemtechnischen Grundlagen formuliert werden. Diese bestehen in der Definition der Unfälle, Gefahren und Sicherheitsbeschränkungen. Die Unfälle in Tabelle C.1 sind Ergebnis der STPA angewendet auf die Automatisierungsstufen Level vier und fünf und werden daher gemeinsam aufgelistet.

Tabelle C. 1: Unfälle aus der STPA, formuliert für ein Fahrzeug Level vier und fünf

Nr.	Beschreibung
U-1	Menschen werden physisch/psychisch verletzt
U-2	Eigentum wird zerstört
U-3	Umweltverschmutzung
U-4	Verlust der Mission
U-5	Verlust sensitiver Informationen
U-6	Verlust des Rufes des Automobilherstellers/Automobilindustrie

A.2 Systemgefahren

Im zweiten Schritt werden die Systemgefahren formuliert, welche zu den im ersten Teilschritt definierten Unfällen führen. Eine Gefahr muss nicht zwangsläufig in einem einzigen Unfall resultieren, sondern kann Auslöser mehrerer Unfälle sein. In Tabelle C.2 sind die modellierten Systemgefahren und die verlinkten Unfälle für ein Fahrzeug Level vier und fünf aufgelistet.

Tabelle C. 2: Systemgefahren für ein Fahrzeug Level vier und fünf

Nr.	Gefahr	U
H-1	Dem automatisierten/autonomen Fahrzeug stehen keine Daten der Fahrumgebung zur Verfügung.	1, 2, 3, 4, 6
H-2	Menschen sind während des Aufenthaltes im und im Umkreis des Fahrzeugs schädlichen Bedingungen ausgesetzt.	1,4,6
H-3	Leistungs- bzw. Belastungsgrenzen von Teilsystemen werden nicht eingehalten.	1, 2, 3, 4, 5, 6
H-4	Supportstrukturen sind nicht adäquat vorhanden, um Personen in Not zu unterstützen.	1, 2, 3, 6
H-5	Das Fahrzeug fährt in unsichere Gebiete.	1, 2, 3, 4, 5, 6
H-6	Das Fahrzeug wird manövrierunfähig.	1, 2, 3, 4, 6
H-7	Nicht autorisierte Personen haben Zugriff auf das Fahrzeug.	1, 2, 3, 4, 5, 6
H-8	Die Nutzung des Fahrzeugs verletzt internationale bzw. nationale Regularien.	1, 4, 5, 6
H-9	Der Lebenszyklus eines Fahrzeugs ist inakzeptabel umweltschädlich.	3, 6
H-10	Das Fahrzeug und die mit dem Fahrzeug tangierenden Strukturen unterliegen unzureichenden Standards.	1, 2, 3, 4, 5, 6
H-11	Sensitive Informationen gehen verloren.	1, 5, 6
H-12	Der Zielort wird nicht zum erwarteten Zeitpunkt erreicht.	3, 4, 6
H-13	Solltrajektorie zwischen Fahrzeug und anderen Objekten wird nicht eingehalten.	1, 2, 3, 4, 5, 6

A.3 Sicherheitsbeschränkungen

Im nächsten Schritt werden Sicherheitsanforderungen vorgestellt, um die identifizierten Gefahren zu eliminieren. Die Sicherheitsanforderungen gelten für beide Automatisierungsstufen und sind in Tabelle C.3 zusammengefasst. Jeder Sicherheitsanforderung werden diejenigen Gefahren zugeordnet, welche durch die jeweilige Sicherheitsanforderung eliminiert wird.

Tabelle C. 3: Sicherheitsbeschränkungen abgeleitet aus spezifischen Gefahren

Nr.	Beschreibung	G
SC-1	Dem Fahrzeug müssen während der Nutzung zu jedem Zeitpunkt aktuelle, prädizierte, retrospektive Umgebungsdaten vorliegen.	1, 2, 4, 5, 6, 10
SC-2	Menschen um/im Fahrzeug dürfen zu keinem Zeitpunkt schädlichen (physischen und psychischen) Bedingungen ausgesetzt werden.	1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13
SC-3	Das Fahrzeug muss im automatisierten Betriebsmodus bzw. autonom in dem für ihn vorgesehenen Umgebungsbereich betrieben werden.	1, 2, 4, 5, 6, 8, 10, 12, 13
SC-8	Fahrzeugübergreifende Objekte/Personen/Instanzen müssen das Fahrzeug hinreichend sicher bedienen.	1, 2, 6, 7, 12
SC-10	Das Fahrzeug muss die situationsspezifischen Mindestabstände jederzeit zu anderen Objekten/Menschen/Substanzen einhalten.	1, 2, 5, 12
SC-12	Das Fahrzeug muss während der Fahrt jederzeit manövrierfähig sein.	1, 2, 5, 6
SC-13	Der Informationsfluss muss von und zu nicht autorisierten Personen bzw. Objekte vom Fahrzeug unterbunden werden.	7
SC-14	Das Fahrzeug muss Personen in Not im Bereich der Fahrumgebung sowie im Fahrzeug Unterstützung leisten.	2, 4, 7, 10
SC-15	Die am Straßenverkehr teilnehmenden Fahrzeuge müssen den internationalen und nationalen Regularien entsprechen.	8
SC-16	Das Fahrzeug muss entsprechend der gesellschaftlichen Akzeptanz umweltfreundlich betrieben/produziert/verschrottet werden.	2, 8, 9, 10
SC-17	Das Fahrzeug muss die für die jeweilige Fahrt notwendigen Informationen erhalten.	1, 2, 4, 6, 11, 13
SC-18	Sicherheitsstandards müssen für das Fahrzeug und den tangierenden Strukturen hinreichend sein.	1, 2, 3,
SC-23	Das Fahrzeug darf nicht unkontrolliert Energie oder Material freisetzen.	2, 5, 6, 8, 9, 12
SC-25	Die Mission muss innerhalb eines zu erwarteten Zeitraums erfüllt werden.	1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13,12
SC-26	Entwicklungs- und Organisationsstrukturen müssen sich entsprechend des Produktes flexibel an Bedingungen anpassen.	1, 3, 8, 10

A.4 Kontrollstrukturen Fahrzeug Level vier und fünf

Die Kontrollstrukturen, abgeleitet aus den Sicherheitsanforderungen, werden für die Fahrzeugmodelle Level vier und fünf im folgenden Unterkapitel vorgestellt. In Abbildung C.1 ist die überarbeitete Kontrollstruktur des hochautomatisierten Fahrzeugs Level vier, in Abbildung C.2 die Kontrollstruktur des vollautomatisierten Fahrzeugs Level fünf abgebildet. Es werden zunächst die funktionalen Einheiten der Abbildungen erläutert.

Steuerungs- und Regelungssysteme: Steuern und regeln das automatisierte/vollautonome Fahrzeug.

Physikalischer Fahrzeugzustand: Setzt Kontrollaktionen der Steuerungs- und Regelungssysteme um.

Longitudinale Aktuatoren: Umfasst Aktuatoren, die das Fahrzeug beschleunigen oder verzögern.

Laterale Aktuatoren: Lenkung des Fahrzeugs (Gieren, bspw. durch Abbremsen einzelner Räder, sind nicht Bestandteil der Einheit).

Sicherheitskritische Aktuatorik: Aktuatoren, die unabhängig von Längs- und Queraktuatorik, in Abhängigkeit der Umweltbedingung, für eine hinreichend sichere Fahrt notwendig sind, bspw. die Lichtaktuatorik während Nachtfahrten.

Nicht sicherheitskritische Aktuatorik: Aktuatoren, die unabhängig von Längs- und Queraktuatorik, in Abhängigkeit der Umweltbedingung, nicht sicherheitskritisch sind bspw. die Lichtaktuatorik während einer Tagfahrt.

Aktuatoren können situationsbedingt in sicherheitskritische bzw. nicht sicherheitskritische Aktuatorik eingeordnet werden. Die aktivierte Klimaanlage nach einem Crash mit einem in Flammen stehenden Motorraum ist in diesem Modell sicherheitskritisch, hingegen wird ein Crash ohne Brand und aktivierter Klimaanlage als nicht sicherheitskritisch eingeordnet. Regler innerhalb der longitudinalen, lateralen und weiterführenden Aktuatorik werden vernachlässigt.

Fahrzeugsensorik: Erfasst Parameter des physikalischen Fahrzeugzustands und leitet diese an die Steuerungs- und Regelungssysteme des automatisierten Fahrzeugs weiter.

Hersteller: Fungiert unter anderem als kollektive Risikoinstanz.

Sensorische Schnittstelle: Stellvertreter für alle externen Systeme[26], welche digitale Informationen liefern, die innerhalb des Fahrzeugs nicht zur Verfügung stehen und kein Teil der kollektiven Risikoinstanz sind.

HMI: Benutzerschnittstelle zwischen Mensch und Fahrzeug.

Fahrer (Level eins bis vier) bzw. Passagier (Level fünf): Bediener des Fahrzeugs.

Umwelt: Stellt visuelle Umgebungsinformationen bereit.

Im Folgenden sind die Kontrollstrukturen für ein Fahrzeug Level vier und fünf abgebildet. Die blau gefärbten Zahlen sind der Kategorie der Feedbacks, die grünen Zahlen der Kategorie der Kontrollaktionen zugehörig. In den Abbildungen sind die Ausgangskontrollstrukturen, die aus den Anforderungen formuliert wurden, schwarz hinterlegt. Die Elemente, die in der Formulierung der Sicherheitsanforderungen iterativ bestimmt wurden und Auswirkungen auf die Kontrollstruktur hatten, sind rot gekennzeichnet.

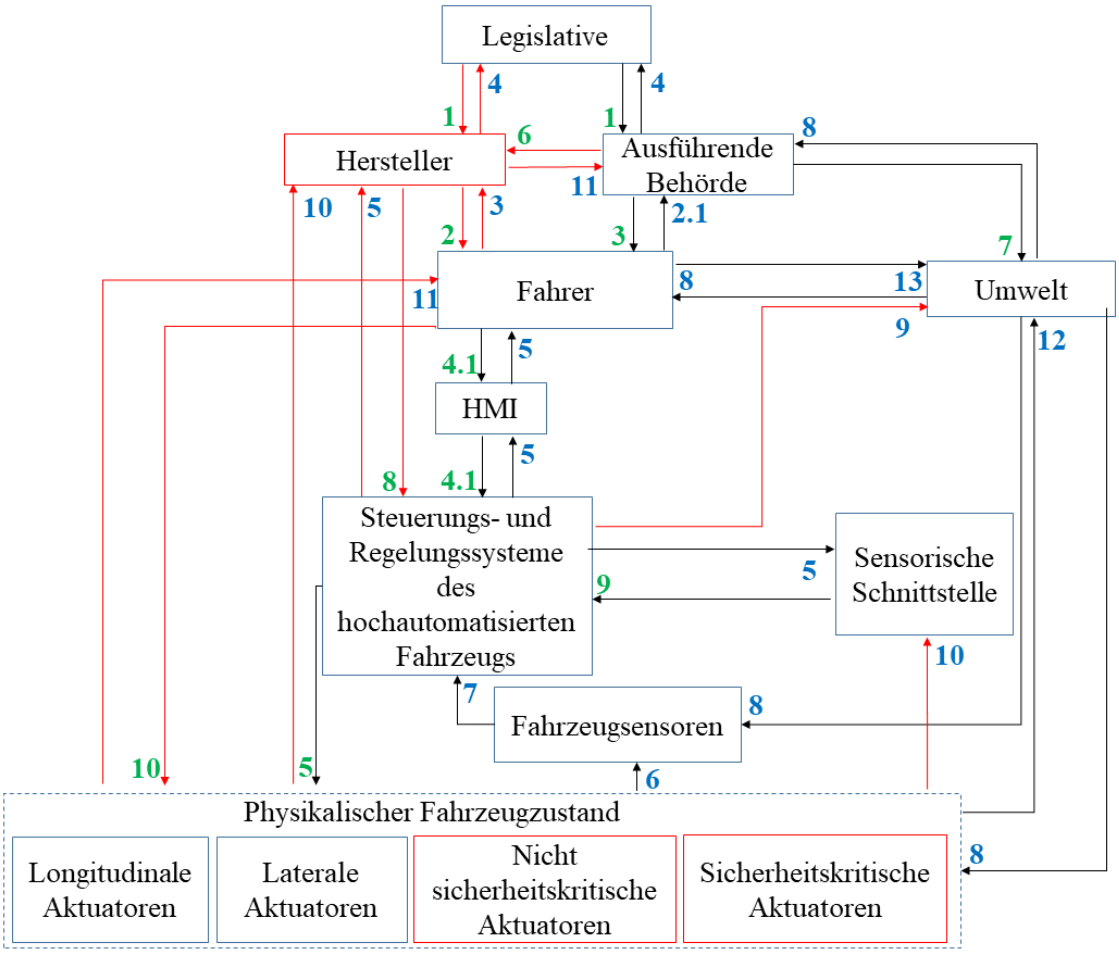

Abbildung C.1: Kontrollstruktur für das Fahrzeug der Automatisierungsstufe vier

[26] Externe Systeme werden als Synonym für fahrzeugsystemübergreifende Systeme terminiert.

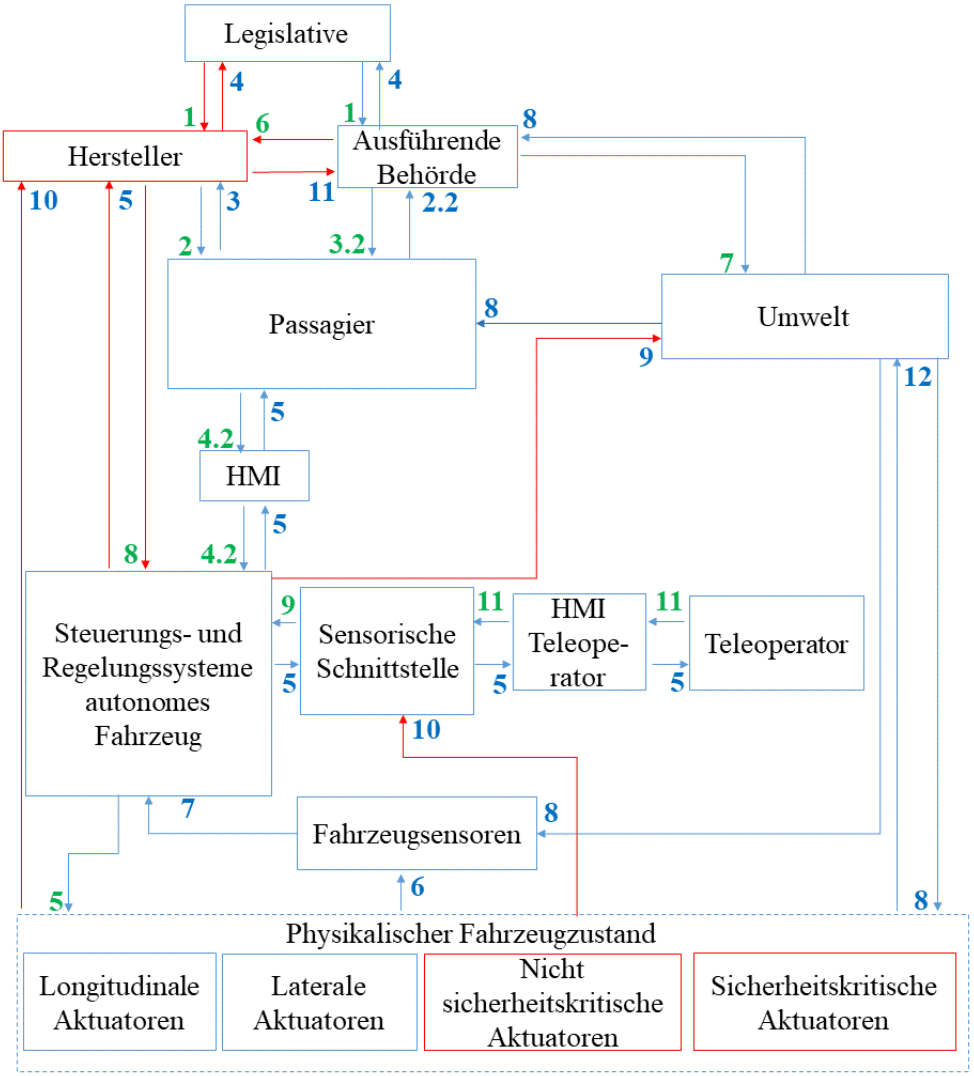

Abbildung C.2: Kontrollstruktur für das Fahrzeug der Automatisierungsstufe fünf

In Tabelle C.4 und Tabelle C.5 sind die Kontrollaktionen und Feedbacks beider Kontrollstrukturen aufgelistet.

Tabelle C.4: Feedbacks der Kontrollstrukturen für das Fahrzeug Level vier und fünf

Nr.	Feedbacks	Erläuterungen
1	Lenkkraft, Pedalkraft, Straßengegebenheiten	Feedback über den physikalischen Fahrzeugzustand übermitteln.
2.1	Ausreichende Prüfungsergebnisse/unzureichende Prüfungsergebnisse des Fahrers um das Fahrzeug hinreichend sicher bedienen bzw. führen zu können	Feedback über die Fähigkeit des Fahrers das Fahrzeug potenziell hinreichend sicher zu führen.
2.2	Ausreichender Wissensstand/unzureichender Wissensstand des Passagiers um das Fahrzeug hinreichend sicher bedienen zu können	Feedback über die Fähigkeit des Passagiers das Fahrzeug potenziell hinreichend sicher zu bedienen.
3	Fahrzeugkauf bzw. Nutzung ja/nein, Feedback über die Konstitution des Fahrzeugs	Feedback über die Konstitution des Fahrzeugs, beispielsweise über Studien vom Hersteller.
4	Gesetze umgesetzt ja/nein	Feedback vom Hersteller und der ausführenden Behörde, bezüglich der Einhaltung von Gesetzen.
5	Physikalischer Fahrzeugzustand, aktueller/prädizierter Fahrzustand, Fahrparameter, sicherheitsrelevante Informationen	Informationen, die der sensorischen Schnittstelle bereitgestellt werden müssen.
6	Physikalischer Fahrzeugzustand, Fahrparameter	Unter Anderem Informationen die den Fahrzeugsensoren bereitgestellt werden.
7	Aktueller Fahrzustand, Physikalischer Fahrzeugzustand, Fahrparameter, Umgebungsinformationen	Unter Anderem Informationen die den Steuerungs- und Regelungssystemen bereitgestellt werden.
8	Umgebungsinformationen	Unter Anderem Informationen die den Fahrzeugsensoren bereitgestellt werden.
9	Physikalischer Fahrzeugzustand, Fahrparameter, aktueller/prädizierter Fahrzustand	Unter Anderem muss der prädizierte Fahrzustand als Feedback der Umwelt übermittelt werden, beispielsweise ob das autonome Fahrzeug die Person am Zebrastreifen erkannt hat.
10	GPS Position Fahrzeug	Die sensorische Schnittstelle muss die GPS Position des Fahrzeugs erfassen.
11	Updates über die Infrastruktur umgesetzt/nicht umgesetzt, Updates über die Konstitution des Fahrzeugs umgesetzt/nicht umgesetzt	Informationen, die der Hersteller der ausführenden Behörde bereitstellen muss.
12	Fahrzustand, Physikalischer Fahrzeugzustand	Unter anderem Informationen die der Umwelt bereitgestellt werden müssen.
13	Mimik, Gestik des Fahrers	Bspw. Augenkontakt mit einem Fußgänger am Zebrastreifen aufnehmen

Tabelle C.5 : Kontrollaktionen für das Fahrzeug Level vier und fünf

Nr.	Kontrollaktionen der Regelstruktur	Erläuterungen
1	Gesetze verabschieden/ updaten	Aktuelle Regularien müssen dem Hersteller und der ausführenden Behörde vorliegen.
2	Bedienungsvorgaben updaten, Gegebenheiten Fahrzeug updaten	Bedienungsvorgaben updaten, zum Beispiel das Fahrzeughandbuch. Die Gegebenheiten des Fahrzeugs überarbeiten, beispielsweise das Design des Innenraums.
3.1	Fahrer zertifizieren/ nicht zertifizieren	Fahrer zertifizieren. Das Fahrzeug überprüft in diesem Modell den adäquaten Fahrerzustand vor Fahrtantritt nicht.
3.2	Passagier zertifizieren/ nicht zertifizieren	Passagier zertifizieren, sodass das Fahrzeug potenziell hinreichend sicher im Straßenverkehr bedienen kann.
4.1	Betriebsmodi manuell bzw. autonom aktivieren/deaktivieren, longitudinal-, lateral-, nichtsicherheitskritische Aktuatorik aktivieren/deaktivieren, sicherheitskritische Aktuatorik aktivieren	Der Fahrer hat während der manuellen Fahrt keinen direkten Zugriff auf das physikalische Fahrzeug. Die Anforderungen werden über die Steuerungs- und Regelungssysteme geleitet und die Daten fusioniert. Sicherheitskritische Aktuatorik kann der Fahrer ausschließlich aktivieren hingegen nicht deaktivieren.
4.2	Nichtsicherheitskritische Aktuatorik aktivieren/deaktivieren, sicherheitskritische Aktuatorik aktivieren	Sicherheitskritische Aktuatorik kann der Passagier ausschließlich aktivieren hingegen nicht deaktivieren.
5	Longitudinal-, lateral-, nichtsicherheitskritische-, sicherheitskritische Aktuatorik aktivieren/deaktivieren	Kontrollaktionen die an den physikalischen Fahrzeugzustand weitergeleitet werden.
6	Updates über die Infrastruktur freigeben/nicht freigeben	Informationen wie beispielsweise über den Aufbau neuer Streckenabschnitte freigeben/ nicht frei geben.
7	Infrastruktur updaten	Informationen die an die Umwelt weitergeleitet werden.
8	Minimum Risk Maneuver (MRM) durchführen/nicht durchführen, Updates Over-The-Air durchführen/nicht durchführen, sicherheitskritische Fahrzustände überwachen/nicht überwachen	Kontrollaktionen die vom Hersteller an die Steuerung- und Regelungssysteme weitergeleitet werden.
9	Weitergabe des aktuellen/ prädizierten Status Fahrumgebung, Weitergabe sicherheitsrelevanter Informationen, Längs- und Querregelung	Aktueller und prädizierter Status Fahrumgebung beispielsweise über Car-to-X Kommunikation weiterleiten. Längs- und Querregelung bis maximal x km/h muss durch Sicherheitskräfte möglich sein.
10	Fahrzeug öffnen/schließen	Die Möglichkeit das Fahrzeug verlassen und einsteigen zu können.
11	Betriebsmodi teleoperieren bzw. autonom aktivieren/deaktivieren, longitudinal-, lateral-, sicherheitskritische Aktuatorik aktivieren	Anforderungen des Teleoperators werden über die sensorische Schnittstelle geleitet. Sicherheitskritische Aktuatorik kann der Teleoperator ausschließlich aktivieren hingegen nicht deaktivieren.

A.5 Unsichere Kontrollaktionen und Sicherheitsanforderungen

Zusammenfassend konnten in der STPA für das Fahrzeug Level vier über 270 Anforderungen aus 252 unsicheren Kontrollaktionen formuliert werden. Im Folgenden werden die definierten Regelkreise[27], mit den daraus abgeleiteten unsicheren Kontrollaktionen und Sicherheitsanforderungen vorgestellt. Die Ergebnisse werden mit Hilfe von Tabellen dargelegt. In Tabelle C.6 wird stellvertretend für die gesamten Kontrollaktionen anhand eines Beispiels einer Kontrollaktion aus dem Regelkreis HMI-Steuerungs- und Regelungssysteme Sicherheitsanforderungen und die unsicheren Kontrollaktionen vorgestellt.

Tabelle C.6: Unsichere Kontrollaktion identifiziert aus dem Regelkreis HMI-Steuerungs- und Regelungssysteme- Fahrer für ein Fahrzeug Level vier

Gefahr: Solltrajektorie zwischen Fahrzeug und anderen Objekten wird nicht eingehalten.				
Kontrollaktion	**Nicht bereitgestellte Kontrollaktion die zu einer Gefahr führt**	**Bereitgestellte Kontrollaktion die zu einer Gefahr führt**	**Kontrollaktion wird zu früh/zu spät/falsch bereitgestellt, die zu einer Gefahr führt**	**Kontrollaktion wird zu früh gestoppt/zu lange durchgeführt was zu einer Gefahr führt**
Betriebsmodus „Autonom“ aktivieren	**UCA-1**: Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen nicht bereit, während der Fahrer die autonome Fahrfunktion aktiviert hat.	**UCA-2**: Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen bereit, während der Fahrer diese nicht angefordert hat.	**UCA-3**: Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen zu früh bereit, während der Fahrer zu dem Zeitpunkt mit einer manuellen Fahrt rechnet.	**UCA-4**: Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen zu spät bereit, wenn der Fahrer nicht in der Lage ist, manuell zu fahren.

[27] Siehe Kapitel 7.2.4

Die in Tabelle C.6 identifizierten unsicheren Kontrollaktionen werden in folgende Sicherheitsanforderungen formuliert:

UCA-1: Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen nicht bereit, während der Fahrer die autonome Fahrfunktion aktiviert hat.

SC-1: Es muss sichergestellt werden, dass die HMI Schnittstelle keine nicht autorisierten Anforderungen umsetzt.

UCA-2: Die HMI Schnittstelle leitet die Anforderung der Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen vom Fahrer weiter, während das Fahrzeug nicht in der Lage ist autonom zu fahren.

SC-2: Es muss sichergestellt werden, dass der Fahrer die autonome Fahrfunktion, x Sekunden bevor das das Fahrzeug nicht autonom geführt werden kann, nicht aktivieren kann.

UCA-3: Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen zu früh bereit, während der Fahrer zu dem Zeitpunkt mit einer manuellen Fahrt rechnet

SC-3: Es muss sichergestellt werden, dass der Fahrmoduswechsel innerhalb von x Sekunden stattfindet, wenn die Übernahmephase manuell in autonom beendet ist.

UCA-4: Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion den Steuerungs- und Regelungssystemen zu spät bereit, wenn der Fahrer nicht mehr in der Lage ist manuell zu fahren.

SC-4: Es muss ein MRM eingeleitet werden, wenn der Fahrer nicht manövrierfähig ist, und das Fahrzeug innerhalb von x Sekunden nicht autonom fahren kann.

Im Anhang B werden die identifizierten unischeren Kontrollaktionen und die Sicherheitsanforderungen der STPA vorgestellt. Die unsicheren Kontrollaktionen und Sicherheitsanforderungen des Fahrzeugs Level vier und fünf werden regelkreisspezifisch in Tabellen aufgelistet.

B Anhang: Ergebnisse Sicherheitsanforderungen und unsichere Kontrollaktionen

B.1 Regelkreise „Legislative-Hersteller-Ausführende Behörde“

Tabelle B.1: Unsichere Kontrollaktionen aus den Regelkreisen “Legislative-Hersteller-Ausführende Behörde” Level vier und fünf

UCA „Legislative-Hersteller-Ausführende Behörde“ Level vier und fünf	
1	Legislative erlässt keine Gesetze, während die Entwicklung von Fahrzeugen umweltschädlich/personenschädlich ist.
2	Legislative erlässt keine Gesetze, während die Bedienung/Nutzung von Fahrzeugen umweltschädlich/personenschädlich ist.
3	Legislative stellt Normen bereit, die während der Entwicklung von Fahrzeugen umweltschädliche/personenschädliche Anreize setzt.
4	Legislative erlässt Gesetze zu spät während Umwelt bzw. Personen schädlichen Bedingungen ausgesetzt sind.
5	Legislative erlässt Gesetze zu früh während Umwelt bzw. Personen schädlichen Bedingungen ausgesetzt sind.
6	Behörde stellt Einweisungen bereit, während die ausführende Behörde nicht in der Lage ist die Einweisungen umzusetzen.
7	Behörde stellt keine adäquaten Einweisungen bereit, wenn die ausführende Behörde die vorgegebenen Einweisungen nicht ausführen kann.
8	Behörde stellt Einweisungen bereit, während die ausführende Behörde andere bzw. unvollständige Einweisungen durchführt.
9	Behörde stellt Einweisungen zu früh bereit, während Fahrzeuge/Straßenverkehr/Personen im Straßenverkehr auf die aktuellen Reglementierungen nicht angepasst sind.
10	Behörde stellt Einweisungen zu früh bereit, während die notwendigen Gesetze nicht erlassen sind.
11	Behörde stellt Einweisungen bereit, während die ausführende Behörde die neuen Einweisungen nicht adäquat umsetzen kann.
12	Behörde stellt Einweisungen zu spät bereit, während neue Gesetze erlassen sind, die neue Einweisungen erfordern.
13	Behörde stellt neue Einweisungen zu spät bereit, während alte Prozeduren von ausführender Behörde aufgrund von Umweltbedingungen nicht mehr durchgeführt werden können.
14	Die Behörde gibt Einweisungen vor, die dem Ziel einer gesetzlichen Veränderung nicht angemessen sind.

Tabelle B.2: Sicherheitsanforderungen für die Regelkreise „Legislative-Hersteller-Ausführende Behörde“ Level vier und fünf

SC „Legislative-Hersteller-Ausführende Behörde“ Level vier und fünf		Beschreibung
1	Es muss sichergestellt werden, dass eine hinreichend sichere Fahrt länderübergreifend durchgeführt werden kann.	Verkehrszeichen, Straßenbegrenzungsmarkierungen
2	Es muss sichergestellt werden, dass die Informationsübertragung über die sensorische Schnittstelle länderübergreifend normiert wird.	Datenübertragungsraten usw. Infrastrukturelle Unterschiede bezüglich Informationsübertragung müssen global angepasst werden.
3	Es muss sichergestellt werden, dass Wartungsintervalle nach x gefahrenen km x Mal durchgeführt werden.	
4	Es muss sichergestellt werden, dass die Infrastruktur in x Tagen x Mal sowie auf Basis von spezifischen Umweltbedingungen (z. B. Unwetter) variabel gewartet wird, damit dem Fahrzeug adäquate Merkmale für die automatisierte Fahrt vorliegen.	Fraglich ist, ob das autonome Fahrzeug ein Nischenprodukt wird. Wenn ja, lohnt es sich dann diesen Aufwand zu betreiben? Hoher Kostenaufwand. Wenn autonome Fahrzeuge zugelassen werden, ist die Wartung jedoch eine Notwendigkeit.
5	Es muss sichergestellt werden, dass im autonomen Fahrzeug ein Tutorial bezüglich der Nutzung des Fahrzeugs bereitgestellt wird, wenn Updates aufgespielt werden, die das Bedienkonzept im Vergleich zum vorherigen Bedienkonzept verändert haben.	
6	Es muss sichergestellt werden, dass das Tutorial zur Bedienung x Sekunden, nachdem ein Bedienupdate auf das Fahrzeug aufgespielt wurde, zur Verfügung steht.	
7	Es muss sichergestellt werden, dass das Tutorial zur Bedienung des Fahrzeugs ausschließlich in einer für die Dauer des Tutorials notwendigen Zeit, in einem sicheren Zustand durchgeführt werden kann.	
8	Es muss sichergestellt werden, dass Warnsignale der HMI Schnittstelle an den Fahrer/Passagier jederzeit verständlich in Abhängigkeit der Umweltsituation interpretierbar sind.	Wie viel Personalisierung ist in einem autonomen Fahrzeug akzeptabel? Warnsignale werden aufgrund spezifischer Charakteristika (Ton, Tonfolge usw.) als Warnsignal gedeutet (Polizeisirene). Länderübergreifend personalisieren spezifisch im Hinblick wandelnder Mobilitätskonzepte?
9	Es muss sichergestellt werden, dass die Infrastruktur angepasst wird, bevor das erste Fahrzeug mit veränderten Anforderungen im Straßenverkehr am Straßenverkehr teilnimmt.	Bsp: Parkbuchten zum sicheren Ein- und Ausstieg aus dem Fahrzeug
10	Es muss sichergestellt werden, dass ein unabhängiges Risikomanagement gegründet wird, welches sicherheitskritische Prozesse im Straßenverkehr und im Fahrzeug untersucht.	Eine Organisation muss die Feedbackprozesse adäquat auswerten und daraus geeignete Maßnahmen ableiten (ausschließlich autorisierte Updates laden, Softwareupdates autorisieren)

Tabelle B.3: Sicherheitsanforderungen für den Regelkreis "Legislative-Hersteller-Ausführende Behörde" Level vier und fünf

11	Es muss sichergestellt werden, dass das Risikomanagement nicht von Interessen außerhalb des Sicherheitsaspektes manipuliert/beeinflusst werden kann.	
12	Es muss sichergestellt werden, dass die Bedienung des Fahrzeugs in dem jeweiligen Medium der Informationsübertragung des jeweiligen Nutzers/Fahrers durchgeführt werden kann.	Sicherheitsfaktor: Nicht die Gesamtheit der Nutzer sprechen/verstehen beispielsweise Englisch bzw. Deutsch. Weiter sind nicht alle Personen in der Lage beispielsweise akustisch oder visuell Informationen aufzunehmen.
13	Es muss sichergestellt werden, dass die Infrastruktur entsprechend ausgebaut ist, sodass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs und gleichzeitig der Nutzer das Fahrzeug hinreichend sicher bedienen können.	Verkehrszeichen für eine autonome Fahrt müssen vom Fahrer, von Personen außerhalb des Fahrzeugs und von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs erkannt werden.
14	Es muss sichergestellt werden, dass die Updates von der Behörde an die ausführende Behörde adäquat übermittelt werden.	
15	Es muss sichergestellt werden, dass Informationen an die Umwelt und an den Fahrer/Passagier innerhalb von x Sekunden übertragen werden.	
16	Es muss sichergestellt werden, dass die Infrastruktur entsprechend ausgebaut ist, sodass Personen außerhalb des Fahrzeugs im Mischverkehr keinen schädlichen Bedingungen ausgesetzt sind.	
17	Es muss sichergestellt werden, dass die Datenübertragungsraten über die sensorische Schnittstelle in jedem Gebiet, in dem automatisiert gefahren wird, eine Abweichung von maximal x ms zur Referenzdatenübertragung aufweisen.	Beispielsweise im Level fünf: Straßenverkehrsordnung erlernen, damit nach einem Unfall der Fahrer die Verkehrssituation einschätzen kann Level vier: Bedienung des Fahrzeugs im manuellen Betriebsmodus.
18	Die Behörde muss die aktuellen Einweisungen für den Fahrer innerhalb von x Tagen bereitstellen, nachdem die Gesetze erlassen werden.	
19	Die Infrastruktur muss innerhalb von x Tagen verändert werden, nachdem Gesetze, die eine Veränderung der Infrastruktur fordern, erlassen werden.	
20	Es muss sichergestellt werden, dass die Automobilindustrie x Tage nach Ratifizierung der Gesetze Veränderungen umsetzt.	
21	Die Einweisungen, vorgegeben von der Behörde, müssen von der auszuführenden Behörde in einem Zeitraum von x Tagen durchführbar sein.	Wenn eine Person das automatisierte Fahrzeug x Jahre nicht nutzt, und x kritische Updates aufgespielt werden, wie sollen diese an die vorherigen anknüpfen?

Tabelle B.4: Sicherheitsanforderungen für den Regelkreis "Legislative-Hersteller-Ausführende Behörde" Level vier und fünf

22	Es muss sichergestellt werden, dass Kontrollen durchgeführt werden, sodass der Fahrer/Passagier nach x kritischen Sicherheitsupdates das Fahrzeug hinreichend sicher bedienen kann.	
23	Es muss sichergestellt werden, dass Werkstätten in der Lage sind, automatisierte Fahrzeuge hinreichend warten zu können.	Autonomes Fahrzeug muss bspw. autonom auf die Hebebühne gefahren werden können. Normierte Werkstätten als regulatorische Maßnahme?
24	Es muss sichergestellt werden, dass Maßnahmen eingeleitet werden, um Personen außerhalb des automatisierten Fahrzeugs erste Hilfe zu leisten.	Autonomes Fahrzeug bzw. Fahrzeug im automatisierten Fahrzeug kann nicht einschätzen, ob eine verunfallte Person Hilfe benötigt, Abgrenzung zur Verkehrskontrolle? Ähnliche Charakteristika. Wie soll beispielsweise ein autonomes Fahrzeug innerhalb von maximal x Metern Umkreis anhalten, ohne Verkehrsregeln zu brechen.
25	Es muss sichergestellt werden, dass die Verfügbarkeitsanforderung des autonomen Betriebsmodus bei >x % im Verhältnis zur Gesamtstrecke liegt, wenn ein Fahrzeug als automatisiertes Fahrzeug verkauft wird.	Sind große Teile autonomer bzw. automatisierter Fahrten nicht freigegeben, dann sollte das Fahrzeug nicht als autonomes Fahrzeug verkauft werden. (Verlust des Images des Automobilherstellers)
26	Es muss sichergestellt werden, dass die Darstellungsweise der HMI Schnittstelle automobilherstellerübergreifend und länderübergreifend gesetzlich vereinheitlicht wird.	Fahrer sollten sich nicht bei Fahrtantritt auf unterschiedliche Designs einstellen (hebt das Gefahrenpotential). Layout der Betriebsorganisation könnte sich verändern, nicht jede Person besitzt ein Fahrzeug, Fahrzeuge werden der Allgemeinheit angeboten, wechselnde Bedienkonzepte heben das Gefahrenpotential an, wenn sie sicherheitskritischer Struktur unterliegen.
27	Es muss sichergestellt werden, dass Anhänger und Aufbauten, welche die äußere Form des Fahrzeugs verändern, nicht hinzugefügt werden, ohne dass die Steuerungs- und Regelungssysteme die veränderten Abmessungen kalkuliert hat.	
28	Es muss sichergestellt werden, dass Updates bezüglich Aktualisierungen der Navigationsdaten/Straßendaten herstellerübergreifend geladen werden.	Es muss ein Mindestmaß an Sicherheit bezüglich Navigationsdaten eingeführt werden (wie beispielsweise Mindestanforderungen für Airbags). Nachregulierung in diesem neuen Umfeld scheint notwendig.
29	Es muss sichergestellt werden, dass während der manuellen Fahrt der Fahrer über sicherheitsrelevante Informationen von der HMI Schnittstelle informiert wird.	Bsp: Aquaplaning auf Streckenabschnitt, Falschfahrer, heutzutage noch nicht verpflichtend. Regulatorische Maßnahme notwendig?
30	Es muss sichergestellt werden, dass bei Missachtung von Regeln eine angemessene Bestrafung des Verantwortlichen erfolgt.	

Tabelle B.5: Sicherheitsanforderungen aus dem Regelkreis "Legislative-Hersteller-Ausführende Behörde" Level vier

SC Level vier		Beschreibung
31	Es muss sichergestellt werden, dass der Fahrer das autonome Fahrzeug Level vier physisch und psychisch hinreichend sicher manuell führen kann, wenn die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs eine Übernahmeanforderung stellen.	Es ist nicht sinnvoll dem Fahrer das Fahrzeug manuell zu übergeben, wenn dieser keine Fahrroutine hat, wenn zuvor hauptsächlich autonom gefahren wurde.
32	Es muss sichergestellt werden, dass im autonomen Fahrzeug bis einschließlich Level vier sich zu jedem Zeitpunkt mindestens ein Fahrer mit Fahrerlaubnis im Fahrzeug befindet.	Auch, wenn die Fahrt ausschließlich autonom bewältigt wird, mit Fahrerlaubnis wird regulatorisch sichergestellt, dass der Fahrer physisch und psychisch in der Lage ist das Fahrzeug hinreichend sicher zu führen (Kein Alkohol am Steuer).
33	Es muss sichergestellt werden, dass der Fahrer das automatisierte Fahrzeug die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs nicht jederzeit überstimmen kann.	Fahrer überstimmt hektisch in einer von ihm unsicher beurteilten Situation. Gefahrenpotential steigt trotzdem, da dieser beispielsweise die Verkehrssituation zuvor nicht adäquat einschätzen konnte. Es wird regulatorisch festgelegt, dass nicht jederzeit überstimmt werden kann.

Tabelle B.6: Sicherheitsanforderungen aus dem Regelkreis „Legislative-Hersteller-ausführende Behörde“ Level fünf

SC Level fünf		Beschreibung
34	Es muss sichergestellt werden, dass das autonome Fahrzeug Level fünf von Personen hinreichend sicher bedient werden kann.	Ist es sinnvoll Personen, die nicht zurechnungsfähig sind, autonom fahren zu lassen?
35	Es muss sichergestellt werden, dass das autonome Fahrzeug Level fünf von körperbehinderten Menschen mit den Behinderungen x hinreichend sicher bedient werden kann.	
36	Es muss sichergestellt werden, dass Wartungspersonal in der Lage ist das autonome Fahrzeug Level fünf bezüglich der Längs- und Querführung anzuleiten.	Beispielsweise Möglichkeit des Rangierens auf Privatgelände.
37	Im autonomen Fahrzeug ist es keine notwendige Bedingung, dass sich mindestens ein Fahrer mit Fahrerlaubnis bei einer Fahrzeuggeschwindigkeit v>0km/h im Fahrzeug befindet.	Kann das vollautonome Fahrzeug die Fahrsituation nicht mehr hinreichend sicher bewältigen, wird teleoperiert bzw. ein MRM eingeleitet.
38	Es muss sichergestellt werden, dass der Fahrer das autonome Fahrzeug nicht überstimmen kann.	
39	Es muss sichergestellt werden, dass der Fahrer des autonomen Fahrzeugs hinsichtlich der Bedienung des autonomen Fahrzeugs zertifiziert wurde.	Fahrer muss informiert sein: "Was mache ich, während eines fehlerhaften Modus" Bedienerlaubnis vs. Fahrerlaubnis: Grobe Vorgehensweisen sollte man kennen als Bediener, Verhalten im Straßenverkehr bei einem Unfall. Wie sicherheitskritisch ist der Ausstieg (Autobahn versus Landstraße).

B.2 Regelkreise „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“

Tabelle B.7: Unsichere Kontrollaktionen aus den Regelkreisen „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für ein Fahrzeug Level vier und fünf

UCA „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ Level vier und fünf	
15	Der Fahrer/Passagier hat die autonome Fahrfunktion nicht aktiviert, während der Fahrer/Passagier nicht in der Lage ist das Fahrzeug manuell zu führen.
16	Der Fahrer/Passagier hat die Aktivierung der autonomen Fahrfunktion bereitgestellt, während das Fahrzeug nicht in der Lage ist autonom zu fahren.
17	Der Fahrer/Passagier hat die autonome Fahrfunktion nicht aktiviert, während die Umweltfaktoren eine Aktivierung der autonomen Funktion erfordert (Maintenance, Ausstieg in der Stadt und das Auto fährt weiter).
18	Die Aktivierung des autonomen Fahrmodus wird bereitgestellt, während Operationen am Fahrzeug durchgeführt werden (Fahrzeug wird während Operation angefragt).
19	Der Fahrer/Passagier hat die autonome Fahrfunktion nicht aktiviert, wenn die Legislative dieses vorgibt.
20	Der Fahrer/Passagier aktiviert die autonome Fahrfunktion, obwohl die HMI Schnittstelle nicht aktiviert ist.
21	Der autonome Fahrmodus wird aktiviert, wenn das Fahrzeug nicht fahrbereit ist (Beispiel: Türen nicht geschlossen).
22	Der Fahrer/Passagier hat die Aktivierung der autonomen Fahrfunktion zu früh bereitgestellt, während das Fahrzeug nicht in der Lage ist autonom zu fahren.
23	Der Fahrer/Passagier hat die Aktivierung der autonomen Fahrfunktion zu spät gestoppt, während die Aktivierung der Fahrfunktion x Sekunden benötigt.
24	Der Fahrer/Passagier hat die Deaktivierung der autonomen Fahrfunktion nicht bereitgestellt, während das Fahrzeug zum Übernahmezeitpunkt nicht autonom betrieben werden konnte.
25	Der Fahrer/Passagier hat die Deaktivierung der autonomen Fahrfunktion bereitgestellt, obwohl die Umwelt mit einer Aktivierung des autonomen Fahrmodus rechnet.
26	Der Fahrer/Passagier hat eine Bedienung der HMI Schnittstelle durchgeführt in einem Zeitraum, in dem die HMI Schnittstelle die Aktion nicht verarbeiten kann.
27	Der Fahrer/Passagier aktiviert die „andere Aktuatorik“ "Hupe" während das Fahrzeug autonom fährt.

Tabelle B.8: UCA aus den Regelkreisen "Fahrer/Passagier-HMI", "HMI-Steuerungs- und Regelungssysteme" und "Fahrer/Passagier-Physikalisches Fahrzeug" für ein Fahrzeug Level vier und fünf

28	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion nicht bereit, während der Fahrer/Passagier die autonome Fahrfunktion aktiviert hat.
29	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion bereit, während der Fahrer/Passagier diese nicht angefordert hat.
30	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion bereit, während das Fahrzeug nicht in der Lage ist autonom zu fahren.
31	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion zu früh bereit, während das Fahrzeug nicht in der Lage ist autonom zu fahren.
32	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion zu spät bereit, während das Fahrzeug nicht in der Lage ist autonom zu fahren.
33	Die HMI Schnittstelle stellt ein Kommando zu früh bereit, wenn das autonome System nicht in der Lage ist die Kontrollaktion umzusetzen.
34	Die Steuerungs- und Regelungssysteme senden der HMI Schnittstelle Informationen, während die HMI Schnittstelle sich außer Betrieb befindet.
35	Die HMI Schnittstelle stellt die Deaktivierung des autonomen Fahrmodus nicht bereit, wenn das Fahrzeug nicht in der Lage ist autonom geführt zu werden.
36	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion zu spät bereit, wenn das Fahrzeug nicht in der Lage ist manuell geführt zu werden (Hinweis: Beispielsweise Teleoperation im autonomen Fahrzeug).
37	Der Fahrer/Passagier hat die Aktivierung der autonomen Fahrfunktion bereitgestellt, während das Fahrzeug nicht in der Lage ist autonom zu fahren.
38	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion zu früh bereit, wenn die Aktivierung zur gleichen Zeit beziehungsweise x Sekunden vorher durchgeführt wird.
39	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion zu früh bereit, wenn das Fahrzeug nicht in der Lage ist manuell geführt zu werden.
40	Die HMI Schnittstelle hat die Deaktivierung der autonomen Fahrfunktion zu früh gestoppt, während der manuelle Fahrmodus in x Sekunden aktiviert wird.
41	Die HMI Schnittstelle hat die Deaktivierung der autonomen Fahrfunktion zu spät gestoppt, während der manuelle Fahrmodus in x Sekunden aktiviert wird.

Tabelle B.9: UCA aus den Regelkreisen "Fahrer/Passagier-HMI", "HMI-Steuerungs- und Regelungssysteme" und "Fahrer/Passagier-Physikalisches Fahrzeug" Level vier

UCA „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ Level vier	
42	Der Fahrer hat die Aktivierung der autonomen Fahrfunktion bereitgestellt, wenn das Fahrzeug nach Übernahmezeit in den autonomen Fahrmodus nicht mehr hinreichend sicher autonom fahren kann.
43	Der Fahrer hat die autonome Fahrfunktion aktiviert, während der Fahrer manuell fährt bzw. fahren wollte.
44	Der Fahrer hat die Aktivierung der autonomen Fahrfunktion zu früh bereitgestellt, während der Fahrer zum Zeitpunkt der Aktivierung darauf eingestellt war manuell zu fahren.
45	Der Fahrer hat die Aktivierung der autonomen Fahrfunktion zu spät bereitgestellt, während der Fahrer nicht in der Lage war das Fahrzeug zu führen, da zu diesem Zeitpunkt die Aktivierung der Fahrfunktion noch nicht abgeschlossen war.
46	Der Fahrer hat die Aktivierung der autonomen Fahrfunktion zu früh gestoppt, während die Aktivierung der Fahrfunktion x Sekunden benötigt.
47	Der Fahrer hat die Aktivierung der autonomen Fahrfunktion zu spät bereitgestellt, weil der Fahrer davon ausgeht, dass das Fahrzeug zum Übernahmezeitpunkt autonom fährt.
48	Der Fahrer hat die Deaktivierung der autonomen Fahrfunktion bereitgestellt, während der Fahrer nicht in der Lage ist das Fahrzeug manuell zu führen.
49	Der Fahrer hat die Deaktivierung der autonomen Fahrfunktion bereitgestellt, während das Fahrzeug nicht in der Lage ist manuell geführt zu werden.
50	Der Fahrer hat die Deaktivierung der autonomen Fahrfunktion zu früh bereitgestellt, während der Fahrer nicht in der Lage ist das Fahrzeug manuell zu führen.
51	Der Fahrer hat die Deaktivierung der autonomen Fahrfunktion zu früh bereitgestellt, während das Fahrzeug nicht in der Lage ist manuell geführt zu werden.
52	Der Fahrer stellt die Deaktivierung zu früh bereit, wenn x Sekunden zuvor die Aktivierung durchgeführt wird.
53	Der Fahrer hat die Deaktivierung der autonomen Fahrfunktion zu spät bereitgestellt, während das Fahrzeug die Verkehrssituation nicht autonom bewältigen kann.
54	Der Fahrer hat die autonome Fahrfunktion zu kurz deaktiviert, während eine Aktivierung x Sekunden benötigt.
55	Der Fahrer hat die autonome Fahrfunktion zu lange deaktiviert, während eine Deaktivierung x Sekunden benötigt.

Tabelle B.10: UCA aus den Regelkreisen "Fahrer/Passagier-HMI", "HMI-Steuerungs- und Regelungssysteme" und "Fahrer/Passagier-Physikalisches Fahrzeug" Level vier

56	Der Fahrer hat die Deaktivierung der manuellen Fahrfunktion nicht bereitgestellt, während das Fahrzeug nicht mehr manuell fahren/bedient werden kann.
57	Der Fahrer hat die manuelle Fahrfunktion deaktiviert, wenn die autonome Fahrfunktion nicht aktiviert werden kann.
58	Der Fahrer hat die manuelle Fahrfunktion nicht aktiviert, wenn das Fahrzeug nicht mehr autonom fahren kann.
59	Der Fahrer hat die manuelle Fahrfunktion aktiviert, wenn diese nicht zur Verfügung steht.
60	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion nicht bereit, während der Fahrer nicht in der Lage ist manuell zu fahren.
61	Der Fahrer hat die manuelle Fahrfunktion aktiviert, wenn ein MRM eingeleitet wurde.
62	Der Fahrer hat die manuelle Fahrfunktion aktiviert, wenn eine manuelle Fahrfunktion durch rechtliche Rahmenbedingungen nicht aktiviert werden darf.
63	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion nicht bereit, während das Fahrzeug nicht in der Lage ist manuell geführt zu werden.
64	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion zu früh bereit, während der Fahrer zum Zeitpunkt der Aktivierung mit einer manuellen Fahrt rechnet.
65	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion zu früh bereit, wenn das Kommando der Deaktivierung des manuellen Betriebsmodus gleichzeitig oder x Sekunden vor Aktivierung des autonomen Betriebsmodus umgesetzt wird.
66	Die HMI Schnittstelle stellt die Aktivierung der autonomen Fahrfunktion zu spät bereit, wenn der Fahrer nicht in der Lage ist manuell zu fahren (bzw. das Prozessmodell verletzt -> Irritation).
67	Die HMI Schnittstelle hat die Aktivierung der autonomen Fahrfunktion zu früh gestoppt, während der autonome Fahrmodus in x Sekunden aktiviert wird.
68	Die HMI Schnittstelle hat die Aktivierung der autonomen Fahrfunktion zu spät gestoppt, während der autonome Fahrmodus in x Sekunden aktiviert wird.
69	Die HMI Schnittstelle stellt die Deaktivierung des autonomen Fahrmodus nicht bereit, wenn der Fahrer eine Deaktivierung angefordert hat.
70	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion bereit, wenn der Fahrer nicht in der Lage ist manuell zu fahren.

Tabelle B.11: UCA aus den Regelkreisen "Fahrer/Passagier-HMI", "HMI-Steuerungs- und Regelungssysteme" und "Fahrer/Passagier-Physikalisches Fahrzeug" Level vier

71	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion bereit, während das Fahrzeug nicht in der Lage ist manuell zu fahren.
72	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion zu früh bereit, während der Fahrer nicht in der Lage ist das Fahrzeug manuell zu führen (Sekundenanzeige wann übernommen wird).
73	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion zu spät bereit, während der Fahrer nicht in der Lage ist das Fahrzeug manuell zu führen (Warnhinweis Übermüdung, Vorschlag autonom zu fahren).
74	Die HMI Schnittstelle stellt die Deaktivierung der autonomen Fahrfunktion zu spät bereit, wenn das Fahrzeug nicht in der Lage ist manuell geführt zu werden.

Tabelle B.12: UCA aus dem Regelkreis "Fahrer/Passagier-Physikalisches Fahrzeug" Level vier

75	Der Fahrer stellt die Zunahme der Fahrparameter nicht bereit, während das Prozessmodell des automatisierten Systems die Zunahme der Fahrparameter annimmt.
76	Der Fahrer stellt die Zunahme der Fahrparameter nicht bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
77	Der Fahrer stellt die Zunahme der Fahrparameter nicht bereit, während die Umweltbedingungen diese für Manövrierfähigkeit des Fahrzeugs erfordern.
78	Der Fahrer stellt die Zunahme der Fahrparameter bereit, während die Umweltbedingungen für eine Manövrierfähigkeit eine Abnahme oder Konstanz erfordern.
79	Der Fahrer stellt die Zunahme der Fahrparameter zu früh bereit, während das Prozessmodell des automatisierten Fahrzeugs eine Abnahme bzw. Konstanz vermutet.
80	Der Fahrer stellt die Zunahme der Fahrparameter zu früh bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
81	Der Fahrer stellt die Zunahme der Fahrparameter bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
82	Der Fahrer stellt die Zunahme der Fahrparameter zu früh bereit, während der Sicherheitsabstand zu anderen Objekten Personen unterschritten wird.
83	Der Fahrer stellt die Zunahme der Fahrparameter zu früh bereit, während das Fahrzeug bei Zunahme verkehrswidrig fährt.
84	Der Fahrer stellt die Zunahme der Fahrparameter zu früh bereit, während die Umweltbedingungen für die Manövrierfähigkeit keine Zunahme erfordern.
85	Der Fahrer hat die Zunahme der Fahrparameter zu spät bereitgestellt, während das Prozessmodell des autonomen Fahrzeugs eine andere Aktion vermutet hätte.
86	Der Fahrer hat die Zunahme der Fahrparameter zu spät bereitgestellt, während Personen schädlichen Bedingungen ausgesetzt sind.
87	Der Fahrer hat die Zunahme der Fahrparameter zu spät bereitgestellt, während der Sicherheitsabstand zu anderen Objekten unterschritten wird.
88	Der Fahrer hat die Zunahme der Fahrparameter zu spät bereitgestellt, obwohl die Verkehrsordnung das vorgibt.
89	Der Fahrer hat die Zunahme der Fahrparameter zu spät bereitgestellt, während die Umweltbedingungen diese erfordern.
90	Der Fahrer stellt die Zunahme der Fahrparameter zu spät bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
91	Der Fahrer stoppt die Zunahme der Fahrparameter zu früh, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten wird.

Tabelle B.13: UCA aus dem Regelkreis "Fahrer/Passagier-Physikalisches Fahrzeug" Level vier

92	Der Fahrer stoppt die Zunahme der Fahrparameter zu früh, während, aufgrund der Umweltbedingungen, eine Zunahme erforderlich ist, um manövrierfähig zu sein.
93	Der Fahrer stoppt die Zunahme der Fahrparameter zu früh, während das Prozessmodell des autonomen Systems eine Zunahme vermutet.
94	Der Fahrer stoppt die Zunahme der Fahrparameter zu früh, während Personen bei Abnahme bzw. Konstanz schädlichen Bedingungen ausgesetzt sind.
95	Der Fahrer stoppt die Zunahme der Fahrparameter zu früh, während das Fahrzeug sich bei Konstanz bzw. Abnahme nicht verkehrskonform verhält.
96	Der Fahrer stoppt die Zunahme der Fahrparameter zu spät, während das Prozessmodell des autonomen Systems eine Abnahme bzw. Konstanz der Fahrparameter vermutet.
97	Der Fahrer stoppt die Zunahme der Fahrparameter zu spät, während Personen schädlichen Bedingungen ausgesetzt sind.
98	Der Fahrer stoppt die Zunahme der Fahrparameter zu spät, während das Fahrzeug sich bei weiterer Zunahme verkehrswidrig verhält.
99	Der Fahrer stoppt die Zunahme der Fahrparameter zu spät, während die Umweltbedingungen eine Abnahme oder Konstanz der Parameter erfordern, um manövrierfähig zu sein.
100	Der Fahrer stoppt die Zunahme der Fahrparameter zu spät, während der Sicherheitsabstand zu anderen Objekten Personen unterschritten wird.
101	Der Fahrer stellt die Abnahme der Fahrparameter nicht bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
102	Der Fahrer stellt die Abnahme der Fahrparameter nicht bereit, während das Prozessmodell des autonomen Systems die Abnahme der Fahrparameter, initiiert durch den Fahrer, vermutet.
103	Der Fahrer stellt die Abnahme der Fahrparameter nicht bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
104	Der Fahrer stellt die Abnahme der Fahrparameter nicht bereit, während das Fahrzeug sich verkehrswidrig verhält.
105	Der Fahrer stellt die Abnahme der Fahrparameter nicht bereit während aufgrund der Umweltbedingungen das Fahrzeug manövrierunfähig ist.
106	Der Fahrer stellt die Abnahme der Fahrparameter bereit, während das Prozessmodell des autonomen Fahrzeugs eine andere Aktion vom Fahrer vermutet hätte.
107	Der Fahrer stellt die Abnahme der Fahrparameter bereit, während das Fahrzeug sich verkehrskonform verhält.
108	Der Fahrer stellt die Abnahme der Fahrparameter bereit, während das Fahrzeug aufgrund der Umweltbedingungen manövrierfähig ist.
109	Der Fahrer stellt die Abnahme der Fahrparameter bereit, während der Sicherheitsabstand zu anderen Objekten unterschritten bzw. überschritten wird.
110	Der Fahrer stellt die Abnahme der Fahrparameter zu früh bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
111	Der Fahrer stellt die Abnahme der Fahrparameter zu früh bereit, während das Prozessmodell des autonomen Fahrzeugs eine andere Aktion vermutet.
112	Der Fahrer stellt die Abnahme der Fahrparameter zu früh bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
113	Der Fahrer stellt die Abnahme der Fahrparameter zu früh bereit, während das Fahrzeug sich verkehrswidrig verhält.

Tabelle B.14: UCA aus dem Regelkreis "Fahrer/Passagier-Physikalisches Fahrzeug" Level vier

114	Der Fahrer stellt die Abnahme der Fahrparameter zu früh bereit, während das Fahrzeug aufgrund der Umweltbedingungen manövrierunfähig ist.
115	Der Fahrer stellt die Abnahme der Fahrparameter zu spät bereit, während das Prozessmodell des autonomen Fahrzeugs davon ausgeht, dass diese früher eingeleitet wird.
116	Der Fahrer stellt die Abnahme der Fahrparameter zu spät bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
117	Der Fahrer stellt die Abnahme der Fahrparameter zu spät bereit, während das Fahrzeug aufgrund der Umweltbedingungen manövrierunfähig ist.
118	Der Fahrer stoppt die Abnahme der Fahrparameter zu früh, während das Prozessmodell des autonomen Systems eine weitere Abnahme vermutet.
119	Der Fahrer stellt die Abnahme der Fahrparameter zu spät bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten wird.
120	Der Fahrer stoppt die Abnahme der Fahrparameter zu früh, während der Sicherheitsabstand zu anderen Objekten unterschritten bzw. überschritten wird.
121	Der Fahrer stoppt die Abnahme der Fahrparameter zu früh, während Personen schädlichen Bedingungen ausgesetzt sind.
122	Der Fahrer stoppt die Abnahme der Fahrparameter zu früh, während sich das Fahrzeug verkehrswidrig verhält.
123	Der Fahrer stoppt die Abnahme der Fahrparameter zu früh, während das Fahrzeug aufgrund der Umweltbedingungen manövrierunfähig ist.
124	Der Fahrer hat die Abnahme der Fahrparameter zu spät gestoppt, während das Prozessmodell des autonomen Systems eine andere Aktion vermutet.
125	Der Fahrer hat die Abnahme der Fahrparameter zu spät bereitgestellt, während Personen schädlichen Bedingungen ausgesetzt sind.
126	Der Fahrer hat die Abnahme der Fahrparameter zu spät gestoppt, während der Sicherheitsabstand zu anderen Objekten unterschritten wird.
127	Der Fahrer hat die Abnahme der Fahrparameter zu spät bereitgestellt, während der Sicherheitsabstand zu anderen Objekten unterschritten wird.
128	Der Fahrer hat die Abnahme der Fahrparameter zu spät gestoppt, obwohl die Verkehrsordnung andere Parameter für diese Situation vorgibt.
129	Der Fahrer hat die Abnahme der Fahrparameter zu spät gestoppt,während die Umweltbedingungen diese erfordern.

Tabelle B.15: UCA aus dem Regelkreis "Fahrer/Passagier-Physikalisches Fahrzeug" Level vier und fünf

130	Das autonome System stellt den fahrbereiten Zustand zur Verfügung, bevor alle Systeme aktiviert sind, welche das Fahrzeug hinreichend sicher fahrbereit machen.
131	Das autonome System stellt die Aktivierung "andere Aktuatorik" zu spät bereit, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen (falsche Aktuatorik bereitgestellt).
132	Das autonome System stoppt die Aktivierung "andere Aktuatorik" zu früh, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen.
133	Das autonome Systems stellt die Aktivierung des Stillstands bereit, wenn das Fahrzeug v>0km/h hat.
134	Das autonome System stoppt die Aktivierung der "anderen Aktuatorik", bevor die die Aktuatorik die Information der Aktivierung erhalten hat.
135	Das autonome System stoppt die Aktivierung "andere Aktuatorik" zu spät, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen.
136	Das autonome System stellt die Deaktivierung "anderer Aktuatorik" nicht bereit, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen (Dunkelheit).
137	Das autonome System stellt die Deaktivierung der anderen Aktuatorik nicht bereit, wenn ein Unfall mit schädigenden Umweltbedingungen im Fahrzeug auftritt (Tür wird nicht geöffnet).
138	Das autonome System stellt die Deaktivierung der Türöffnung bereit, obwohl Personen schädlichen Bedingungen im Fahrzeug ausgesetzt sind.
139	Das autonome System stellt die Deaktivierung "anderer Aktuatorik" bereit, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen (Dunkelheit).
140	Das autonome System stellt die Deaktivierung der anderen Aktuatorik bereit, wenn das autonome System nicht aktiviert ist.
141	Das autonome System stellt die Deaktivierung des fahrbereiten Zustands bereit, während das Fahrzeug v>0km/h fährt.
142	Das autonome System stellt die Deaktivierung "anderer Aktuatorik" zu früh bereit, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen (Dunkelheit).
143	Das autonome System stellt die Deaktivierung des fahrbereiten Zustands zur Verfügung, während das Fahrzeug v>0km/h fährt.
144	Das autonome System stoppt die Deaktivierung "anderer Aktuatorik" zu früh, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen (Dunkelheit).
145	Das autonome System stellt die Deaktivierung der Stillstandssicherung während der Aktivierung der Stillstandssicherung bereit.
146	Das autonome System stellt die „andere Aktuatorik“ in Situationen, in der die Aktuatorik für eine hinreichend sichere Fahrt benötigt wird, nicht bereit.
147	Das autonome System stellt die Aktivierung der Türöffnung bereit, wenn das Fahrzeug v>0 hat.
148	Das autonome System aktiviert die Aktuatorik nicht, bevor das Fahrzeug in Betrieb genommen wird.
149	Das autonome System stellt die Aktivierung anderer Aktuatorik nicht bereit, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen (Beispiel: Dunkelheit).
150	Das autonome System stellt die Aktivierung anderer Aktuatorik bereit, während die Umweltbedingungen das Fahrzeug manövrierunfähig machen (falsche Aktuatorik bereitgestellt).
151	Das autonome System stellt die „andere Aktuatorik“ bereit, während diese sich außer Funktion befindet.

Tabelle B.16: Sicherheitsanforderungen aus dem Regelkreis „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für das Fahrzeug Level vier und fünf

SC „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ Level vier und fünf		Beschreibung
40	Die Informationen der HMI Schnittstelle an den Fahrer müssen hinsichtlich einer hinreichend sicheren Fahrt priorisiert werden.	Kritische Informationen sollten vor unkritischen Informationen angezeigt werden.
41	Es muss sichergestellt werden, dass nicht autorisierte Person keinen Zugriff auf das Fahrzeug haben.	Cyber Crime, Fahrzeug soll nicht als Waffe genutzt werden.
42	Es muss sichergestellt werden, dass eine Person keinen Zugriff auf das Fahrzeug hat, wenn das Fahrzeug nicht hinreichend sicher genutzt werden kann.	Wartungsabstände konnten nicht eingehalten werden, Umweltbedingungen für eine Fahrt nicht geeignet (Unwetter)
43	Es muss sichergestellt werden, dass keine Objekte in der Fahrgastzelle während der Fahrt v>0km/h das Fahrzeug verlassen.	Müll verschmutzt Sensorik nachfolgender Autos. Umweltverschmutzung minimieren.
44	Es muss sichergestellt werden, dass bei einer verbleibenden Nutzungsenergiemenge E= Xh J des Fahrzeugs die HMI den Fahrer über diesen Zustand informiert.	
45	Es muss sichergestellt werden, dass die HMI Schnittstelle sich auf Tageszeit, Umweltbedingungen und Verkehrsbedingung dynamisch anpasst, sodass der Fahrer die Informationen während der gesamten Fahrt wahrnehmen kann.	Bsp: Display reflektiert Sonnenlicht, Daten sind nicht mehr lesbar. Im Dunkeln bzw. reduzierter Helligkeit muss Display lesbar sein, HMI an Lichtverhältnisse anpassen (Kontrast, Helligkeit).
46	Es muss sichergestellt werden, dass bei Ausfall der HMI Schnittstelle das Fahrzeug ein MRM einleitet.	HMI und die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs müssen unabhängig voneinander agieren.
47	Es muss sichergestellt werden, dass Kontrollaktionen und Feedbacks der HMI Schnittstelle körperbehinderten Menschen mit den Behinderungen x übermittelt werden können.	
48	Es muss sichergestellt werden, dass die HMI die Aktivierung der Betriebszustände genau x Sekunden später anzeigt.	Beispielsweise im Level vier: Autonome Fahrt beginnt, HMI übersendet die Information jedoch erst 10 Sekunden später-> kritisch.
49	Es muss sichergestellt werden, dass die HMI die Deaktivierung der Betriebszustände maximal x Sekunden später anzeigt.	
50	Es muss sichergestellt werden, dass vor der Aktivierung des fahrbereiten Zustands durch die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs, der Fahrer und die sensorische Schnittstelle die Fahrt ebenfalls freigeben müssen.	Bsp: Checks: Türen geschlossen, Navigationssignal erhalten, sensorische Schnittstelle überprüft die Fahrtstrecke bezüglich Umweltbedingungen

Tabelle B.17: Sicherheitsanforderungen aus dem Regelkreis „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für das Fahrzeug Level vier und fünf

51	Es muss sichergestellt werden, dass die HMI den Fahrer am Ende der Mission auffordert, die Fahrt zu bestätigen.	
52	Es muss sichergestellt werden, dass bei Nichtbestätigung des Fahrers der Fahrt nach x min, eine Notfallkette eingeleitet wird.	1. Sicherheitskritisch, da Fahrer Hilfe benötigen könnte. Fahrer wird ohnmächtig. Hitzetot im Fahrzeug 2. Fahrzeug wird blockiert (Fahrer schläft) Schaden für die Betreiber. Dies ist ebenso eine Frage der Regulatorik: Ist der Fahrzeughersteller verpflichtet Menschen im Fahrzeug zu helfen, wenn diese ohne jegliche äußere Einwirkung Hilfe benötigen. Fraglich ist, wenn Personen noch X h im Fahrzeug Zeitung lesen wollen.
53	Es muss sichergestellt werden, dass die Aktivierung/Deaktivierung der Betriebsfunktionen, durchgeführt durch den Fahrer mittels der HMI Schnittstelle, sich eindeutig abgrenzt gegenüber allen anderen Aktionen, welche ein Fahrer im Fahrzeug durchführen kann.	Bsp Lösung: Knöpfe zur Aktivierung/Deaktivierung des Betriebsmodus mit beiden Händen bedienen. Sonst könnte ein Betriebsmodus ungewollt aktiviert werden.
54	Während der Nutzung des Fahrzeugs muss jederzeit angezeigt werden, welcher Betriebsmodus aktiviert ist.	

Tabelle B.18: Sicherheitsanforderungen aus dem Regelkreis „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für das Fahrzeug Level vier

SC „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ Level vier		**Beschreibung**
55	Es muss sichergestellt werden, dass dem Fahrer während der Fahrt im autonomen Betriebsmodus angezeigt wird, über welchen Zeitraum das Fahrzeug auf Basis der aktuellen Datenlage potentiell noch autonom geführt werden kann bevor eine Übernahmeanforderung an den Fahrer ausgegeben wird.	Sicherheit: Fahrer kann sich auf Übernahme vorbereiten Komfort: E-Mails checken oder doch lieber einen Film gucken->angenehmer
56	Es muss sichergestellt werden, dass die personenspezifischen Einstellungen, um das Fahrzeug hinreichend sicher im manuellen Betriebsmodus bedienen zu können, vor Fahrtantritt ausgerichtet werden.	Sitzeinstellung, Lenkradeinstellung, usw…
57	Es muss sichergestellt werden, dass die personenspezifischen Einstellungen, um das Fahrzeug hinreichend sicher im manuellen Betriebsmodus bedienen zu können, vor Beginn der Übernahmephase wieder ausgerichtet sind.	Während der autonomen Fahrt könnten die Sitze wieder verstellt worden sein. Vor Aktivierung der manuellen Fahrt muss wieder auf die personenspezifische Sitzposition ausgerichtet worden sein.
58	Es muss sichergestellt werden, dass die HMI den Fahrer vor Fahrtantritt auffordert, den Zielort einzugeben.	
59	Es muss sichergestellt werden, dass die HMI Schnittstelle jederzeit aktiv ist, um Kontrollaktionen vom Fahrer und Feedback vom Steuerungs- und Regelungssystem des autonomen Fahrzeugs adäquat zu verarbeiten.	
60	Es muss sichergestellt werden, dass der Fahrer sich nicht in einem hoch emotionalen Zustand befindet, wenn er das Fahrzeug bedient.	
61	Es muss sichergestellt werden, dass dem Fahrer die Ereignisabfolge im Übergangsprozess vom autonomen in den manuellen Fahrmodus bekannt ist.	Übergangszeiten können eingeschätzt werden.
62	Es muss sichergestellt werden, dass der Fahrer die autonome Betriebsfunktion innerhalb von x Sekunden aktiviert, wenn vorliegende Streckenabschnitte ausschließlich autonom bewältigt werden können.	
63	Es muss sichergestellt werden, dass ein MRM vom Fahrer manuell überstimmt werden kann.	

Tabelle B.19: Sicherheitsanforderungen aus dem Regelkreis „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für das Fahrzeug Level vier

64	Übernimmt der Fahrer das Fahrzeug manuell, muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs innerhalb von x Sekunden die Kontrolle übergeben.	
65	Es muss sichergestellt werden, dass der Fahrer das Fahrzeug manuell führen kann, wenn die Übernahmekriterien in der Übernahmephase vollständig erfüllt sind.	Die Übernahmephase muss abgeschlossen sein, damit der Fahrer das Fahrzeug manuell führen kann.
66	Es muss sichergestellt werden, dass der aktuelle Fahrzeugzustand dem Fahrer über die HMI Schnittstelle vor Fahrtantritt übermittelt wird.	Zustand der Reifen anzeigen, um als Fahrer Traktion einschätzen zu können.
67	Es muss sichergestellt werden, dass während der Übernahmephase im autonomen Fahrzeug Level vier die Zwischenzustände mit maximal x Sekunden zeitlich befristet werden.	Beispiel: Fahrer lenkt das Fahrzeug, das Gaspedal wird jedoch noch autonom bedient. Dieser Zustand sollte zeitlich begrenzt sein.
68	Es muss sichergestellt werden, dass während der Übernahmephase in den manuellen Fahrmodus in einem autonomen Fahrzeug Level vier dem Fahrer keine weiteren Anforderungen gestellt werden, welche nicht den Übernahmeprozess unterstützen.	Fokus soll auf Übernahme liegen.
69	Es muss sichergestellt werden, dass dem Fahrer erneut eine Fahrübernahmeanforderung in den manuellen Modus gestellt wird, wenn der Fahrer die manuelle Fahrt bei Übergang in den autonomen Fahrmodus in einem autonomen Fahrzeug Level vier nach x Sekunden nicht beendet.	Hat bspw. ungewollt falschen Knopf gedrückt.
70	Es muss sichergestellt werden, dass die Bedienelemente, um eine hinreichend sichere manuelle Fahrt durchzuführen, aktivierbar sind, wenn der Fahrer das Fahrzeug in der Übernahmephase manuell übernimmt.	Beispielscenario: Fahrer will manuell übernehmen, Lenkrad ist jedoch noch nicht ausgefahren.
71	Es muss sichergestellt werden, dass der Fahrer nicht gleichzeitig den manuellen und autonomen Fahrmodus in einem autonomen Fahrzeug Level vier aktivieren kann.	HMI Schnittstelle dementsprechend designen, gleichzeitige Aktivierung sollte nicht zu Systemabstürzen führen.

Tabelle B.20: Sicherheitsanforderungen aus dem Regelkreis „Fahrer/Passagier-HMI“ und „HMI- Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für das Fahrzeug Level fünf

SC „Fahrer/Passagier-HMI“ und „HMI-Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ Level fünf		Beschreibung
72	Es muss sichergestellt werden, dass die HMI Schnittstelle jederzeit aktiv ist, um sicherheitskritische Informationen, Fahrzustände und Fahrzeugzustande jederzeit anzeigen zu können.	
73	Es muss sichergestellt werden, dass die Latenzzeit der Teleoperation <x Sekunden beträgt.	
74	Es muss sichergestellt werden, dass der Teleoperator das Fahrzeug erst führen kann, wenn der Teleoperator die Verkehrssituation x Sekunden beobachten konnte, um das mentale Prozessmodell von Umgebung und Fahrzeugs zu validieren.	
75	Es muss sichergestellt werden, dass teleoperiert werden kann, wenn das autonome Fahrzeug Level fünf die Verkehrssituation nicht mehr hinreichend sicher autonom bewältigen kann und gleichzeitig das Fahrzeug hinreichend sicher teleoperiert werden kann.	Ausfall Licht am Fahrzeug? Teleoperation nicht hinreichend sicher, Straße muss beleuchtet sein, damit Teleoperator das Fahrzeug hinreichend sicher führen kann.
76	Es muss sichergestellt werden, dass der Teleoperator die Elemente bedienen kann, um das Fahrzeug hinreichend sicher zu führen.	"andere Aktuatorik" beispielsweise Scheibenwischer oder Fernlicht muss der Teleoperator im Fahrzeug aktivieren können.
77	Es muss sichergestellt werden, dass die zu teleoperierende Fahrsituation im Teleoperatorraum entsprechend nachgestellt wir, dass diese so realitätsnah wie möglich wiedergeben wird.	Feedback auf allen Sinnesebenen notwendig (hören, sehen, fühlen).
78	Es muss sichergestellt werden, dass dem Teleoperator Feedbacks des physikalischen Fahrzeugs übermittelt werden können.	Beispielsweise: Kopfsteinpflaster. Bei Schnee erhöht sich die Wahrscheinlichkeit, dass Fahrzeug manövrierunfähig wird. Teleoperator muss eine angemessene Geschwindigkeit auswählen.
79	Es muss sichergestellt werden, dass dem Teleoperator angezeigt wird, ob der Teleoperationsmodus oder der autonome Fahrmodus aktiv ist.	
80	Es muss sichergestellt werden, dass der Teleoperator die Freigabe für die Fortführung der autonomen Fahrt, im autonomen Fahrzeug Level fünf, nach beenden der Teleoperation den Steuerungs- und Regelungssystem des autonomen Fahrzeugs aktiv erteilt.	Steuerungs- und Regelungssysteme werden erst wieder aktiviert, wenn Teleoperation beendet ist. Keine Überscheidung!
81	Es muss sichergestellt werden, dass erst teleoperiert werden kann, wenn das autonome Fahrzeug Level fünf die Möglichkeit zur Teleoperation erteilt.	

Tabelle B.21: Sicherheitsanforderungen aus dem Regelkreis „Fahrer/Passagier-HMI“ und „HMI- Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für das Fahrzeug Level fünf

82	Es muss sichergestellt werden, dass die Sensibilität der Bedienelemente des Teleoperators, um das Fahrzeug zu teleoperieren, nicht der Sensibilität des zu teleoperierenden Fahrzeugs entsprechen.	Jedes Fahrzeug hat beispielsweise andere Bremsparameter oder Lenkwinkelgradienten. Das muss während der Teleoperation berücksichtigt werden und in das imaginäre Fahrzeug des Teleoperators übersetzt werden. Andere Lösung: Teleoperator zeigt an wo hin sich das Fahrzeug mit welcher Geschwindigkeit bewegen soll. Langs- und Querregelung wird dabei dem autonomen Fahrzeug überlassen.
83	Alternativ: Es muss sichergestellt werden, dass der Teleoperator angeben kann, in welche Richtung das Fahrzeug über x Metern und mit welcher Geschwindigkeit das Fahrzeug bis zu einem bestimmten Wegpunkt fahren muss.	Fahrzeug regelt selbst die Quer,- und Längsführung. Ortspunkte könnten bspw. angegeben werden, das würde die Aufgabe des Teleoperators vereinfachen.
84	Es muss sichergestellt werden, dass dem Teleoperator angezeigt wird, in welche Richtung das autonome Fahrzeug navigiert werden soll.	
85	Es muss sichergestellt werden, dass das autonome Fahrzeug Level fünf dem Teleoperator übermittelt, welche Fahrsituation bewältigt werden muss.	
86	Es muss sichergestellt werden, dass der Teleoperator alle notwendigen Fahrzeug- und Fahrzustandsparameter beobachten kann, um eine zu teleoperierende Situation hinreichend sicher durchzuführen.	Geschwindigkeitsanzeige bzw. welcher Gang ist eingelegt/ Rückwärtsgang oder Vorwärtsgang
87	Es muss sichergestellt werden, dass das autonome Fahrzeug Level fünf dem Teleoperator im Übernahmezeitpunkt in einem definierten Fahrzustand übergeben wird.	Geschwindigkeit 0 km/h und im Stillstand gehalten/gesichert wird.
88	Es muss sichergestellt werden, dass die Bedienelemente des Teleoperators zur Lenkung des autonomen Fahrzeugs Level fünf individuell auf den Teleoperator angepasst werden können.	Möglichkeit Bedienelemente den Konstitutionen des menschlichen Körpers anpassen.
89	Es muss sichergestellt werden, dass der Teleoperator Sicherheitshinweise von der sensorischen Schnittstelle erhalten kann.	Falschfahrer.
90	Es muss sichergestellt werden, dass bei Verbindungsabbruch zum Teleoperator während der Teleoperation > x Sekunden, das autonome Fahrzeug Level fünf ein MRM einleitet.	

Tabelle B.22: Sicherheitsanforderungen aus dem Regelkreis „Fahrer/Passagier-HMI“ und „HMI- Steuerungs- und Regelungssysteme“ und „Fahrer/Passagier-Physikalisches Fahrzeug“ für das Fahrzeug Level fünf

91	Es muss sichergestellt werden, dass der Teleoperator hinreichend sicher anhält, wenn Personen Hilfe benötigen.	Wer muss in diesem Fall aktiv werden? Wer haftet? Fahrerflucht? Lösung derzeit nicht eindeutig.
92	Es muss sichergestellt werden, dass der Teleoperator x Sekunden nach Übernahmeanforderung vom autonomen Fahrzeug Level fünf zur Verfügung steht.	
93	Es muss sichergestellt werden, dass ein MRM eingeleitet wird, wenn der Teleoperator nach Übernahmeaufforderung nach >x Sekunden nicht zur Verfügung steht.	
94	Es muss sichergestellt werden, dass der Teleoperator physisch und psychisch in der Lage ist das Fahrzeug hinreichend sicher zu teleoperieren.	Fahrberechtigung, physische und psychische Konstitution des Teleoperators usw…
95	Es muss sichergestellt werden, dass der Nutzer des autonomen Fahrzeugs informiert ist, in welchem Fahrmodus das Fahrzeug operiert.	Fahrzeug steht am Straßenrand und wartet auf Teleoperation, Nutzer muss Informationen erhalten, warum das Fahrzeug anhält.

B.3 Regelkreise in denen ”Steuerungs- und Regelungssysteme“ als Kontroller fungieren

Tabelle B.23: Unsichere Kontrollaktionen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

UCA „Steuerungs- und Regelungssysteme“	
152	Das autonome System stellt die Zunahme der Fahrparameter nicht bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten wird.
153	Das autonome System stellt die Abnahme der Fahrparameter nicht bereit, wenn andere Objekte tangiert werden.
154	Das autonome System stellt die Zunahme der Fahrparameter nicht bereit, obwohl der Fahrer und das Fahrzeug fahrbereit sind.
155	Das autonome System stellt die Zunahme der Fahrparameter in einem unangemessenen Level bereit.
156	Das autonome System stellt die Zunahme der Fahrparameter bereit, wenn der Fahrweg nicht eindeutig ist.
157	Das Autonome System stellt die Zunahme der Fahrparameter nicht bereit, während das Prozessmodell des Fahrers vom Fahrzeug die Zunahme der Fahrparameter vermutet.
158	Das Autonome System stellt die Zunahme der Fahrparameter nicht bereit, wenn Personen schädlichen Bedingungen ausgesetzt sind.
159	Das autonome System stellt die Zunahme der Fahrparameter nicht bereit, wenn aufgrund der Umweltbedingungen das Fahrzeug manövrierunfähig ist.
160	Das autonome System stellt die Zunahme der Fahrparameter in eine nicht intendierte Richtung bereit.
161	Das Autonome System stellt die Zunahme der Fahrparameter bereit, während der Sicherheitsabstand zu anderen Objekten unterschritten wird bzw. für eine hinreichend sichere Fahrt angemessen ist.
162	Das autonome System stellt die Zunahme der Fahrparameter bereit, wenn das Ziel erreicht ist.
163	Das autonome System stellt die Zunahme der Fahrparameter bereit, wenn das physikalische Fahrzeug kein Signal erwartet.
164	Das autonome System stellt die Fahrparameter inkorrekt zur Verfügung während des fahrbereiten Fahrmodus.
165	Das autonome System stellt die Zunahme der Fahrparameter bereit, wenn Menschen physisch oder psychisch gefährdet werden.
166	Die Zunahme der Fahrparameter wird bereitgestellt, wenn sich das Fahrzeug im sicheren Gebiet befindet und der Fahrer keine Zunahme erwartet.
167	Die Zunahme der Fahrparameter wird bereitgestellt, wenn das physikalische System gesichert ist. (Stillstandssicherung)
168	Das autonome System stellt die Zunahme der Fahrparameter bereit, wenn das Fahrzeug diese nicht umsetzen kann.
169	Das autonome System stellt die Zunahme der Fahrparameter bereit, während das Prozessmodell des Fahrers vom Fahrzeug die Abnahme der Fahrparameter vermutet.

Tabelle B.24: Unsichere Kontrollaktionen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

170	Das Autonome System stellt die Zunahme der Fahrparameter bereit, wenn aufgrund der Umweltbedingungen das Fahrzeug durch eine Abnahme der Fahrparameter das Fahrzeug manövrierunfähig ist.
171	Das autonome System stellt die Zunahme der Fahrparameter zu früh bereit, während der Sicherheitsabstand zu anderen Objekten unterschritten ist.
172	Das autonome System stoppt die Zunahme der Fahrparameter zu früh, bevor die notwendigen Parameter einer hinreichend sicheren Fahrt erreicht werden.
173	Das autonome System stellt die Zunahme der Fahrparameter an die Aktuatorik bereit, welche die Anforderungen nicht umsetzen kann.
174	Das autonome System stellt die Zunahme der Fahrparameter zu früh bereit, während das Prozessmodell des Fahrers keine Zunahme vermutet.
175	Das Autonome System stellt die Zunahme der Fahrparameter zu früh bereit, während Personen bei einer Zunahme schädlichen Bedingungen ausgesetzt sind.
176	Das Autonome System stellt die Zunahme der Fahrparameter zu früh bereit, wenn aufgrund der Umweltbedingungen eine Abnahme die Manövrierfähigkeit sicherstellt.
177	Das autonome System stellt die Zunahme der Fahrparameter zu spät bereit, wenn das physikalische System die Anforderungen nicht umsetzen kann.
178	Das autonome System stellt die Zunahme der Fahrparameter zu spät bereit, während das Prozessmodell des Fahrers zu einem früheren Zeitpunkt die Zunahme vermutet.
179	Das Autonome System stellt die Zunahme der Fahrparameter zu spät bereit, während der Sicherheitsabstand zu anderen Objekten unterschritten bzw. überschritten wird.
180	Das Autonome System stellt die Zunahme der Fahrparameter zu spät bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
181	Das Autonome System stellt die Zunahme der Fahrparameter zu spät bereit, während das Fahrzeug sich verkehrswidrig verhält.
182	Das autonome System hat die Zunahme der Fahrparameter zu früh gestoppt, wen das Fahrzeug noch keinen hinreichend sicheren Zustand eingenommen hat.
183	Das autonome System stellt die Zunahme der Fahrparameter zu früh bereit, wenn das physikalische System diese Anforderungen nicht umsetzen kann.
184	Das autonome System stoppt die Zunahme der Fahrparameter zu früh, wenn der Fahrer das Fahrzeug nicht manuell übernommen hat.
185	Das autonome System stoppt die Zunahme der Fahrparameter zu früh, während das Prozessmodell des Fahrers vom Fahrzeug eine weitere Zunahme erwartet hätte.
186	Das autonome System stoppt die Zunahme der Fahrparameter zu früh, während Personen schädlichen Bedingungen ausgesetzt sind.
187	Das Autonome System stoppt die Zunahme der Fahrparameter zu früh, während das Fahrzeug sich verkehrswidrig verhält, wenn keine Zunahme erfolgt.

Tabelle B.25: Unsichere Kontrollaktionen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

188	Das Autonome System hat die Zunahme der Fahrparameter zu früh gestoppt, während die Umweltbedingungen diese erfordern.
189	Das Autonome System hat die Zunahme der Fahrparameter zu früh gestoppt, während der Sicherheitsabstand zu anderen Objekten unterschritten wird.
190	Das Autonome System stoppt die Zunahme der Fahrparameter zu spät, während der Sicherheitsabstand zu anderen Objekten unterschritten bzw. überschritten wird.
191	Das autonome System stoppt die Zunahme der Fahrparameter, wenn das Fahrmanöver nicht beendet ist.
192	Das autonome System stoppt die Zunahme der Fahrparameter, wenn diese sich nicht auf einem hinreichend sicherem Level befinden.
193	Das autonome System stoppt die Zunahme der Fahrparameter zu spät, während das Prozessmodell des Fahrers vom Fahrzeug eine vorzeitige Zunahme vermutet hat.
194	Das Autonome System stoppt die Zunahme der Fahrparameter zu spät, während Personen schädlichen Bedingungen ausgesetzt sind.
195	Das autonome System stoppt die Zunahme der Fahrparameter zu spät, während sich das Fahrzeug verkehrswidrig verhält.
196	Das autonome System stoppt die Zunahme der Fahrparameter zu spät, während aufgrund der Umweltbedingungen eine Zunahme erforderlich ist, um manövrierfähig zu sein.
197	Das autonome System stellt die Abnahme der Fahrparameter nicht bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
198	Das autonome System stellt die Abnahme der Fahrparameter nicht bereit, wenn das Fahrzeug kollidiert ist.
199	Das autonome System stellt die Abnahme der Fahrparameter nicht bereit, wenn das Fahrzeug das Ziel erreicht hat.
200	Das autonome System stellt die Abnahme der Fahrparameter nicht bereit, während das Prozessmodell des Fahrers die Abnahme der Fahrparameter vermutet.
201	Das autonome System stellt die Abnahme der Fahrparameter nicht bereit, während Personen bei Konstanz und Zunahme schädlichen Bedingungen ausgesetzt sind.
202	Das autonome System stellt die Abnahme der Fahrparameter nicht bereit, wenn sich das Fahrzeug aufgrund einer Zunahme bzw. Konstanz der Fahrparameter verkehrswidrig verhält.
203	Das Autonome System stellt die Abnahme der Fahrparameter nicht bereit, während das Fahrzeug aufgrund von Umweltbedingungen manövrierunfähig ist.
204	Das Autonome System stellt die Abnahme der Fahrparameter bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
205	Das autonome System stellt die Abnahme der Fahrparameter bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
206	Das autonome System stellt die Abnahme der Fahrparameter bereit, während die Umweltbedingungen konstante oder zunehmende Fahrparameter um manövrierfähig zu sein erfordern.

Tabelle B.26: Unsichere Kontrollaktionen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

207	Das autonome System stellt die Abnahme der Fahrparameter bereit, während das Prozessmodell des Fahrers eine Zunahme oder Konstanz vermutet.
208	Das Autonome System stellt die Abnahme der Fahrparameter zu früh bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
209	Das autonome System stellt die Abnahme der Fahrparameter zu früh bereit, während das Prozessmodell des Fahrers eine Zunahme bzw. Konstanz erwartet.
210	Das autonome System stellt die Abnahme der Fahrparameter zu früh bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
211	Das autonome System stellt die Abnahme der Fahrparameter zu spät bereit, während das Prozessmodell des Fahrers vom Fahrzeug eine Abnahme erwartet.
212	Das Autonome System stellt die Abnahme der Fahrparameter zu spät bereit, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
213	Das autonome System stellt die Abnahme der Fahrparameter zu spät bereit, während Personen schädlichen Bedingungen ausgesetzt sind.
214	Das autonome System stellt die Abnahme der Fahrparameter zu spät bereit, während das Fahrzeug sich verkehrswidrig verhält.
215	Das Autonome System stellt die Abnahme der Fahrparameter zu spät bereit, während die Umweltbedingungen eine Konstanz oder Zunahme der Fahrparameter erfordern.
216	Das autonome System stoppt die Abnahme der Fahrparameter zu früh, wenn das Fahrzeug kollidiert.
217	Das autonome System stoppt die Abnahme der Fahrparameter zu früh, während das Prozessmodell des Fahrers vom Fahrzeug eine Abnahme vermutet.
218	Das autonome System stoppt die Abnahme der Fahrparameter zu früh, während Personen schädlichen Bedingungen ausgesetzt sind.
219	Das Autonome System stoppt die Abnahme der Fahrparameter zu früh, während das Fahrzeug ohne weitere Abnahme nicht hinreichend sicher ist.
220	Das Autonome System stoppt die Abnahme der Fahrparameter zu früh, während die Umweltbedingungen eine weitere Abnahme erfordern, um manövrierfähig zu sein.
221	Das autonome System stoppt die Abnahme der Fahrparameter zu spät, während das Prozessmodell des Fahrers vom Fahrzeug eine andere Aktion vermutet.
222	Das autonome System stoppt die Abnahme der Fahrparameter zu früh, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
223	Das Autonome System stoppt die Abnahme der Fahrparameter zu spät, während der Sicherheitsabstand zu anderen Objekten bzw. Personen unterschritten bzw. überschritten wird.
224	Das Autonome System stoppt die Abnahme der Fahrparameter zu spät, während Personen schädlichen Bedingungen ausgesetzt sind.
225	Das autonome System deaktiviert die Stillstandssicherung nicht, wenn das Fahrzeug fahrbereit ist und eine Geschwindigkeit v>0 km/h angenommen werden soll.

Tabelle B.27: Unsichere Kontrollaktionen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

226	Das Autonome System stoppt die Abnahme der Fahrparameter zu spät, während die Umweltbedingungen eine andere Aktion erfordern.
227	Das autonome System stellt die Zunahme der Fahrparameter bereit, während das Fahrzeug bei Abnahme in einem hinreichend sicheren Zustand ist.
228	Das autonome System aktiviert die Stillstandssicherung nicht, wenn das Fahrzeug sich im autonomen Fahrmodus befindet und das Fahrzeug vom Fahrer/Passagier verlassen wird.
229	Das autonome System aktiviert die Stillstandssicherung, wenn das Fahrzeug sich mit einer Geschwindigkeit >0 km/h bewegt.
230	Das autonome System aktiviert die Stillstandssicherung zu spät, wenn das Fahrzeug eine Geschwindigkeit von 0 km/h hat und sich im autonomen Fahrmodus befindet.
231	Die Teleoperation wird nicht aktiviert, wenn das Fahrzeug nicht mehr hinreichend sicher autonom fahren kann.
232	Die Teleoperation wird bereitgestellt, wenn das Fahrzeug die Fahrsituation hinreichend sicher autonom passieren kann.
233	Die Teleoperation wird aktiviert, bevor das Fahrzeug mit einer manuellen Fahrt rechnet.
234	Die Teleoperation wird zu spät aktiviert, wenn die Steuerungs- und Regelkreise davon ausgehen, dass die Teleoperation aktiv ist.
235	Die Teleoperation wurde zu früh aktiviert, wenn die Steuerungs- und Regelungssysteme mit einer manuellen Fahrt rechnen.
236	Die Teleoperation dauert zu lange an, während die Steuerungs- und Regelungssysteme das Fahrzeug wieder autonom übernehmen sollen.

Tabelle B.28: Unsichere Kontrollaktionen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level fünf

237	Die Teleoperation wird nicht aktiviert, wenn das Fahrzeug nicht mehr hinreichend sicher autonom fahren kann.
238	Die Teleoperation wird bereitgestellt, wenn das Fahrzeug die Fahrsituation hinreichend sicher autonom passieren kann.
239	Die Teleoperation wird aktiviert, bevor das Fahrzeug mit einer manuellen Fahrt rechnet.
240	Die Teleoperation wird zu spät aktiviert, wenn die Steuerungs- und Regelkreise davon ausgehen, dass die Teleoperation aktiv ist.
241	Die Teleoperation wurde zu früh aktiviert, wenn die Steuerungs- und Regelungssysteme mit einer manuellen Fahrt rechnen.
242	Die Teleoperation dauert zu lange an, während die Steuerungs- und Regelungssysteme das Fahrzeug wieder autonom übernehmen sollen.

Tabelle B.29: Unsichere Kontrollaktionen aus dem Regelkreis „Steuerungs- und Regelungssysteme-Sensorische Schnittstelle“ Level vier und fünf

UCA „Steuerungs- und Regelungssysteme-Sensorische Schnittstelle“	
243	Das autonome System stellt den Fahrzeugstatus nicht bereit, während die "Car to X Kommunikation" die Informationen benötigt.
244	Das autonome System stellt den autonomen Fahrmodus nicht bereit, während in der Umweltsituation der autonome Fahrmodus hinreichend sicher agiert.
245	Das autonome System stellt den autonomen Fahrmodus bereit, während das Fahrzeug im autonomen Fahrmodus nicht hinreichend sicher agiert.
246	Das autonome System stoppt den autonomen Fahrmodus zu früh, obwohl die HMI Schnittstelle diese Informationen nicht anzeigt.
247	Das autonome System stellt die Deaktivierung des autonomen Fahrmodus nicht bereit, während in der Situation der autonome Fahrmodus nicht hinreichend sicher agiert.
248	Das autonome System stellt die Deaktivierung des autonomen Fahrmodus bereit, während das Fahrzeug im autonomen Fahrmodus hinreichend sicher agiert.
249	Das autonome System stellt die Deaktivierung des autonomen Fahrmodus zu früh bereit, wenn der Passagier/Fahrer mit einer Aktivierung rechnet.
250	Das autonome System stellt die Deaktivierung des autonomen Fahrmodus zu spät bereit, wenn das autonome System nicht mehr hinreichend sicher autonom fahren kann.
251	Das autonome System stoppt die Deaktivierung des autonomen Fahrmodus zu früh, obwohl die HMI Schnittstelle die Informationen nicht anzeigt.
252	Das autonome System stoppt den autonomen Fahrmodus zu spät, wenn Personen außerhalb des Fahrzeugs mit einer vorzeitigen Deaktivierung gerechnet haben.

Tabelle B.30: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

SC Regelkreis mit der funktionalen Einheit „Steuerungs- und Regelungssysteme“ als Kontroller Level vier und fünf		Beschreibung
105	Es muss sichergestellt werden, dass die Umgebungsmerkmale, um eine hinreichend sichere Fahrt durchzuführen, länderübergreifend normiert werden.	
106	Es muss sichergestellt werden, dass während der gesamten Nutzungsdauer des Fahrzeugs genau ein Betriebsmodus aktiviert ist.	
107	Es muss sichergestellt werden, dass die Aktivierung der autonomen Fahrfunktion erst möglich ist, wenn das Fahrzeug in der Lage ist > x Sekunden hinreichend sicher autonom zu fahren.	Es ist nicht sinnvoll die autonome Betriebsfunktion beispielsweise für nur 1 Sekunde zu aktivieren und kurz darauf den Fahrer aufzufordern das Fahrzeug erneut manuell zu übernehmen.
108	Es muss sichergestellt werden, dass im MRM ein Fahrzustand mit minimalem Risiko für Leib und Leben eingenommen wird.	
109	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs von externen Eingriffen nicht autorisierter Personen.	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs müssen eine unabhängige Berechnungseinheit sein (Cyber Crime entgegenwirken) bzw. sensitive Informationen müssen verschlüsselt versendet werden.
110	Organisationen hinreichend isoliert werden, damit keine vom Fahrer ungewollte Aktivierung oder Deaktivierung eines Fahrmodus bzw. Aktion durchgeführt wird.	
111	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs so wenig Schnittstellen wie möglich und so viele Schnittstellen wie nötig haben.	Cybercrimerisiko reduzieren.
112	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme manipulationssicher sind.	
113	Es muss sichergestellt werden, dass sicherheitsrelevante Informationen verschlüsselt versendet werden.	
114	Es muss sichergestellt werden, dass die potentiellen, zukünftigen und aktuellen Fahrzustände und die aktuellen Fahrzeugzustände des autonomen Fahrzeugs innerhalb von x Sekunden von der HMI Schnittstelle angezeigt werden.	Abgleich des mentalen Prozessmodells vom Fahrer mit dem Prozessmodell des autonomen Fahrzeugs.
115	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs dürfen im autonomen Fahrmodus die Zunahme der Längsaktuatorik nicht bereit stellen, wenn der Abstand x Metern zu anderen Objekten/Personen unterschritten wird.	

Tabelle B.31: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

116	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs dürfen im autonomen Fahrmodus die Zunahme der Queraktuatorik nicht bereitstellt, wenn der Abstand x Metern zu anderen Objekten/Personen unterschritten wird.	
117	Es muss sichergestellt werden, dass Datenlogging bezüglich Fahrzeugzustand- und Fahrzustandsdaten während der Nutzung des Fahrzeugs betrieben wird, sodass die Möglichkeit besteht diese Daten im Nachhinein zu überprüfen.	Es muss sichergestellt werden, dass die Daten im Fahrzeug gespeichert werden und ausgelesen werden können, damit diese ausgewertet werden.
118	Es muss sichergestellt werden, dass inadäquate Kennwerte, welche auf eine nicht hinreichend sichere Fahrt hindeuten, nach maximal x Sekunden an die sensorische Schnittstelle übermittelt werden, um mögliche Fehler zeitnah, nach Auftreten der Diskrepanz, zu identifizieren.	
119	Es muss sichergestellt werden, dass ohne Hilfe externer Informationen von der sensorischen Schnittstelle für einen Zeitraum von x Sekunden das Fahrzeug hinreichend sicher im autonomen Betriebsmodus geführt werden kann.	
120	Es muss sichergestellt werden, dass das Fahrzeug ein MRM einleitet, wenn die Kommunikation zur sensorischen Schnittstelle >x Sekunden unterbrochen ist.	
121	Es muss sichergestellt werden, dass das Fahrzeug im autonomen Betriebsmodus verbleibt, wenn die Kommunikation zur sensorischen Schnittstelle <x Sekunden unterbrochen ist.	GPS bricht für x Sekunden ab, wird kurz darauf aber wieder hergestellt.
122	Es muss sichergestellt werden, dass die Betriebsmodiwechsel (Teleoperation, manuell, autonom) in einem Zeitpunkt durchgeführt werden, wenn die Verkehrssituation eine hinreichend sichere Übernahme erlaubt.	Beispiel Level vier: In einem Zeitpunkt in dem die Fahrsituation leicht überschaubar ist, muss das Fahrzeug manuell vom Fahrer übernommen werden. Während eines komplexen Überholvorgangs im Stadtverkehr beispielsweise nicht.
123	Es muss sichergestellt werden, dass das Fahrzeug kollisionsfrei geführt wird.	
124	Es muss sichergestellt werden, dass das Fahrzeug nach Kontakt mit einem Objekt/Person in den Stillstand überführt wird.	Wie das umgesetzt werden soll, ist derzeit nicht eindeutig: 1. Beule im Fahrzeug, wie soll das detektiert werden? 2. Was, wenn Fahrradfahrer Fahrzeug nur berührt, ein leichter Aufschlag kann für einen Fußgänger jedoch schon schwerwiegende Folgen haben.

Tabelle B.32: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

125	Es muss sichergestellt werden, dass das Fahrzeug nach Kontakt mit einem Objekt und/oder Person nach maximal x Metern in den Stillstand überführt wird.	Unterscheidung zwischen einem Unfall, der den Fahrer/Passagier im Fahrzeug gefährdet und einem Unfall, in dem andere Personen geschädigt werden: Bspw. Nächste Haltemöglichkeit erst in 5 km? Vom Unfall zu weit entfernt, um anderen Personen zu helfen. Autonomes Fahrzeug müsste dazu Verkehrsregeln brechen, um Anforderung gerecht zu werden in der Nähe des Unfalls zu halten, falls es keine adäquate Haltemöglichkeit gibt. Zu Punkt 1, bei gravierendem Schaden sofort in den Stillstand verzögern.
126	Es muss sichergestellt werden, dass nach einem Unfall, nachdem das Fahrzeug nicht mehr hinreichend sicher geführt werden kann, das Fahrzeug nach maximal x Metern in den Stillstand überführt wurde.	Tunnel/Baustelle sofort sicher anhalten? Macht keinen Sinn, Ausnahmeregelungen einführen.
127	Das autonome Fahrzeug muss Objekte zwischen überfahrbar und nichtüberfahrbar unterscheiden können.	Umsetzung kritisch: 1. Bsp: Reh bzw. Waschbär vom Menschen unterscheiden. 2. Ist es sicherer dem Reh auszuweichen oder es zu überfahren (Körpergröße bzw. Gewicht muss dazu bewertet werden) Wie sollen Gegenstände auf der Straße hinsichtlich einer hinreichend sicheren Fahrt korrekt eingeschätzt werden? Vollbremsung bei einfacher Plane auf der Straße? Gefährdungspotential könnte bei einer Vollbremsung deutlich höher sein, als darüber hinwegzufahren, wenn beispielsweise weitere Fahrzeuge folgen.
128	Es muss sichergestellt werden, dass der Fahrzeugzustand im fahrbereiten Modus in regelmäßigen Abständen von x Sekunden überprüft wird.	Bsp: Reifen platzt während der Fahrt, nicht ausschließlich nur zu Beginn der Fahrt prüfen-> fortlaufend
129	Es muss sichergestellt werden, dass Fahrzustandsparameter in Abhängigkeit der Fahrdaten vorausschauend berechnet werden können, wenn diese während der Fahrt nicht messbar sind.	Beispiel: Reifenabrieb muss vorausschauend berechnet werden können, damit das autonome Fahrzeug nicht während der autonomen Fahrt den Grenzbereich überschreitet, manövrierunfähig wird und anschließend darauf reagiert. -> Das Fahrzeug sollte das Manöver abbrechen, **bevor** es manövrierunfähig wird.

Tabelle B.33: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

130	Es muss sichergestellt werden, dass der Fahrzeugzustand zu Beginn der Fahrt hinsichtlich einer hinreichend sicheren Fahrt überprüft wird.	
131	Es muss sichergestellt werden, dass das Fahrzeug nach einem kritischen Unfall, wenn eine hinreichend sichere Fahrt nicht mehr möglich ist, innerhalb von x Sekunden in einen Standbymodus überführt wird	Im Standbymodus können keine Anforderungen an die Aktuatorik des Fahrzeugs gestellt werden. Beispiel: Andere Fahrer sollten das Fahrzeug für eine weitere Fahrt nicht mehr buchen können, wenn es zuvor kollidiert ist.
132	Es muss sichergestellt werden, dass das Fahrzeug nach maximal x km, nachdem das Fahrzeug unkritisch beschädigt wurde, in die Werkstatt überführt wird. Mit einer unkritischen Beschädigung kann hinreichend sicher gefahren werden.	Beule am Fahrzeug. Kein sicherheitskritisches Scenario! Kann aber rufschädigend sein, wenn der Betreiber der Fahrzeuge zerbeulte Fahrzeuge anbietet. Fraglich in diesem Requirement ist die Entwicklung, wie werden autonome Fahrzeuge zukünftig betrieben?!
133	Es muss sichergestellt werden, dass Fahrzeuge nach einer Nutzungsdauer von x km in die Werkstatt überführt werden.	
134	Es muss sichergestellt werden, dass die Mission im sicheren Zustand begonnen wird.	Es muss beispielsweise sichergestellt werden, dass das autonome Fahrzeug zum Fahrzeugein- und ausstieg an einem hinreichend sicheren Ort hält.
135	Es muss sichergestellt werden, dass die Mission im sicheren Zustand beendet wird.	
136	Es muss eine Postcrashsequence eingeleitet werden, wenn das Fahrzeug verunfallt und Personen geschädigt wurden.	
137	Es muss sichergestellt werden, dass im autonomen Fahrmodus bei einer Restenergiemenge von x J ein MRM eingeleitet wird.	Dem Fahrzeug sollte im autonomen Fahrmodus immer ausreichend Energie zur Verfügung stehen. Es muss sichergestellt werden, dass das Fahrzeug während der autonomen Fahrt nicht abgeschaltet wird, da keine Energie mehr zur Verfügung steht.
138	Es muss sichergestellt werden, dass die Energieversorgung des Fahrzeugs während der Fahrt gewährleistet ist.	

Tabelle B.34: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

139	Es muss sichergestellt werden, dass die Wettervorhersage vor Fahrtantritt überprüft wird und das Fahrzeug nicht fahrbereit ist, wenn das Fahrzeug bzw. Personen während der Fahrt wetterbedingt geschädigt werden könnten.	Nutzer würde geringeres Verantwortungsbewusstsein gegenüber dem Fahrzeug haben, wenn die Nutzer der Fahrzeuge nicht gleichzeitig Eigentümer wären. Nutzer würde Verkehrssituationen beispielsweise Hagel, Orkan eher in Kauf nehmen.
140	Es muss sichergestellt werden, dass das Fahrzeug mit Personen außerhalb des Fahrzeugs im Fahrzeugumkreis von x Meter kommunizieren kann.	Person an Zebrastreifen...hat das Fahrzeug mich erkannt? Maßnahme: Banner auf Fahrzeug mit dem Feedback gegeben werden kann.
141	Es muss sichergestellt werden, dass das Verhalten des Systems der Erwartungshaltung anderer Verkehrsteilnehmer in Bezug auf eine defensive und vorsichtige Fahrweise gerecht wird.	Akzeptanz von Verkehrsbeteiligten steigt für die Technologie, Loss: "Schädigung des Rufs" mit diesem Requirement entgegen wirken, Beispiel: Reißverschlussverfahren einhalten, Kein Ausbremsen von anderen Fahrzeugen auf der Autobahn, höfliche und zuvorkommende Programmierung. Könnte man mit Umfrage statistisch bewerten.
142	Es muss sichergestellt werden, dass sich das Fahrzeug zu Beginn jeder der Fahrt initialisiert und sich bezüglich Updates und Plausibilität checkt.	Bsp: Längere Standzeiten? Aktualisierung notwendig. Wie werden Fahrzeuge gehandhabt, die beispielsweise 10 Jahre nicht mehr genutzt wurden?
143	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs zu jedem Zeitpunkt Daten von maximal x Quellen mit höchster Priorität einer h, welche Informationen an die Steuerungs-, und Regelungssysteme versenden, gleichzeitig verarbeiten können.	Was ist, wenn nicht autorisierte Quellen das System überlasten wollen, indem sie das autonome System mit Daten überfluten. Grenze wäre sinnvoll.
144	Es muss sichergestellt werden, dass der autonome Fahrmodus nicht aktiviert werden kann, wenn der autonome Fahrmodus nicht hinreichend sicher ist.	
145		
146	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme den autonomen Fahrmodus stoppen, bevor eine autonome Fahrt nicht mehr hinreichend sicher ist".	
147	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs müssen Verkehrsregeln und soziale Normen während der autonomen Fahrt befolgen.	

Tabelle B.35: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

148	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs müssen zwischen Verkehrsregeln, psychische und physische Belastung von Menschen und Umweltbelastungen adäquat priorisieren.	
149	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs die Zunahme der Fahrparameter auf einem angemessenen Level und in einer adäquaten Art und Weise bereitstellen, sodass Personen im und um das Fahrzeug keinen schädlichen Bedingungen ausgesetzt sind.	Fußgänger benötigen Reaktionszeit, um auf Fahrzeug im Straßenverkehr zu reagieren. Bsp: Straße wird überquert. Diese Reaktionszeit muss beispielsweise berücksichtigt werden, auch wenn beispielsweise im vollautonomen Straßenverkehr deutlich schneller gefahren werden könnte.
150	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs dürfen im autonomen Fahrmodus die Zunahme der Fahrparameter nicht x Sekunden zu früh bereitstellen, wenn der Sicherheitsabstand zu anderen Fahrzeugen unterschritten wird.	
151	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs müssen die Abnahme der Fahrparameter bereitstellen, bevor das autonome Fahrzeug nicht mehr adäquat längs- und/oder quergeführt werden kann.	Blitzeis auf der Straße, wie soll das frühzeitig korrekt detektiert werden, sodass kein unsicherer Zustand entsteht und das Fahrzeug manövrierunfähig wird.
152	Der Algorithmus der Steuerungs- und Regelungssysteme des autonomen Fahrzeugs müssen erkennen, wenn die Eingangsdaten fehlerhaft sind.	
153	Es muss sichergestellt werden, dass eine Stillstandssicherung gewährleistet ist, wenn das Fahrzeug autonom in den Stillstand überführt wird.	In welcher Form die Stillstandssicherung durchgeführt werden soll, ob Scheibenbremsen oder Anker ausgeworfen wird, ist nicht die Frage.
154	Es muss sichergestellt werden, dass die Stillstandssicherung in keinem Betriebsmodus während der Fahrt aktiviert sein kann.	
155	Es muss sichergestellt werden, dass die Stillstandssicherung im autonomen Betriebsmodus deaktiviert wird, wenn das Fahrzeug eine Geschwindigkeit > 0km/h einnehmen soll.	
156	Es muss sichergestellt werden, dass die Stillstandssicherung im autonomen Betriebsmodus nicht deaktiviert wird, wenn das Fahrzeug sich im Stillstand befindet und keine Geschwindigkeit >0km/h einnehmen soll.	

Tabelle B.36: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

157	Es muss sichergestellt werden, dass die Fahrzeugtüren x Sekunden nach beenden der Fahrt in einem sicheren Zustand entriegelt werden, sodass diese geöffnet werden können.	
158	Es muss sichergestellt werden, dass das Fahrzeug fahrbereit ist, bevor eine Geschwindigkeit von v>0km/h eingenommen wird.	
159	Es muss sichergestellt werden, dass x Sekunden nach Aktivierung des Betriebsmodus dem Fahrer eine Bestätigung über die HMI Schnittstelle übermittelt wird.	
160	Es muss sichergestellt werden, dass x Sekunden nach Deaktivierung des Betriebsmodus dem Fahrer eine Bestätigung über die Deaktivierung über die HMI übermittelt wird.	
161	Es muss sichergestellt werden, dass ein Sicherheitsabstand in Abhängigkeit der Geschwindigkeit von >x m zu anderen Objekten und Personen eingehalten wird.	Bremsperformance ist nicht von allen Fahrzeugen gleich, daher ist auch im vollautonomen Straßenverkehr ein Sicherheitsabstand notwendig.
162	Es muss sichergestellt werden, dass Anomalien in der Datenverarbeitung erkannt werden, analysiert werden und an das Risikomanagement weitergeleitet werden.	
163	Es muss sichergestellt werden, dass im Straßenverkehr ausschließlich Sicherheitskräfte Fahrzeuge im autonomen Betriebsmodus bezüglich der Längs- und/oder Querführung anweisen können.	Anweisungen von Feuerwehr/Polizei wird teilweise verbal durchgeführt. Bsp: Rettungsgasse muss aufgrund eines versperrten Weges im Vergleich zu standardisierten Situationen gebildet werden. Autonome Fahrzeuge müssen darauf reagieren Alternative: Sicherheitsfahrzeuge müssen autonom fahren, dann Kommunikation mit dem autonomen Fahrzeug möglich. Unterscheidung Polizist an der Ampel von einer Person im Faschingskostüm, Identifikationssensor für Sicherheitskräfte als Maßnahme?!
164	Es muss sichergestellt werden, dass die Anweisungen der Sicherheitskräfte gegenüber Verkehrsregeln priorisiert werden.	Bsp: Unfall, Polizist leitet autonomes Fahrzeug über den Bürgersteig.
165	Es muss sichergestellt werden, dass autonome Fahrzeuge hinreichend sicher abgeschleppt werden können.	
166	Es muss sichergestellt werden, dass ausschließlich autorisierte Software geladen wird.	

Tabelle B.37: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

167	Es muss sichergestellt werden, dass die Updates nacheinander geladen werden.	Systemüberlastung verhindern.
168	Es muss sichergestellt werden, dass die Updates in der gleichen Reihenfolge geladen werden, wie sie dem Fahrzeug gesendet werden.	
169	Es muss sichergestellt werden, dass genau die Updates im Fahrzeug geladen werden, welche von den autorisierten Instanzen an das Fahrzeug gesendet werden.	Updates in den Steuerungs- und Regelungskreisen autorisieren. Während der Übertragung vom Sender zum Empfänger sollten die Updates von nicht autorisierten Organisationen/Personen nicht verändert werden können. (Cyber Crime)
170	Es muss sichergestellt werden, dass das autonome Fahrzeug erkennt, wenn Informationen versendet werden, die von nicht autorisierten bzw. identifizierten Absendern stammen.	
171	Es muss sichergestellt werden, dass Updates erst geladen werden, wenn die Updates autorisiert worden sind.	
172	Es muss sichergestellt werden, dass das Fahrzeug nicht als Waffe missbraucht werden kann, sodass Menschen gefährdet bzw. Objekte zerstört werden.	
173	Es muss sichergestellt werden, dass das autonome Fahrzeug maximal x Meter entfernt von einer Unfallstelle bei denen Personen in Not sind und < x Personen helfen in den Stillstand verzögert.	Fahrerflucht, wenn Fahrzeug an einem Unfall vorbei fährt und keiner hilft? Nicht umsetzbar, wie soll eingeschätzt werden, ob jemand Hilfe benötigt, was ist wenn man innerhalb dieses Umkreises nicht hinreichend sicher halten kann? Sollte das Hilfefahrzeug in Gefahr gebracht werden?
174	Es muss sichergestellt werden, dass im Falle eines Cyber Angriffs das Fahrzeug ein MRM einleitet und das Risikomanagement informiert.	Im Falle eines Cyber Angriffs! Autonomes Fahrzeug muss deaktiviert werden können, wenn das Fahrzeug gehackt wurde.
175	Es muss sichergestellt werden, dass alle notwendigen Komponenten und Funktionen, um eine hinreichend sichere Fahrt durchzuführen, vor Fahrtantritt von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs auf adäquate Funktionsfähigkeit überprüft werden.	
176	Es muss sichergestellt werden, dass alle notwendigen Komponenten und Funktionen, um eine hinreichend sichere Fahrt durchzuführen, vor Fahrtantritt von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs auf Plausibilität überprüft werden.	

Tabelle B.38: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

177	Es muss sichergestellt werden, dass ein MRM eingeleitet wird, wenn die x/y Position des Fahrzeugs, detektiert durch die sensorische Schnittstelle, nicht mit den Daten übermittelt von den Steuerungs- und Regelungssystemen übereinstimmen.	
178	Steuerungs- und Regelungssysteme sensorische Schnittstelle	
179	Es muss sichergestellt werden, dass die Umgebungsmerkmale, um eine hinreichend sichere Fahrt durchzuführen, länderübergreifend interpretierbar sind.	Gegenstände auf der Straße, die in gemäßigten Gebieten harmlos überfahrbar sind im Vergleich zu gleichen Gegenständen, die in Gebieten mit beispielsweise Extremen Wetterbedingungen nicht hinreichend sicher überfahrbar sind.
180	Es muss sichergestellt werden, dass Informationen vom Fahrzeugzustand und Fahrzustand, von allen Fahrzeugen, welche am Straßenverkehr teilnehmen, jede x Sekunde an die sensorische Schnittstelle übertragen werden.	Oldtimer dürfen beispielsweise nicht am Straßenverkehr teilnehmen, außer sie können diese Daten übertragen. Keine Kommunikation bedeutet nicht, dass sich dort kein Fahrzeug befindet. Es muss ein Feedback von jedem Objekt im Straßenverkehr vorliegen.
181	Es muss sichergestellt werden, dass kritische Updates nach maximal x Minuten geladen wurden.	
182	Es muss sichergestellt werden, dass unkritische Updates nach maximal x h geladen werden.	
183	Es muss sichergestellt werden, dass neue Updates erst geladen werden, wenn vorherige Updates geladen werden.	Was ist, wenn Updates aufeinander aufbauen? Reihenfolge.
184	Es muss sichergestellt werden, dass Fahrzeuge mit v > 0 km/h in den Stillstand überführt werden, wenn kritische Updates geladen werden müssen.	Kritische Updates: Beispielsweise Veränderung des Bedienkonzeptes, dieses sollte sich während der Fahrt nach einem Update nicht verändern, bevor der Fahrer sich das Tutorial mit Aktualisierungen nicht angesehen hat.
185	Es muss sichergestellt werden, dass die die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs der sensorischen Schnittstelle Feedback über Abweichungen größer x % bezüglich Informationen der Sensorik und der sensorischen Schnittstelle übermitteln.	Hinweis auf inadäquate Arbeitsweise der Sensorik bzw. falsche Informationen der sensorischen Schnittstelle.
186	Es muss sichergestellt werden, dass aktuelle Informationen, Vorausschaudaten und zukünftige vorhersehbare Zustandsänderungen des autonomen Fahrzeugs im zeitlichen Propagationspfad mit Verkehrsbeteiligten, mit denen potentiell in Wechselwirkung getreten wird, zu jedem Zeitpunkt ausgetauscht werden.	Kritisches Beispielszenario: Leiten beide Fahrzeuge ein Ausweichmanöver ein und plausibilisieren diese Informationen anschließend nicht, dann kollidieren diese Fahrzeuge trotzdem, obgleich sich zunächst einander ausweichen.

Tabelle B.39: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier und fünf

187	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs der sensorischen Schnittstelle jede x Sekunde während einer Geschwindigkeit v>0 km/h die Standortdaten sendet, sodass nach einem Unfall die letzte bekannte Position identifiziert werden kann.	Kann die Standortposition des Fahrzeugs aufgrund des Unfalls nicht mehr gesendet werden, dann kann hingegen die letzte bekannte Position bestimmt werden, bevor das Fahrzeug kollidiert.
188	Es muss sichergestellt werden, dass die sensorische Schnittstelle x Sekunden nach Auftreten eines Unfalls eine Unfallkausalkette einleitet.	Unfallkausalkette: 1. Sicherheitskräfte Unfall melden, 2. Fahrzeuge im Umkreis informieren usw.
189	Es muss sichergestellt werden, dass die sensorische Schnittstelle die Informationen der Steuerungs- und Regelungssysteme des autonomen Fahrzeugs plausibilisieren kann.	
190	Es muss sichergestellt werden, dass sensible/sicherheitskritische Informationen der Steuerungs- und Regelungssysteme des autonomen Fahrzeugs verschlüsselt an die sensorische Schnittstelle übertragen werden.	Unerlaubtes Abgreifen der Informationen muss verhindert werden
191	Es muss sichergestellt werden, dass über das Risikomanagement jederzeit ein MRM eingeleitet werden kann.	Im Falle eines Cyber Angriffs! Sensorische Schnittstelle muss Betriebsmodus des Fahrzeugs einleiten können, wenn das Fahrzeug beispielsweise gehackt wurde. Fahrzeug kann somit nicht als "Waffe" genutzt werden, da es in den sicheren Zustand überführt wird.
192	Es muss sichergestellt werden, dass das Risikomanagement den aktuellen Betriebsmodus mindestens x Minuten überstimmen kann.	Es ist nicht sinnvoll, wenn ein MRM für eine Sekunde aktiviert werden kann, und anschließend das autonome Fahrzeug wieder durch nicht autorisierte Personen übernommen werden kann.
193	Es muss sichergestellt werden, dass die Betätigung des Notausknopfes durch den Fahrer, die Anforderungen des Risikomanagements an das autonome Fahrzeug und die Anforderungen des autonomen Fahrzeugs selbst überstimmen kann.	Falls die Verbindung vom Risikomanagement gehackt wurde, muss eine weitere Rückfallebene aktiviert werden können, nämlich der Notausknopf im Fahrzeug.
194	Es muss sichergestellt werden, dass der Fahrer informiert wird, wenn der Verdacht besteht, dass das Fahrzeug gehackt wurde.	

Tabelle B.40: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier

SC Regelkreis mit der funktionalen Einheit „Steuerungs- und Regelungssysteme“ als Kontroller Level vier		Beschreibung
195	Es muss sichergestellt werden, dass in der Übernahmephase in den manuellen Betriebsmodus im autonomen Fahrzeug Level vier folgende Vorgänge durchgeführt werden: 1. Aktivierung des Betriebsmodus vom Fahrer 2. Validierung des Betriebsmodus vom Fahrer.	
196	Es muss sichergestellt werden, dass die Automatisierung der Ursprungsphase im autonomen Fahrzeug Level vier nicht beendet werden darf, bis alle Übernahmebedingungen erfolgt sind.	Beispiel Übernahme: Zunächst wird die Lenkung übernommen, anschließend das Gaspedal usw…
197	Es muss sichergestellt werden, dass nach Erfüllung des ersten Übernahmekriteriums im autonomen Fahrzeug Level vier alle weiteren Übernahmekriterien innerhalb von x Sekunden übernommen werden.	Die Zwischenzustände müssen zeitlich begrenzt werden, da Zwischenzustände unsichere Zustände sind.
198	Es muss sichergestellt werden, wenn der Fahrer das autonome Fahrzeug Level vier nach Fahrerübernahmeaufforderung nicht manuell übernimmt, dass ein MRM eingeleitet wird.	
199	Es muss sichergestellt werden, dass vor der manuellen Übernahme des autonomen Fahrzeugs Level vier ein Zeitraum x implementiert wird, in dem sich der Fahrer auf die aktuelle Fahrsituation und den Fahrzeugzustand einstellen kann, um bei der Übernahme ein vollumfängliches Bild der Verkehrssituation zu haben, damit das Fahrzeug hinreichend sicher bedient werden kann.	
200	Es muss sichergestellt werden, dass das autonome Fahrzeug Level vier das MRM einleitet, wenn das Fahrzeug weder manuell noch autonom hinreichend sicher geführt werden kann.	Rückfallebene: Degradation oder Verzögerung in den Stillstand.
201	Es muss sichergestellt werden, dass eine Varianzzeit x Sekunden exakt im Moment der Fahrerübernahme in einem autonomen Fahrzeug Level vier in den manuell Betriebsmodus implementiert wird.	Bsp. wird der autonome/manuelle Fahrmodus in x Sekunden bereitgestellt, die Übernahme vom Fahrer erfolgt jedoch in x+1 Sekunden -> Reaktionszeiten vom Fahrer berücksichtigen.
202	Es muss sichergestellt werden, dass die autonome Fahrfunktion in einem autonomen Fahrzeug Level vier aktiviert wird bzw. das MRM eingeleitet wird, wenn der Fahrer die manuelle Fahrfunktion aktiviert, aber im vorgegebenen Validierungszeitraum nicht validiert.	Cyber Crime entgegenwirken, da der Fahrer nach Aktivierung erneut bestätigen muss. Validierung bedeutet das Prozedere der Übernahmephase durchzuführen.

Tabelle B.41: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier

203	Es muss sichergestellt werden, dass ein MRM eingeleitet wird, wenn in der Übernahmephase in den manuellen Fahrmodus das Fahrzeug nicht mehr hinreichend sicher autonom geführt werden kann.	Während der Übernahmephase kann plötzlich nicht mehr hinreichend sicher autonom geführt werden, da beispielsweise plötzlich eine Baustelle auf dem Weg detektiert wird, die nicht autonom bewältigt werden kann.
204	Es muss sichergestellt werden, dass die Übernahme des manuellen Fahrmodus dementsprechend eingeleitet wird, sodass mindestens ein Zeitpuffer, nachdem das Fahrzeug manuell übernommen wurde, von x Sekunden besteht, in dem noch hinreichend sicher autonom gefahren werden könnte.	Es wird nicht adäquat berechnet wie lange noch potenziell autonom gefahren werden kann, in der Übernahmephase für den manuellen Fahrmodus ist der autonome Fahrmodus nicht mehr hinreichend sicher, daher Zeitpuffer integrieren, damit die Übernahmephase frühzeitig aktiviert wird.
205	Es muss sichergestellt werden, dass der Fahrer die manuelle Kontrolle nach einer Übernahmeaufforderung in einem autonomen Fahrzeug Level vier innerhalb von x Sekunden von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs erhält.	
206	Es muss sichergestellt werden, dass bei ungleicher Informationsgebung von Sensorik und sensorischer Schnittstelle in einem autonomen Fahrzeug Level vier eine Übernahmeanforderung an den Fahrer gestellt wird.	Unsicher welche Informationen korrekt sind, daher Übernahmeanforderung.
207	Es muss sichergestellt werden, dass der Betriebsmodus in einem autonomen Fahrzeug Level vier in den Übergangsphasen der Fahrmodus jederzeit zurück gewechselt werden kann.	Fahrer aktiviert ausversehen beispielsweise manuellen Betriebsmodus, das Fahrzeug muss kurz darauf den autonomen Betriebsmodus wieder aktivieren können ohne dass zunächst in den manuellen Betriebsmodus gewechselt werden muss.
208	Es muss sichergestellt werden, dass der autonome Betriebsmodus im autonomen Fahrzeug Level vier aktiviert wird bzw. ein MRM eingeleitet wird, wenn sich während der manuellen Fahrt mind. x Sekunden keine Hand am Lenkrad befindet.	

Tabelle B.42: Sicherheitsanforderungen aus dem Regelkreis „Steuerungs- und Regelungssysteme“ Level vier

209	Die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs müssen den autonomen Fahrmodus im autonomen Fahrzeug Level vier bereitstellen, wenn der autonome Fahrmodus in der aktuellen Fahrsituation hinreichend sicher ist und der Fahrer den Fahrmodus anfordert.	
210	Es muss sichergestellt werden, dass das Fahrzeug x Sekunden nach der Aktivierung des autonomen Betriebsmodus durch den Fahrer, autonom fährt.	
211	Es muss sichergestellt werden, dass eine Stillstandssicherung gewährleistet ist, wenn das Fahrzeug manuell in den Stillstand überführt wird.	
212	Es muss sichergestellt werden, dass die Steuerungs-, und Regelungssysteme x Sekunden vor dem Betriebsmoduswechsel eine Übernahmeanforderung stellen, sodass die Übernahme in der verbleibenden Zeit hinreichend sicher erfolgen kann.	
213	Vorausschau wie lange autonom gefahren werden kann, was ist, wenn diese nicht stimmt, Es muss ein Warnhinweis gegeben werden, wenn die Vorausschau nicht stimmt.	

Tabelle B.43: Sicherheitsanforderungen für ein Fahrzeug Level fünf mit der funktionalen Einheit „Steuerungs- und Regelungssysteme“ als Kontroller

SC Regelkreis mit der funktionalen Einheit „Steuerungs- und Regelungssysteme“ als Kontroller Level fünf		**Beschreibung**
214	Es muss sichergestellt werden, dass nach Übersendung unterschiedlicher Informationen von der Sensorik und der sensorischen Schnittstelle ans autonome Fahrzeug ein MRM eingeleitet wird.	Es ist nicht eindeutig, ob die Sensorik oder das Backend korrekte Informationen liefert.
215	Es muss sichergestellt werden, dass in einem autonomen Fahrzeug Level fünf der Fahrer zu keinem Zeitpunkt die Möglichkeit hat in die Längs- und/oder Querführung des Fahrzeugs einzugreifen.	

B.4 Regelkreise „Physikalisches Fahrzeug“ als zu kontrollierender Prozess

Tabelle B.44: Sicherheitsanforderungen für den Regelkreis „Physikalisches Fahrzeug“ Level vier und Level fünf

SC Regelkreis „Physikalisches Fahrzeug“ als Kontroller Level vier und fünf		Beschreibung
216	Es muss sichergestellt werden, dass die Umgebungsmerkmale, um eine hinreichend sichere Fahrt durchzuführen, länderübergreifend normiert werden.	Verkehrszeichen, Straßenbegrenzungsmarkierungen
217	Es muss sichergestellt werden, dass die Parameter der Fahrumgebung und des Fahrzeugzustands, welche von der Sensorik gemessen werden sollen, sich zu keinem Zeitpunkt in einem Wertebereich befinden, der von der Sensorik nicht adäquat verarbeitet werden kann.	"Out of Range" Daten (siehe Definition).
218	Es muss sichergestellt werden, dass "andere Aktuatorik" bereitgestellt wird, wenn Personen im Fahrzeug schädlichen Bedingungen ausgesetzt sind.	Sibirien: Beispielsweise Klimaanlage muss aktiviert werden, sonst ist beispielsweise eine ohnmächtige Person erfroren, bevor sie gerettet wurde.
219	Es muss sichergestellt werden, dass die Parameter, welche die Umweltbedingungen in der Fahrgastzelle definieren, innerhalb von x Sekunden adäquat angepasst werden, sodass Personen im Fahrzeug zu keinem Zeitpunkt schädlichen Bedingungen ausgesetzt sind.	Luftqualität, Temperatur (Im Level fünf: Säuglinge werden autonome gefahren, deaktivierte Klimaanlage bei -10 Grad Außentemperatur wäre schädlich).
220	Es muss sichergestellt werden, dass die "andere Aktuatorik" betriebsmodusübergreifend von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs aktiviert werden können.	
221	Es muss sichergestellt werden, dass die "andere Aktuatorik" betriebsmodusübergreifend manuell vom Fahrer aktiviert werden kann.	
222	Es muss sichergestellt werden, dass die "andere Aktuatorik" ausschließlich automatisch von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs deaktiviert werden können.	Im Tunnel aktiviert das Fahrzeug automatisch Licht, um mit Kameradaten Fahrt zu validieren, manuelle Abschaltung des Lichts ist dann problematisch.
223	Es muss sichergestellt werden, dass mehr als eine technische Ressource genutzt wird, um Umgebungsbedingungen zu plausibilisieren.	Radar+Lidar+Infrarot gleichzeitig nutzen, um zu plausibilisieren.
224	Es muss sichergestellt werden, dass mehr als eine technische Ressource genutzt wird, um den Fahrzeugzustand zu plausibilisieren.	Es muss sichergestellt werden, dass die Geschwindigkeit mit Hilfe unterschiedlicher Technologien gemessen wird/ Geschwindigkeit als maßgeblicher Parameter während autonomer Fahrten.

Tabelle B.45: Sicherheitsanforderungen für den Regelkreis „Physikalisches Fahrzeug“ Level vier und Level fünf

225	Es muss sichergestellt werden, dass nach Betätigen des Notausknopf ein MRM eingeleitet wird.	Betätigung des Notausknopfs sollte nicht dazu führen, dass das Fahrzeug während der Fahrt ausgeschaltet wird.
226	Es muss sichergestellt werden, dass der Notausknopf in jedem Fahrzeugzustand aktiviert werden kann.	HMI defekt, Notausknopf könnte nun nicht mehr betätigt werden.
227	Es muss sichergestellt werden, dass ein Notausknopf verbaut wird, um das Fahrzeug in einen hinreichend sicheren Zustand überführen zu können.	
228	Es muss sichergestellt werden, dass die Geschwindigkeit im Fahrzeug absolut gemessen wird.	
229	Es muss sichergestellt werden, dass die Personen außerhalb des Fahrzeugs im Umkreis von x Metern keinen schädlichen Bedingungen ausgesetzt sind.	Fahrzeug darf Beispielsweise keine schädlichen Stoffe während der Fahrt emittieren.
230	Es muss sichergestellt werden, dass die Sensorik alle Objekte bzw. Personen, mit denen potenziell in Wechselwirkung getreten wird, detektiert.	Verkehrszeichen mit Aufkleber müssen ebenfalls detektiert werden.
231	Es muss sichergestellt werden, dass das physikalische Fahrzeug alle Kontrollaktionen, gefordert von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs, umsetzen kann.	Fahrzeug darf nicht in einen unsicheren Zustand überführt werden, in dem es nicht manövrierfähig ist und die Kontrollaktionen der Steuerungs- und Regelungssysteme nicht mehr umsetzen kann.
232	Es muss sichergestellt werden, dass das Fahrzeug nach einem kritischen Unfall, bei dem das Fahrzeug beschädigt wurde, sodass es nicht mehr hinreichend sicher geführt werden kann, ein MRM einleitet und in den Standbymodus überführt wird.	
233	Es muss sichergestellt werden, dass im Standbymodus Funktionen entsprechend aktiviert bzw. deaktiviert werden, um eine Bergungsaktion hinreichend sicher durchzuführen.	Scheibenwischer muss nicht aktiviert werden, wenn Fahrzeug kollidiert ist/ Andere potenzielle Nutzer sollten das Fahrzeug nach einem Crash nicht mehr anfordern können.
234	Es muss sichergestellt werden, dass der Fahrer "andere Aktuatorik" Hupe jederzeit bedienen kann.	
235	Es muss sichergestellt werden, dass die "andere Aktuatorik" von den Steuerungs- und Regelungssystemen entsprechend aktiviert wird, sodass bei allen Umweltbedingungen Personen außerhalb des Fahrzeugs, das autonome Fahrzeug wahrnehmen können, sodass diese nicht geschädigt werden.	Licht müsste im Dunkeln in der Stadt aktiviert werden, damit Fußgänger das Fahrzeug erkennen, auch wenn es für die Steuerung und Regelung in diesem Fall nicht benötigt werden würde. Im autonomen Fahrmodus Level fünf, beziehungsweise im autonomen Betriebsmodus Level vier benötigt man beispielsweise nicht jederzeit Licht, da Fahrzeuge über Car 2 X kommunizieren.

Tabelle B.46: Sicherheitsanforderungen für den Regelkreis „Physikalisches Fahrzeug“ Level vier und fünf

236	Die "andere Aktuatorik" muss x Sekunden, nachdem die Umweltbedingungen diese erfordern, von den Steuerungs- und Regelungssystemen des autonomen Fahrzeugs automatisch bereitgestellt werden.	Beispielszenario Level vier: Manueller Betriebsmodus wird eingeleitet. Während der Übernahmephase fängt es an zu regnen. Automatische Aktivierung des Scheibenwischers, damit Fahrzeug hinreichend sicher übergeben werden kann.
237	Es muss sichergestellt werden, dass im autonomen Fahrzeug der Fahrer die Kontrollaktionen der Steuerungs- und Regelungssysteme an das physikalische Fahrzeug zu keinem Zeitpunkt überstimmen kann.	Weder in Level vier, noch in Level fünf soll der Fahrer überstimmen können.

Tabelle B.47: Sicherheitsanforderungen aus dem Regelkreis „Physikalisches Fahrzeug“ für ein Fahrzeug Level vier

SC Regelkreis „Physikalisches Fahrzeug“ als Kontroller Level vier		Beschreibung
238	Es muss sichergestellt werden, dass ein MRM im autonomen Fahrzeug Level vier eingeleitet wird, wenn "andere Aktuatorik", ohne diese man das Fahrzeug nicht mehr hinreichend sicher manuell fahren kann, ausfällt.	Lichtausfall auf Autobahn, in diesem Fall keine Übernahmeanforderung an den Fahrer stellen, sondern MRM einleiten. Der Fahrer kann das Fahrzeug ohne Licht nämlich auch nicht mehr hinreichend sicher führen.
239	Es muss sichergestellt werden, dass die Fahrgastzelle im autonomen Fahrzeug Level vier entsprechend designed wird, sodass die Fahrumgebung vom Fahrer so realitätsnah wie möglich aufgenommen werden kann.	Beispielsweise sollten keine Fenster verbaut sein, welche die Umgebungsbedingungen verzerren: Mentales Prozessmodell von der Umwelt muss adäquat sein.
240	Es muss sichergestellt werden, dass die Möglichkeit besteht, die Fahrzeugtüren eines Level vier Fahrzeugs nach einem Crash mechanisch zu öffnen.	Fahrerlaubnis für Fahrt mit Fahrzeug Level vier notwendig, eine Person befindet sich im Fahrzeug, dem die Verkehrsregeln bekannt sind (siehe Requirement Regulatorik). Dieser Fahrer sollte die umgebende Fahrsituation hinsichtlich eines hinreichend sicheren Ausstiegs adäquat einschätzen können (Verlassen des Fahrzeugs auf Autobahn) -> Daher sollte Tür mechanisch zu öffnen sein, Problematik: Verwirrte Fahrer nach Crash.
241	Es muss sichergestellt werden, dass Reaktionen des physikalischen Fahrzeugs Level vier auf die Fahrumgebung an den Fahrer realitätsnah weitergeben werden.	Fraglich ist, wie viel Komfortfunktionen verträgt ein Fahrzeug? Reaktionen des Fahrzeugs beim Überfahren eines Schlaglochs werden verharmlost, könnte aber ein sicherheitskritisches Scenario sein (Fahrzeug wurde beschädigt und Sensorik hat das nicht detektiert).
242	Es muss sichergestellt werden, dass dem Fahrer im Falle eines Eingriffs ABS usw. zur Verfügung steht. Daher nicht mit Datenfusion.	
243	Es muss sichergestellt werden, dass Updates in Gebieten bzw. Verkehrssituationen durchgeführt werden, in denen die Durchführung für Verkehrsteilnehmer hinreichend sicher ist.	Update im Stillstand vor einem Bahnübergang

Tabelle B.48: Sicherheitsanforderungen für den Regelkreis „Physikalisches Fahrzeug“ ausschließlich für ein Fahrzeug Level fünf

SC Regelkreis „Physikalisches Fahrzeug“ als Kontroller Level vier und fünf		Beschreibung
244	Es muss sichergestellt werden, dass im autonomen Fahrzeug Level fünf ein MRM eingeleitet wird, wenn "andere Aktuatorik", ohne diese man das Fahrzeug nicht mehr hinreichend sicher teleoperieren kann, ausfällt.	
245	Es muss sichergestellt werden, dass die Fahrgastzelle des Teleoperators entsprechend designed wird, sodass die Fahrumgebung vom Teleoperator so realitätsnah wie möglich aufgenommen werden kann.	
246	Es muss sichergestellt werden, dass die Steuerungs- und Regelungssysteme des autonomen Fahrzeugs Level fünf in Abhängigkeit des Fahrzeugzustands, der Verkehrssituation und des Zustands der Personen die Türen zum Ausstieg öffnen.	Kritisches Szenario: Fraglich ist der Umgang mit verwirrten Personen, die beispielsweise die Autobahn überqueren wollen bzw. Kinder, die aussteigen möchten, jedoch die Verkehrssituation nicht einschätzen können.
247	Es muss sichergestellt werden, dass Reaktionen des physikalischen Fahrzeugs Level fünf auf die Fahrumgebung an Fahrzeuginsassen realitätsnah weitergeben werden.	Möglichkeit wäre zum Ende der Fahrt abzufragen, ob Ungewöhnliches aufgefallen ist, als Hinweis für die Werkstatt.

B.5 Allgemeine Sicherheitsanforderungen geltend für Gesamtheit der Regelkreise

Tabelle B.49: Sicherheitsanforderungen Allgemein identifiziert aus den UCA

SC Regelkreis Allgemein Level vier und fünf		Beschreibung
248	Es muss sichergestellt werden, dass die Prozessmodelle aller funktionalen Einheiten aus dem Regelkreis und das mentale Prozessmodell des Fahrers adäquat aufeinander angepasst sind.	
249	Es muss sichergestellt werden, dass die Verfügbarkeitsanforderung x bezüglich Fehlerschwelle und Fehlerhäufigkeit von Funktionen und Komponenten im zu untersuchenden Gesamtsystem jederzeit erfüllt ist.	Ob eine redundante Auslegung oder eine Auslegung mit hohen Belastungsgrenzen von Komponente oder Funktion bleibt dem Entwickler überlassen.
250	Es muss sichergestellt werden, dass das Gesamtsystem sicher reagiert, wenn die Kontrollereingangsdaten innerhalb der festgelegten Fehlerschwelle liegen.	
251	Es muss sichergestellt werden, dass die Ausgangsdaten eines Kontrollers validiert werden.	
252	Es muss sichergestellt werden, dass die Leistungsgrenzen der Komponenten und Funktionen im Gesamtsystem nicht überschritten werden.	
253	Es muss sichergestellt werden, dass die Kontrollanweisungen bezüglich maximaler/minimaler Datenrate und Kompatibilität an die Empfangseinheit adäquat versendet werden, sodass diese verarbeitet werden können.	
254	Es muss sichergestellt werden, dass die Empfangseinheiten aktiviert sind, wenn Kontrollaktionen an die Empfangseinheit versendet werden.	
255	Es muss sichergestellt werden, dass Fehler im System geheilt werden.	
256	Es muss sichergestellt werden, dass Fehler und sicherheitsrelevante Informationen im System in einem Format protokolliert werden, sodass die Kontrolleinheit welche die Aufzeichnungen auswertet, die Ergebnisse adäquat auswerten kann.	
257	Es muss sichergestellt werden, dass die Fehlerprotokolle des autonomen Fahrzeugs nach maximal x Sekunden der Auswertungseinheit übermittelt sind.	Kritische Fehler sollten zeitnah verarbeitet werden können, um andere Fahrzeuge mittels beispielsweise Updates zu schützen.
258	Es muss sichergestellt werden, dass die Einheit welche die Fehlerprotokolle auswertet, die Ergebnisse innerhalb von x h hinsichtlich kritischer und unkritischer Fehler bewertet.	

Tabelle B.50: Sicherheitsanforderungen Allgemein identifiziert aus den UCA

259	Es muss sichergestellt werden, dass die Empfangseinheiten nach jeder Kontrollaktion Feedback an die Sendeeinheiten übermitteln.	
260	Es muss sichergestellt werden, dass das Datenformat der Kontrollaktionen und Feedbacks in die Einheit transformiert wird, die vom Empfänger verarbeitet werden kann.	
261	Es muss sichergestellt werden, dass im gesamten Regelkreis die übertragenen Daten, wenn möglich, ein einheitliches Format haben	Fehler in der Verarbeitung können dementsprechend entgegengewirkt werden.
262	Es muss sichergestellt werden, dass in allen Regelkreisen eine in sich konsistente Referenzzeit zur UTC implementiert wird	
263	Es muss sichergestellt werden, dass in allen Regelkreisen die gleiche Referenzzeit implementiert wird	Regelkreise stimmen sich zeitlich ab, die Zeitbasis muss in jedem Regelkreis korrekt sein.
264	Es muss sichergestellt werden, dass Prozesse in den Verarbeitungseinheiten eingeführt werden, welche die Feedbacks adäquat auswerten	
265	Es muss sichergestellt werden, dass Parameter im gesamten Regelkreis mit einer regelkreisspezifischen Genauigkeit von mindestens x % verarbeitet werden	
266	Es muss sichergestellt werden, dass Feedbacks innerhalb von x Sekunden von der Empfangseinheit verarbeitet werden.	
267	Es muss sichergestellt werden, dass die Feedbacks adäquat an die Verarbeitungseinheit übermittelt werden.	
268	Es muss sichergestellt werden, dass die Kontrollaktionen innerhalb von x Sekunden an die Verarbeitungseinheit übermittelt werden.	
269	Es muss sichergestellt werden, dass die Kontrollaktionen adäquat an die Verarbeitungseinheit übermittelt werden.	
270	Es muss sichergestellt werden, dass die Kontrollaktionen in der Verarbeitungseinheit innerhalb von x Sekunden verarbeitet werden.	