Agiler Lebenszyklusprozess für die modellbasierte Gewährleistung der Betriebssicherheit hochautomatisierter Fahrfunktionen

Zur Erlangung des akademischen Grades eines

DOKTORS DER INGENIEURWISSENSCHAFTEN (Dr.-Ing.)

von der KIT-Fakultät für Elektrotechnik und Informationstechnik des
Karlsruher Instituts für Technologie (KIT)
angenommene

DISSERTATION

von

M.Eng. Jannis Erz

geb. in Blaubeuren

Tag der mündlichen Prüfung	09.03.2026
Hauptreferent:	Prof. Dr. Eric Sax
Korreferent:	Prof. Dr. Simon Burton

Kurzfassung

Die Gewährleistung der Betriebssicherheit hochautomatisierter Kraftfahrzeuge erweist sich als eine der grundsätzlichen Herausforderungen bei deren Markteinführung. Die vorliegende Dissertation leistet hierzu einen wissenschaftlichen Beitrag, indem ein normativ integrierter, agiler und modellbasierter Betriebssicherheitslebenszyklusprozess entwickelt wird, der sowohl standardisierungsbezogene Anforderungen als auch industrielle Entwicklungsrealitäten systematisch miteinander verbindet.

Zu diesem Zweck wird zunächst der Problemraum strukturiert analysiert und die bestehenden Herausforderungen im Umgang mit offenen, hochvariablen Betriebsbereichen automatisierter Fahrfunktionen herausgearbeitet. Auf Basis einer Untersuchung der Grundlagen der System-, Produkt- und Sicherheitsentwicklung sowie der sicherheitsbezogenen Normen ISO 26262 und ISO 21448 werden die Forschungsfragen abgeleitet, die den wissenschaftlichen Ansatz dieser Arbeit bestimmen.

In der ersten Konzeptionsphase wird eine vertikale Erweiterung des bestehenden Sicherheitslebenszyklus entwickelt, die neue normative Anforderungen, wie Betriebskonzept und Betriebsbereichsdefinition, szenariobasierte Betrachtungen sowie die Einbindung rechtlicher und regulatorischer Vorgaben, methodisch integriert und damit strukturelle Lücken in den aktuellen Sicherheitsnormen bzw. -standards schließt.

Die zweite Konzeptionsphase führt eine horizontale Erweiterung ein, welche den Sicherheitslebenszyklus durch einen agilen SafeDevOps-Ansatz, iterativ-inkrementelle Reifegradmodelle und eine Synchronisation mit dem Automotive-Produktentstehungsprozess inkl. der nahtlosen Anknüpfung der Phase des Betriebs, der Wartung und Außerbetriebnahme industriell operationalisiert.

Darauf aufbauend erfolgt im Verlauf der dritten Konzeptionsphase die Synthese eines modell- und simulationsbasierten Systementwicklungsrahmenwerks. Dieses zielt insbesondere darauf ab, die modellbasierte Systementwicklung auf der einen Seite als auch die Simulationsentwicklung auf der anderen Seite innerhalb einer ganzheitlichen Modellierungsmethode zu konsolidieren. Hierdurch entsteht ein durchgängiger, evidenzbasierter und wiederholbar evaluierbarer Ansatz zur Betriebssicherheitsentwicklung, welcher Unsicherheiten des offenen Kontexts adressiert und eine simulationsgestützte Sicherheitsargumentation ermöglicht.

Die abschließende Anwendung bzw. Fallstudie im Hinblick auf einen hochautomatisierten SAE-Level 4 Autobahnpiloten zeigt exemplarisch, wie der entwickelte Lebenszyklusprozess zu einer modellbasierten und simulativ ausführbaren Betriebssicherheitsargumentation führt. Auf Grundlage dessen wird der wissenschaftliche Mehrwert des Ansatzes im Hinblick auf Normungsfähigkeit, industrielle Umsetzbarkeit und methodische Erweiterbarkeit dargelegt.

Abstract

Ensuring the operational safety of highly automated road vehicles presents one of the fundamental challenges for their market introduction. This dissertation contributes to this challenge by developing a normatively integrated, agile, and model-based operational safety life-cycle process that systematically aligns standardization-related requirements with industrial development realities.

To this end, the dissertation first structures the problem space and analyzes the challenges that arise when handling open and highly variable operational design domains of automated driving functions. Building on an examination of core principles in systems, product, and safety engineering as well as the safety-related standards ISO 26262 and ISO 21448, the work derives the research questions that guide its scientific approach.

In the first conception phase, the dissertation develops a vertical extension of the existing safety life cycle that incorporates new normative requirements, such as the operational concept, the operational design domain definition, scenario-based analyses, and the integration of legal and regulatory specifications, and closes structural gaps in current safety norms and standards.

The second conception phase introduces a horizontal extension that industrializes the safety life cycle through an agile SafeDevOps approach, iterative maturity-level models, and synchronization with the automotive product development process, including seamless continuity into operation, maintenance, and decommissioning.

Building on this foundation, the third conception phase synthesizes a model- and simulation-based systems engineering framework. This framework unifies model-based systems engineering and simulation development within a single, coherent modeling methodology. As a result, the dissertation presents a continuous, evidence-driven, and repeatably evaluable approach to operational safety engineering that addresses uncertainties in open contexts and supports simulation-based safety argumentation.

A final application and case study focusing on a highly automated SAE-Level 4 highway pilot illustrates how the developed life-cycle process enables a model-based and simulation-executable operational safety argument. On this basis, the dissertation demonstrates the scientific added value of the approach with respect to standardization potential, industrial applicability, and methodological extensibility.

Danksagung

Mein besonderer Dank gilt meinem Doktorvater, Prof. Dr.-Ing. Eric Sax. Seine exzellente Betreuung, geprägt von fortwährender Unterstützung, fachlicher Klarheit und einem stets offenen, vertrauensvollen Austausch, hat diese Arbeit in entscheidender Weise geprägt. Ich danke ihm zutiefst dafür, dass er sich stets die Zeit genommen hat, meine Anliegen gründlich zu besprechen, und dass ich aus jedem Gespräch, wie auch aus unserem schriftlichen Austausch, mit einem klaren Plan und wertvollen neuen Impulsen hervorgegangen bin. Dadurch konnte ich mich fachlich ebenso wie persönlich weiterentwickeln. Besonders schätze ich, dass er mir auch während mehrerer industrieseitiger Betreuerwechsel sowie nach meinem Ausscheiden aus der Robert Bosch GmbH unverändert und ohne jede Einschränkung zur Seite stand.

Mein Dank gilt auch Prof. Dr. Simon Burton für die Übernahme des Korreferats und seinen weiterführenden und wertvollen Anmerkungen, die zur Schärfung dieser Dissertation beigetragen haben. Des Weiteren hat er mich bei der Veröffentlichung zweier Konferenzbeiträge mit großem Engagement unterstützt.

Ein weiterer Dank geht an meine ehemaligen Kollegen der Robert Bosch GmbH für das gemeinsame Brainstorming, die kritische Auseinandersetzung mit Konzepten, die anregenden Diskussionen und die erfolgreiche Zusammenarbeit in den frühen Jahren meiner Promotion. Besonders möchte ich hier an Marcel Mausser erinnern, der uns viel zu früh verlassen hat. Ebenso danke ich herzlich Hans-Leo Ross, Patrick Bertsch, Ole Hans und Armin Reisgys für ihren fachlichen Rat und ihre inhaltliche Unterstützung.

Auch möchte ich mich bei meinen aktuellen Kollegen Lailong Song, Ludwig Drees und Mehdi Farid bedanken, die mich nun intensiv darin unterstützen, die entwickelten Ansätze aus der Dissertation in Form eines szenariobasierten und datengetriebenen Sicherheitsrahmenwerks innerhalb der BMW Group zu verankern.

Mein tief empfundener Dank gilt schließlich meiner Familie. Dies gilt vor allem meinen Eltern, Matthias und Ana, welchen ich von Herzen für ihre unerschütterliche Unterstützung, ihren Glauben an mich und dafür, dass sie mir in allen Phasen dieser Arbeit den Rücken frei gehalten haben, danke.

Inhaltsverzeichnis

1 Einleitung

„Dies ist nicht das Ende. Es ist nicht einmal der Anfang vom Ende. Aber es ist, vielleicht, das Ende des Anfangs."

Sir Winston Churchill

Die Gesellschaft des 21. Jahrhunderts befindet sich in einem tiefgreifenden Transformationsprozess. Bereits 1995 veröffentlichte der Rat für Forschung, Technologie und Innovation folgende Aussage: *„Die Arbeits- und Lebensformen ändern sich weit fundamentaler als dies vielen Menschen heute noch erscheinen mag; die Welt ändert sich nicht nur in ihren technologischen, sondern auch in ihren wirtschaftlichen und kulturellen Strukturen. Die Gesellschaft befindet sich inmitten einer dritten technologischen Revolution, die in Form neuer Informations- und Kommunikationstechnologien alle Bereiche, vor allem Wissenschaft, Wirtschaft und Politik, aber auch den sozialen und kommunikativen Lebensbereich der Menschen schlechthin erfasst"* [1]. Im Jahre 2000 prognostizierte Achim Bühl die „virtuelle Gesellschaft des 21. Jahrhunderts" [2]. Heute, 24 Jahre später, ist bereits von einer vierten technologischen Revolution die Rede [3]. Schlagwörter wie Digitalisierung, Industrie 4.0, Internet der Dinge und Big Data haben sich im Sprachgebrauch fest verankert und nehmen vermehrt Einfluss auf das gesellschaftliche Leben [4]. Allerdings fällt dieser Transformationsprozess weltweit von Region zu Region unterschiedlich aus und wird von Nationen forciert, welche über eine hohe Wirtschaftsleistung verfügen [5]. Aufgrund dessen wird im Zuge der Dissertation der geografische Betrachtungsrahmen auf die Mitgliedsstaaten der Wirtschaftskommission für Europa der Vereinten Nationen (engl. *United Nations Economic Commission for Europe {UNECE}*) [6] begrenzt.

1.1 Mobilitätstrend automatisiertes Fahren

Der sich abzeichnende technologische Wandel beeinflusst auch die Mobilität. Diesbezüglich fordert die moderne Gesellschaft neue Mobilitätslösungen, um den Ansprüchen des Umweltschutzes, effizienter und ressourcenschonender Energieumwandlung, Verkehrsraum und Sicherheit gerecht zu werden. Schutz von Insassen, Fußgängern und Radfahrern vor den Risiken des Individualverkehrs wie beispielsweise dem konventionellen Automobil bzw. Kraftfahrzeug, nehmen bei der Fahrzeugsicherheit einen hohen Stellenwert ein. Nachfolgend wird unter einem Kraftfahrzeug ein Straßenfahrzeug verstanden, welches in der Lage ist, sich gewissermaßen „frei" auf der festen Erdoberfläche bzw. Straße zu bewegen. Demzufolge ist dieses nicht an Schienen, Stromleitungen oder Stromschienen fixiert. Dabei handelt es sich beispielsweise um einen Last- oder Personenkraftwagen. Im Zuge des sich anbahnenden Wandels spielen bei der individuellen Mobilität auf der Straße Themen wie Elektromobilität, alternative Antriebe sowie zukünftige Fahrzeug- und Mobilitätskonzepte wie das autonome bzw. automatisierte Fahren, vernetzte Fahrzeuge und geteilte Mobilität in zunehmendem Maße eine Rolle [7].

Im Kontext der Wissenschaft und Technik wird der Begriff „autonom" in den Forschungsbereichen der Robotik und künstlichen Intelligenz verwendet, um Systeme zu charakterisieren, welche die Fähigkeit haben Entscheidungen unabhängig bzw. autark zu treffen. In der Zwischenzeit hat sich diese Verwendung innerhalb des allgemeinen Sprachgebrauchs dahingehend erweitert, nicht nur die Entscheidungsfindung zu betreffen, sondern die gesamte Systemfunktionalität zu umfassen. Dadurch entwickelte sich der Begriff

„autonom“ zum Synonym des Begriffs „automatisiert“. Des Weiteren bezieht sich der Begriff der „Autonomie“ in der Rechtsprechung auf die Fähigkeit der „Selbstverwaltung“. In diesem Kontext ist die Verwendung des Begriffs „autonom“ im Sinne des automatisierten Fahrens inadäquat, da selbst die in Bezug auf die Technik am weitest fortgeschrittenen Systeme nicht „selbstverwaltend“ sind. Vielmehr basieren diese auf Algorithmen und befolgen ansonsten Befehle des Anwenders [8]. Auf Basis dieser Argumentation wird hier im weiteren Verlauf nur noch vom „automatisierten Fahren“ gesprochen.

Zur Kategorisierung des automatisierten Fahrens definiert die „Society of Automotive Engineers“ (SAE) [8] insgesamt sechs Automatisierungsstufen (vgl. Unterabschnitt 2.2.2). Diese reichen von keiner Automatisierung (Stufe 0), Fahrerassistenz (Stufe 1), Teilautomatisierung (Stufe 2), bedingte Automatisierung (Stufe 3), Hochautomatisierung (Stufe 4) bis hin zur Vollautomatisierung (Stufe 5). Das Gros der traditionellen Automobilbranche verfolgt Stand heute den Ansatz, Fahrerassistenzsysteme[1] als Entwicklungsgrundlage für das automatisierte Fahren zu verwenden. Fahrerassistenzsysteme mit maschineller[2] Wahrnehmung sind u.a. der Abstandsregeltempomat (engl. *Adaptive Cruise Control {ACC}*), der Spurhalteassistent (engl. *Lane Keeping Assistance System {LKAS}*), der Parkassistent (engl. *Parking Assistant*) sowie der Notbremsassistent (engl. *Emergency Brake Assistant*) (vgl. Abschnitt 2.2).

2016 waren 62 % der in Deutschland neu zugelassenen Personenkraftwagen mit einem Parkassistenzsystem ausgestattet. Rund 38 % der Neuwagen waren mit einem automatischen Notbremssystem versehen. Innerhalb eines Jahres verdoppelte sich der Anteil der Spurassistenzsysteme von 16 auf 32 %. Zwischen 2013 und 2016 wuchs die Anzahl der verbauten Abstandsregeltempomaten von 4 auf 19 % [9]. Dieser Trend galt auch für die europäischen Nachbarstaaten. Die Nachfrage nach Fahrerassistenzsystemen soll auch in den nächsten Jahren weiter zunehmen. Treiber der stetigen Weiterentwicklung von Fahrerassistenzsystemen sind u.a. Sicherheit, Komfort und Umweltschutz. Des Weiteren setzt beispielsweise die Europäische Union (EU) in einer neuen Verordnung „(EU) 2019/2144“ verstärkt auf Fahrerassistenzsysteme, um die Zahl der Getöteten und Schwerverletzten bei Straßenverkehrsunfällen weiter zu reduzieren [10]. Somit lässt sich eine Tendenz in Bezug auf die sukzessive Weiterentwicklung von Fahrerassistenzsystemen in Richtung von Fahrzeugführungssystemen[3] seitens der Gesetzgebung als auch des Mainstreams der Automobilbranche erkennen [11], [12]. Daraus resultierend soll der Fahrer bei der Bewältigung der Fahraufgabe[4] mehr und mehr entlastet werden und die Rolle eines Überwachers[5] einnehmen. Jedoch werden bei dieser Herangehensweise neue Herausforderungen und Probleme der Interaktion zwischen Mensch und Fahrzeugführungssystem hervorgerufen.

1.1.1 Stufenweise Einführung des automatisierten Fahrens

Bereits 1983 war in [13] von sogenannten „Ironien der Automatisierung“ die Rede. Dort wird u.a. aufgeführt, dass durch die Automatisierung[6] nicht per se Schwierigkeiten beseitigt werden, sondern dies paradoxerweise sogar zu Komplikationen für den menschlichen Bediener führen kann (vgl. Unterabschnitt 2.2.3). In [14] werden aus der Perspektive menschlicher Faktoren Fragen des Systemdesigns sowie der Forschung der Interaktion zwischen Mensch und automatisiertem System behandelt. Sowohl in [13] als

[1] Fahrerassistenzsystem (vgl. Definition 2.5)

[2] Maschinelle Wahrnehmung im Sinne der visuellen Wahrnehmung bzw. Perzeption der externen Kraftfahrzeug- und Verkehrsumgebung.

[3] Fahrzeugführungssystem (vgl. Definition 2.6)

[4] Fahraufgabe (vgl. Definition 2.1)

[5] Überwachung (vgl. Definition 2.7)

[6] Automatisierung (vgl. Definition 2.4)

auch in [14] kommt man zum Ergebnis, dass der Mensch im Allgemeinen nicht dazu prädestiniert ist, automatisierte Systeme zu überwachen. Tritt ein Fehler ein, hat der menschliche Überwacher nur ein bestimmtes Zeitfenster, um die Situation fürs Erste zu erfassen, daraufhin richtig zu interpretieren und schließlich korrekt einzugreifen. In summa stellt dies den Menschen vor neue Herausforderungen [15], [16], [17]. In [18] führen die dort angestellten Untersuchungen gar zur Hypothese, dass im Fehlerfall Systeme des automatisierten Fahrens, bei denen ein Eingriff des Fahrers erwartet wird, mit geringerer Automatisierungsstufe sicherer sind als jene mit höherer Automatisierungsstufe. Weitere Studien wie [19] stützen diese Hypothese. Google-Tochter Waymo hat nach nur sechs Monaten dessen Versuchsprogramm eines fahrerüberwachten Autopiloten aufgrund der mangelnden Achtsamkeit der Probanden eingestellt. Ähnlich wie bei Waymo hat die National Aeronautics and Space Administration (NASA) festgestellt, dass Menschen bei Autopilotsystemen mit einem hohen Reifegrad, bei denen beinahe keine Interaktion mehr erforderlich ist, Schwierigkeiten haben, ihre Aufmerksamkeit dauerhaft auf die Überwachung eines solchen Systems zu richten [20]. Des Weiteren kommen ungeklärte Themen der Rechtsprechung und Haftung im Falle eines Unfalls erschwerend hinzu [21].

Bis heute bleiben somit Fragen in Bezug auf die Erfassung und allgemeingültige Beschreibung der Interaktion zwischen Mensch und automatisiertem System bei der kooperativen Bewältigung der Fahrzeugführung ungeklärt. In der Zwischenzeit wird diskutiert, ob sich hierbei ein evolutionäres oder aber ein revolutionäres Entwicklungskonzept durchsetzen wird [22], [23]. Die revolutionäre Herangehensweise sieht vor, die gesamte Verantwortung der Durchführung der Fahraufgabe in dafür vorgesehenen Betriebsbereichen[7] des Straßenverkehrs auf das hochautomatisierte Kraftfahrzeug zu übertragen, und zwar auch im Fehlerfall. Neue Akteure auf dem Automobilmarkt, wie z.B. die Google-Tochter Waymo, verfolgen diesen radikaleren Ansatz [24], [25]. Die von der Europäischen Union ausgerufene „Vision Zero“ beinhaltet die Reduzierung bzw. Eliminierung verkehrsbedingter Unfälle mit schwereren Verletzungen oder gar Todesfolge. Aber auch die Verringerung der Umweltverschmutzung sowie Steigerung der mobilen Effizienz in punkto Energie, Zeit und Ressourcen sind elementarer Teil dieser Maßgabe [26]. Die Erhöhung der Verkehrssicherheit gilt als stärkster Motivator des hochautomatisierten Fahrens, da laut [27] 90 % der Verkehrsunfälle auf menschliches Fehlverhalten zurückzuführen sind. Ferner bietet das hochautomatisierte Fahren Chancen bei der Verbesserung des Verkehrsflusses.

Des Weiteren würde hochautomatisiertes Fahren in Sachen Komfort und Wirtschaftlichkeit neue Möglichkeiten eröffnen. Die Anwender solcher Kraftfahrzeuge könnten sich während der Fahrt anderen Tätigkeiten zuwenden und würden dadurch Zeit gewinnen. Hierdurch könnte je nach Tätigkeitsfeld bereits auf dem Arbeitsweg mit der Arbeit begonnen oder diese fortgesetzt werden. Aber auch für Anbieter von Online-Diensten wie Google, Amazon, Facebook etc. bietet der Zugewinn an Zeit möglicher Kunden entsprechendes Marktpotenzial. Auf den weltweiten Straßenverkehr bezogen beinhaltet durchschnittlich jede freie extra Minute im Kraftfahrzeug einen möglichen Umsatz von bis zu fünf Milliarden Euro jährlich [28]. Im öffentlichen Personentransport als auch im Güterverkehr könnten Mobilitäts- und Transportdienstleistungen verwirklicht werden, welche derzeit noch von einem menschlichen Berufsfahrer abhängig und somit teilweise unwirtschaftlich sind. Zum einen bieten sich durch das Ersetzen des menschlichen Fahrers Einsparpotenziale, was Lohnkosten betrifft. Zum anderen offerieren hochautomatisierte Kraftfahrzeuge eine höhere Flexibilität der Einsatzzeiten, da nicht mehr auf die vorgeschriebenen Ruhepausen der Fahrer Rücksicht genommen werden müsste [29]. Darüber hinaus würden sich neue Mobilitätskonzepte wie beispielsweise die geteilte Mobilität verwirklichen lassen [30], [31]. Allein in Deutschlands Städten könnte

[7] Betriebsbereich (vgl. Definition 2.10)

bis ins Jahr 2035 der Betrieb von hochautomatisierten Fahrdienstflotten ein jährliches Umsatzvolumen von bis zu knapp 17 Milliarden Euro generieren [32].

Industrie und Forschung arbeiten seit Jahren an der Marktreife solcher Systeme. Trotz Ankündigungen verschiedener Hersteller bleibt die Markteinführung hochautomatisierter Kraftfahrzeuge für den privaten Personenverkehr bisher aus [33]. Expertenschätzungen zufolge kann dies noch mehrere Jahre in Anspruch nehmen [34], [35]. Die Gründe hierfür sind differenziert. Auf der technischen Seite sind Schwierigkeiten bei der Integration von Funktionen, die auf künstlicher Intelligenz (KI) bzw. maschinellem Lernen[8] beruhen, hervorzuheben. Hinzu kommen Themen der Echtzeit- und Datenanalyse sowie die Validierung[9], die Verifizierung[10] und das Testen hochautomatisierter Systeme. Auf der nichttechnischen Seite rangieren Herausforderungen der Zulassung, Haftung, Gesetzgebung, Ethik und Moral sowie Kundenakzeptanz an oberster Stelle [37]. Laut einer in Deutschland im Jahr 2024 durchgeführten Umfrage sieht etwa nur die Hälfte der Befragten die Möglichkeit des hochautomatisierten Fahrens positiv [38]. Die geringe Akzeptanz lässt sich auf ein Zusammenspiel von sicherheitsbezogenen Vorbehalten, mangelndem Vertrauen in technologische Systeme, ethischen Dilemmata sowie kulturell bedingten Werthaltungen zurückführen. Eine andere Studie kommt zum Ergebnis, dass sich potenzielle Kunden hochautomatisierter Kraftfahrzeuge nur über eine valide Erfolgsbilanz des sicheren Einsatzes solcher Fahrzeuge im öffentlichen Straßenverkehr überzeugen ließen [39]. Konkret würde dies bedeuten, dass nachweislich durch die Anwendung hochautomatisierter Kraftfahrzeuge die Anzahl von verkehrsbedingten Unfällen mit schwereren Verletzungen oder gar Todesfolge signifikant reduziert wird.

In [40] wird davon ausgegangen, dass die Wahrscheinlichkeit eines durch einen Unfall verursachten Todesfalls pro Stunde menschlichen Fahrens weltweit statistisch gesehen bei ca. 10^{-6} liegt. Dabei handelt es sich um einen Durchschnittswert, welcher unabhängig von den regionalen Streckenverhältnissen, Witterungsbedingungen etc. ist. Weiter wird in [40] die Annahme getroffen, dass die Gesellschaft hochautomatisierte Fahrzeuge nur dann akzeptieren wird, wenn die Todesrate um drei Größenordnungen reduziert wird, was einer Wahrscheinlichkeit von 10^{-9} pro Stunde[11] entspräche. Überträgt[12] man diese Hypothese beispielsweise auf die USA, so müsste sich die dortige Anzahl Verkehrstoter von 37806 pro Jahr auf 70 reduzieren[13]. Bis heute herrscht allerdings weder in Industrie und Forschung noch innerhalb der Gesetzgebung des Straßenverkehrs Konsens darüber, was für ein quantifizierbarer Wert in Bezug auf die Wahrscheinlichkeit eines durch einen Unfall verursachten Todesfalls pro Stunde hochautomatisierten Fahrens aus der Perspektive der Gesellschaft als tolerierbar angesehen würde. Zumindest besteht Einigkeit dahingehend, dass hochautomatisierte Kraftfahrzeuge in deren Sicherheitsbilanz besser abschneiden müssen als der menschliche Durchschnittsfahrer [42]. Sonst wird es nicht möglich sein, eine breite Akzeptanz in

[8] Maschinelles Lernen als Teilgebiet der künstlichen Intelligenz (KI).

[9] Der Begriff „Verifikation“ kann informell mit der Frage beschrieben werden, ob das Produkt richtig entwickelt wird [36].

[10] Der Terminus „Validierung“ kann informell mit der Frage beschrieben werden, ob das richtige Produkt entwickelt wird [36].

[11] 10^{-9} ist ein Wert, der auf das Versagen von technischen Systemen abgebildet wird. Darauf werden Daten mit der tatsächlichen Unfallhäufigkeit projiziert. Konkret basiert diese Abschätzung auf dem technischen Versagen von Airbags sowie auf Luftfahrtstandards, worin festgelegt wird, dass die Wahrscheinlichkeit des Ablösens einer Tragfläche eines Flugzeugs pro Flugstunde 10^{-9} nicht überschreiten darf [40].

[12] Unter der Annahme, dass herkömmliche Kraftfahrzeuge vollständig durch vollautomatisierte Kraftfahrzeuge ersetzt werden. Des Weiteren wird davon ausgegangen, dass sowohl die Gesamtzahl an gefahrenen Kilometern als auch die verbrachte Dauer an Stunden im Kraftfahrzeug unverändert bleiben.

[13] Zahlen beziehen sich auf das Jahr 2016 in den USA. Diese sind auch Mitgliedstaat der UNECE. Dort kamen bei Verkehrsunfällen insgesamt 37806 Personen zu Tode [41]. Bei einer geschätzten Dauer von 70 Mrd. Stunden im Kraftfahrzeug über das Jahr gerechnet, ergibt das eine Wahrscheinlichkeit von 0.54×10^{-6}. Um bei gleicher Dauer eine Wahrscheinlichkeit von 10^{-9} zu erreichen, müsste die Anzahl von Toten um den Faktor 540 auf insgesamt 70 reduziert werden.

Bezug auf die Gesellschaft, die Gesetzgebung als auch die Medien zu erreichen. Die öffentliche Diskussion von Unfällen mit automatisierten Kraftfahrzeugen würde zu einer Verunsicherung seitens potenzieller Kunden führen. Beispiele wie der tödliche Uber-Unfall [43] sowie Unfälle in Verbindung mit der Anwendung des Tesla-Autopiloten [44] bestätigen dies.

1.1.2 Gewährleistung der Betriebssicherheit hochautomatisierter Kraftfahrzeuge im Produktlebenszyklus

Die grundsätzlichen Aufgaben des menschlichen Fahrers im Straßenverkehr liegen in der Bestimmung der Spur, in der Überwachung der Kraftfahrzeug- und Verkehrsumgebung sowie im sicheren Führen des Kraftfahrzeugs (vgl. Unterabschnitt 2.1.1). Durch das Ersetzen des menschlichen Fahrers werden diese Aufgaben auf das hochautomatisierte Kraftfahrzeug übertragen. Dies führt dazu, dass dieses in einen anderen Bezug bzw. Kontext, was die Kraftfahrzeug- und Verkehrsumgebung angeht, gesetzt wird. Hochautomatisierte Kraftfahrzeuge gelten als sogenannte offene Systeme, welche mit der Fahrzeugumgebung vernetzt sind und dabei Materie sowie Energie austauschen [45]. Dabei werden solche Fahrzeuge während ihrer Nutzung Myriaden an unterschiedlichsten Betriebssituation ausgesetzt sein und dadurch in deren Verhalten maßgeblich beeinflusst (siehe Abbildung 1.1). Diese Situationen reichen über Straßen- und Witterungsverhältnisse wie Nebel, Schnee, Rauch etc. (vgl. Unterabschnitt 2.2.3) bis hin zu Angriffen auf die Informations- und Datenintegrität (engl. *Cybersecurity*) sowie Sabotageakten wie beispielsweise das widerrechtliche Entfernen der Straßenbeschilderung vor gefährlichen Streckenabschnitten. Zusätzlich können kritische Situationen wie z.B. Reifenpannen, Sensor- und Aktuatorenausfälle bzw. deren Fehlverhalten sowie Fehler in den Algorithmen der Wahrnehmung und Entscheidungsfindung entstehen [46]. Unter all diesen Bedingungen muss ein sicheres Kraftfahrzeugverhalten gewährleistet werden.

Des Weiteren führt das Ersetzen des menschlichen Fahrers dazu, dass das hochautomatisierte Kraftfahrzeug in einen neuen Kontext, was die Gesetzgebung des Straßenverkehrs betrifft, gebracht wird (siehe Abbildung 1.1). Dadurch müssen hochautomatisierte Kraftfahrzeuge befähigt sein, die situationsbedingten Straßenverkehrsregeln wie beispielsweise *„Wer am Verkehr teilnimmt hat sich so zu verhalten, dass kein anderer geschädigt, gefährdet oder mehr, als nach den Umständen unvermeidbar, behindert oder belästigt wird“* [47] stets zu erkennen und einzuhalten. Des Weiteren müssen diese im Stande sein den Insassen das Gefühl zu vermitteln, dass das Verhalten des Fahrzeugs nachvollziehbar und rational ist. Zudem müssen hochautomatisierte Kraftfahrzeuge das Verhalten anderer Fahrzeuge antizipieren als auch mit den menschlichen Fahrern konventioneller Kraftfahrzeuge interagieren können [48].

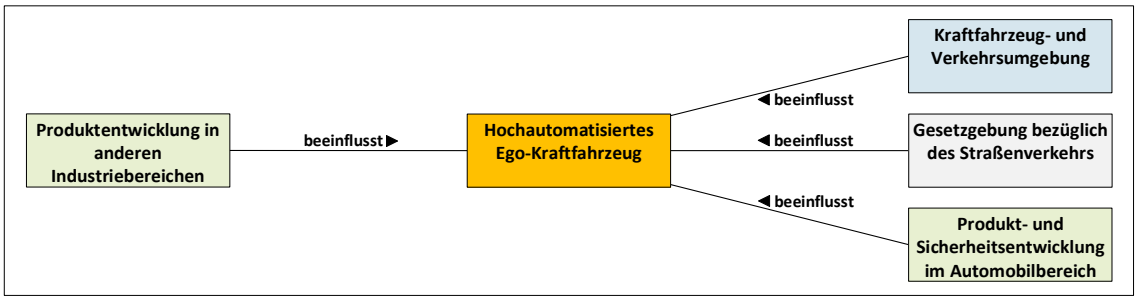


Abbildung 1.1: Kontext eines hochautomatisierten Ego-Kraftfahrzeugs inklusive der Domänen bzw. Interessenvertreter, welche die Gewährleistung der Sicherheit über den gesamten Produktlebenszyklus beeinflussen.

Beispielsweise könnte entweder ein zu vorsichtiger oder aber auch ein zu aggressiver Fahrstil im hochautomatisierten Kraftfahrzeug implementiert sein. Die Folge wäre zumindest die Störung des Verkehrsflusses und im schlimmeren Falle gar größere Sicherheitsprobleme. Erschwerend kämen hier Verkehrsteilnehmer jeder Art hinzu, welche sich nicht an die gegebenen Verkehrsregeln halten und aus der Perspektive des hochautomatisierten Kraftfahrzeugs irrationales Verhalten aufweisen [49]. Alles in allem müssen sich hochautomatisierte Kraftfahrzeuge in deren Umgebung derart verhalten, dass dies für alle anderen Verkehrsteilnehmer wie Radfahrer, Fußgänger usw. verständlich, vernünftig und vor allem vorhersehbar erscheint.

Auch was die Produktentwicklung im Automobilbereich angeht, wird das Kraftfahrzeug durch den Prozess[14] der Hochautomatisierung in einen andersgearteten Bezug gesetzt (siehe Abbildung 1.1). Bei der Planung und Durchführung eines Projekts bezüglich der Entwicklung und Inbetriebnahme eines sicherheitsrelevanten Produkts, wird durch das normative Umfeld (Automotive-Sicherheitsnorm ISO 26262 [50] sowie generische Sicherheitsnorm IEC 61508 [51]) die Anwendung eines phasenorientierten Vorgehensmodells[15] wie das V-Modell verlangt [52]. Innerhalb der Automobilindustrie hat sich das V-Modell als Prozessreferenz (vgl. Unterabschnitt 3.2.3) etablieren können und wird dort demzufolge eingesetzt [53]. Dabei wird der gesamte Produktlebenszyklus[16] berücksichtigt.

Agile Methoden und Ansätze (vgl. Unterabschnitte 3.2.4 und 3.2.5) motivieren sich aus der höheren Flexibilität von softwaregetriebenen Umfängen und verfolgen im Gegensatz zum klassischen V-Modell einen iterativ-inkrementellen Ansatz. Diese fokussieren sich vornehmlich auf die reine Erstellung von Arbeitsprodukten und versehen deren Planung, Steuerung und Dokumentation mit einer geringeren Priorität. Dies steht wiederum in direktem Widerspruch zur grundlegenden Stringenz der Planung sowie der Dokumentations- und Nachweispflicht gemäß V-Modell. Hier spielen die Abstimmung zwischen verschiedenen Verantwortungsbereichen und Domänen, die Planungssicherheit entlang der Lieferketten und klar definierte Entwicklungsziele eine tragende Rolle.

In Bezug auf die Sicherheitsentwicklung im Automobilbereich gilt die ISO 26262 als der maßgebende Standard. Dieser hat seit seiner Einführung einen fundamentalen Einfluss auf die Entwicklung von elektrisch/elektronischen (E/E)-Systemen genommen. Das Schlüsselkonzept der ISO 26262 besteht darin, systematische und zufällige Fehler der technischen E/E-Systeme so zu beherrschen, dass daraus keine inakzeptablen Fehlfunktionen entstehen, auch wenn nicht alle potenziellen Fehler vollständig vermieden werden können (vgl. Unterabschnitt 5.2.1). Hierbei beschreibt diese einen sogenannten Sicherheitslebenszyklus[17]. Somit beeinflussen die Anforderungen an Sicherheit sämtliche Phasen des Produktentwicklungsprozesses und darüber hinaus auch den gesamten Produktlebenszyklus von sicherheitsbezogenen E/E-Systemen und E/E-Architekturen (siehe Abbildung 5.2). Jedoch wird in der ISO 26262 eine Betrachtung eines hochautomatisierten Kraftfahrzeugs als Gesamtsystem sowie dessen Zusammenspiel mit der Kraftfahrzeug- und Verkehrsumgebung im Sinne der Fahrdynamik nicht adressiert.

[14] Prozess (vgl. Definition 3.5)

[15] Vorgehensmodell (vgl. Definition 3.4)

[16] Ein Produktlebenszyklus umfasst sämtliche Phasen, angefangen bei der Planung und Entwicklung über die Produktion und Inbetriebnahme bis hin zur Außerbetriebnahme und Entsorgung, eines Produkts [54].

[17] Ein Sicherheitslebenszyklus umfasst die wichtigsten Sicherheitsmaßnahmen während der Konzeptphase, Produktentwicklung, Produktion, Betrieb, Service und Außerbetriebnahme [50].

In Ergänzung zur ISO 26262 wurde 2022 die ISO 21448, welche auch als sogenannte „Safety Of The Intended Functionality“ (SotiF) Norm bezeichnet wird, veröffentlicht [55]. Deren Schwerpunkt liegt in der Entwicklung und Absicherung von automatisierten Fahrzeugführungssystemen. Die ISO 21448 soll dabei die in der ISO 26262 fehlende Betrachtung von Gefährdungen, die jeweils durch begrenzte Leistungsfähigkeit der Nominalfunktionen, Sensortechnologien, Algorithmen oder vorhersehbarem Missbrauch wie z.B. Nutzerüberlastung verursacht werden, übernehmen (vgl. Unterabschnitt 5.2.2). Allerdings werden Aspekte wie eine systematische Beschreibung des sicheren dynamischen Fahrzeugverhaltens als auch der Kraftfahrzeug- und Verkehrsumgebung im Sinne des Betriebsbereichs weder prozessual noch methodisch abgedeckt. Auch die sicherheitstechnische Betrachtung von Fahrzeug-zu-Fahrzeug-Kommunikation (engl. *Vehicle-to-Vehicle-Communication {V2V}*) sowie der Fahrzeug-zu-Infrastruktur-Kommunikation (engl. *Vehicle-to-Infrastructure-Communication {V2I}*) im Sinne von V2X (engl. *Vehicle-to-Everything-Communication*) wird nicht umfassend berücksichtigt. Diese Kommunikationsmöglichkeiten könnten z.B. verwendet werden, um Fahrerunterstützung und aktive Sicherheitsdienste wie Kollisionswarnung, aktuelle Verkehrs- und Wetterinformationen oder aktive Navigationssysteme zu realisieren [56].

Dadurch fehlt ein ganzheitlicher Standardisierungs- bzw. Normungsansatz, welcher die jeweiligen Sicherheitsthemen im Sinne eines gesamtheitlichen Betriebssicherheitslebenszyklusprozesses für die Entwicklung als auch den Betrieb hochautomatisierter Kraftfahrzeuge harmonisiert und zusammenführt. Demzufolge ist es erforderlich, dass die Produktentwicklung einschließlich der Sicherheitsentwicklung den richtigen Bezug bzw. Kontext und somit die richtige Perspektive findet, um sichere hochautomatisierte Kraftfahrzeuge entwickeln zu können. Aufgrund dessen ist es auch zweckdienlich, dass Methoden und Techniken aus anderen Industriebereichen, wie beispielsweise der Automatisierungstechnik, der Robotik, der Luftfahrt usw. in Betracht gezogen werden, da diese über mehr Erfahrung und ein fundierteres Systemwissen im Bereich der Automatisierung verfügen (siehe Abbildung 1.1).

Alles in allem lässt sich die Herausforderung der Gewährleistung der Sicherheit bzw. Betriebssicherheit[18] hochautomatisierter Fahrzeuge auf zwei Kernthemen konzentrieren. Zum einen ist dies der Paradigmenwechsel in der Entwicklung der Fahraufgabe in der Kraftfahrzeug- und Verkehrsumgebung, welche durch die Automatisierung vom Menschen auf das hochautomatisierte Kraftfahrzeug übertragen wird. Hierdurch entstehen Abhängigkeiten zwischen hochautomatisiertem Kraftfahrzeug und dessen Betriebsbereich, die sich angefangen auf der Systemebene bis hin zur Implementierung bzw. Realisierung auf Hardware- und Softwareebene auswirken. Zum anderen ist dies die Multi- und Interdisziplinarität der beteiligten Domänen bzw. Interessenvertreter (engl. *Stakeholder*) (siehe Abbildung 1.1).

Hinzu kommt die Problematik immer umfangreicherer software-basierter Funktionalitäten, hervorgerufen durch Automatisierung und Konnektivität. Dies führt zu einer Verlagerung weg von verteilten hin zu zentralisierten Systemarchitekturen und zur Einführung wesentlich anspruchsvollerer Hardware-Plattformen und Software-Architekturen (vgl. Abschnitt 4.2). Die Anzahl der implementierten Funktionen hat in den vergangenen Jahrzehnten kontinuierlich zugenommen. Für die Zukunft ist mit einer weiteren Steigerung der funktionalen Vielfalt pro Fahrzeug zu rechnen (siehe Abbildung 1.2). In Zahlen ausgedrückt hatte ein Kraftfahrzeug 2010 in etwa 10 Millionen Software Codezeilen. 2016 waren es bereits 150 Millionen [57]. Jaguar Land Rover rechnet für die Verwirklichung des hochautomatisierten Fahrens mit mindestens einer Milliarde Software Codezeilen [58]. All dies führt zu einer Komplexität, welche nicht mit einer ein-

[18] Betriebssicherheit (vgl. Definition 5.16)

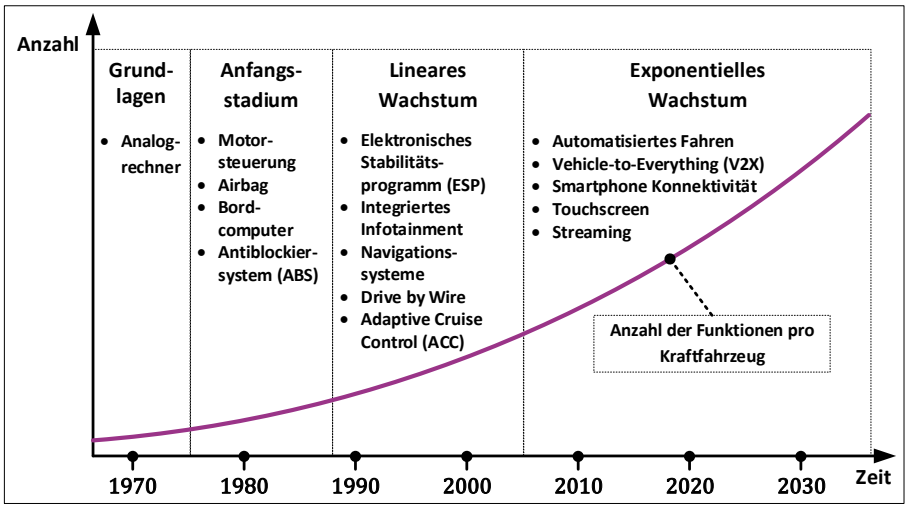


Abbildung 1.2: Zunahme der Anzahl an Funktionen im Kraftfahrzeug (in Anlehnung an [59]).

All dies führt zu einer Komplexität, welche nicht mit einer einzelnen rein technischen Lösung zu bewältigen ist, sondern einen inter- und multidisziplinären Systementwicklungsansatz unter Einbeziehung iterativ-inkrementeller Vorgehensweisen aus dem agilen Umfeld erfordert.

1.2 Zielsetzung, methodisches Vorgehen, Bewertungskriterien und Aufbau der Dissertation

Um die Herausforderungen im Zuge der Gewährleistung der Betriebssicherheit hochautomatisierter Kraftfahrzeuge zukünftig beherrschbarer zu machen, leistet diese Dissertation einen Beitrag durch die Gestaltung eines Betriebssicherheitslebenszyklusprozesses. Das Themengebiet und damit den Schwerpunkt der Dissertation bildet hierfür die Domänen der Automotive-System- und Sicherheitsentwicklung. Basierend auf einer Analyse von Wissenschaft, Forschung und Technik (vgl. Abschnitte 6.2, 6.3 und 6.4) stehen folgende Forschungsfragen (FF) im Fokus:

- **FF 1: Wie lässt sich ein Lebenszyklusprozess entwickeln, der die Automotive-Sicherheitsnormen ISO 26262 und ISO 21448 erweitert, um die Betriebssicherheit hochautomatisierter Fahrfunktionen sicherzustellen?**

- **FF 2: Wie kann dieser betriebssicherheitsbezogene Lebenszyklusprozess ausgestaltet werden, um eine agile und industrielle Umsetzung zu ermöglichen?**

- **FF 3: Wie kann dieser agile Betriebssicherheitslebenszyklusprozess im Rahmen eines modellbasierten Systementwicklungsrahmenwerks methodisch und praktisch umgesetzt werden?**

Zur Beantwortung dieser Forschungsfragen wird ein mehrstufiges systematisches Vorgehen angewandt:

1. **Analytisch-deskriptiver Ansatz:** Systematische Untersuchung bestehender Normen, Standards, Entwicklungsprozesse und Forschungsarbeiten zur Betriebssicherheit hochautomatisierter Kraftfahrzeuge.

2. **Konzeptionelle Synthese:** Entwicklung eines Betriebssicherheitslebenszyklusprozesses, bestehend aus einer vertikalen Erweiterung der klassischen Sicherheitsnormen sowie einer horizontalen Erweiterung durch iterative, inkrementelle Entwicklungs- und Nachweiszyklen.

3. **Modellbasierte Methodenanwendung:** Integration des Prozessmodells in ein modellbasiertes Systementwicklungsrahmenwerk zur strukturierten Verknüpfung von funktionalen, logischen und technischen Architekturmodellen.

4. **Validierung durch Fallstudie:** Methodische und praktische Evaluation des Ansatzes anhand eines exemplarischen hochautomatisierten SAE-Level-4 Autobahnpiloten. Dies umfasst u.a. eine modellbasierte Betriebsbereichsdefinition, die Szenarioanalyse sicherheitskritischer Manöver sowie eine simulationsbasierte Nachweisführung.

Mit Hilfe dieses methodischen Ablaufs wird sichergestellt, dass sowohl ein wissenschaftlich fundierter Beitrag geleistet als auch eine praxisnahe Umsetzbarkeit der entwickelten Lösungsansätze demonstriert wird. Für die systematische Bewertung der wissenschaftlichen Aktivitäten und des entwickelten Lösungsansatzes werden im Rahmen dieser Dissertation entsprechende Kriterien herangezogen (siehe Tabelle 1.1). Diese bilden die Grundlage für die spätere Evaluation der Ergebnisse (vgl. Unterabschnitt 9.2.2).

Tabelle 1.1: Kriterien zur Bewertung der wissenschaftlichen Ergebnisse der Dissertation.

Kriterium	Beschreibung
Skalierbarkeit	Fähigkeit des entwickelten Prozess- oder Methodenansatzes, auf unterschiedliche System-, Architektur- oder Granularitätsebenen übertragen zu werden.
Kompatibilität	Anschlussfähigkeit des Ansatzes an bestehende Normen, Industriestandards und etablierte Entwicklungs-, Test- und Verifikationsprozesse.
Kohärenz der Nachweisführung	Konsistenz und Nachvollziehbarkeit entlang von Evidenzen, Argumenten und Behauptungen über alle Lebenszyklusphasen hinweg.
Modellbasierte Integrationstiefe	Durchgängigkeit, Wiederverwendbarkeit und Abdeckung modellbasierter Artefakte über mehrere Abstraktionsebenen hinweg.
Praktische Anwendbarkeit	Industrielle Umsetzbarkeit und Unterstützung der Sicherheitsargumentation und Verifikation.
Umgang mit Unsicherheiten	Identifizierung und Behandlung epistemischer (unvollständiges Wissen) und aleatorischer (unvermeidbare Variabilität oder Zufälligkeit) Unsicherheiten sowie Handhabung verbleibender Limitierungen.

Abbildung 1.3 stellt den strukturellen Aufbau dieser Dissertation dar. Die Grundlagen des automatisierten Fahrens in Kapitel 2 werden durch den aktuellen Stand von Wissenschaft und Technik in Bezug auf den Produktlebenszyklus in Kapitel 3, die Systementwicklung in Kapitel 4 sowie der Sicherheit im Automobilbereich in Kapitel 5 ergänzt. Auf Basis des aktuellen Stands von Wissenschaft und Technik wird der Forschungsbedarf in Kapitel 6, welcher im Zuge der Dissertation bearbeitet wird, identifiziert. Die Kapitel 1 - 6 bilden somit den Problemraum der Dissertation ab. Auf dem identifizierten Forschungsbedarf basierend, wird in Kapitel 7 ein agiler Betriebssicherheitslebenszyklusprozess für die Hochautomatisierung von Kraftfahrzeugen entworfen. Dieser bildet wiederum die Grundlage für die Synthese einer modellbasierten si-

mulativ ausführbaren Betriebssicherheitsargumentation für die Längs- und Querführung eines hochautomatisierten Autobahnpiloten in Kapitel 8. Dementsprechend repräsentieren die Kapitel 7 - 8 den Lösungsraum dieser Dissertation. Kapitel 9 fasst die Ergebnisse sowie den wissenschaftlichen Beitrag dieser Dissertation zusammen und zeigt im Ausblick mögliche Anknüpfungspunkte auf.

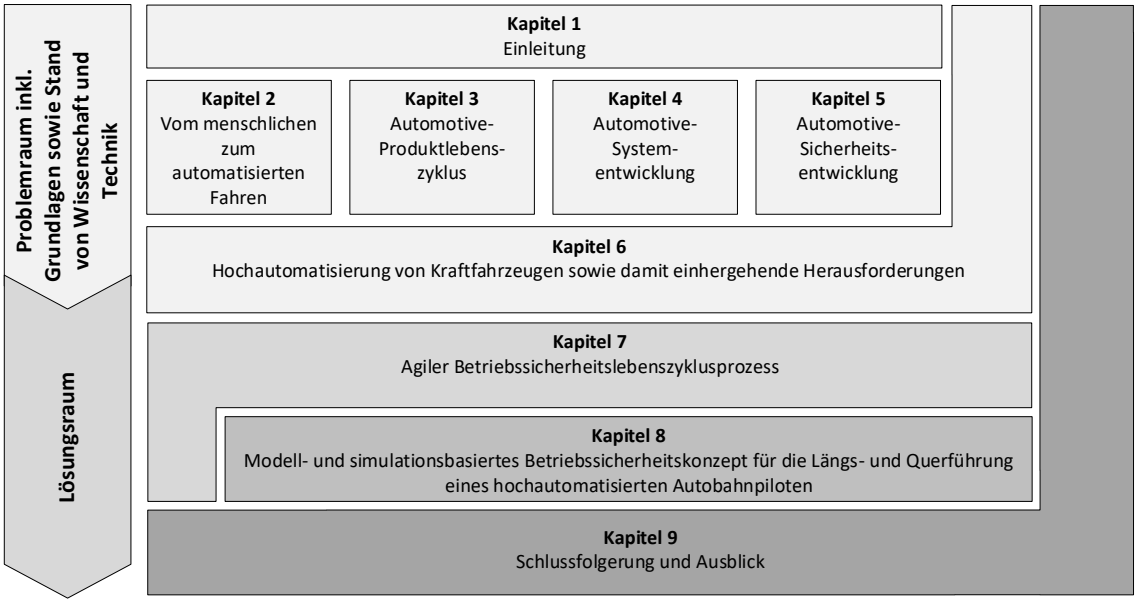


Abbildung 1.3: Aufbau der Dissertation.

2 Vom menschlichen zum automatisierten Fahren

„Wir haben unsere Umwelt so radikal verändert, dass wir uns jetzt selbst ändern müssen, um in dieser neuen Umwelt existieren zu können."

Norbert Wiener

Die Geschichte des Automobils begann, initiiert durch die Erfindung von Carl Benz 1886, vor mehr als 130 Jahren. Zwei Jahre später unternahm Bertha Benz die erste Fernfahrt von Mannheim nach Pforzheim und legte dabei eine Distanz von über 100 km zurück [60]. In den darauffolgenden Jahrzehnten revolutionierte das Automobil die Fortbewegung der modernen Gesellschaft und ermöglicht dem Großteil der Bevölkerung bis zum heutigen Zeitpunkt individuelle Mobilität. Zudem errang dieses in ökonomischen Gesichtspunkten außerordentliche Bedeutung und gilt fortwährend als Innovationstreiber innerhalb von Industrie und Forschung. Das Automobil wurde seit dessen Erfindung technologisch kontinuierlich weiterentwickelt. Allerdings hat sich an der Rolle des menschlichen Fahrers seit der Jungfernfahrt von Bertha Benz grundsätzlich nicht geändert. Dessen Hauptaufgaben im Straßenverkehr liegen in der Wahrnehmung der Kraftfahrzeug- und Verkehrsumgebung, der Planung von Handlungen zur Navigation und Bahnführung sowie in der Ansteuerung der Aktuatorik des Kraftfahrzeugs. Hierbei haben Fahrerassistenzsysteme den Zweck, den menschlichen Fahrer bei dessen Aufgaben zu unterstützen. Der Mobilitätstrend des automatisierten Fahrens geht darüber hinaus und versucht diesen mehr und mehr zu entlasten oder gar vollständig zu ersetzen. Daher werden im Verlauf dieses Kapitels zunächst die für das Verständnis dieser Dissertation notwendigen Aspekte der Rolle des menschlichen Fahrers im Straßenverkehr illustriert. Daraufhin werden Fahrerassistenzsysteme sowie entsprechende Grundlagen und ein aktueller Stand von Wissenschaft und Technik in Bezug auf das automatisierte Fahrens dargestellt.

2.1 Der menschliche Fahrer als Vorbild automatisierter Systeme

Die Führung eines Kraftfahrzeugs im öffentlichen Straßenverkehr bzw. in der dynamischen Kraftfahrzeug- und Verkehrsumgebung wird täglich von Millionen von Menschen bewältigt. Bei dieser Handlung geht es überwiegend darum, wahrgenommene Informationen in angebrachte Reaktionen umzusetzen. Dabei entstehen permanente Wechselwirkungen zwischen menschlichem Fahrer, Ego-Kraftfahrzeug als auch Kraftfahrzeug- und Verkehrsumgebung (siehe Abbildung 2.1). In diesem Zusammenhang nimmt der Fahrer Facetten wie den Straßenverlauf, geltende Verkehrsvorschriften sowie das aktuelle Verkehrsgeschehen wahr. Des Weiteren beobachtet dieser das unmittelbare Kraftfahrzeugverhalten und manipuliert dieses bei gegebener Notwendigkeit. Das Ego-Kraftfahrzeug reagiert auf die Handlungen des Fahrers sowie auf Einflüsse aus der Kraftfahrzeug- und Verkehrsumgebung wie z.B. Straßen- und Witterungsbedingungen mit einer entsprechenden Fahrzeugbewegung bzw. Fahrdynamik. Infolgedessen löst der Mensch bei dessen Tätigkeit als Fahrzeugführer komplizierte Aufgabenstellungen der Wahrnehmung, Wissensverarbeitung und Verhaltensumsetzung [61]. Hierbei bietet es sich an, bei der Entwicklung des automatisierten Fahrens ein Verhalten zu entwerfen, das dem menschlichen Fahrstil ähnelt [62].

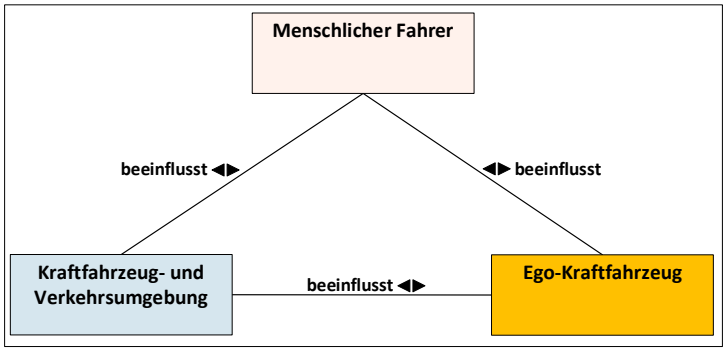


Abbildung 2.1: Dreieck der Wechselwirkungen zwischen menschlichem Fahrer, Ego-Kraftfahrzeug sowie Kraftfahrzeug- und Verkehrsumgebung bei der Fahrzeugführung.

Des Weiteren ist dies erforderlich, um zum einen den Insassen das Gefühl zu vermitteln, dass die jeweiligen Verhaltensweisen plausibel und zweckgemäß sind. Zum anderen manifestiert sich diese Notwendigkeit bei der Interaktion mit menschlichen Fahrern konventioneller Kraftfahrzeuge. Daher ist die Analyse des menschlichen Fahrverhaltens ein integraler Bestandteil, um die Anforderungen an Fahrerassistenz- und Fahrzeugführungssysteme abzuleiten [63].

2.1.1 Die Rolle des menschlichen Fahrers im Straßenverkehr

Die Rolle des menschlichen Fahrers bei der Fahrzeugführung lässt sich prinzipiell als sogenannte Steuerungs- und Regelungstätigkeit mit kontinuierlicher Informationsverarbeitung charakterisieren [64]. Bezogen auf diesen Sachverhalt besteht die Fahraufgabe aus primären, sekundären und tertiären Tätigkeiten [65]. Bei der primären Tätigkeit geht es darum, das Kraftfahrzeug mit einer bestimmten Geschwindigkeit auf Kurs zu halten und somit sicher von A nach B zu bringen. Je nach Verkehrssituation können sekundäre Tätigkeiten wie Blinken, Hupen oder Auf- und Abblenden erforderlich sein, um die primäre Fahraufgabe zu unterstützen. Tertiäre Tätigkeiten wie die Bedienung von Klimaanlage, Sitzeinstellung, Radio, Telefon, Infotainment usw. [66] dienen der Komfortverbesserung und werden in dieser Arbeit nicht weiter betrachtet. Daraus lassen sich für die Fahraufgabe die Hauptaktivitäten Sinnes- und Wahrnehmungsprozesse, Beurteilungsleistungen, Entscheidungs- und Denkprozesse sowie die Bedienung der Aktuatorik ableiten [64].

Im Folgenden werden die Begriffe Fahraufgabe und Fahrzeugführungsaufgabe synonym verwendet. Zudem lassen sich die strategische und dynamische Fahraufgabe als Unterkategorien der Fahraufgabe betrachten (siehe Abbildung 2.2).

Beim Sinnes- und Wahrnehmungsprozess geht es darum, andere Verkehrsteilnehmer, die Charakteristik der Fahrstrecke, die Beschaffenheit der Fahrbahnoberfläche, Wetter- und Sichtbedingungen sowie Verkehrszeichen zu perzipieren. Darüber hinaus müssen hierbei auch optische Anzeigen (Geschwindigkeitsanzeige, Informationen des Bordcomputers, Warn- und Fehlermeldungen etc.) und akustische Informationen (Sprachausgabe des Navigationssystems, des Radios etc.) im Fahrzeuginneren erfasst werden. Auf Basis der Wahrnehmungen müssen Abstände zu oder zwischen anderen Verkehrsteilnehmern bzw. Objekten, die Geschwindigkeit des eigenen Fahrzeugs und anderer Verkehrsteilnehmer sowie kritische Verkehrssituationen (knappes Einscheren eines Fahrzeugs, Kind läuft unvermittelt auf die Fahrbahn etc.) antizipiert und beurteilt werden.

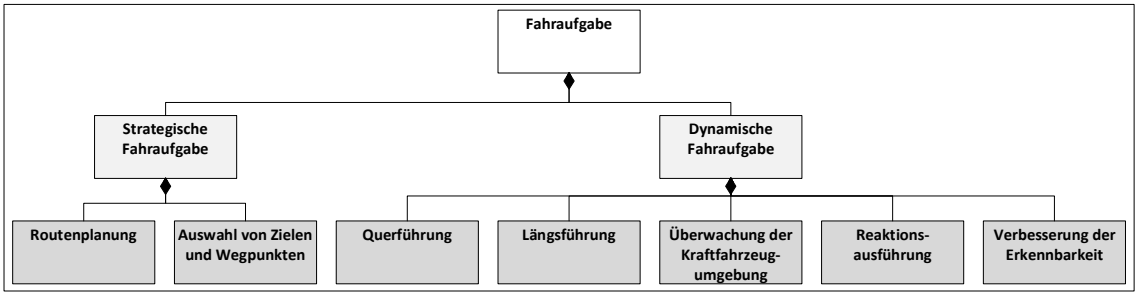


Abbildung 2.2: Hierarchischer Aufbau der Fahraufgabe und strategische sowie dynamische Handlungen für den Betrieb eines Kraftfahrzeugs im Straßenverkehr.

Definition 2.1 Fahraufgabe.
Die Fahraufgabe (engl. Driving Task) umfasst alle Handlungen, die für den Betrieb eines Kraftfahrzeugs im Straßenverkehr erforderlich sind, sowohl im Hinblick auf die strategische als auch auf die dynamische Fahraufgabe.

Definition 2.2 Strategische Fahraufgabe.
Die strategische Fahraufgabe (engl. Strategic Driving Task) umfasst alle strategischen Handlungen, die für den Betrieb eines Kraftfahrzeugs im Straßenverkehr erforderlich sind, jedoch keinen kritischen Echtzeitbedingungen unterliegen:

- *Routenplanung (strategisch);*
- *Auswahl von Zielen und Wegpunkten (strategisch);*

Definition 2.3 Dynamische Fahraufgabe [8].
Die dynamische Fahraufgabe (engl. Dynamic Driving Task) umfasst alle operativen und taktischen Handlungen, die für den Betrieb eines Kraftfahrzeugs im Straßenverkehr unter ggf. kritischen Echtzeitbedingungen erforderlich sind, einschließlich:

- *Querführung des Kraftfahrzeugs über die Lenkung (operativ);*
- *Längsführung des Kraftfahrzeugs über die Beschleunigung und Verzögerung (operativ);*
- *Überwachung der Kraftfahrzeugumgebung durch Objekt- und Ereigniserkennung, Klassifizierung und Reaktionsvorbereitung (operativ und taktisch);*
- *Ausführung der Reaktionen auf die Objekt- und Ereigniserkennung (operativ und taktisch);*
- *Kenntnis und Einhaltung der geltenden Verkehrsregeln und Vorschriften (operativ und taktisch);*
- *Manöverplanung (taktisch);*
- *Verbesserung der Erkennbarkeit durch Beleuchtung, Signalisierung und Gestikulation usw. (taktisch).*

Daraus müssen wiederum im Zuge des Entscheidungs- und Denkprozesses, Handlungen zur Navigation (Fahrtroute, Richtungsentscheidungen an Knotenpunkten etc.) und Bahnführung (Wahl der Geschwindigkeit, des Abstands, des Fahrstreifens etc.) des Kraftfahrzeugs selektiert werden. Die getroffenen Entscheidungen werden mittels der Bedienung entsprechender Elemente (Fahrpedal, Bremspedal, Lenkrad, Gangwahlhebel, Fahrtrichtungsanzeiger, Beleuchtungsschalter, Fahrmodus-Schalter etc.) und der Ansteuerung der jeweiligen Aktuatorik (Antriebsstrang, Bremse, Lenkung, Beleuchtungseinrichtungen etc.) umgesetzt [64]. Zusätzlich leiten sich aus der Straßenverkehrsordnung (StVO) [67] weitere Pflichten an den Fahrzeugführenden ab. Diese sind demnach die Überwachung des Fahrzeugzustands (Warnleuchten der Bordinstrumente, Außenbeleuchtung, Reifendrücke, Geräusche, Vibrationen, Gerüche etc.) und der Ladung auf

einer Ladefläche oder in einem Anhänger sowie die Beaufsichtigung und Unterstützung der Fahrzeuginsassen (Sicherung durch Anschnallgurt etc.). Benötigen andere Verkehrsteilnehmer beispielsweise bei Unfällen Hilfe, ist der Fahrer verpflichtet dies zu leisten [68].

2.1.2 Ansätze zur Modellierung der menschlichen Fahrzeugführung

Zur Erlangung eines tiefgreifenden Verständnisses der Rolle des menschlichen Fahrers, werden je nach Fragestellung Fahrerverhaltensanalysen durchgeführt, um die daraus gewonnenen Erkenntnisse in Fahrerverhaltensmodelle zu übertragen. Anwendungsgebiete für die Modellierung und Beschreibung des menschlichen Fahrerverhaltens sind Fahrverhaltensoptimierungen, Verkehrsflusssimulationen, Verkehrsteilnehmer-Simulationen in Fahrsimulatoren, Verschleiß-, Emissions- und Lastuntersuchungen, Auslegung und Bewertung von Fahrerassistenzsystemen und die Sicherheitsforschung [69]. Eine extensive Übersicht in Bezug auf die verschiedenen Ansätze zur Fahrerverhaltensmodellierung ist in [69], [70] und [71] zu finden.

Im Bereich der Fahrerassistenz sowie des automatisierten Fahrens hat sich das sogenannte „Drei-Ebenen-Modell“ für zielgerichtete Tätigkeiten des Menschen nach Rasmussen [72] im Ensemble mit der „Drei-Ebenen-Hierarchie“ der Fahraufgabe nach Donges [73] als Referenz für die Fahrerverhaltensmodellierung etablieren können (siehe Abbildung 2.3). Das Drei-Ebenen-Modell nach Rasmussen für zielgerichtete Tätigkeiten des Menschen gehört zur Gruppe der kognitiven[1] Modellansätze. Hierbei wird angenommen, dass menschliches Handeln bzw. Verhalten zirkulär auf drei unterschiedlichen Abstraktionsebenen, namentlich der fertigkeitsbasierten, der regelbasierten sowie der wissensbasierten Ebene, vonstattengeht (siehe linker Teil Abbildung 2.3).

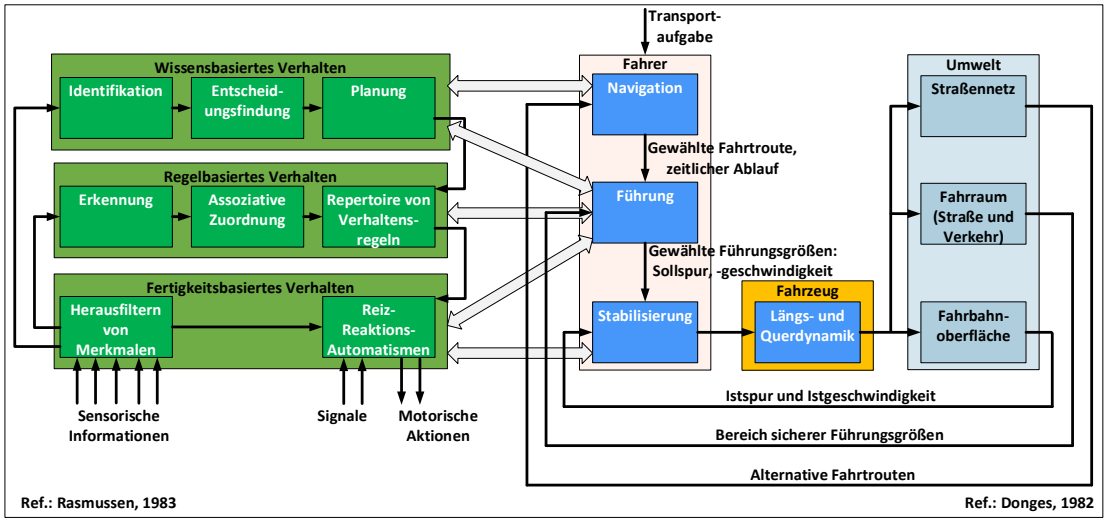


Abbildung 2.3: Zusammenhang (grau hinterlegte Pfeile) des Drei-Ebenen-Modells für zielgerichtete Tätigkeiten des Menschen nach Rasmussen und Drei-Ebenen-Hierarchie der Fahraufgabe nach Donges (entnommen aus [76]).

[1] Innerhalb der Psychologie wird unter Kognition die Gesamtheit der geistigen bzw. mentalen Aktivitäten im Zusammenhang mit Denken, Wissen, Erinnern und Kommunizieren verstanden. Im Gegensatz zur behavioristischen Perspektive (Mensch als „Black-Box“) versucht die kognitionspsychologische Perspektive in diesen hineinzuschauen (Mensch als „White-Box“) [71].

Des Weiteren sind die Ebenen hinsichtlich ihrer Repräsentationsform und ihrem Zeithorizont zu kontrastieren. Top-Down betrachtet läuft auf der obersten Ebene das „wissensbasierte Verhalten“ (engl. *Knowledge-based Behavior*) ab. Dies geschieht dann, wenn für den Menschen bisher unbekannte komplizierte Situationen auftreten. Dementsprechend muss dieser mit untrainierten Handlungsweisen reagieren, um die vorliegenden Problemstellungen zu bewältigen. Als Resultat werden Regeln bzw. Verhaltensmuster an die nächste daruntergelegene Ebene des „regelbasierten Verhaltens“ (engl. *Rule-based Behavior*) übergeben.

Die dort zugehörigen situativen Konstellationen sind dem Menschen aus bereits früher gemachten Erfahrungen bekannt. Ergo kann dieser auf ein Repertoire aggregierter Verhaltensmuster, d.h. einfache „Wenn-dann-Regeln“, zurückgreifen und selektiert hierbei die subjektiv am besten erscheinende Variante. Daraufhin wird das ausgewählte Handlungsmuster an die niedrigste Ebene des „fertigkeitsbasierten Verhaltens“ (engl. *Skill-based Behavior*) weitergereicht. Diese kennzeichnet sich durch reflexartige vom Menschen nicht bewusst kontrollierte und somit routinemäßig wiederkehrende Reiz-Reaktions-Mechanismen, welche im Zuge eines vorangegangenen Lernprozesses eingeübt wurden [76].

Allerdings können die Ebenen auch bottom-up durchlaufen werden, da der Mensch im Allgemeinen zunächst versucht, eine auftretende Situation mit einstudierten Automatismen handzuhaben. Scheitert dieser Versuch, wird auf der nächst höher gelegenen Ebene nach einem Verhaltensmuster aus ähnlichen bereits absolvierten Situationen Ausschau gehalten. Fehlt ein solches Handlungsmuster in Gänze wird auf oberster Ebene ein neues generiert [63]. Konsequenterweise wächst der erforderliche Zeithorizont bzw. die Reaktionszeit von unten nach oben stetig an.

Demgegenüber kann die Fahraufgabe bzw. das menschliche Fahrerverhalten ebenfalls anhand von drei hierarchischen Ebenen strukturiert werden (siehe rechter Teil Abbildung 2.3). Die Drei-Ebenen-Hierarchie der Fahraufgabe nach Donges gehört dabei zur Kategorie der adaptiven Regelungsmodelle, worin der menschliche Fahrer auf „Navigations“-, „Führungs“- und „Stabilisierungsebene“ die Mess-, Steuerungs- und Regelungsinstanz repräsentiert [63]. Auf der Navigationsebene wird die Auswahl einer adäquaten Transport- bzw. Fahrtroute in Abhängigkeit unterschiedlicher Aspekte wie verfügbares Straßennetz, voraussichtlicher Zeit- und Energiebedarf etc. getroffen. Ist der Verkehrsraum im Zuge dessen für den Fahrer noch unbekannt, erfordert die Navigationsaufgabe einen Prozess aktiver Planung, der folglich auf der wissensbasierten Ebene abläuft. Um diese Aufgabe adäquat abzuwickeln, nimmt der Fahrer die Rolle eines Überwachers ein, welcher die Fahrtroute mittels spezifischer Landmarken observiert [76].

Auf der Führungsebene leitet der menschliche Fahrer antizipatorisch im Sinne einer Steuerung, basierend auf der vorab determinierten Route sowie der aktuellen Verkehrssituation, die subjektiv für sinnvoll eingeschätzten Führungsgrößen wie Sollfahrstreifen und Sollgeschwindigkeit ab. Auf der Stabilisierungsebene fungiert der Fahrer dann durch korrigierende Stelleingriffe über Fahrpedal, Lenkrad etc. in einem geschlossenen Regelkreis. An dieser Stelle werden die wahrgenommenen Regelabweichungen auf ein für den Fahrer akzeptables Maß kompensiert und stabilisiert [76]. Demzufolge wird die dynamische Fahraufgabe[2] auf Führungs- und Stabilisierungsebene in Übereinstimmung mit der regel- und fertigkeitsbasierten Ebene vollzogen (siehe Fahrer Abbildung 2.3). Die qualitative Verteilung der Aufgaben auf Führungs- und Stabilisierungsebene auf die regel- und fertigkeitsbasierte Ebene wird maßgeblich von der individuellen Erfahrung des jeweiligen Fahrers sowie der Frequenz an bereits erlebten Verkehrssituationen beeinflusst.

[2] Dynamische Fahraufgabe (vgl. Definition 2.3)

Zur Einordnung der Leistungsfähigkeit des Menschen bei der Bewältigung hochdynamischer Prozesse wie der Fahrzeugführung, bietet es sich an, die Signallaufzeiten als auch die Verarbeitungsgeschwindigkeit eintreffender Informationen näher zu begutachten. Dadurch richtet sich der Fokus auf die menschliche Reaktionszeit, welche das zeitliche Intervall zwischen dem Eintreten eines Reizes und dem Beginn der ersten darauf reagierenden Handlungsweise umfasst. Ohne das Vorhandensein von bewusst gewollten Verzögerungen liegt die Reaktionszeit auf der fertigkeitsbasierten Ebene bzw. Stabilisierungsebene (siehe unterer Teil Abbildung 2.3) bei ca. 100 - 300 ms. Des Weiteren ist zu berücksichtigen über welchen Informationskanal die jeweiligen Reize wahrgenommen werden. Optisch perzipierte Informationen rufen Reaktionszeiten zwischen 200 ms und 400 ms, akustisch wahrgenommene Informationen zwischen 100 ms und 150 ms und haptisch erfasste Informationen zwischen 80 ms und 150 ms hervor. Zudem müssen Umsetzzeiten wie beispielsweise der Wechsel vom Fahrpedal auf das Bremspedal von ca. 200 ms einkalkuliert werden. Ferner sind Antizipationszeiten von ca. 1 s sowie Totzeiten von ca. 0.5 s bei geschlossenem Regelkreisverhalten zu berücksichtigen [77].

Der regelungsbasierte Vorgang auf Stabilisierungsebene kann wiederum anhand zweier Zustände erfasst werden: Homöostase[3] und Manöver [78]. Im Hinblick auf die Längsführung versucht der menschliche Fahrer längsdynamische Sollwerte einzuregeln und möglichst konstant zu halten. Dabei kann in Folgefahrt- und Freifahrthomöostase unterschieden werden. Im Hinblick auf die Folgefahrt wird wiederum die Zeitlücke t_{gap} oder der Relativabstand d_{rel} zum vorausfahrenden Fahrzeug herangezogen (siehe Abbildung 2.4). Diesbezüglich ist der Relativabstand als die Differenz der Absolutabstände der beiden Fahrzeuge entlang derselben Achse (hier: X_E-Achse der Straße) definiert. Der jeweilige Absolutabstand bezieht sich auf die Position der Fahrzeuge innerhalb des ortsfesten X_E, Y_E, Z_E-Koordinatensystems (vgl. Anhang A.4).

Dabei ergeben sich implizite Sollwert- bzw. Handlungsbereiche des menschlichen Fahrers im Sinne einer Fahrhülle bzw. eines sogenannten Fahrschlauchs als Analogon zu den innerhalb der Luftfahrt herangezogenen Flugenveloppen (engl. *Flight Envelope*):

$$\text{Handlung des menschlichen Fahrers bei Folgefahrt: } \begin{cases} Manöver, wenn\ d_{rel} < A_3 & (1) \\ Korrektur, wenn\ A_4 < d_{rel} < A_2 & (2) \\ Beibehaltung, wenn\ A_3 < d_{rel} < A_1 & (3) \\ Korrektur, wenn\ A_2 < d_{rel} < A_0 & (4) \\ Freifahrt, wenn\ d_{rel} > A_0 & (5) \end{cases}$$

Im Zuge von Modus (1) ist der Relativabstand zum vorausfahrenden Fahrzeug zu gering, so dass ein Abbremsmanöver durchgeführt werden muss. Die Modi (2) und (4) können mit dem Fahrpedal durch Segeln oder durch Beschleunigungen im Sinne von Korrekturmanöver abgehandelt werden, um den Wunschrelativabstand einzuregeln. Modus (3) umfasst die Beibehaltung des Relativabstands durch das Konstanthalten des Fahrpedals. Überschreitet der Relativabstand zum vorausfahrenden Fahrzeug den Schwellwert A_0, wird ein Übergang in den Modus (5) gemäß der Freifahrt vollzogen. Innerhalb der Freifahrt wird wiederum eine Sollgeschwindigkeit v_X^* eingeregelt. Gleichermaßen lässt sich die Querhomöostase in Bezug auf die Querführung beschreiben, wobei der Fokus darauf liegt, den jeweiligen Ego-Fahrstreifen nicht ungewollt zu verlassen. Weiterführende Details hierzu sind der Arbeit von Kupschick [78] zu entnehmen.

[3] Nach Karl Steinbuch [79] umfasst Homöostase die Gesamtheit aller Regelvorgänge, welche bewirken, dass bestimmte Zustände eines Organismus, wie z.B. Körperhaltung, Körpertemperatur, Blutzuckergehalt, Blutsauerstoffgehalt usw., innerhalb der für das Weiterleben zulässigen Grenzen bleiben. Insgesamt handelt es sich dabei um die Aufrechterhaltung eines biologischen Gleichgewichtszustands.

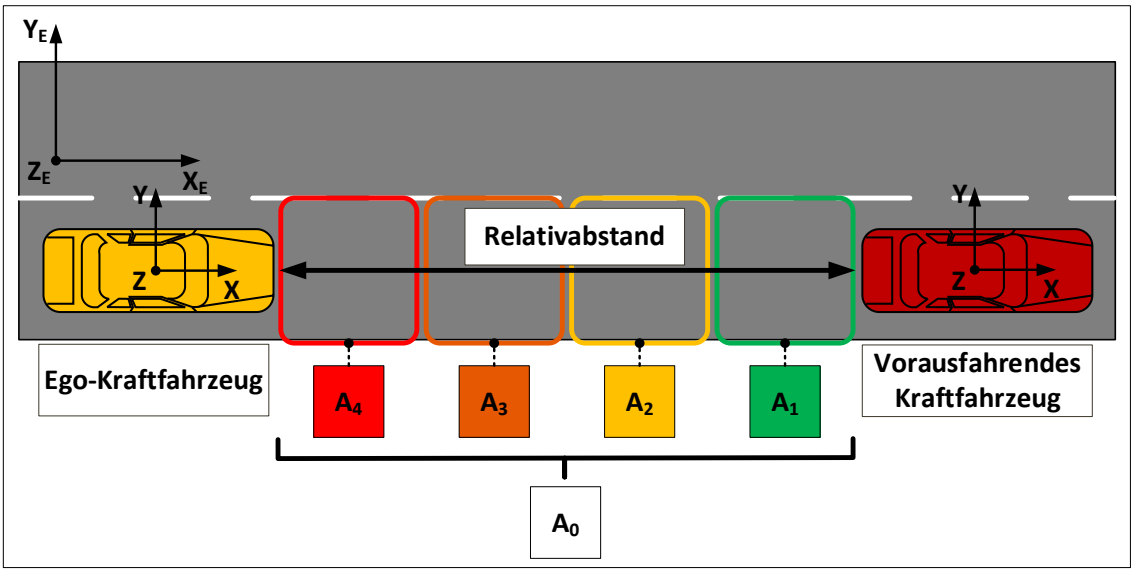


Abbildung 2.4: Implizite Sollwerte für die Längshomöstase während der Folgefahrt.

2.2 Automatisierung von Kraftfahrzeugen

Alles in allem bewältigt der menschliche Fahrer die an ihn gestellten Aufgaben der Fahrzeugführung überwiegend unbedenklich. Insbesondere verfügt der Mensch über außerordentliche Fähigkeiten bei der Umgebungswahrnehmung sowie der Abarbeitung von gegebenen Problemstellungen über eingelernte Automatismen und Regeln. Nichtsdestotrotz sind laut [27] 90 % der Verkehrsunfälle auf menschliches Fehlverhalten zurückzuführen. Demzufolge wird der Fahrer als erfassender, steuernder und regelnder Bestandteil innerhalb der Regelkaskaden der Fahrzeugführung (siehe rechter Teil Abbildung 2.3) bei Unfällen seiner Funktion nur unzureichend gerecht. Diese Unzulänglichkeiten resultieren zunächst aus der nicht ausreichend präzisen Abschätzung von Regelgrößen, Führungsgrößen sowie anderen Nebenbedingungen, was u.a. darauf basiert, dass der Mensch sich nur auf einen begrenzten Erfassungsbereich fokussieren kann. Zudem treten bei der Entscheidungsfindung innerhalb von kritischen sowie unbekannten Situationen und unter Zeitdruck Schwierigkeiten auf. Des Weiteren weist der menschliche Fahrzeugführer über eine beschränkte Exaktheit und Schnelligkeit bei der Handlungsumsetzung und damit beim Einregeln der Regelgrößen auf. Ferner führen Ermüdung als auch innere Befindlichkeiten der Motivation und Emotion zur Beeinträchtigung der Aufmerksamkeit und ergo zu einer Verringerung des Auflösungsgrads der Wahrnehmung der Kraftfahrzeug- und Verkehrsumgebung sowie der Fahrzeugregelung selbst [63].

Um diesen Limitierungen entgegenzuwirken, beschäftigen sich Industrie und Forschung zum einen mit Fahrerassistenzsystemen, welche den Fahrer in bestimmten Situationen unterstützen und dadurch kooperativ dessen Schwächen kompensieren sollen. Zum anderen werden Ansätze verfolgt, mithilfe von technischen Lösungen bzw. Fahrzeugführungssystemen (vgl. Unterabschnitt 2.2.1) einzelne Elemente oder gar die Gesamtheit der Fahraufgaben zu automatisieren.

Definition 2.4 Automatisierung [80].
Das Ausrüsten einer Einrichtung, so dass sie ganz oder teilweise ohne Mitwirkung des Menschen bestimmungsgemäß arbeitet.

Der Begriff „Fahrerassistenz“ deckt ein zunächst weitreichendes Feld ab. Gemäß [81] kann hierunter bereits ein technisches System wie z.B. ein Tachometer, eine automatische Scheibenwischerbetätigung oder Rückstellung des Blinkers verstanden werden, dass den Fahrzeugführer im Sinne von *„Beistand“* oder *„Mithilfe“* assistiert. Je nach Fragestellung lassen sich in der Fachliteratur unterschiedliche Ansätze zur Kategorisierung von Fahrerassistenzsystemen finden. Eine mögliche Systematisierung ist beispielsweise die Unterscheidung in Systeme der aktiven und passiven Sicherheit. Erstere gelten als unfallvermeidend (z.B. Antiblockiersystem (ABS), Elektronisches Stabilitätsprogramm (ESP), Notbremsassistent etc.) wohingegen letztere als unfallmildernd (z.B. Airbag) konzipiert werden [82]. Zusätzlich können Fahrerassistenzsysteme dem Komfortbereich (z.B. Navigationssystem welches den Fahrer auf Navigationsebene (siehe rechter oberer Teil Abbildung 2.3) Unterstützung leistet) zugeordnet werden.

Fahrerassistenzsysteme können gemäß [81] in „konventionelle Fahrerassistenzsysteme“ und „Fahrerassistenzsysteme mit maschineller[4] Wahrnehmung“ unterschieden werden. Konventionelle Fahrerassistenzsysteme sind exemplarisch das ABS und das ESP. Ein ABS z.B. soll das Blockieren eines Rades verhindern. Sowohl ABS als auch ESP sind auf der Stabilisierungsebene einzuordnen (siehe rechter unterer Teil Abbildung 2.3). Fahrerassistenzsysteme mit maschineller Wahrnehmung sind u.a. der Abstandsregeltempomat, der Spurhalteassistent, der Parkassistent sowie der Notbremsassistent. Diese sollen dem Fahrer bei der Bewältigung der dynamischen Fahraufgabe zu Hilfe kommen und im Zusammenspiel mit diesem eine Art Symbiose ergeben. Dabei operieren diese auch weitestgehend auf der Stabilisierungsebene (siehe rechter unterer Teil Abbildung 2.3). Konkret bedeutet dies, dass solche Systeme den Fahrer in Situationen, welche „visuell wahrgenommen“ werden müssen, unterstützen [81].

Definition 2.5 Fahrerassistenzsystem mit maschineller Wahrnehmung [81].
Fahrerassistenzsysteme mit maschineller Wahrnehmung (engl. Advanced Driver Assistance Systems) unterstützen den menschlichen Fahrer in Situationen, welche in Bezug auf die Kraftfahrzeugumgebung (statische und dynamische Objekte) „wahrgenommen“ werden müssen, wobei der menschliche Fahrer die Verantwortung für die Bewältigung der dynamischen Fahraufgabe[5] trägt.

Dabei greifen die technischen Systeme zur Erkennung der Umgebung auf Fähigkeiten der maschinellen bzw. visuellen Wahrnehmung wie Radar, Kamera, Lidar oder Ultraschall zu.

2.2.1 Fahrzeugführungssysteme

Im Vergleich zu Fahrerassistenzsystemen umfassen Fahrzeugführungssysteme, je nach Automatisierungsgrad (vgl. Unterabschnitt 2.2.2), zusätzliche Entwicklungsstufen. Durch ein solches System kann der menschliche Fahrer entweder temporär oder gar permanent von dessen Fahraufgaben teilweise bis vollständig entlastet werden. Hierbei muss dieser bei den zeitweise aktiven Systemen nur noch bei zwingender Notwendigkeit z.B. bei einem Fehler als Überwacher[6] bzw. Rückfallebene[7] eingreifen.

[4] Maschinelle Wahrnehmung im Sinne einer Detektion und Verarbeitung optischer und akustischer Wellen zur Erkennung von Objekten aus der externen Kraftfahrzeug- und Verkehrsumgebung.
[5] Dynamische Fahraufgabe (vgl. Definition 2.3)
[6] Überwachung (vgl. Definition 2.7)
[7] Rückfallebene (vgl. Definition 2.8)

Im Zuge dieser Dissertation wird die Definition eines Fahrzeugführungssystems[8] im Vergleich zu [8] dahingehend erweitert, dass je nach Funktionsumfang auch strategische Aufgaben auf der Navigationsebene (siehe rechter oberer Teil Abbildung 2.3) wie die Routenplanung sowie die Auswahl von Zielen und Wegpunkten übernommen werden können. Folglich ist ein derartiges System in der Lage, die gesamte Fahraufgabe über die Wahrnehmung und Lokalisierung der Kraftfahrzeug- und Verkehrsumgebung, die Planung von Fahrentscheidungen bis hin zur Ansteuerung der Aktuatorik durchzuführen.

Definition 2.6 Fahrzeugführungssystem [8].
Ein Fahrzeugführungssystem (engl. Automated Driving System) umfasst die Hardware und Software (Sensorik und Regelung), die gemeinsam in der Lage sind, Teile bis hin zur gesamten Fahraufgabe temporär oder gar dauerhaft zu übernehmen, unabhängig davon, ob diese auf einen bestimmten Betriebsbereich[9] beschränkt ist.

Ulbrich et al. [83] stellen eine Systemarchitektur für automatisierte Kraftfahrzeuge vor, welche als Referenz innerhalb von Industrie und Forschung eingeordnet werden kann. Infolgedessen wird diese als Ausgangspunkt für die vorliegende Dissertation herangezogen. Dadurch ergeben sich drei Hauptsäulen auf drei unterschiedlichen Abstraktionsebenen (siehe Abbildung 2.5). Diese sind die strategische Ebene zur Handlungsplanung, die taktische Ebene zur Aktionsauswahl bzw. Manöverentscheidung sowie die operative Ebene zur reaktiven Aktionsüberwachung bzw. Stabilisierung, welche zudem den Ebenen Navigation, Führung und Stabilisierung nach Donges zugeordnet werden können. Die Module Umgebungs- und Fahrzeugsensorik sowie Aktuatorik sind der operativen Ebene zuzuteilen. Für eine detaillierte Beschreibung der grundlegenden Funktionen der Hauptsäulen wird auf Ulbrich et al. [83] verwiesen.

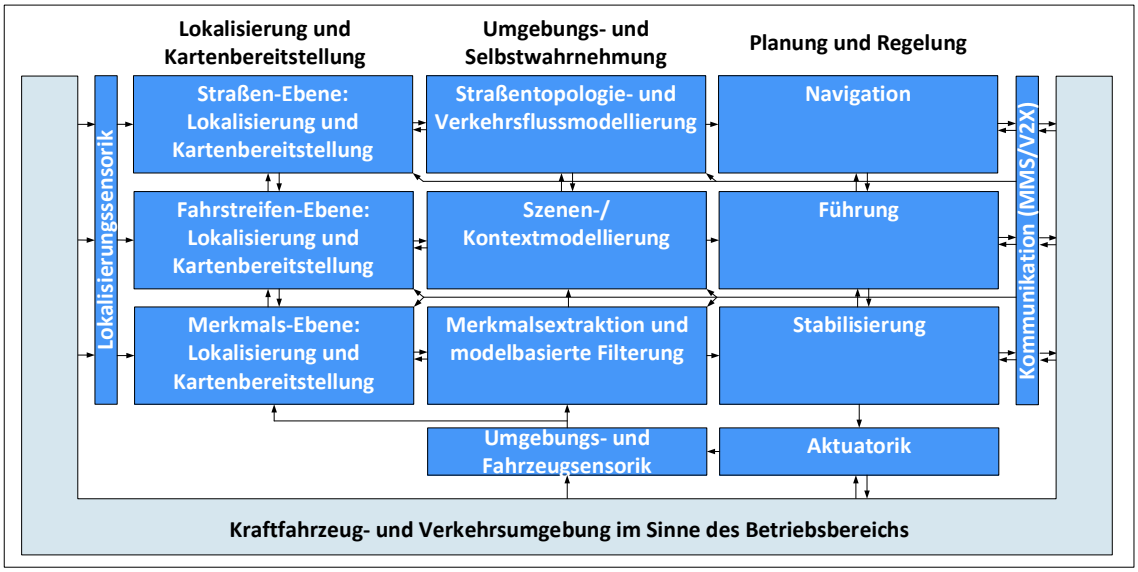


Abbildung 2.5: Referenzarchitektur eines automatisierten Kraftfahrzeugs eingebettet in die Kraftfahrzeug- und Verkehrsumgebung (menschlicher Fahrer bzw. Passagiere werden hier als Teil des Betriebsbereichs angenommen) in vereinfachter Darstellung (in Anlehnung an [83] und [84]).

[8] Gemäß [8] ist der Funktionsumfang eines Fahrzeugführungssystems auf die dynamische Fahraufgabe beschränkt. Strategische Funktionen wie die Routenplanung als auch die Auswahl von Zielen und Wegpunkten sind dementsprechend nicht berücksichtigt.
[9] Betriebsbereich (vgl. Definition 2.10)

2.2.2 Automatisierungsstufen des automatisierten Fahrens

Neben der SAE [8] haben u.a. auch die Bundesanstalt für Straßenwesen (BASt) [85] sowie der Verband der Automobilindustrie e.V. (VDA) [86] Automatisierungsstufen zur Kategorisierung des automatisierten Fahrens definiert. Es ist anzumerken, dass die vorliegende Dissertation, u.a. aufgrund der internationalen Tragweite der SAE-Automatisierungsstufen, sich jedoch primär auf deren vorgenommene Kategorisierung beruft. Die Unterscheidung der Stufen orientiert sich u.a. an der Übernahme der dynamischen Fahraufgabe[10] in der Längs- und/oder Querführung des Kraftfahrzeugs, der Aufgabe der Überwachung des Fahrzeugführungssystems sowie des Betriebsbereichs, der Rückfallebene als auch der Leistungsfähigkeit des Fahrzeugführungssystems.

Definition 2.7 Überwachung [8].
Die Überwachung (engl. *Monitoring*) beschreibt eine *Aktivität zur Bewertung, ob das Fahrzeugführungssystem einen Teil oder die gesamte dynamische Fahraufgabe ordnungsgemäß ausführt.*

Definition 2.8 Rückfallebene [8].
Die Rückfallebene (engl. Fallback) umfasst die Reaktion des Anwenders oder des Fahrzeugführungssystems, um entweder die dynamische Fahraufgabe zu übernehmen oder den Zustand minimalen Risikos zu erreichen, nach dem Auftreten eines der Leistungsfähigkeit der dynamischen Fahraufgabe betreffenden Systemausfalls oder Verlassen des festgelegten Betriebsbereichs.

Definition 2.9 Zustand minimalen Risikos [8].
Der Zustand minimalen Risikos (engl. Minimal Risk Condition) definiert einen Zustand, in den ein Fahrzeug durch Reaktion des Anwenders oder des Fahrzeugführungssystems im Falle eines Rückfalls der dynamischen Fahraufgabe gebracht werden kann, um das Risiko eines Unfalls zu reduzieren, wenn eine bestimmte Fahrt nicht abgeschlossen werden kann oder sollte.

Ergänzend zu den sechs spezifizierten Automatisierungsgraden der SAE werden hier die Kategorien der BASt als auch der VDA eingeordnet. Darüber hinaus wird die Begrenzung des Betriebsbereichs (vgl. Unterabschnitt 2.2.3) mitberücksichtigt (siehe Tabelle 2.1). Umfassende Erläuterungen der jeweiligen Automatisierungsstufen sind in [8] zu finden.

2.2.3 Signifikanz des Betriebsbereichs und der Mensch-Maschine-Interaktion bei der Automatisierung

Sowohl zur Kategorisierung der Automatisierungsstufen als auch für die Entwicklung und Spezifikation von Fahrzeugführungssystemen nimmt die Thematik des Betriebsbereichs einen zunehmenden Stellenwert ein.

Definition 2.10 Betriebsbereich [8].
Der Betriebsbereich (engl. *Operational Design Domain {ODD}*) *beinhaltet Betriebsbedingungen, wie Umwelt-, geographische und Tageszeitbeschränkungen sowie das Vorhandensein oder Fehlen von bestimmten Verkehrs- oder Fahrbahnmerkmalen, unter denen eine hierfür speziell entwickelte Funktion des Fahrzeugführungssystems zu funktionieren hat.*

[10] Dynamische Fahraufgabe (vgl. Definition 2.3)

Tabelle 2.1: Übersicht der Automatisierungsstufen gemäß der SAE [8] unter zusätzlicher Darstellung der BASt [85] und VDA [86] Stufen.

SAE-Stufe	SAE-Bezeichnung	Ausführung von Längs- und Querführung	Rückfall-ebene	Betriebs-bereich	BASt/VDA Stufe
Menschlicher Fahrer überwacht die Kraftfahrzeug- und Verkehrsumgebung					
0	Keine Automatisierung	Menschlicher Fahrer	Menschlicher Fahrer	Nichtzutref-fend	Driver only
1	Fahrerassistenz	Menschlicher Fahrer und Fahrzeug-führungssystem	Menschlicher Fahrer	Begrenzt	Assistiert
2	Teil-automatisierung	Fahrzeug-führungssystem	Menschlicher Fahrer	Begrenzt	Teil-automatisiert
Fahrzeugführungssystem überwacht die Kraftfahrzeug- und Verkehrsumgebung					
3	Bedingte Automatisierung	Fahrzeug-führungssystem	Menschlicher Fahrer	Begrenzt	Hoch-automatisiert
4	Hoch-automatisierung	Fahrzeug-führungssystem	Fahrzeug-führungs-system	Begrenzt	Voll-automatisiert
5	Voll-automatisierung	Fahrzeug-führungssystem	Fahrzeug-führungs-system	Unbegrenzt	Fahrerlos

Dementsprechend umfasst der Betriebsbereich bzw. die ODD per Definition prinzipiell einen festgelegten Teil des Verkehrsraums bzw. der Kraftfahrzeug- und Verkehrsumgebung, auf welchen ein automatisiertes Kraftfahrzeug im Laufe des gesamten Lebenszyklus treffen kann. Paraphrasiert können darunter auch sämtliche Situationen[11] bzw. der mögliche vom Fahrzeugführungssystem zu beherrschende Szenarienraum[12] verstanden werden. Diese Bedingungen reichen über Länder, Regionen, Verkehrsnetz, Straßentopologie, Verkehrsregeln und -zeichen, Umwelt- und Witterungsverhältnisse wie Nebel, Schnee, Rauch etc., das Vorhandensein eines Mobilfunknetzes für V2X-Kommunikation bis hin zum dynamischen Verhalten anderer Verkehrsteilnehmer wie Kraftfahrzeuge, Passanten oder Tiere.

Im Kontext von Wissenschaft und Industrie werden in der Zwischenzeit unterschiedliche Ansätze zur taxonomischen Klassifizierung und Kategorisierung des Betriebsbereichs vorgestellt und diskutiert. Czarnecki [87], [88], [89] beschreibt eine umfassende Ontologie und Taxonomie eines sogenannten „Operational World Models“. Weitere mögliche Betrachtungsweisen werden in der PAS 1883 „Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification“ [90] und der darauf basierenden ISO 34503 „Road vehicles – Test scenarios for automated driving systems - Specification for operational design domain“ [91], in der DOT HS 812 623 der „National Highway Traffic Safety Administration“ (NHTSA) [92] sowie in wissenschaftlichen oder industriellen Publikationen wie [93], [94] und [95] vorgeschlagen. Die genannten Ansätze erfassen dieselben Informationen, aber in jeweils unterschiedlichen Ausprägungen.

[11] Situation (vgl. Definition 4.34)

[12] Szenario (vgl. Definition 4.31)

Die vorliegende Dissertation stützt sich auf die beschriebene Taxonomie der PAS 1883 [90]. Hierbei wird der Betriebsbereich bzw. die ODD in Attribute der Szenerie[13] der Umweltbedingungen sowie in Attribute dynamischer Elemente gruppiert. Über mehrere Granularitätsebenen werden diese systematisch weiter verfeinert (siehe Abbildung 2.6). Entsprechende Details sind der PAS 1883 zu entnehmen, werden aber hier nicht näher beschrieben. Gemäß den unterschiedlichen Automatisierungsstufen kann ein Fahrzeugführungssystem für den alleinigen Einsatz innerhalb eines festgelegten und begrenzten Betriebsbereichs konzipiert werden. Beispielsweise könnte ein Level 3 System nur für den Betrieb auf Autobahnen vorgesehen werden. Hierbei müsste ein solches System zudem das Verlassen des Betriebsbereichs erkennen und den menschlichen Fahrer auffordern, die Fahrzeugführung wieder zu übernehmen (vgl. Unterabschnitt 2.2.2).

Selbst ein Fahrzeugführungssystem der Stufe 5, welches das hochautomatisierte Kraftfahrzeug unter allen vom menschlichen Fahrer beherrschbaren Betriebsbedingungen innerhalb einer gegebenen Region der Welt manövriert (vgl. Unterabschnitt 2.2.2), profitiert davon, einen explizit definierten Betriebsbereich zu haben. Dadurch lässt sich erst kommunizieren, was mit „alle vom menschlichen Fahrer beherrschbaren Bedingungen“ im Sinne des zu beherrschenden Szenarienraums tatsächlich gemeint ist [95]. Infolgedessen ist die Definition eines Betriebsbereichs zum einen der erste Schritt im Entwicklungsprozess für die Ableitung von Systemanforderungen. Des Weiteren ist diese von hoher Relevanz für die Verifikation[14], die Validierung[15] und das Testen[16] der Leistungsfähigkeit eines Fahrzeugführungssystems. Ferner dient eine konsistente Betriebsbereichsdefinition als Kommunikationsgrundlage für die jeweils im Produktlebenszyklus beteiligten Stakeholder.

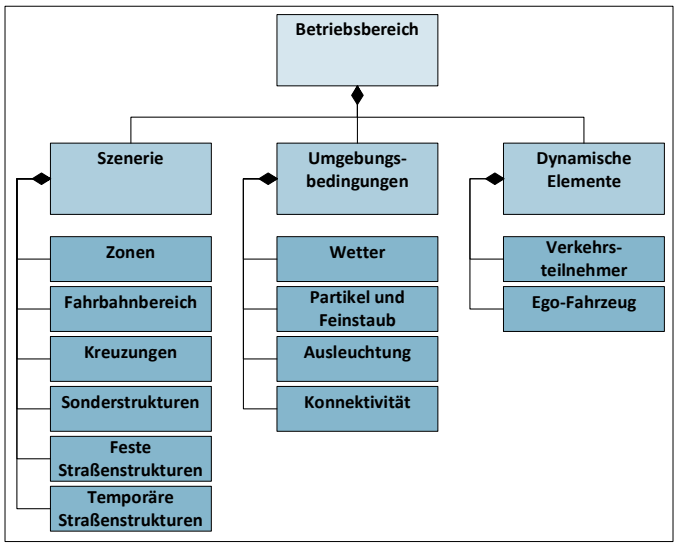


Abbildung 2.6: Taxonomie der Betriebsbereichs- bzw. ODD-Attribute auf oberster Ebene gemäß ISO 34503 (in Anlehnung an [91] und [90]).

[13] Szenerie (vgl. Definition 4.32)
[14] Verifikation (vgl. Definition 3.9)
[15] Validierung (vgl. Definition 3.10)
[16] Testen (vgl. Definition 3.11)

Zum anderen ist diese neben dem sicheren Betrieb auch für die Konformität mit geltenden Gesetzen und Vorschriften als auch die Erfüllung weiterer Ziele wie z.B. Mobilitäts- und Komfortbedürfnisse notwendig. Dadurch kann sichergestellt werden, dass die Öffentlichkeit die jeweiligen Fahrzeugführungssysteme mit angemessenen Erwartungen wahrnimmt. Ein weiterer elementarer Aspekt des automatisierten Fahrens ist die Mensch-Maschine-Interaktion. Im Zuge der stufenweisen Automatisierung von Teilen der Fahraufgabe bis hin zur Vollautomatisierung werden entsprechende Funktionen nach und nach vom Menschen auf das Fahrzeugführungssystem verlagert.

Dadurch wird dieser vom aktiven Bediener zum passiven Überwacher. Ergo führt dies bei der Fahrzeugführung zu einem Wandel der Anforderungen in Bezug auf die menschliche Informationsverarbeitung und deren Prozesse. Als Konsequenz daraus können auf der einen Seite eingeübte Handlungsmuster wie z.B. die Durchführung von Lenkmanövern immer seltener vollzogen und damit verlernt werden. Auf der anderen Seite müssen neue Tätigkeitsformen wie die permanente Systemüberwachung und ein grundsätzlich neues Systemverständnis einstudiert werden. Dies erfordert eine Modifizierung sowie Restrukturierung der für die menschliche Fahrzeugführung zugrundeliegenden mentalen Modelle [96].

Definition 2.11 Mensch-Maschine-Interaktion [97].
Die Mensch-Maschine-Interaktion (engl. Human-Machine Interaction) kennzeichnet sich als optische, akustische oder haptische Interaktion, bei welcher Informationen vom Menschen auf die Maschine als auch umgekehrt übertragen werden.

Insgesamt kann die temporäre Entkopplung des Fahrzeugführers von der Steuerungs- und Regelungstätigkeit zu mangelndem oder gar übertriebenem Vertrauen in die Automatisierung führen [98]. Diese sogenannten „Out-of-the-loop"- bzw. Entkopplungseffekte lassen sich anhand des mangelnden Situationsbewusstseins akzentuieren. Hierbei ist dieses auf eine ungenügende Überwachung des Systems, modifizierte oder gänzlich ausbleibende Rückmeldungen wie beispielsweise das Lenkradzucken über den haptischen Kanal, unzureichende Transparenz und Kenntnislücken im Hinblick auf das automatisierte System zurückzuführen [96]. Daraus resultiert die inhärente Gefahr, einerseits den Anwender von Systemen der Automatisierungsgrade 1 - 3 (vgl. Unterabschnitt 2.2.2) in den Bereich der Unterforderung, z.B. durch langanhaltendes monotones Überwachen zu leiten. Andererseits kann dieser auch in den Bereich der Überforderung, beispielsweise durch irrationales Systemverhalten sowie plötzliche Aufforderungen zur Übernahme der Fahrzeugführung, gezwungen werden.

Schlussendlich werden Teile der Fahrzeugführung aufgrund der Unzulänglichkeiten des Menschen automatisiert, aber eben genau jener soll dann wiederum ein solches System überwachen und im Fehlerfall als Rückfallebene einspringen können [96]. Dieser Sachverhalt lässt sich auch als „Ironien der Automatisierung" [13] artikulieren und wird seitens einschlägiger Studien manifestiert (vgl. Unterabschnitt 1.1.1). Demnach ergibt sich die Herausforderung, die Rolle des Menschen auf diesem stufenweisen Entwicklungspfad psychologisch sinnvoll und nutzergerecht zu definieren. Hierbei müssen die Fahrzeugführungssysteme zum einen den natürlichen Fähigkeiten der menschlichen Informationsverarbeitung und zum anderen den Erwartungen als auch Bedürfnissen der Anwender als auch anderer Verkehrsteilnehmer Genüge leisten. Diese Fragestellungen sind aufgrund der mannigfaltigen Individualität eines jeden einzelnen Menschen bis zum heutigen Zeitpunkt nicht vollständig geklärt [96].

3 Automotive-Produktlebenszyklus

„Alles sollte so einfach wie möglich sein, aber nicht einfacher“

Albert Einstein

Die progressive technologische Evolution des Automobils im Zuge des 20. und insbesondere 21. Jahrhunderts bekräftigt jeher dessen Rolle als Innovationstreiber innerhalb von Industrie und Forschung. In der Zwischenzeit bahnt sich eine digitale Transformation [99] an, welche sich im Sinne der Digitalisierung und Vernetzung im Automobilbereich sowie am Automobil selbst bemerkbar macht. Der Einzug von Aspekten aus dem Sektor der Unterhaltungselektronik sowie automatisiertes Fahren und vernetzte Mobilität verschieben den Fokus auf softwaregetriebene Innovationen. Ferner steigen die Kundenanforderungen hinsichtlich Varianz, Individualisierung und Skalierbarkeit. Hinzu kommt aus dem immer volatiler werdenden Automobilmarkt die Forderung nach immer kürzeren Produktentwicklungszyklen. Infolgedessen werden definierte Vorgehensweisen zur Beherrschung dieser Herausforderungen unabdingbar [100]. Dementsprechend werden im Verlauf dieses Kapitels die für das Verständnis dieser Dissertation notwendigen Grundlagen der eingesetzten Vorgehensmodelle und Prozessreferenzen im Produktlebenszyklus von Kraftfahrzeugen veranschaulicht.

3.1 Produktentstehungsprozess

Im Laufe der letzten Jahrzehnte haben sich innerhalb der Automobilindustrie Methoden und Ansätze für die Entwicklung, Herstellung und Vermarktung von Kraftfahrzeugen etabliert, um den Anforderungen globaler und sich dynamisch wandelnder Märkte sowie wachsendem Konkurrenzdruck Genüge zu leisten. Des Weiteren werden im Zuge der Globalisierung die Schwellen über Länder- und Kontinentalgrenzen fortwährend aufgeweicht, was zu einer fortschreitenden Zusammenarbeit und Kopplung zwischen den Fahrzeugherstellern (engl. *Original Equipment Manufacturer {OEM}*) als auch Tier-1, Tier-2 und Tier-3 Zulieferern führt. Korrelativ zu den technologischen Herausforderungen, welche u.a. mit den Themen der Digitalisierung und Vernetzung eingehen, fordern die internationalen Märkte die kontinuierliche Verringerung von Durchlaufzeiten, die Erhöhung der Absicherung im Sinne der Produkthaftung sowie die Reduktion der Kosten über den Lebenszyklus [101]. Daraus resultierend ergibt sich die Zielsetzung, den maximalen Produktnutzen für Kunden und Hersteller über den gesamten Produktlebenszyklus mit möglichst geringem ökonomischem, ökologischem und sozialem Aufwand sowie Risiko zu erreichen [102].

Der Produktlebenszyklus kann grundsätzlich in die Phasen Entwicklung, Produktion, Betrieb und Service sowie Außerbetriebnahme [54] differenziert werden. Bei Kraftfahrzeugen wird mit einem Produktlebenszyklus von bis zu 25 Jahren gerechnet. Dabei fallen ca. vier bis fünf Jahre auf die Entwicklungszeit, etwa sieben Jahre auf den Produktionszeitraum und bis zu 15 Jahre auf den Betrieb und Service [100]. Innerhalb des Produktlebenszyklus eines Kraftfahrzeugs nimmt der Produktentstehungsprozess (PEP) eine Schlüsselrolle ein und bildet den übergeordneten Rahmen für die Baureihenentwicklung, angefangen bei der Forschung und Vorausentwicklung bis hin zur Serie (siehe Abbildung 3.1). Während des gesamten PEP partizipieren und kooperieren unterschiedliche Unternehmen und Disziplinen.

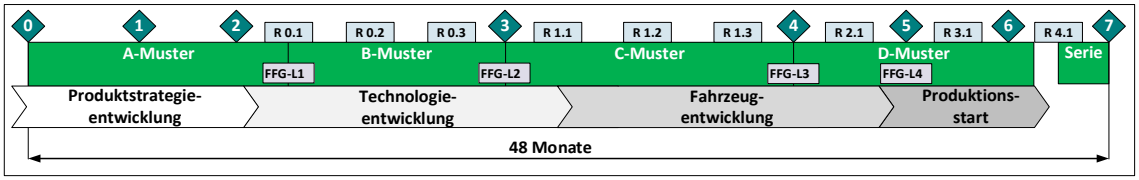


Abbildung 3.1: Chronologische Abfolge der Produktstrategie-, Technologie-, und Fahrzeugentwicklung sowie des Produktions- und Verkaufsstarts des PEPs gemäß [103] entlang der Reifegradabsicherungsmeilensteine (RGA-MS) gemäß VDA [104] unter Berücksichtigung der Musterphasen, der Fahrfreigabe-Level (FFG-L) sowie der Freigaben (R).

Hierbei kann der OEM als Spitze bzw. oberste Ebene einer sich darunter aufbauenden Zulieferpyramide angesehen werden. Auf der zweiten Ebene befinden sich sogenannte „Tier-1“ Unternehmen, welche als Kernlieferanten Systeme oder Module dem OEM zur Verfügung stellen. Auf der dritten Ebene werden Bauteile sowie Untergruppen dem Tier-1 oder dem OEM durch die Komponentenlieferanten als Tier-2 zugebracht. Final lassen sich auf der untersten Ebene die Produzenten von Rohmaterial, Halbleitern oder Normteilen als Tier-3 verorten, welche die Komponentenlieferanten versorgen [105], [106].

Definition 3.1 Baureihe [107].
Die Baureihe repräsentiert einen Ansatz zur Rationalisierung von Produktentwicklungen, bei dem dieselbe Funktion mithilfe eines einheitlichen Lösungskonzepts und möglichst identischen Eigenschaften für einen erweiterten Größenbereich realisiert werden soll. Im Automobilbereich ist darunter eine Serie von Kraftfahrzeugen zu verstehen, welche aus technischen und wirtschaftlichen Gründen nach einem einheitlichen Grundkonzept bzw. Muster entwickelt wurde und sich lediglich durch Antriebsvarianten, Ausstattungen und/oder Karosserieformen unterscheidet.

Dabei spielen Funktionalität und Kosten in Relation zur Entwicklungszeit die tragenden Rollen. Zudem haben die innerhalb des PEPs zu Beginn getroffenen Entscheidungen maßgeblichen Einfluss und können weitreichende Konsequenzen in Bezug auf den weiteren Verlauf des gesamten Produktlebenszyklus nach sich ziehen [108]. Der PEP selbst kann wiederum in Phasen der Produktstrategieentwicklung, der Technologieentwicklung, der Fahrzeugentwicklung sowie des Produktions- und Verkaufsstarts unterteilt werden, worin zu vorgegebenen Entwicklungszeitpunkten die dazu erforderlichen Liefergegenstände im Sinne von abgesicherten und abgenommenen Freigaben fertiggestellt bzw. der notwendige Produktreifegrad erreicht werden muss (siehe Abbildung 3.1).

Definition 3.2 Freigabe [109].
Eine Freigabe (engl. Release {R}) bezieht sich auf die abgesicherte und abgenommene Version bzw. den Liefergegenstand eines Produkts zu einem bestimmten Zeitpunkt, welcher spezifische Bestandteile oder aber das Gesamtprodukt umfassen kann.

Definition 3.3 Reifegrad [110], [111].
Der Reifegrad (engl. Maturity Level {ML}) ist die objektive Beurteilung eines Produkts anhand von festgelegten Indikatoren, wie z.B. Sicherheit, Umfang der spezifischen Bestandteile des Gesamtprodukts etc. Während des PEP repräsentiert der Produktreifegrad ein Qualitätsmaß dahingehend, inwiefern ein Produkt die spezifizierten Indikatoren bereits erfüllt.

Entlang des PEPs dienen verschiedene Musterstände (A-, B-, C-, D-Muster) der Validierung von Funktionsprinzipien, der Erprobung sowie letztlich der Erreichung der Serienfreigabe (siehe Abbildung 3.1). Diese Musterstände werden gemäß den Vorgaben des VDA [104] wie folgt charakterisiert, wobei im Hinblick

auf die Entwicklung von Fahrerassistenz- sowie Fahrzeugführungssystemen sogenannte Fahrfreigabe-Level (FFG-L) miteinbezogen werden:

- **A-Muster:** Hierbei geht es um erste, nur bedingt fahrtaugliche Funktionsmuster, welche ihrerseits zur Bestätigung des grundlegenden Funktionsprinzips und zur Demonstration der Funktionsfähigkeit herangezogen werden, dar. Der Einsatz im öffentlichen Straßenverkehr ist für sicherheitsrelevante Systeme nicht gestattet, wodurch die Nutzung auf Labor-, Simulations- oder Prüfstandstests (vgl. Abschnitt 4.7) begrenzt ist.
    - **FFG-L1 – Fahrfreigabe für Teststrecken**
- **B-Muster:** Darunter fallen funktionsfähige und fahrtaugliche Prototypen, welche über den erforderlichen Grad an Betriebssicherheit[1] für erste Erprobungen verfügen. Die jeweiligen Prototypen können somit mittels Sondergenehmigungen der Zulassungsbehörde im öffentlichen Straßenverkehr betrieben werden. Dadurch wird die Erprobung[2] des jeweils im Fokus liegenden Funktionsumfangs zur Identifikation und Behebung von Schwachstellen ermöglicht. Darüber hinaus erfüllen die B-Muster alle Hardware- und Funktionsanforderungen, wobei diese noch nicht vollständig für die Serienproduktion geeignet sind.
    - **FFG-L2 – Experten- und Dauerlauf-Straßenfahrfreigabe**
- **C-Muster:** Diese dürfen ebenfalls nach einer erteilten Sonderzulassung im öffentlichen Straßenverkehr betrieben werden. Im Unterschied zum B-Muster sind bei C-Mustern jedoch keine technischen Einschränkungen gestattet, welche die Betriebssicherheit beeinträchtigen könnten. Die Fertigung erfolgt mit Serienwerkzeugen unter seriennahen Bedingungen, wobei Abweichungen von der geplanten Serienproduktion noch zulässig sind. Die C-Muster erfüllen dementsprechend sämtliche Anforderungen.
    - **FFG-L3 – Allgemeine Straßenfahrfreigabe**
- **D-Muster:** Dabei handelt es sich um Typgenehmigungsmuster für die behördliche Zulassung (vgl. Abschnitt 5.1), welche für die Freigabe des Produktionsprozesses und des Produkts verwendet werden. Diese Muster sind vollständig funktionsfähig, verfügen über die Serienfunktionalität und erfüllen sämtliche Qualitätsanforderungen.
    - **FFG-L4 – Serienfahrfreigabe**

Darüber hinaus werden die Phasen des PEPs gemäß dem VDA-Standard „Reifegradabsicherung für Neuteile“ [104] durch acht Reifegradabsicherungsmeilensteine (RGA-MS) koordiniert. Diese beziehen sich auf die Bestimmung und Sicherstellung des Produktreifegrads zu definierten Zeitpunkten (siehe Abbildung 3.1):

- **RGA-MS 0 – Innovationsfreigabe für Serienentwicklung:** Im Zuge der Produktstrategieentwicklung wird eine umfassende Produktstrategie konzipiert (siehe Abbildung 3.1). Die Liefergegenstände beziehen sich dabei auf die Definition der grundsätzlichen Vermarktungs- und Produktstrategie als auch die Spezifikation der groben Zielsetzung einschließlich einer Zeit- und

[1] Betriebsbereich (vgl. Definition 5.16)

[2] Erprobung (vgl. Definition 3.14)

Budgetvorgabe. Ferner werden Technologien und Funktionen aus der Forschung und Vorentwicklung in Bezug auf deren Machbarkeit bewertet und miteinbezogen. Auf Grundlage der vorangegangenen Aktivitäten werden abschließend kundenerlebbare Funktionen (engl. *Feature*) über funktionale Innovationen definiert [104].

- **RGA-MS 1 – Anforderungsmanagement für Vergabeumfang:** Im Rahmen dessen müssen gesetzliche Anforderungen sowie der Impact aus relevanten Standardisierungsgremien in Betracht gezogen werden. Des Weiteren werden wirtschaftliche Kriterien, das zur Verfügung stehende Budget sowie die Rentabilität eines möglichen Business Case erörtert [104].

- **RGA-MS 2 – Festlegung der Lieferkette und Vergabe der Umfänge:** Im Zuge dessen wird die Produktstrategieentwicklung finalisiert (siehe Abbildung 3.1), indem die Plausibilität des sogenannten Produkt-Business-Cases bestätigt und eine Vorauswahl von Lieferanten für die Technologieentwicklungsphase gebildet wird [104].

- **RGA-MS 3 – Freigabe technische Spezifikation:** Daraufhin gliedert sich die Phase der Technologieentwicklung an (siehe Abbildung 3.1), worin auf bereits bestehenden Plattformkonzepten und E/E-Architekturen (vgl. Abschnitt 4.2) zurückgegriffen wird, um ein spezifisches Architekturkonzept zu entwerfen. Dieses muss in der Lage sein, die neuartigen kundenerlebbaren Funktionen zu integrieren. Außerdem müssen Optimierungs- und Kostenkriterien zusätzlich erfüllt werden. Dahingehend hat sich innerhalb der Automobilindustrie der Ansatz etabliert, Innovationen oder neue Technologien meist in Baureihen aus dem Premiumsegment als Erstes einzuführen. Dadurch sollen die bei möglichen Rückrufaktionen anfallenden Gesamtkosten aufgrund niedrigerer Stückzahlen geringgehalten werden [103]. Abschließend erfolgt die Spezifikation des Serienentwicklungskonzepts einschließlich Anforderungen und Funktionen für Produkt und Produktion als auch die Generierung des Verifikationsberichts technischer, zeitlicher und kommerzieller Zielsetzungen und deren realisierbarer Lösungen [104].

- **RGA-MS 4 – Produktionsplanung abgeschlossen:** Während der sich anschließenden Fahrzeugentwicklung werden erste Prototypen aufgebaut und bis zur sogenannten „Nullserie“ weiterentwickelt (vgl. Abschnitt 3.2). Dies ermöglicht die frühzeitige Integration und Testen einzelner Komponenten sowie deren Zusammenspiel als auch am Ende die Überprüfung in Bezug auf das Gesamtfahrzeug. Simultan werden Aktivitäten der Werkzeugentwicklung, Abläufe der Fließbandproduktion, Anpassungen der Fertigungskapazitäten und die Einrichtung von Arbeitsplätzen für die spätere Serienproduktion hochgefahren [103]. Demgemäß ist die Bestätigung der Herstellbarkeit, Machbarkeit, der Serienlieferanten, des gesamten Zielkatalogs zu erbringen sowie der Beginn der Auftragsvergabe einzuleiten (siehe Abbildung 3.1). Des Weiteren sind sämtliche Detailentwicklungen abzuschließen [104], [112].

- **RGA-MS 5 – Serienwerkzeugfallende Teile und Serienanlagen verfügbar:** Der Produktionsstart bildet den Abschluss des PEPs (siehe Abbildung 3.1). Demzufolge werden die Produktion und Serienfertigung konsequent vorangetrieben. Damit der Produktionsstart (engl. *Start of Production {SOP}*) und abschließend die Markteinführung sowie der Verkauf initialisiert werden können, müssen zuvor die in das Fahrzeug integrierten Systeme und deren Funktionalitäten bis zur Serienreife verifiziert und validiert werden [103]. Darunter fällt auch die Montage unter seriennahen Herstellungsprozessbedingungen sowie die Verifikation der Serienwerkzeuge als auch des Vorserienherstellungsprozesses [104].

- **RGA-MS 6 – Produktionsprozess- und Produktfreigabe:** Diesbezüglich ist die Bestätigung der Herstellbarkeit und Taktzeiten unter vorgegebenen Serienbedingungen bei der Produktion als auch den Zulieferern zu erbringen. Hinzu kommt die Bestätigung der Erreichung der Entwicklungsziele mit Vorserienfahrzeugen [104].

- **RGA-MS 7 – Projektabschluss, Verantwortungsübergabe an Serie, Start Requalifikation:** Hierbei handelt es sich um den Abschluss des PEPs (siehe Abbildung 3.1), wobei die jeweilige Auslieferung und Übergabe an die Kunden erfolgt [112].

3.2 Vorgehensmodelle und Methoden für die Umsetzung des Automotive-Produktentstehungsprozesses

Um den Umfang abzuleistender Aufgaben, die Planung als auch Verteilung von Ressourcen und somit einen möglichst reibungs- und nahtlosen Ablauf innerhalb des Automotive-PEP zu Wege zu bringen, wird dieser durch Vorgehensmodelle, unterlagerte Prozesse und Methoden gestützt. Diese beinhalten das Konzept der Arbeitsteilung sowie eine Zusammensetzung von Entwicklungs- und Testphasen über Meilensteine und ermöglichen dadurch ein transparentes, planbares und beherrschbares Entwicklungsbestreben [113].

Definition 3.4 Vorgehensmodell [114].
Ein Vorgehensmodell (engl. Life Cycle Model) bezeichnet ein Rahmenkonzept von Prozessen und Aktivitäten, die sich mit dem Lebenszyklus befassen, in Stufen organisiert sein können und als gemeinsame Referenz für die Kommunikation und das Verständnis dienen.

Definition 3.5 Prozess [114].
Ein Prozess (engl. Process) ist ein Satz von zusammenhängenden oder interagierenden Aktivitäten, die Eingaben in Ausgaben umwandeln.

Definition 3.6 Methode [115].
Eine Methode [griechisch mēthodos = Weg oder Gang einer Untersuchung, eigentlich = Weg zu etwas hin] ist ein Verfahren, welches auf einem Regelsystem basiert und darauf abzielt, wissenschaftliche Erkenntnisse oder praktische Ergebnisse zu erlangen. Sie beschreibt die systematische Art und Weise, wie ein Vorgehen einerseits strukturiert und andererseits durchgeführt wird.

3.2.1 Wasserfallmodell

Das Wasserfallmodell zur Entwicklung von Softwaresystemen entstammt den Ideen von Royce [116] und gilt als Ursprung der in Phasen und Abschnitte unterteilten Automotive-Vorgehensmodelle. Dieses besteht aus sequenziellen und linear aufeinander folgenden Projektphasen gemäß dem Top-Down-Prinzip. Die bildhafte Anordnung der Phasen anhand einer Kaskade, bei welcher das Wasser nur bergabwärts fließen kann, verleiht dem Wasserfallmodell die Bezeichnung. In dieser Hinsicht ist jede Phase in sich abgeschlossen und liefert ein Ergebnis, welches als Ausgangsdokument für die nachfolgende Phase herangezogen wird (siehe Abbildung 3.2).

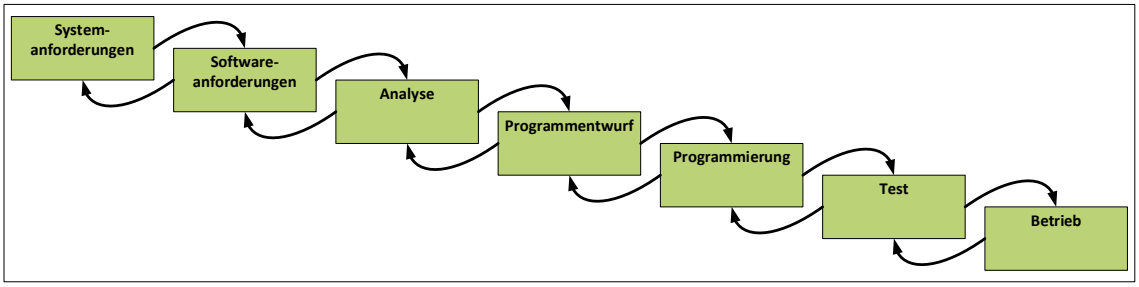


Abbildung 3.2: Struktur des Wasserfallmodells mit Iterationen zwischen aufeinander folgenden Phasen (in Anlehnung an [116]).

Hierbei kann eine neue Phase erst dann eingeleitet werden, wenn die vorherige vollständig abgeschlossen ist. Insgesamt kennzeichnet sich das Wasserfallmodell durch dessen einfache Struktur im Sinne eines disziplinierten, kontrollierbaren und transparenten Prozessablaufes und ist ergo mit geringem Aufwand handzuhaben. Als besonders nachteilig erweist sich jedoch die stringente Prozessabfolge, da der Übergang in die nachfolgende Phase nur bei vollständigem Abschluss der vorherigen vollzogen werden soll. Dieser Umstand führt dazu, dass Abweichungen lediglich zu einem späten Zeitpunkt im Entwicklungsprozess festgestellt werden können. Müssen zur Behebung der festgestellten Abweichungen Änderungen im Softwareentwurf und der -implementierung vorgenommen werden, so resultiert dies durch die erneut durchzuführenden Testaufwände in hohen Kosten und Zeitverlusten. Aufgrund dessen entwickelte sich aus der ursprünglichen Version eine erweiterte Form des Wasserfallmodells, die Iterationen[3] zwischen den aufeinanderfolgenden Phasen ermöglicht (siehe Abbildung 3.2). Dadurch können Fehler vor Abschluss des gesamten Prozesses korrigiert und Anpassungen vorgenommen werden, die den weiteren Verlauf beeinflussen.

3.2.2 Spiralmodell

Auf Basis der gemachten Erfahrungen im Zuge der Anwendung des Wasserfallmodells konzipierte Boehm [117] das sogenannte Spiralmodell für die Softwareentwicklung. Dieses stellt einen Rahmen für die systematische Anwendung unterschiedlicher anerkannter Entwicklungsverfahren, Methoden und Techniken bereit (siehe Abbildung 3.3).

Mittels vier Quadranten werden die wesentlichen Stufen zur Identifizierung von Zielen, Randbedingungen, Alternativen, Risiken als auch zur Planung und Realisierung illustriert. Ferner sieht dieses Vorgehensmodell den sequentiellen Ablauf der jeweiligen Prozessphasen und Iterationen anhand einer Spirale vor. Hierbei visualisiert das Winkelmaß den Fortschritt innerhalb des jeweiligen Entwicklungszyklus, während der Spiralradius die damit verbundenen aggregierten Kosten darstellt. Am Ende eines jeden Zyklus wird eine Überprüfung durchgeführt, in der alle Beteiligten entweder ihre Verpflichtung zur nächsten Projektphase bestätigen oder das Projekt beenden.

Das Vorgehen innerhalb eines Iterationszyklus im Spiralmodell folgt dabei dem grundlegenden Schema, das entsprechend der durchgeführten Risikobewertung angepasst wird. Zu Beginn eines Entwicklungszyklus werden die aktuellen Entwicklungsziele, mögliche Umsetzungsalternativen und bestehende Rahmenbedingungen ermittelt.

[3] Iteration (vgl. Definition 3.15)

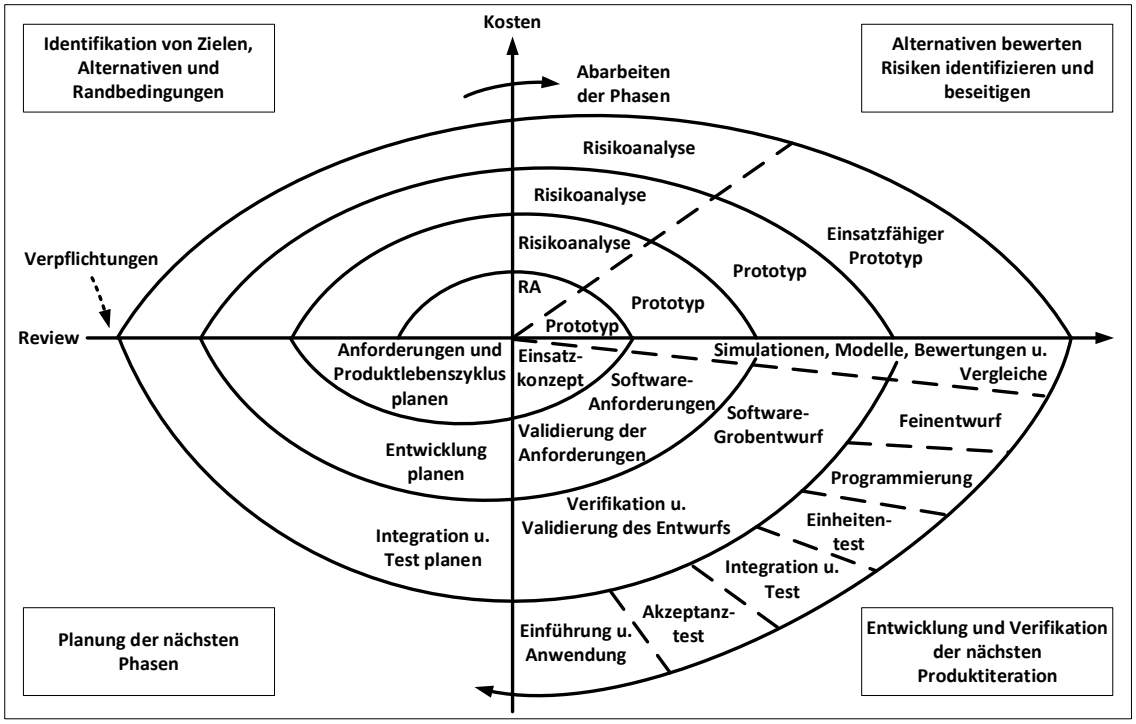


Abbildung 3.3: Spiralmodell für die Softwareentwicklung und -verbesserung (in Anlehnung an [117]).

Die Zielsetzung liegt darin, notwendige und geeignete Handlungsstrategien einerseits zur Risikominimierung und andererseits zur Erreichung des Iterationsziels aufzusetzen. In frühen Projektphasen haben Prototyping und Simulation eine hohe Relevanz für die Validierung von Nutzerkonzepten und die Bewertung neuer Technologien. In späteren Phasen, wenn der Fokus auf der korrekten Umsetzung und Absicherung der validierten Konzepte liegt, steht gemäß Boehm die Minimierung von Risiken durch fehlerhafte Implementierungen im Vordergrund (siehe Abbildung 3.3). Insgesamt erweist sich das Spiralmodell aufgrund des expliziten Verzichts eines stringent linearen Vorgehens im Vergleich zum Wasserfallmodell als agiler an und bietet zudem den Vorteil der frühzeitigen Validierung technologischer Lösungen. Allerdings ist dieses von projektspezifischer Ausprägung, was die Generalisierbarkeit und Wiederverwendbarkeit einschränkt. Ferner sind Schätzungen von Budget und Zeit zu Beginn des Projekts schwieriger zu beurteilen, da sich die Anforderungen im Laufe des Prozesses erst entwickeln. Dadurch entsteht das Risiko der Nichteinhaltung des ursprünglichen Budgets oder Zeitplans.

3.2.3 V-Modell

Das V-Modell wurde für die Entwicklung von informationstechnischen (IT)-Systemen konzipiert. Dabei durchlief dieses, angefangen beim V-Modell 92, über das V-Modell 97 bis hin zum V-Modell XT, mehrere Iterationsschleifen. Im Jahr 2005 wurde das V-Modell XT als Reaktion auf den fortschreitenden Stand der Informationstechnologie veröffentlicht [118]. Der Zusatz "XT" steht für "Extreme Tailoring" und unterstreicht die hohe Flexibilität des Modells in der Anpassung an verschiedene Projekte und Organisationen. An dieser Stelle sei allerdings anzumerken, dass aus Gründen der Übersichtlichkeit und der grafischen Veranschaulichung sich die vorliegende Dissertation am V-Modell 97 orientiert. Insgesamt stellt das V-

Modell ein umfassendes Prozess- und Vorgehensmodell dar, welches die während der Produktentwicklung notwendigen Aktivitäten, die resultierenden Produkte einschließlich deren Zustände als auch die benötigten Rollen vorgibt [119]. Darüber hinaus nimmt das V-Modell die Rolle des Referenzmodells für das „Capability Maturity Model Integration“ (CMMI) [120] als auch dem ASPICE [121] ein, welche die Verbesserung und Bewertung von Prozessen zum Zwecke haben.

Zu diesem Zweck ist dieses in vier Submodelle Systemerstellung (SE), Qualitätssicherung (QS), Konfigurationsmanagement (KM) sowie Projektmanagement (PM) untergliedert. Das Submodell PM regelt die Aufgaben und Funktionen des technischen Projektmanagements innerhalb des Entwicklungsprozesses. Die darin festgelegten Aktivitäten umfassen die Planung, Überwachung und Steuerung der internen Projekttätigkeiten, die Vergabe von internen Rollen und die Einrichtung einer Schnittstelle zu Einheiten außerhalb des Projekts wie beispielsweise dem Auftragnehmer. Des Weiteren können im Zuge dessen ein zyklisches Risikomanagement als auch eine projektspezifische Adaption des V-Modells im Sinne des „Tailoring“ umgesetzt werden. Die QS regelt die Aufgaben und Funktionen des Qualitätsmanagementsystems innerhalb des Systementwicklungsprozesses. Dabei spezifiziert diese Qualitätsanforderungen, Testfälle sowie Kriterien und überprüft die Produkte als auch die Konformität mit Normen und Standards. Das Submodell KM gewährleistet, dass alle Produkte eindeutig identifizierbar sind, Wechselbeziehungen und Abweichungen verschiedener Versionen oder Varianten einer Konfiguration nachvollziehbar bleiben und Produktänderungen nur geregelt vorgenommen werden können [119].

Die Wesenskern des V-Modells liegt im Submodell SE. Dieses ist wiederum in neun sogenannte Vorgehensbausteine unterteilt, welche in Form eines „V“ angeordnet sind und ihrerseits weitere Aktivitäten beinhalten. Auf dem linken Schenkel startet der Top-Down-Entwurfsprozess auf Systemebene mit der Systemanforderungsanalyse (SE1) und mündet in den Systementwurf (SE2) (siehe Abbildung 3.4).

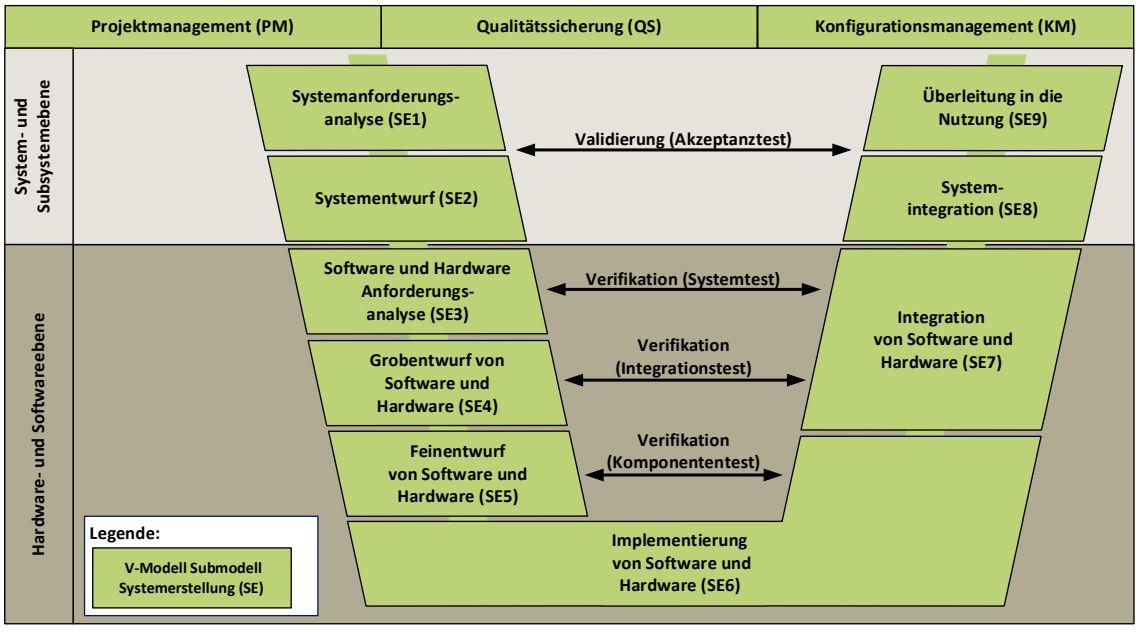


Abbildung 3.4: Submodell Systemerstellung (SE) des V-Modells 97 inkl. der übergeordneten Submodelle des Projektmanagements (PM), der Qualitätssicherung (QS) und des Konfigurationsmanagements (KM) (in Anlehnung an [119]).

Definition 3.7 Anforderung [122].
Eine Bedingung oder Fähigkeit, die von einem System, einer Komponente, einem Produkt oder einer Dienstleistung erfüllt werden/vorhanden sein muss, um eine Vereinbarung, einen Standard, eine Spezifikation oder andere formale Dokumente zu erfüllen.

Definition 3.8 Spezifikation [122].
Eine detaillierte Formulierung in Form eines Dokumentes, welche eine maßgebliche Beschreibung eines Systems zum Zweck der Entwicklung, Verifikation oder Validierung bereitstellt.

Auf Hardware- und Softwareebene wird anschließend mit der Hardware- und Softwareanforderungsanalyse (SE3) fortgefahren. Diese wird über den Grobentwurf der Hardware und Software (SE4) bis hin zum Feinentwurf von Hardware und Software (SE5) kontinuierlich konkretisiert. Der Entwurfsprozess endet schließlich mit der Implementierung von Hardware und Software (SE6) [123] (siehe Abbildung 3.4).

Der rechte Schenkel repräsentiert auf Hardware- und Softwareebene die Bottom-Up-Integration von Software und Hardware (SE7) als auch den Verifikationsprozess [124]. Im Zuge dessen kann jedem Arbeitsergebnis bzw. -produkt, welches aus dem linken Schenkel hervorgeht, eine Verifikation auf dem rechten Schenkel zugewiesen werden [123]. Auf Systemebene des rechten Schenkels erfolgt die Systemintegration (SE8), der Validierungsprozess, welcher der Systemanforderungsanalyse (SE1) gegenübergestellt ist [123], und abschließend die Überleitung in die Nutzung (SE9) (siehe Abbildung 3.4).

Definition 3.9 Verifikation [100].
Die Verifikation ist der Prozess zur Beurteilung eines Systems mit dem Ziel festzustellen, ob die Resultate einer gegebenen Entwicklungsphase den Vorgaben bzw. Anforderungen für diese Phase entsprechen. Die Verifikation ist demnach die Prüfung, ob eine Implementierung bzw. technische Lösung der für den betreffenden Entwicklungsschritt vorgegebenen Spezifikation im Sinne der zu erfüllenden Anforderungen genügt.

Definition 3.10 Validierung [100].
Die Validierung ist der Prozess zur Beurteilung eines Systems mit dem Ziel festzustellen, ob der Einsatzzweck oder die Benutzererwartungen erfüllt werden. Funktionsvalidierung ist demnach die Prüfung, ob die Spezifikation die Benutzeranforderungen erfüllt, ob überhaupt die Benutzerakzeptanz durch eine Funktion erreicht wird.

Innerhalb von Verifikation und Validierung kommt dem Testen eine wesentliche Rolle zu. Prinzipiell beruht das Testen auf einer systematischen Herangehensweise [53] und dient dazu, Fehler in der System- oder Komponentenrealisierung sowie das unzureichende Erfüllen einer definierten Anforderung aufzuspüren [125]. Daraus leiten sich auch die automobilspezifischen Rollen des Entwicklers und Testers ab [53]. Im Zuge des Testens kommen unterschiedlichste Methoden und Techniken zum Einsatz, die von einfachem Debugging der Software bis hin zu profunden Qualitäts- und Sicherheitstests des Gesamtfahrzeugs auf der Straße reichen.

Definition 3.11 Testen [122].
Das Testen repräsentiert eine Aktivität, bei welcher ein System unter spezifizierten Bedingungen ausgeführt wird, die Ergebnisse dieser Ausführung beobachtet oder aufgezeichnet werden und ein Aspekt des Systems im Sinne von Pass-/Fail Kriterien bewertet wird.

Des Weiteren werden Testfälle für den systematischen Nachweis einer Anforderungserfüllung durch das zu überprüft werdende Testobjekt deduziert. Wichtig ist hierbei, dass der Testfallumfang sowohl die Funktionalität als auch die Spezifikation vollständig abdeckt.

Definition 3.12 Testfall [126].
Ein Testfall umfasst die erforderlichen Voraussetzungen, Eingaben (einschließlich Aktionen, sofern anwendbar) und erwarteten Ergebnisse, welche entwickelt wurden, um ein Testobjekt auszuführen und zu prüfen, ob es die Testziele wie beispielsweise korrekte Implementierung, Identifikation von Fehlern, Qualitätsprüfung und weitere werthaltige Informationen erreicht.

Definition 3.13 Testobjekt [53].
Das Testobjekt (engl. System Under Test {SUT}), ist das zu testende System-Of-Systems, System, Subsystem oder die zu testende Komponente bzw. Einheit.

In Abhängigkeit der Hierarchieebenen des V-Modells (siehe Abbildung 3.4) wird zwischen Einheitentest, Komponententest, Integrationstest, Systemtest und Akzeptanztest unterschieden, wobei die ersten vier der Verifikation zugehören, während der letzte der Validierung zuzuteilen ist [127]. Der Testinhalt auf jeder Teststufe wird dabei in funktionale und nicht-funktionale Tests separiert. Im Zuge funktionaler Tests wird die Funktion bzw. die Zweckerfüllung bewertet. Dahingegen umfassen nicht-funktionale Tests die Überprüfung von Schnittstellen oder die Erfassung quantitativer Aspekte im Sinne von Ausführungs- und Reaktionszeiten, Genauigkeit etc. Hierbei sind die jeweiligen Integrationsschritte eng mit den Testprozeduren verknüpft [100].

Zum Abschluss erfolgt der Akzeptanztest aus der Perspektive des Benutzers, sprich des Endkunden, und beinhaltet somit den Test gegen die Nutzeranforderungen. Hierbei kommt die organisatorische Trennung der Abteilung für die Freigabe der Fahrzeugfunktionalität von der Entwicklungsabteilung und folglich die Unterscheidung der Rolle des Entwicklers und des Testers besonders zum Tragen [128]. Ein weiteres Element des Akzeptanztests ist die Erprobung anhand von Testfahrten auf Testgeländen und im öffentlichen Straßenverkehr, da der letztendliche Markterfolg eines Fahrzeugs in der Regel durch individuelle menschliche Empfindungen bestimmt wird [53]. Insgesamt spiegelt der Akzeptanztest die Querbeziehung zwischen dem linken und rechten Schenkel des V-Modells (siehe Abbildung 3.4) in finaler Instanz wider und resultiert in der Freigabe des Gesamtsystems im Fahrzeug [128].

Definition 3.14 Erprobung [53].
Die Erprobung ist eine Analyse des Gesamten, der eine vergleichsweise geringe Systematik zugrunde liegt. In der Erprobung steckt das Ausprobieren in einer unbestimmten Situation.

Allerdings wird der Übergang zwischen den Projektphasen beim V-Modell analog zum Wasserfallmodell nur mit finalisierten Arbeitsprodukten angestrebt (vgl. Unterabschnitt 3.2.1). Demnach ist ein inkrementelles und/oder iteratives Vorgehen im klassischen V-Modell-Ansatz nicht vorgesehen.

3.2.4 Scrum

Auf Grundlage des „Agile Manifest“ (Manifesto for Agile Software Development) von 2001 [129] haben sich agile Vorgehensmodelle und Methoden wie Scrum, Kanban und Extreme Programming (XP) etablieren können [130]. Die Motivation zur Formulierung und Unterzeichnung des Agilen Manifests lag in der Erkenntnis der Autoren, dass rigide Entwicklungsprozesse, einschließlich der starren Festlegung auf fehlerhafte Planungen und Ziele, übermäßiger Dokumentationsanforderungen und mangelndem Bewusstsein für die Herausforderungen der Softwareentwickler auf Managementebene, maßgeblich zu Kostensteigerungen und Verzögerungen bei Softwareprojekten beitragen. Das Agile Manifest priorisiert dementsprechend eine handlungsorientierte Entwicklung über eine detaillierte Planung, Steuerung und

Dokumentation. Nach Auffassung des „Agile Manifest“ wird der Projekterfolg vornehmlich durch die Interaktionen der beteiligten Personen, ihre Fähigkeit zur Reaktion auf Veränderungen und durch funktionierende Software gewährleistet.

Scrum gehört zu den führenden agilen Methoden und wird von den Autoren als „Rahmenwerk zur Entwicklung und Erhaltung komplexer Produkte“ beschrieben [131]. Dieses Rahmenwerk ermöglicht die Integration verschiedener Vorgehensweisen und Techniken der Produktentwicklung, ähnlich dem Spiralmodell (vgl. Unterabschnitt 3.2.2). Hierbei basiert Scrum auf einem iterativen, erkenntnistheoretischen Ansatz zur Prozesssteuerung, wobei sämtliche alle Entscheidungen auf vormals getätigte Erfahrungen basieren. Die Pfeiler dieses Ansatzes sind Transparenz, ein gemeinsames Verständnis der Vorgehensweise, Ziele und Fertigstellungskriterien (engl. *Definition of Done*), kontinuierliche Überprüfung der Arbeitsprodukte (engl. *Inspection*) sowie die Adaption der Arbeitsweise und -mittel (engl. *Adaptation*) auf Grundlage der während der Inspektion festgestellten Problemstellungen.

Anstelle detailliert spezifizierter Prozessschritte und Arbeitsprodukte legt Scrum den Fokus auf die Eigenverantwortung der jeweiligen Individuen des Entwicklungsteams. Innerhalb eines fest vorgegebenen Zeitraums wird anhand von Iterationen bzw. Sprints eine Teilmenge der für die Zielerreichung benötigten Arbeitsprodukte im Sinne von Inkrementen finalisiert.

Definition 3.15 Iteration bzw. Sprint [131].
Die Iteration bzw. der Sprint bezieht sich auf einen wiederholten Entwicklungszyklus, bei dem ein Produkt schrittweise überarbeitet sowie anhand von Inkrementen erweitert und/oder verfeinert wird. Dabei kennzeichnet sich die Iteration dadurch, dass Aktivitäten innerhalb einer oder mehrerer Prozessphasen des Vorgehensmodells erneut durchgeführt werden, um die jeweiligen Inkremente zu erzeugen.

Definition 3.16 Inkrement [131].
Ein Inkrement repräsentiert einen Produktbestandteil und bezieht sich auf eine stufenweise sowie messbare Erweiterungs- oder Verbesserungsmaßnahme des Gesamtprodukts. Es handelt sich um eine funktionale oder technische Ergänzung, die einem bestehenden Produkt hinzugefügt und verifiziert wird, um dessen Fähigkeiten, Leistung oder Funktionalität zu optimieren.

Dabei ist jeder Sprint durch vier rekurrierende Termine strukturiert: Sprint-Planung, Tägliches Scrum, Sprint-Review und Sprint-Retrospektive (siehe Abbildung 3.5). An dieser Stelle umfasst das Produkt-Backlog alle potenziellen Anforderungen an das zu entwickelnde Produkt, welche wiederum vom Produkt Owner priorisiert werden. Während der Sprint-Planung wählt das Entwicklungsteam eine Teilmenge dieser Anforderungen aus und transferiert diese in das Sprint-Backlog.

Mit Hilfe von Aufwandsabschätzungen wird wiederum bestimmt, welche Aufgaben im kommenden Sprint abgeschlossen werden können. Im täglichen Scrum-Meeting synchronisiert sich das Scrum Team bezüglich der geleisteten Arbeit, der Tagesplanung und möglicher Hindernisse. Am Ende des Sprints erfolgt das Sprint-Review, in dem die finalisierten Inkremente reflektiert und das Produkt-Backlog an neu gewonnene Erkenntnisse angepasst wird. Die Sprint-Retrospektive dient der Reflexion und Verbesserung der Teamarbeit und Arbeitsabläufe (siehe Abbildung 3.5).

Scrum gibt für alle Meetings feste Zeitfenster vor, um die Fokussierung auf das Wesentliche zu gewährleisten. Der Scrum-Master ist verantwortlich für die regelmäßige Durchführung dieser Termine, die Einhaltung der Zeitvorgaben und die Förderung des Prozessverständnisses. Er übernimmt somit eine koordinierende und vermittelnde Rolle innerhalb des Scrum-Rahmenwerks.

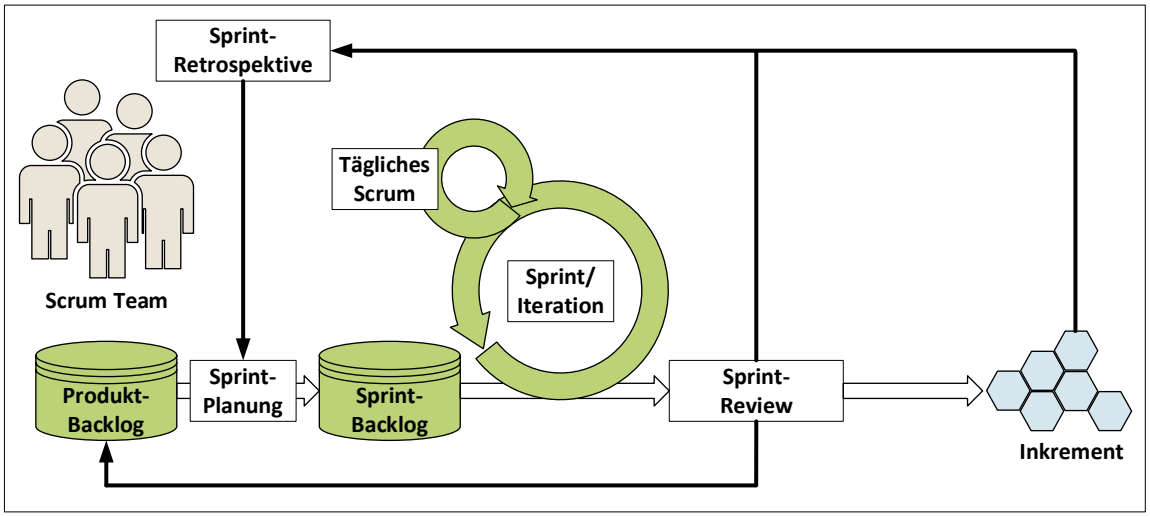


Abbildung 3.5: Scrum-Rahmenwerk für die Produktentwicklung (in Anlehnung an [132]).

3.2.5 DevOps

Zu den agilen Ansätzen gehört auch die kontinuierliche Verbesserung und Erweiterung eines Dienstes anhand von sogenannten „Development & Operations"- (DevOps)-Entwicklungsprinzipien [133]. DevOps ist eine Entwicklungsmethode, die darauf abzielt, die Kluft zwischen Entwicklung (Dev) und Betrieb (Ops) zu überbrücken. Die Kernidee von DevOps besteht darin, die Agilität der Softwareentwicklung mit der Stabilität und Verlässlichkeit des Betriebs zu vereinen. Um dieses Ziel zu erreichen, wird ein iterativer, kontinuierlicher Entwicklungs-, Integrations-, Test- und Bereitstellungszyklus etabliert, was sich in Pipelines für die kontinuierliche Integration (engl. *Continuous Integration {CI}*), den kontinuierlichen Test (engl. *Continuous Test {CT}*) sowie die Bereitstellung (engl. *Continuous Deployment {CD}*) manifestiert (siehe Abbildung 3.6).

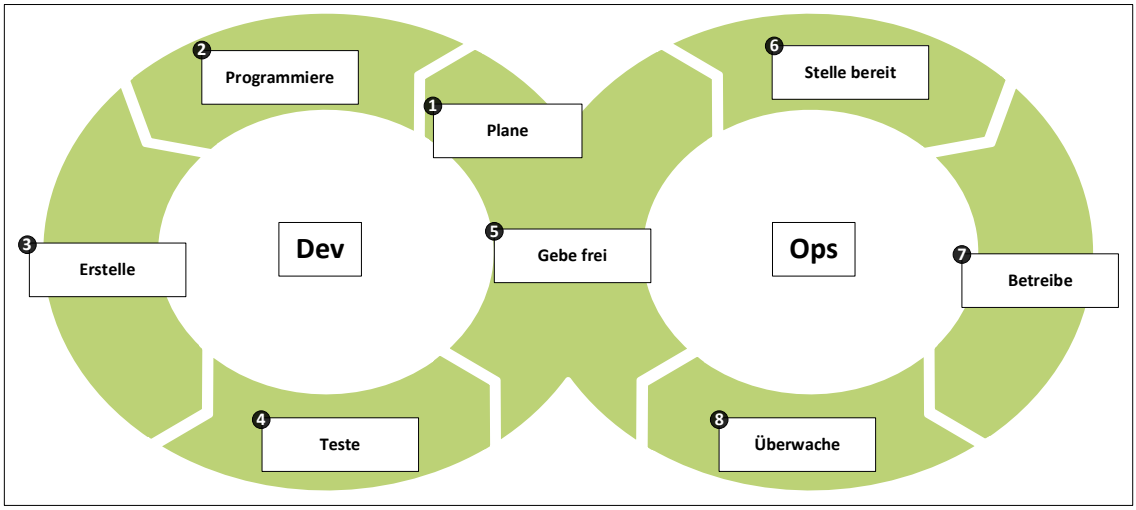


Abbildung 3.6: Zyklischer DevOps-Ansatz (in Anlehnung an [133]).

Die kontinuierliche Bereitstellung von Software basiert auf flexiblen und skalierbaren Produktdefinitionen, die sich auf funktionsweise geclusterte Komponenten konzentrieren und unabhängig voneinander aktualisiert werden können. Im Hinblick darauf werden Entwicklungs- und Betriebsphasen eines Softwareprodukts direkt miteinander verknüpft, indem einerseits Software-Releases gefördert und andererseits kontinuierliche Innovationen auf der Grundlage von Rückmeldungen aus dem Betrieb ermöglicht werden. DevOps setzt dabei auf eine systematische Überwachung und Aufzeichnung (engl. *Logging*), um die Leistung und Verfügbarkeit der Software kontinuierlich zu bewerten und Probleme proaktiv adressieren zu können.

Ein weiterer Aspekt von DevOps ist die Automatisierung von Build-, Test- und Deployment-Prozessen. Dadurch wird sichergestellt, dass Änderungen konsistent und zuverlässig durchgeführt werden, was das Risiko von Fehlern reduziert und die Entwicklungszyklen beschleunigt. Automatisierte Tests sorgen zudem dafür, dass neue Codeänderungen bestehende Funktionalitäten nicht beeinträchtigen und gewährleisten somit eine kontinuierliche Qualitätskontrolle. Hinzu kommt die Förderung einer engen Zusammenarbeit und Kommunikation zwischen den beteiligten Entwicklungsteams. Hierzu gehören regelmäßige Feedback-Schleifen sowie die gemeinsame Verantwortlichkeit über die gesamte Lebensdauer der Software hinweg. Das wiederholte Durchlaufen der Prozesskette führt dazu, dass durch das Monitoring der produktiven Lösung kontinuierlich Daten generiert werden. Diese Rückmeldungen ermöglichen die Bewertung neuer Hypothesen und erlauben es, am Ende eines Zyklus gezielt zwischen erfolgreichen und nicht erfolgreichen Ergebnissen zu unterscheiden.

3.2.6 Multiple- und Agile-V-Modell

Da beim V-Modell die Korrektheit der Spezifikation in der Phase der Integrationstests und damit erst spät im Entwicklungsprozess überprüft werden kann, bietet es sich an, auf Prototypenmodelle zurückzugreifen [134], [135]. Diese können im Zuge der Strategie- und Konzeptphase des PEP (vgl. Abschnitt 3.1) aufgesetzt und zu einem späteren Zeitpunkt während der Serienphase anhand von Musterständen realisiert werden. Hierbei werden für eine frühzeitige Validierung mechatronische Muster, Vorserien- oder Serienfahrzeuge mit Systemen für die prototypische Ausführung der Softwarekomponenten bestückt. Die Musterstände werden je nach Voranschreiten der jeweiligen Projektphase in A-, B-, C- und D-Muster unterteilt (vgl. Abschnitt 3.1).

Die VDA „Reifegradabsicherung für Neuteile“ [104] geht einen Schritt weiter und schlägt die Integration des V-Modells im Sinne des „Multiple-V-Modells“ in den PEP vor (siehe Abbildung 3.7). Das Submodell SE gliedert sich in die System-, Software-, Hardware- und Mechanikentwicklung, wobei das V-Modell in jedem dieser Bereiche im Widerspruch zum klassischen Ansatz iterativ durchlaufen wird. Dabei mündet jede abgeschlossene Phase in einer Freigabe. Die drei Entwicklungsstränge verlaufen asynchron, wobei die Dauer eines V-Modell Durchlaufs je nach Entwicklungsstrang und Phase im Produktentwicklungsprozess unterschiedlich ist. Die Synchronisierung von Software, Hardware und Mechanik erfolgt zu festgelegten Zeitpunkten im PEP anhand von definierten Reifegrad-Meilensteinen und Musterständen (vgl. Abschnitt 3.1).

Zur Sicherstellung der Produktqualität wird somit parallel zum PEP eine Reifegradabsicherung durchgeführt. Hierbei stützt sich die Bewertung des Reifegrads auf festgelegte Indikatoren, für die wiederum ein spezifischer Satz an Mess- und Bewertungskriterien definiert wird.

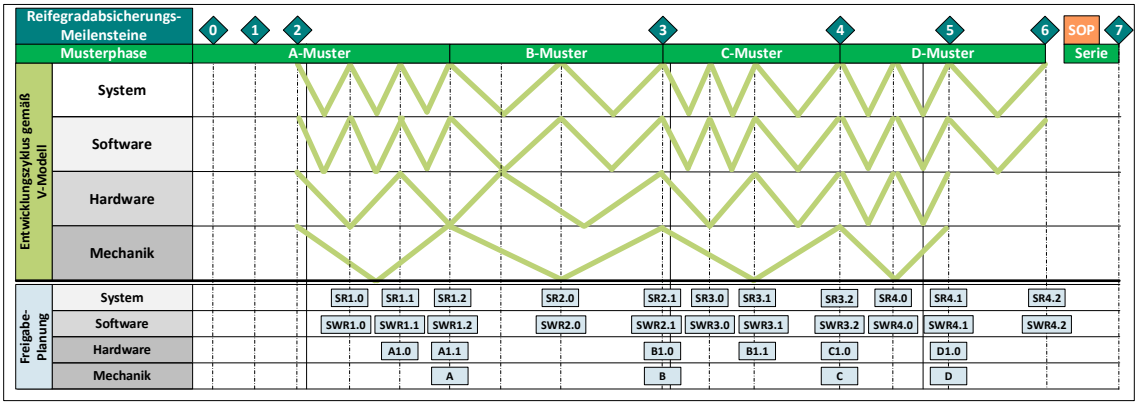


Abbildung 3.7: Multiple-V-Modell gemäß der VDA „Reifegradabsicherung für Neuteile“ (in Anlehnung an [104]).

Die jeweiligen Bewertungskriterien für den Nachweis der Funktionalität im Gesamtfahrzeug umfassen u.a. die vollständige Berücksichtigung aller relevanten Testfälle sowie den Nachweis der Funktionalität mithilfe von Erprobungsfahrzeugen, Prüfständen oder digitalen Prototypen. Die Gesamtbewertung des Reifegrads wird aus der Zusammenführung der Einzelbewertungen abgeleitet, wobei sie dem niedrigsten Wert eines Einzelkriteriums entspricht.

Vor dem Hintergrund der Zusammenführung von „Artificial Intelligence“ (AI) und „Internet of Things“ (IoT) als AIoT-Rahmenwerk [136], wird ein ähnlich gestalteter Ansatz im Sinne des „Agile-V-Modells“ vorgestellt. Dabei werden die agilen Grundsätze des Scrum inkl. kontinuierlicher Integration (CI), kontinuierlicher Test (CT) und kontinuierliche Bereitstellung (CD) in das klassische V-Modell eingebettet [137]. Im Zuge des Agile V-Modells wird sichergestellt, dass die jeweiligen Scrum-Sprints (vgl. Unterabschnitt 3.2.4) selbst zu entsprechenden „Vs“ werden. Jeder V-Sprint kombiniert einen Scrum-Sprint mit einem sprintspezifischen Planungselement. Am Ende jedes Sprints werden die Sprint-Ergebnisse im Sinne eines erzeugten Inkrements mit den ursprünglichen Sprint-Zielen verglichen. Im Bedarfsfall werden gemäß den Ergebnissen Anpassungen durchgeführt. Die aktualisierten Inhalte dienen dann wiederum als Input für die Planung des nächsten Sprints (siehe Abbildung 3.8).

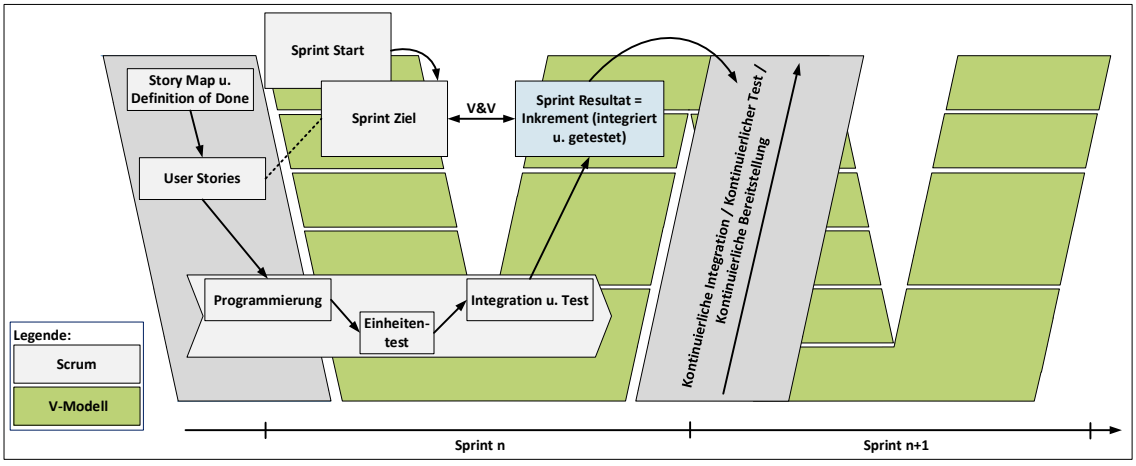


Abbildung 3.8: Agile-V-Modell (in Anlehnung an [137]).

4 Automotive-Systementwicklung

„Das Ganze ist mehr als die Summe seiner Teile. Der Teil ist mehr als der Bruchteil des Ganzen."

Aristoteles

Aufgrund des kontinuierlichen technischen Fortschritts und der damit einhergehenden Multi- und Interdisziplinarität der beteiligten Akteure während des gesamten Produktlebenszyklus, hat sich innerhalb des Automobilsektors eine eigenständige Domäne der Automotive-Systementwicklung bzw. des „Automotive Systems Engineerings" etabliert. Zudem erfordern die kurzen Innovationszyklen im Automobilbereich eine enge Zusammenarbeit zwischen verschiedenen Disziplinen, von der Mechanik über die Elektronik bis hin zur Softwareentwicklung. Insbesondere durch den Einzug von Elektronik, Software und Vernetzung hat sich die Automotive-Systementwicklung als automobilspezifische Ableger der allgemeinen Systementwicklung[1] mit zum Teil spezifischen Methoden, Werkzeugen und Architekturen hervorheben können. Diese umfasst den Prozess der Konzeption, Planung, Implementierung sowie Wartung und berücksichtigt zunehmend Aspekte der Fahrerassistenz, des automatisierten Fahrens und der Elektrifizierung. Infolgedessen werden im Verlauf des vorliegenden Kapitels die im Rahmen dieser Dissertation relevanten Basiskenntnisse der Automotive-Systementwicklung dargelegt. Des Weiteren wird auf die modellbasierte Systementwicklung und deren zunehmende Tragweite eingegangen.

4.1 Einordung des Systembegriffs

Ein System[2] wird prinzipiell durch dessen Bestandteile, deren Beziehungen und Wechselwirkungen sowie die umgebende Umwelt charakterisiert.

Definition 4.1 Allgemeines System [139].
Unter einem allgemeinen System wird eine von der Umwelt abgrenzbare Komposition verstanden, deren Elemente untereinander (innen) ausgeprägtere Beziehungen besitzen als zu anderen Elementen (außen); im Zusammenspiel der einzelnen Elemente ergeben diese eine höhere Qualität als die Summe der einzelnen Elemente (Emergenz). Ein allgemeines System ist die Gesamtheit miteinander verknüpfter und sich gegenseitig beeinflussender Elemente, die entsprechend einem bestimmten Zweck organisiert sind.

Nach Schnieder [140], [141] kann der Systembegriff allgemein anhand von vier Axiomen expliziert werden. Das Strukturprinzip (Axiom 1) besagt, dass ein System aus einer bestimmten Anzahl von Teilen, welche einerseits untereinander und andererseits mit der Systemumgebung reziproke Relationen aufweisen, zusammengesetzt ist. Zudem ist eine gewisse Eigenständigkeit und Resilienz gegenüber Umgebungseinflüssen ausschlaggebend, um das System abgrenzen zu können. Gemäß dem Dekompositionsprinzip (Axiom 2) besteht ein System aus einer Menge von Teilen, welche selbst wiederum in eine Anzahl mitei-

[1] Die Systementwicklung wird fundamental durch das angelsächsische Systems Engineering geprägt. Hierbei hat sich auch der deutsche Begriff der Systemtechnik etabliert. Im Zuge dieser Dissertation werden Systementwicklung und Systemtechnik als Synonym zum Systems Engineering verwendet.

[2] Das Wort System leitet sich vom altgriechischen systema ab, was übersetzt *„aus Teilen Zusammengesetztes"* bedeutet [138].

nander in Interaktion stehender Bestandteile separiert werden können. Diese charakterisieren sich abermals durch generelle Systemeigenschaften. Exemplarisch sind hier der Ansatz von Schäuffele und Zurawka [100] sowie des „Automotive Software Process Improvement and Capability Determination“ (ASPICE) [121] (vgl. Abschnitt 4.2) zu nennen, welche die Unterteilung eines technischen Gesamtsystems in die hierarchischen Granularitätsebenen System, Subsystem, Komponente und Einheit vorsehen, wobei hier noch der Begriff des System-Of-Systems als übergeordnete Klasse eingeführt wird (siehe Abbildung 4.1).

Hierbei sei anzumerken, dass im weiteren Verlauf der Dissertation hauptsächlich der allgemeine Systembegriff verwendet wird. Dieser kann sich jeweils auf ein System-Of-Systems, System, Subsystem, eine Komponente oder eine Einheit beziehen.

Definition 4.2 System-Of-Systems [142].
Ein System-Of-Systems besteht aus einer Menge von Elementen, die zusammenwirken, um eine übergreifende Fähigkeit zu bieten bzw. Zweck zu erfüllen, welchen keines der konstituierenden untergeordneten Systeme für sich allein erreichen kann.

Definition 4.3 System [122].
Ein System repräsentiert ein untergeordnetes Element innerhalb eines umfassenderen bzw. übergeordneten System-Of-Systems und charakterisiert sich dabei als Kombination interagierender Elemente, die so organisiert sind, dass ein oder mehrere explizit definierte Zwecke erreicht werden.

Definition 4.4 Subsystem [122].
Ein Subsystem repräsentiert ein untergeordnetes Element innerhalb eines umfassenderen bzw. übergeordneten Systems.

Definition 4.5 Komponente [122].
Eine Komponente umfasst ein untergeordnetes Element mit diskreter Struktur innerhalb eines Subsystems, wie z.B. eine Hardwarebaugruppe oder ein Softwaremodul, welches auf einer bestimmten Analyseebene betrachtet wird.

Definition 4.6 Einheit [122].
Eine Einheit ist ein für sich prüfbares Element, welches im Entwurf einer Hardware- oder Softwarekomponente spezifiziert ist.

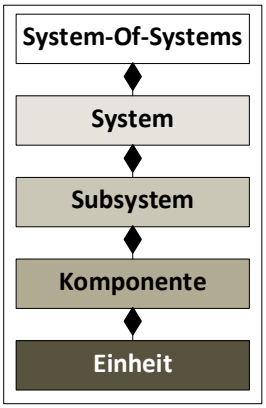


Abbildung 4.1: Unterteilung eines technischen Gesamtsystems in hierarchische Granularitätsebenen.

Dem Kausalitätsprinzip (Axiom 3) zufolge sind die Relationen der Bestandteile eines Systems als auch deren Veränderung eindeutig festgelegt. Demzufolge sind nachfolgende Zustände stets von vorangegangenen abhängig und werden als kausale Logik von zeitlich Abläufen aufgefasst. Das Temporalprinzip (Axiom 4) drückt aus, dass die Struktur oder der Zustand eines Systems zeitlichen Veränderungen unterliegt. Als Temporalität ist der zeitliche Prozess von Sequenzen und Modifikationen zu verstehen [141]. Durch die Eigenschaften Zustand, Struktur, Funktion und Verhalten lässt sich der Systembegriff unter Berücksichtigung der definierten Axiome abermals konkretisieren (siehe Abbildung 4.2) [143]. Funktionen eines Systems bilden die Zustandsmengen der Eingangsgrößen in Zustandsmengen der Ausgangsgrößen (Stoff, Energie, Information) ab.

Auch diese lassen sich gemäß dem Dekompositionsprinzip in miteinander vernetzte Unterfunktionsbausteine (z.B. Speichern, Übertragen, Verarbeiten etc.) zerlegen, welche nur im gemeinsamen Zusammenspiel den Gesamtzweck des Systems erfüllen.

Definition 4.7 Funktion [144], [122].
Unter Funktion ist die Teleologie[3] eines Systems zu verstehen, sprich der Zweck oder die Zielausrichtung des Systems. Dabei beschreibt eine Funktion die Umwandlung von Eingängen in Ausgänge mithilfe entsprechender Mechanismen.

Definition 4.8 Funktionalität [100].
Unter Funktionalität bzw. kundenerlebbare Funktion (engl. Feature) ist ein Ausstattungsmerkmal bzw. eine Eigenschaft aufzufassen, welche ein Kraftfahrzeug bietet, um dessen Leistung, Sicherheit, Komfort, Effizienz, Benutzerfreundlichkeit oder Kundenerlebnis zu verbessern. Dabei können Features sowohl physischer als auch softwarebasierter Charakteristik sein.

Der aktuelle Zustand eines Systems lässt sich durch eine Anzahl von Zustandsgrößen, exemplarisch durch die Angabe von Werten statischer oder dynamischer Attribute, veranschaulichen. Zu einem gegebenen Zeitpunkt und Ort werden durch diese Attribute die stofflichen, energetischen und informatorischen Eigenschaften, Merkmale, Größen und Werte des Systems dargestellt. Das Verhalten eines Systems wird durch dynamische Zustandsänderungen determiniert und fußt auf dem Kausalitäts- und Temporalprinzip. Das Systemverhalten ergibt sich infolgedessen aus einer logischen Reihenfolge sowie einer zeitlichen Abfolge der jeweiligen Zustände als auch deren Transitionen [145]. Demzufolge werden an dieser Stelle das Attribut des Zustands in das Attribut des Verhaltens inkludiert.

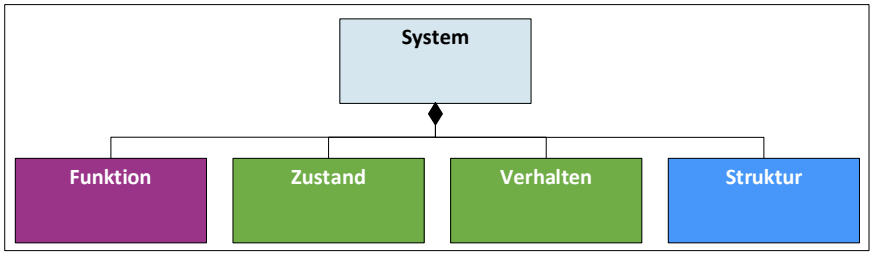


Abbildung 4.2: Funktion (lila), Zustand, Verhalten (jeweils grün) und Struktur (blau) als Eigenschaften bzw. Attribute von Systemen (in Anlehnung an [145]).

[3] Teleologie spiegelt die philosophische Lehre der Zielgerichtetheit von Vorgängen wider. Als zielgerichtet können menschliche Handlungen, Vorgänge aus der Natur und Technik bzw. deren Resultate aufgefasst werden [138].

Definition 4.9 Verhalten [144].
Unter Verhalten einschließlich Zustände sind beobachtbare, messtechnisch erfassbare Attribute, Kausalitäten und/oder physikalische Effekte eines Systems aufzufassen, sprich was das System tut.

Die Struktur eines Systems ist die Gesamtheit der Beziehungen zwischen den Teilen eines Ganzen [146] und basiert folglich auf dem Struktur- und Dekompositionsprinzip. Vor diesem Hintergrund wird das System in mehrere Granularitätsebenen von Ganzheit und Teilen dekomponiert. Hierbei ist die Ganzheit einer Hierarchieebene stets Bestandteil der darüber liegenden, sprich Teile eines Systems können einerseits als Subsysteme und das System selbst andererseits als Teil eines umfassenderen System-Of-Systems wahrgenommen werden.

Definition 4.10 Struktur [144].
Unter Struktur ist die Zusammensetzung der Systembestandteile bzw. -elemente und deren Beziehungen zu verstehen, sprich woraus das System besteht.

Die Disziplin der modernen Systementwicklung als konkreter Anwendungsbereich der Systemtheorie hat ihren Ausgangspunkt beim Telekommunikationsunternehmen „Bell Laboratories“ in den 1940er Jahren und wurde durch das amerikanische Apollo-Raumfahrtprogramm sukzessive weiterentwickelt [147], [148]. In der Zwischenzeit wurde mit dem „International Council on Systems Engineering“ (INCOSE) eine gemeinnützige Mitgliederorganisation instituiert, um interdisziplinäre Prinzipien und Praktiken für die Entwicklung von Systemen zu gestalten und zu verbreiten [149].

Definition 4.11 Systementwicklung [150].
Die Systementwicklung (engl. Systems Engineering) ist ein logischer Prozess von Aktivitäten, der eine Reihe von Anforderungen, welche sich aus einem bestimmten Ziel bzw. Zweck ergeben, in eine vollständige Beschreibung eines Systems umwandelt, welches das Ziel optimal erfüllt. Dieser Prozess stellt sicher, dass alle Aspekte eines Projekts berücksichtigt und in ein einheitliches Ganzes integriert wurden.

Hierbei hat sich das V-Modell (vgl. Unterabschnitt 3.2.3), u.a. auch aufgrund der ausführlichen und transparenten Integration der in der Automobilbranche intensiv genutzten Testprozeduren, als Quasistandard innerhalb der Automotive-Systementwicklung etabliert [53].

4.2 Fahrzeugdomänen und -systemarchitekturen

Was die Automotive-Systementwicklung angeht, haben sich ausgehend vom traditionellen und Maschinenbau geprägten Vorgehen fachliche Kompetenzbereiche bzw. Fahrzeugdomänen wie Antriebsstrang, Chassis, Karosserie, Infotainment und passive Sicherheit zur Gruppierung der Hauptbestandteile des Systems Kraftfahrzeug gebildet. Die Unterteilung in Domänen spiegelt sich wiederum in den Organisationseinheiten der jeweiligen Entwicklungsabteilungen wider [151], wobei in der Zwischenzeit vermehrt domänenübergreifende (engl. *Cross-Domain {X-Domain}*) zentralisierte Systemverbunde angestrebt werden.

Definition 4.12 Eingebettetes System [152].
Ein eingebettetes System (engl. Embedded System) ist immer fester Bestandteil eines technischen Gesamtsystems, welches vorwiegend aus Rechenhardware, Software und mechanischen bzw. mechatronischen Komponenten besteht. Bezogen auf diesen Sachverhalt interagiert das eingebettete System mit seiner Umgebung mit Hilfe von Sensoren und Aktuatoren und führt dabei Regelungs-, Steuerungs- und Datenverarbeitungsaufgaben aus.

Definition 4.13 Sensor [153].
Ein Sensor ist eine Einrichtung zum Feststellen von physikalischen oder chemischen Eingangsgrößen, die optional eine Messwertzuordnung (Skalierung) der Größen treffen kann, sowie ggf. ein digitales bzw. digitalisierbares Ausgangssignal liefern kann.

Definition 4.14 Steuergerät [154].
Ein Steuergerät (engl. Electronic Control Unit) ist die reale Umsetzung eines eingebetteten Systems. Es repräsentiert die Regeleinheit eines mechatronischen Systems, welches Sensoren und Aktuatoren als Peripherie besitzen kann.

Definition 4.15 Aktuator [155].
Ein Aktuator setzt Signale geringer Leistung, die Stellinformationen beinhalten, in leistungsbehaftete Signale um, die in einer zur Prozessbeeinflussung notwendigen Energieform vorliegen. Aktuatoren repräsentieren die Schnittstelle zwischen elektrischer Signal- bzw. Informationsverarbeitung und dem Prozess bzw. der Regelstrecke im Sinne der Mechanik.

Dementsprechend bestehen Fahrzeuge aus in den Betriebsbereich eingebetteten E/E-Systemen, welche prinzipiell aus Sensoren, Steuergeräten, Aktuatoren sowie der Regelstrecke bzw. des zu regelnden technischen Prozesses zusammengesetzt sind. Hierbei werden auf Grundlage von Führungs- und Rückführgrößen innerhalb des Reglers bzw. Steuergeräts Stellgrößen generiert sowie über Daten- und Kommunikationsschnittstellen (schwarz gepunktete Konnektoren) an die Aktuatoren übermittelt.

Diese beeinflussen über physikalisch mechanische Schnittstellen (orange Konnektoren) die Regelstrecke, welche bis in den Betriebsbereich hinein reicht. Innerhalb dieser wirken einerseits Störgrößen und andererseits werden hier die jeweiligen Ausgangs- bzw. Regelgrößen erzeugt. Diese werden über die jeweiligen Schnittstellen messtechnisch erfasst als auch zurückgeführt und der Regelkreis wird geschlossen (siehe Abbildung 4.3). Eine detaillierte Beschreibung der jeweiligen Schnittstelleneigenschaften ist im Anhang A.1 zu finden.

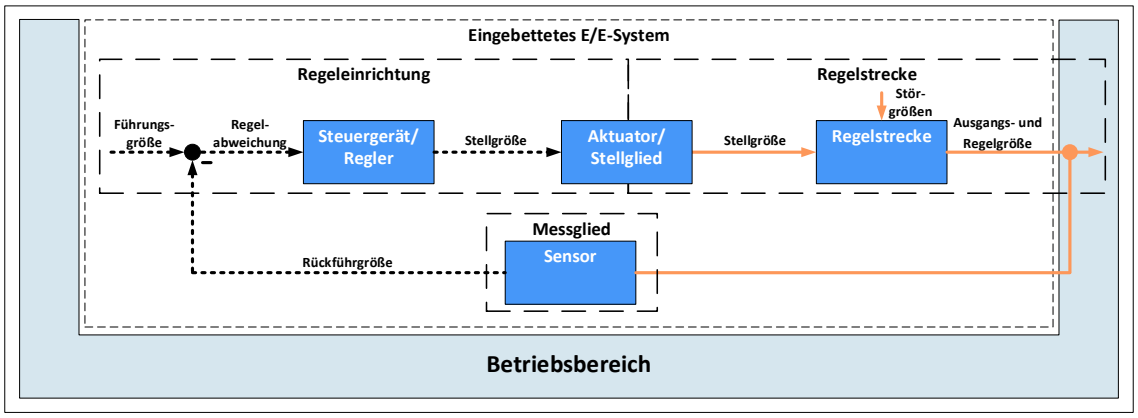


Abbildung 4.3: Sensor, Steuergerät/Regler, Aktuator/Stellglied und Regelstrecke eines in den Betriebsbereich eingebetteten E/E-Systems als geschlossener Regelkreises.

Zudem handelt sich bei den im Fahrzeug eingebetteten E/E-Systemen hauptsächlich um Echtzeitsysteme.

Definition 4.16 Echtzeit [53].
Von „harter Echtzeit" ist die Rede, wenn ein Echtzeitsystem die Einhaltung des Echtzeitkriteriums unter allen Umständen garantiert, bzw. Verstöße detektiert und geeignete Fehlermaßnahmen einleitet. Um „weiche Echtzeit" handelt es sich dagegen, wenn ein System nur in den meisten Fällen das Echtzeitkriterium erfüllt.

Definition 4.17 Echtzeitsystem [53].
Ein Echtzeitsystem verarbeitet seine Eingangs- und Zustandsgrößen innerhalb eines garantierten vorgegebenen Zeitintervalls und erzeugt in diesem Zeitintervall die zugehörigen Ausgangs- und Zustandsgrößen.

Typischerweise greifen diese E/E-Systeme auf signalbasierte und bereits im Entwicklungsprozess starr vorgegebene Informationsflüsse bzw. Botschaften anhand von „Controller Area Network" (CAN), „Local Interconnect Network" (LIN), „FlexRay", „Media Oriented Systems Transport" (MOST) oder „Ethernet" Kommunikationsschnittstellen bzw. Bussysteme zurück. Über Stern-, Bus- oder Ring-Topologien sind die dezentralen und voneinander unabhängigen Kommunikationsnetzwerke quervernetzt [128]. Auch hier spiegelt sich die Strukturierung der Fahrzeugkommunikationsstrukturen an den jeweiligen Domänen wider [151]. In der Zwischenzeit stellen service-orientierte Kommunikationsstrukturen eine Alternative zu den signal-orientierten dar. Diese verwenden ausschließlich Ethernet Kommunikationspfade und basieren nicht mehr auf den gängigen Bustechnologien. Hierbei wird erst zur Laufzeit der Informationsfluss mittels bereitgestellter und genutzter Services zwischen den Softwarekomponenten determiniert. Dadurch soll eine hardwareunabhängigere Implementierung und Aktualisierung der Software erleichtert werden [156]. Darüber hinaus gewinnen Over-the-Air (OTA)-Updates zunehmend an Bedeutung, wobei Updates für Firm- und Software nicht mehr über Datenleitungen, sondern drahtlos erfolgen. Dies kann über verschiedene Funkstandards wie Mobilfunk, WLAN, Bluetooth etc. realisiert werden.

Die Kommunikations- und Interaktionsmöglichkeiten zwischen den unterschiedlichen Steuergeräten als auch deren dynamische Wechselwirkungen führen zu einem hohen Komplexitätsgrad. Hinzu kommen die für den Automobilsektor charakteristischen Komplexitätstreiber der Prozessinnovationen, der Fertigungssysteme sowie der Vielfalt von Kunden, Varianten, Teile und Lieferanten [157].

Definition 4.18 Komplexität [107].
Die Komplexität eines Systems setzt sich aus der Varietät (Anzahl und Ungleichmäßigkeit der Aufteilung einzelnen Elemente), der Konnektivität (Anzahl und Ungleichmäßigkeit der Aufteilung der Relationen), der internen Dynamik des Systems (Anzahl und Arten der möglichen Zustände), den Wechselwirkungen mit der Umgebung sowie den im System enthaltenen Unschärfen zusammen.

Die Unterteilung des Gesamtfahrzeugs in unterschiedliche Domänen ist Gegenstand des sogenannten Architekturparadigmas, das sich innerhalb des Automobilsektors als Säule zur Komplexitätsreduktion von E/E-Systemen etabliert hat. Die Architektur eines Systems repräsentiert dessen Bauplan und versucht die funktionalen, verhaltensbezogenen und strukturellen Systemeigenschaften als Ganzes zu beschreiben [158].

Definition 4.19 Architektur [159].
Eine Architektur stellt grundlegende Konzepte oder Eigenschaften eines Systems, die in dessen internen strukturellen Elementen, Beziehungen oder Prinzipien seines Entwurfs bzw. Entwicklung verankert sind, innerhalb einer bestimmten Umgebung dar.

Das Architekturparadigma ist eng mit dem Systemgedanken (vgl. Abschnitt 4.1) verknüpft und fußt auf dem Prinzip der Trennung von Belangen bzw. Anliegen (*engl. Separation of Concerns*). Bei diesem Prinzip geht es darum, unterschiedliche Facetten eines Problems zu differenzieren und partikulär zu behandeln. Dadurch wird eine arbeitsteilige Bearbeitung entsprechender Fragestellungen der jeweiligen Interessenvertreter eines Systems ermöglicht [160].

Definition 4.20 Systemanliegen bzw. -belang [159].
Ein Systemanliegen bzw. -belang (engl. System Concern) repräsentiert das Interesse an einem System, welches für einen oder mehrere seiner Interessenvertreter relevant ist. Ein Systemanliegen bezieht sich dabei auf jegliche Einwirkung, einschließlich entwicklungsbezogener, technologischer, geschäftlicher, betrieblicher, organisatorischer, politischer, wirtschaftlicher, rechtlicher, regulatorischer, ökologischer und sozialer Einflüsse, auf ein System in dessen Umgebung.

Definition 4.21 Interessenvertreter [159].
Ein Interessenvertreter (engl. Stakeholder) ist eine Einzelperson, ein Team, eine Organisation oder eine Klasse davon, welche in diesem Kontext ein Interesse an einem System haben.

Im Speziellen kann das Prinzip der Trennung von Belangen bzw. Anliegen anhand zweier Dimensionen der Abstraktion praktiziert werden. Die erste Dimension ergibt sich aus dem Prinzip der Dekomposition, welche darauf beruht, die zu betrachtende Gesamtsystemarchitektur im Sinne der Kapselung und Modularisierung in korrelierende Systemarchitekturelemente zu zerlegen (vgl. Abschnitt 4.1). Dieser Vorgang umfasst, je nach Anwendungsfall, mehrere Hierarchie- bzw. Granularitätsebenen. Die zweite Dimension kennzeichnet sich dadurch, relevante Charakteristika bzw. Systemeigenschaften (vgl. Abschnitt 4.1) in Abhängigkeit der spezifischen Perspektive der Interessenvertreter auf ein System bzw. dessen Architektur zu identifizieren und weniger wichtige Details bewusst zu exkludieren [160].

Dies kann anhand mehrerer sich unterscheidender Abstraktionsebenen realisiert werden. Das Prinzip der Trennung von Anliegen ist von Relevanz bei der Konzeption modellbasierter Modellierungs-, Architekturrahmenwerke und -beschreibungssprachen (vgl. Abschnitt 4.6). Nach Broy et al. [161] kann die Fahrzeugsystemarchitektur in eine funktionale, eine logische und eine technische Architektur unterteilt werden (siehe Abbildung 4.4). Innerhalb der funktionalen Architektur wird das zu entwickelt werdende System mittels hierarchisch gegliederter Funktionselemente abgebildet. Diese Funktionen werden ihrerseits innerhalb der logischen Architektur mittels lösungsneutraler logischer Systembausteine implementiert.

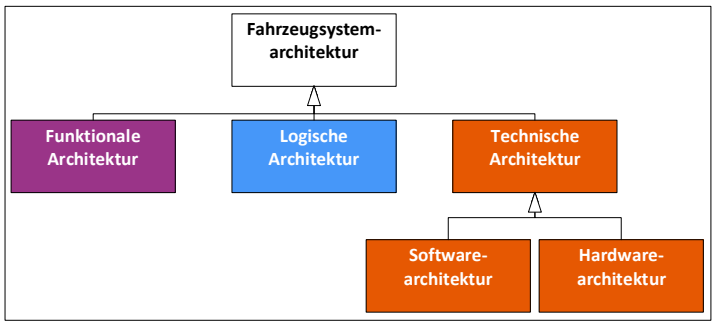


Abbildung 4.4: Fahrzeugsystemarchitekturen anhand von funktionalen, logischen und technischen Architekturen im Kontext der E/E-Entwicklung gemäß Broy et al. [161].

Die technische Architektur repräsentiert schließlich die tatsächlich zu realisierende E/E-Architektur im Sinne der Steuergerätetopologie und das zu implementierende Bussystem und wird weiter anhand der Software- und Hardwarearchitektur konkretisiert. Hierbei stellt die Softwarearchitektur die Strukturierung und Vernetzung der Softwarekomponenten als auch deren Programme und zu verarbeitenden Daten dar. Die Hardwarearchitektur spiegelt die Struktur von Mechanik-, Elektronik- oder anderen Bauteilen wider.

4.3 Modellbasierte Systementwicklung

Die Zunahme der Systemumfänge, die Kooperation unterschiedlicher Entwicklungsabteilungen über Länder- und Kontinentalgrenzen hinweg als auch der steigende Entwicklungsaufwand im Sinne von Kosteneffizienz und immer kürzer werdender Entwicklungszyklen erfordern neue Ansätze innerhalb der Automotive-Systementwicklung [162]. Die modellbasierte Systementwicklung adressiert diese Herausforderungen durch die Verwendung standardisierter Modelle.

Definition 4.22 Modell [163].
Modelle sind [...] Abbildungen, Repräsentationen natürlicher oder künstlicher Originale (Abbildungsmerkmal). Modelle erfassen nicht alle Attribute, [...] nur solche, die [...] relevant scheinen (Verkürzungsmerkmal). Modelle erfüllen ihre Ersatzfunktion für bestimmte Subjekte innerhalb bestimmter Zeitintervalle und unter Einschränkung auf bestimmte gedankliche oder tatsächliche Operationen (pragmatisches Merkmal).

Im Kontext der modellbasierten Systementwicklung können die Modellierungen nach deren Formalisierungsgrad und -art, deren Abstraktionsgrad als auch deren Einsatzgebiet differenziert werden. Des Weiteren lassen sich diese in formale Modelle, welche das erwartete Systemverhalten beschreiben, in konzeptuelle Modelle für Kommunikations- und Dokumentationszwecke, sowie in konstruktive Modelle, welche das betriebsbedingte Verhalten in den Mittelpunkt stellen, separieren [164]. Hierbei unterstützt die modellbasierte Systementwicklung sämtliche Phasen der Automotive-Systementwicklung, angefangen bei der Anforderungsentwicklung über den Entwurf der Systemarchitekturen bis hin zur Verifikation, Validierung als auch den Testaktivitäten.

Definition 4.23 Modellbasierte Systementwicklung [165].
Die modellbasierte Systementwicklung (engl. Model-Based Systems Engineering) ist die formalisierte Anwendung von Modellbildung zur Unterstützung der Aktivitäten der Anforderungsdefinition, des Systemdesigns und der Systemanalyse sowie dessen Verifikation und Validierung, beginnend beim konzeptionellen Entwurf sowie über die Entwicklung und weitere Lebenszyklusphasen hinweg.

Der Fokus liegt auf der Schaffung eines digitalen Datenbestands, welcher alle relevanten Informationen des Systementwurfs beinhaltet und diese als alleinstehende Informationsquelle (engl. *Single Source of Truth*) miteinander in Beziehung setzt [166]. Dies erfolgt durch die frühzeitige Generierung eines Systemmodells als Referenz für die spezifischeren Modelle der jeweiligen Entwicklungsdisziplinen, welches dann als interdisziplinäre Kommunikationsbasis zwischen den Stakeholdern dient und systembezogene Informationen vermittelt [162].

Insgesamt ergeben sich bei den modellbasierten Ansätzen im Vergleich zu den dokumentenbasierten Vorteile wie die einfachere Beherrschung von großen Systemumfängen, eine verbesserte Spezifikation, Kommunikation und Kollaboration zwischen den Entwicklungsabteilungen, eine höhere Entwicklungsgenauigkeit, Qualität und Produktivität, eine stärkere Risikominimierung mittels durchgängiger

Nachverfolgbarkeit sowie eine praktikablere Möglichkeit der Wiederverwendung von im Entwicklungsprozess aggregiertem Wissen [167]. Allerdings ist die modellbasierte Systementwicklung auch mit Aufwänden und Hürden verbunden. Für eine nutzbringende Realisierung sind eindeutig festgelegte Prozesse, Methoden, Werkzeuge als auch eine darauf ausgerichtete Organisation einschließlich der Entwicklungsteams unabdingbar [162]. Daraus leiten sich für eine erfolgreiche modellbasierte Umsetzung die notwendigen Säulen Prozess bzw. Vorgehensmodell (vgl. Abschnitt 3.2), Modellierungsmethode, Modellierungssprache und Modellierungswerkzeug im Sinne von Prozesse, Methoden und Tools (PMT) ab (siehe Abbildung 4.5) [168].

Definition 4.24 Modellierungsmethode bzw. -rahmenwerk [169], [170].
Eine Modellierungsmethode bzw. -rahmenwerk ist ein Verfahren zur systematischen Erkenntnisgewinnung und -darstellung anhand von Modellen. Dabei gibt die Modellierungsmethode durch eine Sammlung von Regeln sowie Anweisungen die Art und Weise als auch die Abfolge der Aktivitäten vor, welche zur Erstellung der einzelnen Modelle durchzuführen sind. Demzufolge beinhaltet eine Modellierungsmethode die benötigten Techniken, um die definierten Aktivitäten durchführen zu können.

Definition 4.25 Modellierungssprache [171].
Die Modellierungssprache ist ein künstliches Regelwerk, das aus einzelnen Elementen fest vorgeschriebener Bedeutung (Semantik) und Regeln zu ihrer Verknüpfung untereinander (Syntax) besteht. Modellierungssprachen werden zur Beschreibung von Modellen (definiert als Vor- oder Abbild eines Originals) mit dem Hauptzweck der eindeutigen Interpretierbarkeit des beschriebenen Inhalts eingesetzt.

Definition 4.26 Modellierungswerkzeug [170].
Ein Modellierungswerkzeug ist ein Instrument, welches auf eine bestimmte Modellierungsmethode und/oder -sprache angewandt wird. Die meisten Werkzeuge, die zur Unterstützung der modellbasierten Systementwicklung eingesetzt werden, sind computer- oder softwarebasiert, welche auch als rechnergestützte Entwicklungswerkzeuge (engl. Computer-Aided Engineering {CAE} Tools) bezeichnet werden.

Die Modellierungsmethoden bzw. -rahmenwerke kennzeichnen sich durch die Vorgabe eines systematischen Vorgehens und spezifischen Handlungsempfehlungen für den Entwickler sowie der im Modell abzubildenden Merkmale des Systems, Subsystems oder der Komponente. Modellierungssprachen beinhalten eine bestimmte Semantik und Syntax und stellen auf Basis der Modellierungsmethode den formalen Rahmen der Modellierung dar. Hierbei kann die Modellierungsmethode bzw. -rahmenwerk die Freiheitsgrade der Modellierungssprache zweckgemäß einschränken. Mit Hilfe rechnergestützter Modellierungswerkzeuge erfolgt unter Berücksichtigung der Semantik und Syntax der Modellierungssprache die Generierung der Modelle [172], [173].

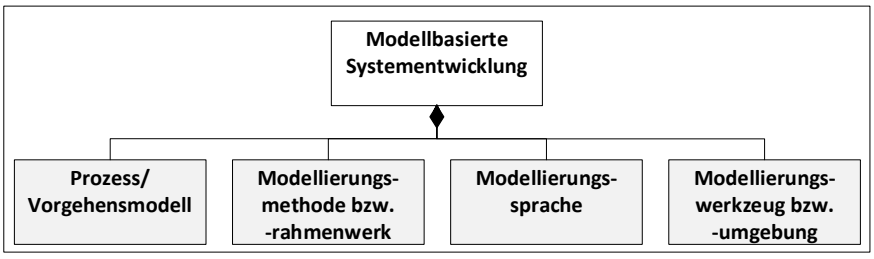


Abbildung 4.5: Säulen der modellbasierten Systementwicklung

4.4 Klassifikation von Modellen im Kontext der modellbasierten Systementwicklung

Eine Klassifikation bzw. Taxonomie entsprechender Modelle im Kontext der modellbasierten Systementwicklung liefert ebenfalls der IEEE-Standard 24641 [174]. Hierbei werden virtuelle bzw. innerhalb von computergestützten Entwicklungsumgebungen zu generierende Modelle und Artefakte in beschreibende sowie analytische Modelle unterteilt (siehe Abbildung 4.6).

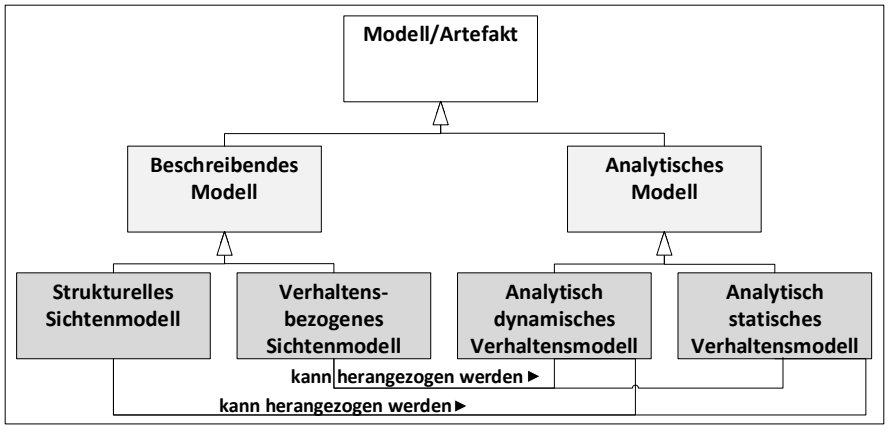


Abbildung 4.6: Klassifikation und Generalisierung von Modellen bzw. Artefakten gemäß der IEEE 24641 [174] mit zusätzlicher Erweiterung der analytischen Modelle in Richtung von analytisch dynamischen als auch analytisch statischen Verhaltensmodellen dargestellt durch Assoziationen.

Strukturelle und verhaltensbezogene Sichtenmodelle, darunter fallen beispielsweise Block-, Anwendungsfall-, Zustands-, Sequenz- sowie Aktivitätsdiagramme (vgl. Abschnitt 4.5), haben die primäre Zielsetzung, die wesentlichen Systemaspekte, einschließlich der Funktion, des Verhaltens, der Struktur und ggf. Parameter und Anforderungen, darzustellen. Dahingegen nutzen analytische Modelle beispielsweise gewöhnliche mathematische Differentialgleichungen (engl. *Ordinary Differential Equations {ODEs}*), um eine simulative bzw. quantifizierbare Analyse entsprechender Systemaspekte und -merkmale zu ermöglichen [174].

An dieser Stelle ist hervorzuheben, dass in Abhängigkeit des jeweils eingesetzten Modellierungswerkzeugs, die strukturellen und verhaltensbezogenen Sichtenmodelle auch im Sinne von statisch als auch dynamisch analytischen Verhaltensmodellen herangezogen werden können. Exemplarisch sei hier auf die Mathworks Entwicklungsumgebungen Simulink [175], Stateflow [176] und System Composer [177] verwiesen, worin Aktivitäts-, Zustands- sowie Sequenzdiagramme mittels ODEs hinterlegt werden, um statische oder aber auch dynamische Zusammenhänge simulieren zu können. Dasselbe gilt auch für die jeweiligen Strukturmodelle, welche um simulative ausführbare bzw. analytische Architekturmetriken, z.B. zur Bewertung von Scheduling- und Timingaspekten, Ressourcenverbrauch, Kosten, Bauraum usw., erweitert werden können. Dieser Sachverhalt ist innerhalb der IEEE 24641 [174] nicht berücksichtigt und wird hier durch Erweiterung der analytischen Modelle in Richtung von analytisch dynamischen als auch analytisch statischen Verhaltensmodellen sowie mit Hilfe von Assoziationen kenntlich gemacht (siehe Abbildung 4.6).

Insgesamt werden dadurch drei Architekturmodelltypen bzw. -sichten generiert, eine funktionale Architektur (F), eine logische (L) als auch eine technische Architektur (T), welche sowohl aufeinander als auch auf jeweils sichtenspezifische Verhaltensaspekte (FB, LB, TB) bezogen und allokiert werden. Die funktionalen, logischen und technischen Architekturmodelle gehören dabei zu den strukturellen Sichtenmodellen, wohingegen sich die funktional, logisch und technisch spezifischen Verhaltensmodelle je nach Ausprägung und Analysegegenstand einerseits als verhaltensbezogene Sichtenmodelle und/oder als analytisch statische bzw. dynamische Verhaltensmodelle erweisen können (siehe Abbildung 4.7).

Zusammen mit einer integrierten Verhaltensmodellierung lassen sich daraus ausführbare Architekturen unterschiedlichen Konkretisierungsgrads entwerfen. Hierbei wird eine Trennung zwischen dem funktional spezifischen Verhaltensmodell (FB) sowie dem logisch (LB) und/oder technisch spezifischen Verhaltensmodell (TB), welche jeweils das zu untersuchende Verhalten konkretisieren, vorgenommen. Simulativ ausführbare Verhaltensmodelle kommen entweder zum Einsatz, bevor die realen Systeme zur Verfügung stehen oder neue Funktionen in eine bereits existierende Architektur integriert werden sollen. Grundsätzlich liegt die Zielsetzung der dynamisch analytischen Verhaltensmodelle darin, durch simulative Ausführung und Stimulierung der Modelle über den Zeitverlauf, das dynamische Verhalten der realen Systemarchitektur nachzubilden.

Definition 4.27 Simulation [178], [179].
Simulation (lt. simulare = dt. vortäuschen) bezeichnet einen Sammelbegriff für die Darstellung oder Nachbildung physikalisch technischer Prozesse oder Systeme durch mathematisch physikalische Modelle. Die Modelle erlauben Rückschlüsse auf die Eigenschaften des realen Systems.

Simulations- bzw. numerische Berechnungsmodelle beruhen auf einheitlichen mathematischen Beschreibungen, wodurch das zeitliche Verhalten von Systemen und Architekturen, wie z.B. technische Systeme aus den Bereichen Elektrotechnik, Maschinenbau und Verfahrenstechnik, aber auch nicht-technischen Systemen wie Biologie, Medizin, Chemie, Physik, Wirtschaft etc. greifbar gemacht werden kann. Dies setzt jedoch voraus, dass die mathematischen Beziehungen für das statische und dynamische Verhalten der Systeme, Subsysteme und/oder ihrer Komponenten bekannt sind. Andernfalls stehen zwei generelle Ansätze für eine Herleitung eines Modells, namentlich die theoretische und die experimentelle Modellierung, zur Verfügung. Bei der theoretischen Modellierung wird das Modell durch Anwendung von Methoden aus der Infinitesimalrechnung auf Gleichungen, wie sie z.B. aus der Physik abgeleitet werden, gewonnen. Dabei werden vereinfachende Annahmen über das System und/oder den Prozess getroffen, da nur so eine mathematische Betrachtung realisiert werden kann.

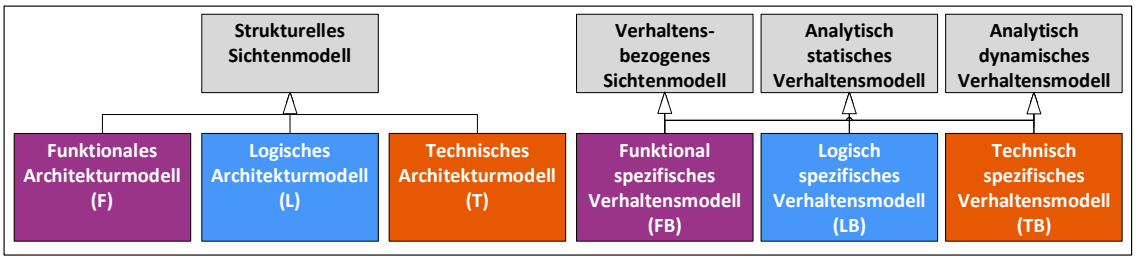


Abbildung 4.7: Hierarchische Konkretisierung und über Generalisierungen hergestellter Zusammenhang der funktionalen (F), logischen (L) und technischen Architekturmodellen (T) als auch funktional (FB), logisch (LB) und technisch spezifischer Verhaltensmodelle (TB).

Im Zuge dessen werden lineare Gleichgewichtsbedingungen (Masse, Energie, Impuls), physikalische oder chemische Zustandsgleichungen (reversible nichtlineare Vorgänge wie z.B. Induktion, phänomenologische Gleichungen (irreversible und in einem weiten Bereich lineare Vorgänge wie Reibung und Wärmeübertragung) sowie Kopplungsgleichungen (beispielsweise Drehmomentbilanzen) anhand von ODEs miteinander verknüpft.

$$\dot{\boldsymbol{x}}(t) = f(\boldsymbol{x}(t), \boldsymbol{u}(t), t) \tag{4.1}$$

$$\boldsymbol{y}(t) = \boldsymbol{x}(t) \tag{4.2}$$

Hierbei repräsentiert $\boldsymbol{x}(t)$ den Vektor der zu differenzierenden Variablen und somit den Zustandsvektor, $\boldsymbol{y}(t)$ ist der Ausgangsvektor, $\boldsymbol{u}(t)$ stellt den Eingangsvektor dar, t beschreibt die unabhängige skalare Zeitvariable und $\dot{\boldsymbol{x}}(t)$ den Vektor der Ableitungen nach der Zeit t als Funktion von $\boldsymbol{x}$ und $\boldsymbol{u}$. Dementsprechend enthalten theoretische Modelle die funktionalen Abhängigkeiten zwischen den physikalischen Eigenschaften eines Systems und dessen Parametern. Daher werden diese Modelle typischerweise bevorzugt, wenn das zu entwickelt werdende System bereits in der Entwurfsphase in seinem analytisch dynamischen Verhalten simuliert und optimiert werden soll. Allerdings kann die theoretische Modellbildung bereits für einfache Systeme mit hohem Aufwand verbunden sein, da die abgeleiteten Modellkoeffizienten nicht präzise genug und nicht alle im System ablaufenden Vorgänge bekannt sind bzw. nicht mit der erforderlichen Genauigkeit mathematisch beschrieben werden können. Dieser Umstand motiviert den Einsatz experimenteller Analysen bzw. Systemidentifikationen. Im Rahmen dessen gibt der jeweilige Anwendungsbereich und Einsatzzweck die erforderliche Modellgenauigkeit und damit den Aufwand, der für die Analyse betrieben werden muss, vor [180].

Der Simulationsvorgang selbst wird durch computergestützte Werkzeuge verwirklicht und ermöglicht die dynamische Verifikation und Validierung der jeweiligen im Fokus stehenden System- bzw. Architekturmerkmale. Hierunter fallen u.a. Entwicklungsumgebungen wie Modelica [181], MATLAB Simscape Power Systems [182] zur Modellierung und Simulation von physikalischen Systemen, MATLAB Simulink [175] für die Entwicklung, Simulation und Code-Generierung regelungstechnischer Systeme, LabVIEW von National Instruments für den Entwurf von Messtechnik-Systemen, SPICE für die Simulation analoger und/oder digitaler elektrischer Schaltungen oder die Modellierung und Simulation von Kommunikationsnetzwerken, exemplarisch sei hier auf OMNeT++ [183] verwiesen. Die simulativ ausführbaren Modelle werden innerhalb der jeweiligen Simulationswerkzeuge mittels einer definierten Modellierungssprache erstellt und basieren auf dem Modellgrundsatz (vgl. Abschnitt 4.3) einer spezifischen Syntax (Notation des Modells), Semantik (Bedeutung und Funktionalität des Modells) als auch Pragmatik (Art und Weise der Anwendung, Editierung und Analyse des Modells) (vgl. Abschnitt 4.5).

4.5 Modellierungssprachen im Kontext der modellgetriebenen Entwicklung

Im Umfeld der modellgetriebenen Systementwicklung wird durch den „Object Management Group“ (OMG[4]) Standard „Meta-Object Facility“ (MOF) [184] vorgegeben, wie Modellierungssprachen anhand ihrer abstrakten und konkreten Syntax[5] als auch statischen und dynamischen Semantik[6] unter Berücksichtigung von Metamodellen[7] zu definieren sind.

Die Metamodellelemente der MOF basieren auf der „Unified Modeling Language“ (UML), welche in den 1990er Jahren für die konsistente Beschreibung von Softwaresystemen entwickelt wurde. Diese ist durch die „OMG UML“ [188] als auch durch die ISO 19501 [189] international standardisiert. Ferner gilt die UML als Basis objektorientierter Modellierungssprachen. Bekanntester Vertreter ist hierbei die „Systems Modeling Language“ (SysML), welche ausgehend von der UML gemeinschaftlich durch INCOSE sowie OMG als Standardsprache für die Systementwicklung konzipiert wurde und in der „OMG SysML“ [187] standardisiert ist (siehe Abbildung 4.8). Die Zielsetzung der SysML liegt zum einen in der Konsolidierung der Sprache der Systemingenieure für eine konsistentere und verbesserte Kommunikation der multidisziplinären Entwicklungsteams. Zum anderen sollen durch die formalisierte grafische Beschreibung von systemübergreifenden Eigenschaften Arbeitsprodukte wie Code, Testfälle oder Dokumentationen (teil-)automatisiert generiert werden können. Die SysML ist kompatibel zur MOF und unterstützt sämtliche Phasen der Produktentwicklung von Systemen und Subsystemen, angefangen bei der Spezifikation, über den Entwurf, die Analyse, die Verifikation bis hin zur Validierung.

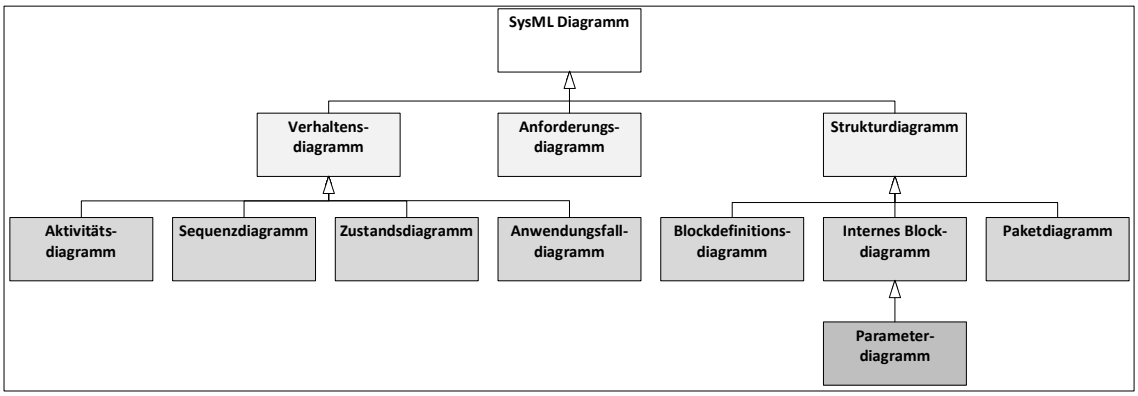


Abbildung 4.8: Diagrammarten der SysML gruppiert nach Verhaltens- und Strukturdiagrammen, wobei das Anforderungsdiagramm eine eigenständige Kategorie einnimmt (in Anlehnung an [187]).

[4] OMG ist ein offenes, gemeinnütziges Standardkonsortium in der Computerbranche.

[5] Durch die Syntax werden die Regeln für die Kombination von Elementen wie Wörter, Zeichen und Symbole einer Modellierungssprache definiert. In diesem Zusammenhang widerspiegelt die abstrakte Syntax die strukturellen Relationen der Sprachelemente zueinander. Anhand der konkreten Syntax wird vorgegeben, wie diese Sprachelemente textuell oder grafisch darzustellen sind [185].

[6] Durch die Semantik einer Modellierungssprache wird die Bedeutung der Syntax dargelegt. Mittels der statischen Semantik wird ein Rahmen für die Charakteristika und Assoziationen zwischen den jeweiligen Modellelementen spezifiziert [165]. Mit Hilfe der dynamischen Semantik wird die abstrakte Syntax auf ein mathematisches oder ausführbares Modell projiziert [186].

[7] Durch ein Metamodell wird die abstrakte Syntax eines Modells illustriert [185].

Dabei können diese Systeme Bereiche der Hardware und der Software sowie Informationen, Prozesse, Personal, Anlagen als auch Einrichtungen umfassen [187]. Hierfür werden dem Anwender neun Diagrammarten zur Modellierung von Systemaspekten wie Struktur, Verhalten und Anforderungen zur Verfügung gestellt (siehe Abbildung 4.8). Eine detaillierte Beschreibung der jeweiligen Diagrammarten und deren Modellartefakte ist in [187] und [190] zu finden.

4.6 Modellierungs- und Architekturrahmenwerke

Sowohl für die Entwicklung eingebetteter Systeme sowie E/E-Architekturen einschließlich Software- und Regelungskomponenten wird innerhalb des Automobilsektors vermehrt von modellbasierten Ansätzen Gebrauch gemacht. Dieser Trend lässt sich auf das kontinuierliche Ansteigen der Anzahl an Systemfunktionen, deren Partitionierung auf verschiedene Steuergeräte und die dadurch einhergehende Zunahme der Vernetzung ehemals separat entworfener Systemkomponenten zurückführen [191]. Verstärkt wird dieser Effekt durch eine wachsende Anzahl an Varianten und Konfigurationen der jeweiligen Baureihen (vgl. Abschnitt 4.2). In diesem Zusammenhang kommt für die Architekturbeschreibung (engl. *Architecture Description*) über den gesamten Produkt- bzw. Systemlebenszyklus die Vorgehensweise der modellgetriebenen Architektur zum Tragen, wobei diese auf den IEEE-Standards 42010 „Systems and software engineering - Architecture description“ [159] sowie IEEE 24641 „Systems and Software engineering - Methods and tools for model-based systems and software engineering“ [174] basiert.

Eine wesentliche Rolle spielen sogenannte Modellierungs- bzw. Architekturrahmenwerke im Sinne einer Modellierungsmethode (vgl. Abschnitt 4.3). Das Ganze erfolgt im Zusammenspiel mit einer Modellierungssprache (siehe Abbildung 4.9) und/oder ggf. einer Architekturbeschreibungssprache (engl. *Architecture Description Language {ADL}*) als domänenspezifischer Ableger (engl. *Domain Specific Language {DSL}*). Eine domänenspezifische Sprache ist explizit auf die Notwendigkeiten einer bestimmten Fachdisziplin zugeschnitten und erweitert oder beschränkt je nach Anwendungsfall, z.B. durch das Herausnehmen nicht benötigter Elemente wie Diagrammarten, Entitäten oder Beziehungen, eine generische Modellierungssprache.

Der Entwicklungsprozess eingebetteter Systeme und E/E-Architekturen charakterisiert sich durch Interessenvertreter[8] mit unterschiedlichen Systemanliegen bzw. -belangen[9]. Ein Modellierungsrahmenwerk basiert auf dem Prinzip der Trennung dieser Belange aus dem Blickwinkel einer interessenvertreterspezifischen Perspektive (vgl. Abschnitt 4.2). Hierbei wird z.B. die Funktionsweise eines Systems von den Implementierungsdetails, sprich in welcherlei Art und Weise jenes System die Fähigkeiten seiner Plattform nutzt, separiert.

Definition 4.28 Modellierungsrahmenwerk [159], [174].
Ein Modellierungsrahmenwerk (engl. Modeling Framework) agiert als Modellierungsmethode und legt eine gemeinsame Vorgehensweise für die Erstellung, Interpretation, Analyse und Verwendung von modellbasierten Beschreibungen und Artefakten innerhalb eines bestimmten Anwendungsbereichs oder einer Interessenvertretergruppierung fest.

Das Modellierungsrahmenwerk enthält eine oder mehrere Sichtweisen, welche einen Rahmen für die interessenvertreterspezifischen Belange bzw. Anliegen bieten und als Konstrukt für die Generierung und

[8] Interessenvertreter (vgl. Definition 4.21).
[9] Systemanliegen (vgl. Definition 4.20).

Verwaltung der verschiedenen Modellartefakte während des Entwicklungsprozesses dienen (siehe Abbildung 4.9) [159].

Definition 4.29 Sichtweise [159], [174].
Eine Sichtweise (engl. Viewpoint) ist das Arbeitsergebnis, welches die Konventionen für den Aufbau, die Interpretation und die Verwendung von Sichten bezüglich Architekturmodellen und sonstigen entwicklungsbezogenen Artefakten (Anforderungen, Testfälle etc.) festlegt, um interessenvertreterspezifischen System Belangen bzw. Anliegen einen Rahmen zu geben.

Die Sichtweisen legen Regeln für die Art und Weise, den Aufbau als auch die Erstellung von Modellen und Artefakten fest, seien diese Architekturmodelle oder Artefakte im Hinblick auf Anforderungen, Testfälle usw., und regulieren eine oder mehrere Sichten. Somit kann eine Sichtweise als ein Schema für die Konzeptionierung interessenvertreterspezifischer Sichten auf ein System als auch dessen Umgebung bezeichnet werden. Sichtweisen werden in Bezug auf ihre Syntax, Semantik und Pragmatik spezifiziert. Dabei handelt es sich u.a. um den Namen der Sichtweise, die adressierten Interessenvertreter Belange sowie Techniken, die während des Entwurfs und der Analyse einer Sicht eingesetzt werden können. Ausgehend von einer Sichtweisenspezifikation kann dann eine Sicht als ein konkretes Modell des Systems charakterisiert werden (siehe Abbildung 4.9). Die Sichten, z.B. Architekturentwurfs- oder Anforderungssicht, bilden die für die Belange bzw. Anliegen relevanten Informationen unter Verwendung der konzeptionellen Struktur der zugrundeliegenden Modell- und Artefaktarten bzw. Klassifikationen einer Modellierungs- oder Architekturbeschreibungssprache ab [159].

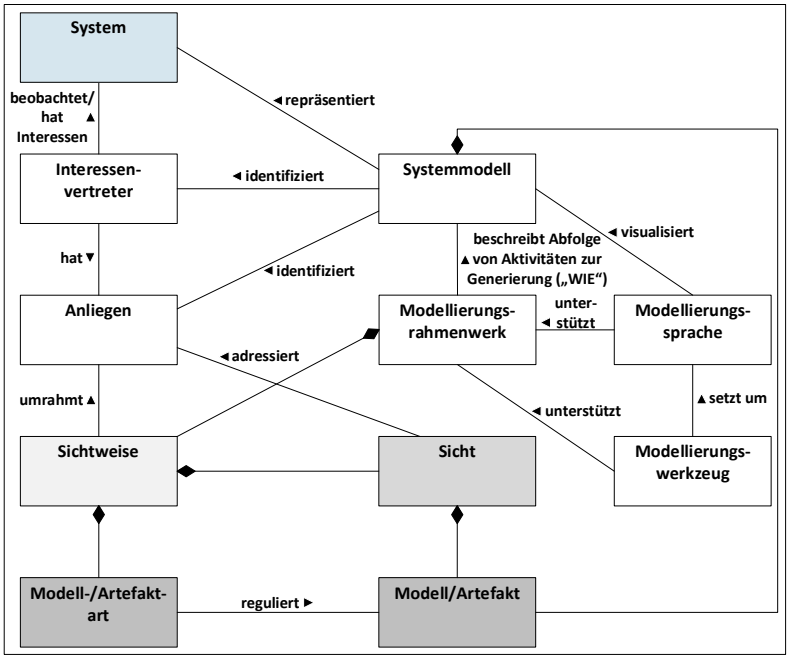


Abbildung 4.9: Systematik im Hinblick auf Modellierungsrahmenwerk, -sprache und -werkzeug sowie Assoziationen bezüglich System, Interessenvertreter, Anliegen etc. (in Anlehnung an [159] und [174]) unter zusätzlicher Darstellung des Systemmodellkonstrukts.

Definition 4.30 Sicht [159], [174].
Eine Sicht (engl. View) ist das Arbeitsprodukt, welches die Architektur und/oder Anforderungen eines Systems aus der Perspektive eines bestimmten System Belangs bzw. Anliegens anhand eines oder mehrerer Modelle bzw. Artefakte ausdrückt.

Hinzu kommt das Konstrukt sogenannter Systemmodelle, welche in Datenbanken abgelegt und verwaltet werden. Hierbei beschreibt das Modellierungsrahmenwerk die Abfolge von Aktivitäten zur Generierung eines oder mehrerer Systemmodelle (siehe Abbildung 4.9). Diese repräsentieren wiederum ein System, werden durch eine Modellierungssprache visualisiert und identifizieren die Interessenvertreter einschließlich deren Anliegen. Des Weiteren umfassen Systemmodelle die generierten Modelle bzw. Artefakte, um Planung, Anforderungen, Architekturentwurf, Analyse, Verifikation und Validierung zu unterstützen. Beim Systemmodellkonstrukt handelt es sich genauer genommen um die Darstellung eines Systems mittels unterschiedlicher Ausprägungen der jeweiligen Formalismen, welche als eine Kombination der jeweiligen Modell- bzw. Artefaktarten visualisiert werden (siehe Abbildung 4.9).

Innerhalb des Automobilbereichs haben sich unterschiedliche Modellierungs- bzw. Architekturrahmenwerke und -beschreibungssprachen für die Entwicklung von eingebetteten Systemen sowie E/E-Architekturen etabliert. Hierunter fällt u.a. das „Software Platform Embedded Systems (SPES) 2020 Modeling Framework" [192] für die Entwicklung eingebetteter Systeme innerhalb der Dömanen Automatisierungstechnik, Automotive, Avionik sowie Energie- und Medizintechnik. Das SPES-Modellierungsrahmenwerk verwendet Sichtweisen und Granularitäts- bzw. Hierarchieebenen als Kernkonzepte. Dadurch soll ein zweidimensionaler Entwicklungsraum geschaffen werden (siehe Abbildung 4.10). Dieser besteht zum einen aus vier verschiedenen Sichtweisen auf der horizontalen Achse. Diese sind die „Anforderungssichtweise" (engl. *Requirements Viewpoint {Req-VP}*), die „Funktionssichtweise" (engl. *Functional Viewpoint {F-VP}*), die „logische Sichtweise" (engl. *Logical Viewpoint {L-VP}*) und die „technische Sichtweise" (engl. *Technical Viewpoint {T-VP}*). Zum anderen erfolgt die Dekomposition des Systems durch die definierten Granularitätsstufen (engl. *Granularity Layer*) auf der vertikalen Achse. Die Level Variable L_n repräsentiert die unterschiedlichen Granularitätsebenen bzw. den jeweiligen Dekompositionsgrad im Sinne der hierarchischen Zerlegung der Sichtweisen (Req-VP, F-VP, L-VP, T-VP) anhand von fünf hierarchisch nummerierten Schichten $L_{1...5}$.

Der Entwicklungsprozess wird mit der Definition lösungsneutraler Anforderungen begonnen. Während des gesamten Prozesses werden die Anforderungen über die verschiedenen Sichtweisen und Granularitätsebenen mehr und mehr zu einer konkreten technischen Umsetzung weiterentwickelt. Dies geschieht so lange, bis die technische Spezifikation auf Komponentenebene erfolgen kann [192]. Dahingehend ergibt sich ein bidirektionaler zickzackförmiger Top-Down- bzw. Bottom-Up-Entwicklungsablauf, welcher im Sinne des Tailoring projektabhängig angepasst und unterschiedlich durchlaufen werden kann (angedeutet durch blauen respektive olivgrünen Entwicklungspfad und gelb hervorgehobenen Matrixelementen). Dabei können Sichtweisen ausgelassen oder erst auf tiefer gelegenen Granularitätsebenen durchschritten werden (siehe Abbildung 4.10).

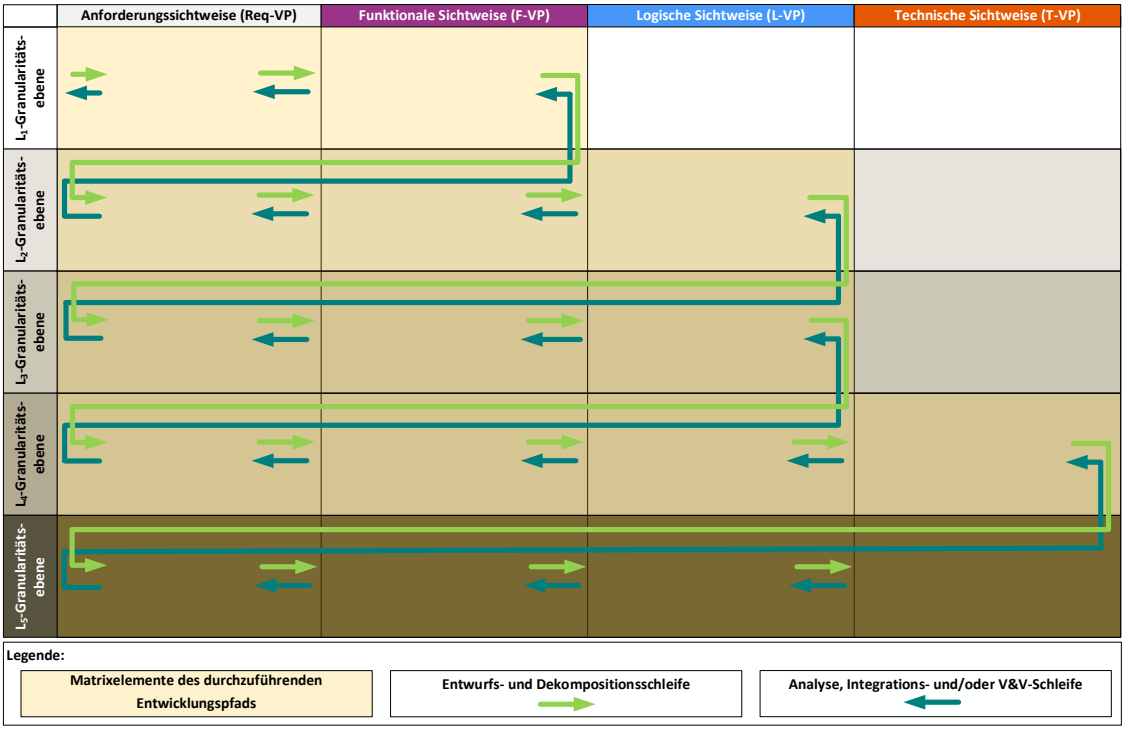


Abbildung 4.10: Matrix des SPES-Modellierungsrahmenwerks gemäß [193].

Die vier Sichtweisen des SPES-Modellierungsrahmenwerks werden im Folgenden näher dargelegt:

- **Anforderungssichtweise (Req-VP):** Im Zuge der Anforderungssichtweise wird der Problemraum sowie das eigentliche Entwicklungsvorhaben systematisch strukturiert. Hierbei werden Stakeholder wie z.B. Anwender, Kunden, Anforderungsmanager und Tester adressiert (**„L_n-A Erfasse Spezifikationen“** siehe Abbildung 4.11). Die Modellierung selbst umfasst dabei die Abgrenzung des Systems und die Darstellung des Systemkontexts. Bezogen auf diesen Sachverhalt werden externe Schnittstellen, je nach Granularitätsstufe, zu benachbarten Systemen, Subsystemen oder Komponenten visualisiert. Außerdem werden auf Basis der Kontextmodelle die Zielmodelle erstellt. Ziele stellen eine Absicht in Bezug auf die Zielsetzung, Eigenschaften oder Verwendung des Systems dar. Des Weiteren werden Szenarien definiert, um mögliche Wege zur Erfüllung der gesteckten Ziele aufzuzeigen. Genau genommen stellen Szenarien das System und dessen Interaktion mit entsprechenden Akteuren dar. Ferner werden lösungsorientierte Anforderungen in Form von funktionalen, strukturellen und verhaltensbezogenen Modellen generiert (**„L_n-B Generiere Wissens- und Betriebskontextmodelle“** siehe Abbildung 4.11). Die Anforderungssichtweise wird darüber hinaus durch Kontextanalysen sowie Verifikations- und Validierungsaktivitäten begleitet (**„L_n-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch“** siehe Abbildung 4.11) [192], [193].

- **Funktionale Sichtweise (F-VP):** Ausgangspunkt für die funktionale Sichtweise sind die in der Anforderungssichtweise erzeugten funktionalen Modelle. Das Hauptanliegen der funktionalen Sichtweise liegt in der Bereitstellung einer formalen und modellbasierten Funktionsspezifikation des Systems (**„L_n-D. Entwerfe funktionale Architektur“** siehe Abbildung 4.11).

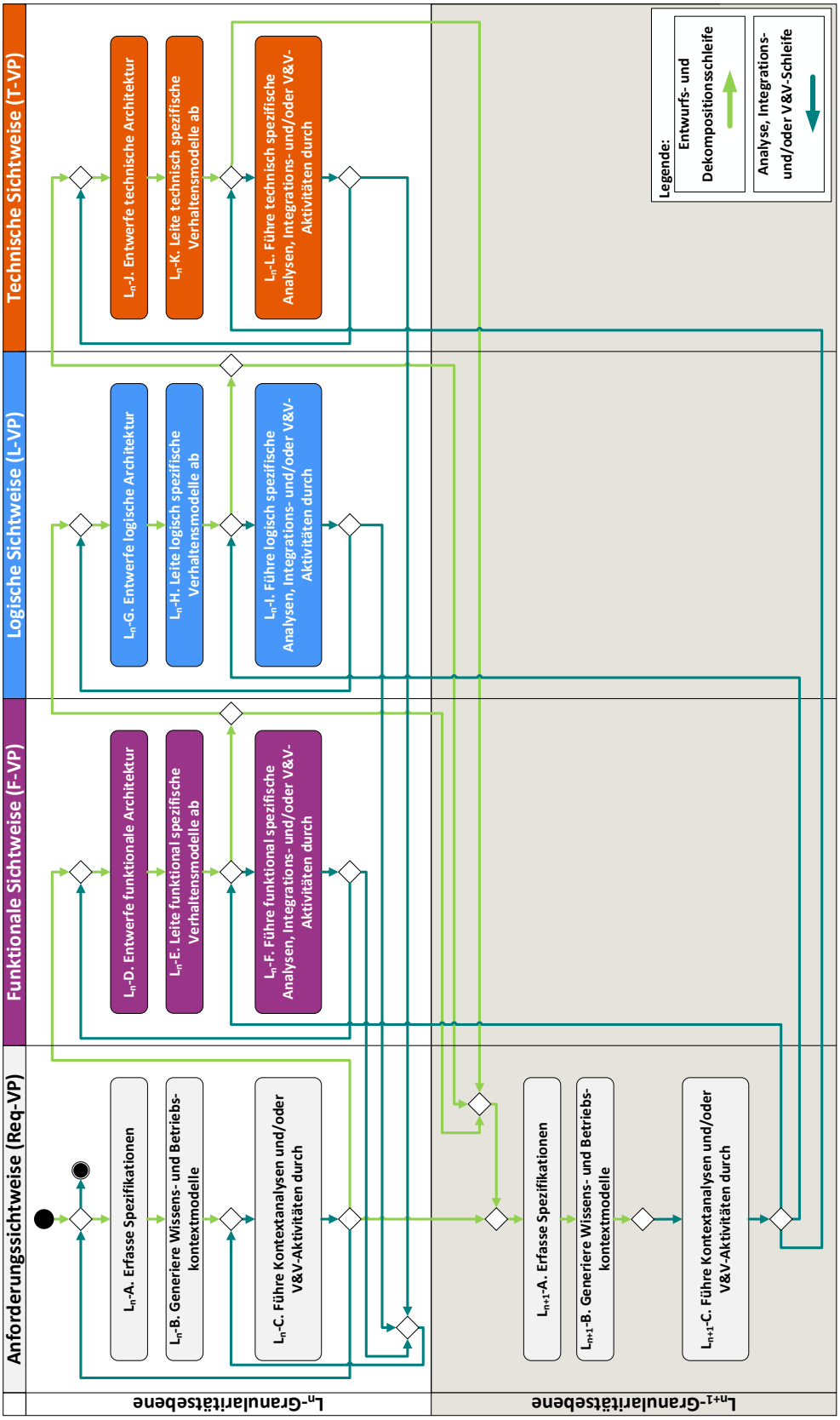


Abbildung 4.11: Detaillierter Aktivitätsablauf des SPES-Modellierungsrahmenwerks über zwei Granularitätsebenen hinweg.

Hierfür werden zwei unterschiedliche Modelltypen für die Strukturierung sowie für die abstrakte Realisierung der funktionalen Anforderungen verwendet. Dabei erfasst eine sogenannte „Nutzerfunktion“ (engl. *User Function*) eine Reihe von lösungsorientierten Anforderungen, welche in den Modellen der Anforderungssichtweise spezifiziert wurden, und integriert diese in ein funktionales Black-Box-Modell, sprich eine funktionale Beschreibung des gesamten Systems. Anschließend werden die Nutzerfunktionen durch ein funktionales White-Box-Modell verfeinert. Das White-Box-Modell bietet eine abstrakte Realisierung der Nutzerfunktion durch Zerlegung in kleinere Funktionseinheiten bzw. sogenannte „Systemfunktionen“ (engl. *System Functions*) und repräsentiert die funktionale Architektur des Systems. Hinzu kommt die Beschreibung des funktional spezifischen Verhaltens (**„L_n-E. Leite funktional spezifische Verhaltensmodelle ab“** siehe Abbildung 4.11). Die funktionale Sichtweise wird wiederum durch funktional spezifische Analysen sowie Integrations-, Verifikations- und Validierungsaktivitäten abgeschlossen (**„L_n-F. Führe funktional spezifische Analysen, Integrations- und/oder V&V-Aktivitäten durch“** siehe Abbildung 4.11) [192], [193].

- **Logische Sichtweise (L-VP):** Hauptaufgabe in der logischen Sichtweise ist die Verteilung der Funktionen aus der funktionalen Sichtweise auf eine hierarchisch strukturierte Architektur logischer Subsysteme und Komponenten, welche im Verbund das System ergeben. Diese Architektur beschreibt hierbei die logischen Subsysteme und Komponenten selbst sowie deren Beziehungen und Kommunikation untereinander (**„L_n-G. Entwerfe logische Architektur“** siehe Abbildung 4.11). Zudem soll die Wiederverwendung bereits vorhandener logischer Subsysteme und Komponenten unterstützt werden. Dabei sollen neugestaltete logische Subsysteme und Komponenten so entwickelt werden, dass sich diese bei Bedarf erneut verwenden lassen.Darüber hinaus wird das logisch spezifische Verhalten des Systems beschrieben (**„L_n-H. Leite logisch spezifische Verhaltensmodelle ab“** siehe Abbildung 4.11). Im Gegensatz zur technischen Sichtweise liegt hier der Fokus nicht auf die im Anschluss realisierte technische Architektur, wie z.B. welche Steuergeräte und Kommunikationssysteme letztens verwendet werden. Die logische Sichtweise wird ihrerseits durch logisch spezifische Analysen sowie Integrations-, Verifikations- und Validierungsaktivitäten finalisiert (**„L_n-I. Führe logisch spezifische Analysen, Integrations- und/oder V&V-Aktivitäten durch“** siehe Abbildung 4.11) [192], [193].

- **Technische Sichtweise (T-VP):** Die Hauptaufgabe in der technischen Sichtweise liegt im Übergang von plattformunabhängigen Modellen (logische Subsysteme und Komponenten) der logischen Sichtweise auf plattformspezifische Modelle (technische Subsysteme und Komponenten). Insbesondere wird dort das System in Komponenten zerlegt, welche dann wiederum durch die unterschiedlichen Entwicklungsdisziplinen Mechanik, Elektronik und Software weiter spezifiziert werden (**„L_n-J. Entwerfe technische Architektur“** siehe Abbildung 4.11). Folglich werden hier die Eigenschaften der ausgewählten technischen Subsysteme und Komponenten (Steuergeräte, Sensoren, Konnektoren, Softwarekomponenten etc.) und ihre bereitgestellten Ressourcen modelliert (**„L_n-K. Leite technisch spezifische Verhaltensmodelle ab“** siehe Abbildung 4.11). Vor diesem Hintergrund kann die Softwareentwicklung in Übereinstimmung mit den Vorgehensweisen des AUTOSAR Standards erfolgen. Analog zu den vorangegangenen Sichtweisen wird die technische Sichtweise durch technisch spezifische Analysen sowie Integrations-, Verifikations- und Validierungsaktivitäten abgeschlossen (**„L_n-I. Führe logisch spezifische Analysen, Integrations- und/oder V&V-Aktivitäten durch“** siehe Abbildung 4.11). Alles in allem beschreibt die technische Sichtweise, wie Software und Hardware zusammenwirken, um die definierten Systemziele zu erreichen [192], [193].

4.7 Modellbasierte Analyse- und Testmethoden

Innerhalb des Automobilsektors werden unterschiedliche modellbasierte Analyse- und Testmethoden verwendet, um frühzeitig im Entwicklungsprozess Aussagen über den Reifegrad der Arbeitsprodukte treffen zu können. Je nach Prozessphase ermöglicht die sogenannte „X-in-the-Loop“ (XiL) Vorgehensweise bereits vorhandene Modelle, Komponenten, Subsysteme oder Systeme in Relation zum Gesamtsystem zu evaluieren. Dieser Ansatz beruht darauf, die restlichen noch nicht vorliegenden Systembestandteile modellbasiert in einer Simulationsumgebung zu komplettieren [194]:

Der „Model-in-the-Loop“ (MiL)-Ansatz charakterisiert sich dadurch, dass sowohl das Testobjekt im Sinne des SUTs als auch die Testumgebung als Modell vorliegen. Hierbei wird die Systemarchitektur (vgl. Abschnitt 4.2), welche in eine vollständig virtuelle Umgebung integriert wird, anhand von Simulationen evaluiert [100]. Hierbei gibt es unterschiedliche Ansätze, die Verhaltensspezifikation und -simulation entsprechender Architekturbestandteile aufzusetzen. Eine Möglichkeit besteht darin, das Verhalten unter Anwendung heterogener Simulations- bzw. Berechnungsmodelle (vgl. Abschnitt 4.4) innerhalb einer oder mehrerer Entwicklungsumgebungen aufzubauen und ggf. miteinander zu verknüpfen. Darunter fallen Co-Simulationen, welche die verschiedenartigen Ausprägungen von E/E-Architekturen im Sinne von vernetzten, eingebetteten Systemen als auch unter Berücksichtigung der jeweils beteiligten Domänen anhand von disziplinspezifischen Modellierungsformalismen, Berechnungsmodellen und Quellwerkzeugen koppeln [195].

Dieser Vorgang zielt darauf ab, die Abhängigkeiten und Korrelationen der involvierten Domänen transparent zu machen. Dabei kommen unterschiedliche Modellierungsformalismen und -sprachen wie Hybrid Automata [196], VHDL-Analog/Mixed-Signal [197] oder SystemC-Analog/Mixed-Signal [198] als auch Simulations- und Architekturwerkzeuge wie MATLAB Simulink [175] System Composer [177] und Stateflow [176] zum Einsatz.

Des Weiteren kann an dieser Stelle zwischen Open-Loop und Closed-Loop Simulationsmodellen unterschieden werden. Open-Loop-Modelle repräsentieren beispielsweise das Verhalten eines Fahrzeugs basierend auf vorgegebenen Eingabedaten, ohne aber die letztendliche Fahrzeugreaktion darauf zu berücksichtigen. Ergo liegt keine Rückkopplungsschleife vor, welche die jeweiligen Fahrzeughandlungsweisen in die Simulation zurückführt, wodurch sich Open-Loop-Modelle für die Analyse von Systemkomponenten eignen, aber weniger für das Testen der Gesamtfahrzeugdynamik. Closed-Loop-Modelle hingegen beinhalten eine Rückkopplungsschleife, bei der die Fahrzeugverhaltensreaktion und/oder die Umgebungsreaktion zurückgeführt wird. Dies ermöglicht eine realistischere Verhaltensrepräsentation, da das Modell kontinuierlich auf Veränderungen reagiert. Dadurch erweisen sich Closed-Loop Modelle als vorteilhaft, wenn es darum geht, das Gesamtfahrzeugverhalten innerhalb unterschiedlicher Szenarien simulationsbasiert zu testen.

Für die Durchführung disziplinübergreifender Co-Simulationen werden wiederum Schnittstellen für den standardisierten Austausch von Verhaltensmodellen unterschiedlicher Basiswerkzeuge notwendig. Darunter fallen u.a. Functional Mock-Up Interfaces (FMI), woraus wiederum Functional Mock-Up Units (FMU) für die Implementierung einer solchen Schnittstelle abgeleitet werden. Diese enthalten eine Schnittstellenspezifikationen anhand des standardisierten Extensible Markup Language (XML)-Austauschformats. Daraus ergibt sich die Option, MiL-Simulationen auf Systemebene mittels Verhaltensspezifikationen auf Basis von modellbasierten Architekturbeschreibungssprachen (vgl. Abschnitt 4.5) durchzuführen. In der Arbeit von Bucher [199] wird dargelegt, dass innerhalb der UML und SysML eine ausführbare

analytisch dynamische Verhaltensbeschreibung nicht realisierbar ist. Deswegen muss auf externe Modelle anhand von FMUs verwiesen werden. Das tatsächliche Verhalten wird dabei durch den manuellen Import eines XML-Platzhalters im Zielwerkzeug beschrieben und anschließend als fertige FMU wieder händisch exportiert. Abschließend werden die FMU-Modelle verknüpft und simulativ ausgeführt [200], [201].

Mittels der „Software-in-the-Loop“ (SiL)-Methode erfolgt die Überprüfung des aus den Modellen erzeugten Codes für die jeweiligen Softwarekomponenten der technischen Architektur. Dabei wird eine von den Umgebungsmodellen getrennte Plattform eingesetzt. Diese unterliegt keinen Echtzeitanforderungen, da keine realen Steuergeräte oder andere Hardwarekomponenten aus der Mechanik und dem E/E-Bereich beansprucht werden [202].

Beim „Processor-in-the-Loop“ (PiL)-Ansatz wird die kompilierte Zielsoftware auf einem Emulator des im Steuergerät implementierten Prozessors ausgeführt. Dabei werden die Schnittstellen des Testobjekts sowie die Basissoftware emuliert, während die übrigen Komponenten in Echtzeit simuliert werden. Die Zielsetzung von PiL besteht vornehmlich darin, Aspekte der Laufzeit und des Speicherbedarfs zu überprüfen [203].

Im Zuge der „Hardware-in-the-Loop“ (HiL)-Verfahrensweise wird das Testobjekt bzw. SUT als reale Hardware- oder Softwarekomponente innerhalb einer echtzeitfähigen Simulationsumgebung eingebettet. Sollte sich die Modellierung von Teilen der Simulationsumgebung als zu aufwändig gestalten oder die Erfüllung von Echtzeitanforderungen nicht möglich sein, können Aktuatoren und Sensoren gleichermaßen als Realkomponenten eingesetzt werden [204]. Die Integration sowie der Test der Einzelkomponenten wird als Komponenten-HiL (K-HiL), wohingegen deren Zusammenschluss zu Teilsystemen oder gar zum Gesamtsystem sowie die Evaluierung des korrekten Zusammenspiels als Integrations-HiL (I-HiL) bezeichnet wird (vgl. Komponententest, Systemtest und Integra-tionstest Unterabschnitt 3.2.3).

Zum Abschluss der XiL-Vorgehensweise werden mit Hilfe der „Vehicle-in-the-Loop“ (ViL)-Methode die Vorzüge der realen Fahrerprobung (vgl. Unterabschnitt 3.2.3) und des simulationsbasierten Testens miteinander verknüpft [205]. In Anbetracht dessen wird das vollständige reale Versuchsfahrzeug in eine virtuelle Umgebung eingebunden. Dabei können der Verkehr und weitere Bestandteile der Fahrzeugumwelt simulativ abgebildet werden. Aus dieser Umgebung heraus wird mittels geeigneter Schnittstellen das zu testende Fahrzeugsystem, exemplarisch sei hier die Sensorik zu nennen, angeregt und bewertet. Insgesamt bildet der ViL Ansatz eine Brücke zwischen Integrations-HiL sowie Akzeptanztest im Sinne der realen Fahrerprobung [206] und ist von besonderer Bedeutung für das Testen von Fahrerassistenz- und Fahrzeugführungssystemen [205].

4.8 Szenariobasierte Vorgehensweisen und Testprozessreferenzen

Bislang konnte der Testnachweis von Systemen wie beispielsweise dem Abstandsregeltempomaten über eine fehlerfreie Funktionsweise innerhalb einer definierten Kilometerlaufleistung anhand von Realfahrten erbracht werden [207]. In [208] wird demonstriert, dass dies beim automatisierten Fahren nicht mehr praktikabel ist. Auch in [209] wird belegt, dass für den statistischen Nachweis der einwandfreien Funktionsweise automatisierter Fahrzeuge Milliarden von Testkilometern notwendig wären. Das szenariobasierte Testen als Spezialfall simulationsbasierter XiL-Testmethoden versucht diese Nachteile auszuräumen.

Stochastische Methoden wie Markov-Ketten und Bayes'sche Netze erlauben die probabilistische Modellierung von Szenarien und mittels Monte-Carlo-Simulationen die Analyse der Übergangswahrscheinlichkeiten zwischen unterschiedlichen Zuständen eines Fahrzeugs oder einer Verkehrssituation unter variierenden Bedingungen. Hinsichtlich der Identifikation und Erstellung von Szenarien existieren wiederum unterschiedliche Herangehensweisen. Eine Möglichkeit besteht darin, Szenarien aus Szenarienkatalogen zu extrahieren oder Felddaten von Realfahrten sowie ggf. Unfalldaten zu verwenden [210], [211]. Im Rahmen von a-posteriori Resimulationen können die aufgezeichneten Daten in das Testobjekt direkt eingelesen werden. Dies hat zum Vorteil, dass die Simulationseingänge realistischen Daten entsprechen und gleichzeitig die Durchführung reproduzierbarer Tests ermöglichen. Es ist jedoch zu beachten, dass keine Closed-Loop-Simulation vorliegt (vgl. Abschnitt 4.7), da die Ausgänge des Testobjekts keinen Einfluss auf das Umgebungsverhalten haben. Im Gegensatz dazu können im Zuge der sogenannten Live Resimulation aufgezeichnete Fahrdaten zur Laufzeit einem innerhalb des Fahrzeugs integrierten Testobjekt zugeführt werden. Dadurch wird beispielsweise ein direkter Vergleich mit dem Verhalten des menschlichen Fahrers ermöglicht. Dieses Vorgehen ähnelt dem sogenannten „Shadow Mode" Ansatz von Tesla [212]. Bei datengetriebenen (engl. *Data-Driven*) Ansätzen zur Generierung von Szenarien werden typischerweise Methoden des maschinellen Lernens oder Ansätze zur Mustererkennung eingesetzt. Eine andere Technik ist die wissensbasierte Szenarienerstellung, bei der Experten Szenarien mithilfe von Ontologien definieren.

Innerhalb des szenariobasierten Testens repräsentiert der Begriff Szenario den Kernaspekt für die Beschreibung aller notwendigen Merkmale einer Simulation, wobei dieser gemeinsam mit den Attributen des Funktionsumfangs (max. zulässige Geschwindigkeit, max. zulässige Verzögerung etc.), des Wunschverhaltens sowie der funktionalen Systemgrenzen unter einen Anwendungsfall einzuordnen ist (siehe Abbildung 4.12). Ein Szenario umfasst die chronologische Abfolge unterschiedlicher Szenenelemente wie Ego-Fahrzeug (Fahrmanöver sowie Eigenschaften des Ego-Fahrzeugs und des Fahrers), Verkehrsteilnehmer (dynamische Elemente wie Fahrzeuge und Fußgänger anhand einer Verhaltensbeschreibung durch Parameter) als auch Umwelt (Straßeninfrastruktur, statische Objekte wie parkende Fahrzeuge, Gebäude, Fahrbahnmarkierungen etc. sowie Wetter- und Lichtverhältnisse), welche wiederum eine Szenerie ergeben [213].

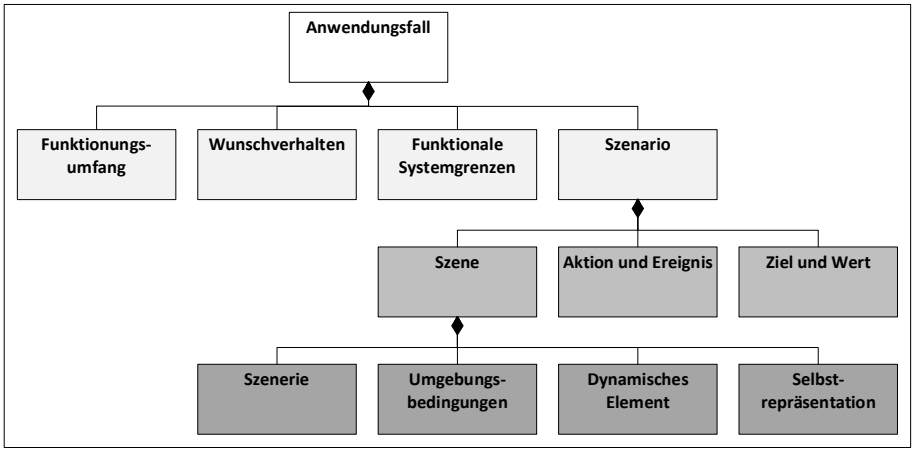


Abbildung 4.12: Einordnung eines Szenarios und dessen Bestandteile innerhalb eines übergeordneten Anwendungsfalls (in Anlehnung an [214], [216]).

Die Szenen stellen eine Momentaufnahme mit den jeweiligen Bestandteilen ohne zeitliche Dauer dar [203], [214] und sind an eine a priori definierte Sequenz einschließlich einer definierten initialen Szene gebunden [215]. Dabei werden die Szenen durch die unterschiedlichen Handlungsweisen, sprich Aktionen und Ereignisse (Manöver wie Fahrstreifenwechsel oder Überholvorgang) sowie Ziele und Werte (z.B. aktuelle Mission, Nutzereingaben oder gesetzliche Anforderungen wie Verkehrsregeln) der partizipierenden Verkehrsteilnehmer miteinander gekoppelt und fügen sich nahtlos aneinander an. Daraus ergibt sich die Dauer des Zeitintervalls eines Szenarios [203]. Die Selbstrepräsentation spiegelt die generellen Systemfähigkeiten und Fertigkeiten der jeweiligen Teilnehmer wider [214].

Definition 4.31 Szenario [214].
Ein Szenario beschreibt die zeitliche Entwicklung von Szenenelementen innerhalb einer Folge von Szenen, welche mit einer Startszene beginnt.

Definition 4.32 Szenerie [203].
Die Szenerie beinhaltet alle räumlich statischen Objekte eines Szenarios, wie geometrische Elemente (z.B. Straßennetz mit Verbindungen und Knoten) und globale Attribute (z.B. das Wetter und die Tageszeit). Der Zustand der räumlich statischen Objekte kann sich mit der Zeit verändern (z.B. Ampeln und Wetter).

Definition 4.33 Szene [214].
Eine Szene repräsentiert die Momentaufnahme der Umgebung einschließlich der Szenerie, dynamischer Elemente, Umgebungsbedingungen und aller Selbstrepräsentationen von Akteuren und Beobachtern sowie der Beziehungen zwischen diesen.

Des Weiteren sind Szenen stets als Gegenstand einer Situation zu betrachten. Eine Situation widerspiegelt die subjektive Perspektive eines Teilnehmers bzw. Beobachters auf eine Szene [214]. Exemplarisch seien hier die Sichten eines menschlichen Fahrers, eines Fahrzeugführungssystems eines automatisierten Kraftfahrzeugs, eines Verkehrsüberwachungssystems bis hin zu Fußgängern und weiterer Entitäten innerhalb des Verkehrsraums zu nennen. Infolgedessen lässt sich eine Situation auf der einen Seite in subjektive und auf der anderen Seite in objektive Gesichtspunkte separieren. Hierbei umfasst die Verkehrssituation die objektive, räumliche und zeitliche Zusammensetzung der verkehrsbezogenen Einflussdimensionen. Wohingegen die Fahrsituation die aus der Verkehrssituation abgeleitete wahrnehmbare Perspektive des Fahrers illustriert. Daraus lässt sich schließlich die subjektive vom Fahrer tatsächlich wahrgenommene Situation deduzieren [217]. Auf Basis der wahrgenommenen Situation leitet der Fahrer entsprechende Handlungs- und Verhaltensmuster ab. Analog dazu lassen sich Situationen und Handlungen für weitere Akteure innerhalb des Verkehrsraums generieren.

Definition 4.34 Situation [203], [214].
Eine Situation repräsentiert den Blick eines Teilnehmers auf die jeweilige Szene. Sie fasst alle relevanten Bedingungen, Möglichkeiten und Bestimmungsfaktoren von Handlungen innerhalb der Szene zusammen, die um die geplanten Verhaltens- und Handlungsmuster sowie funktionsspezifischen Aspekte der Teilnehmer angereichert werden. Folglich ist eine Situation immer subjektiv, indem sie die individuelle Perspektive eines Teilnehmers repräsentiert.

Zudem können die dynamischen Verhaltens- und Handlungsmuster der jeweiligen Verkehrsteilnehmer unter dem Begriff Manöver gefasst werden. Im Kontext der Fahraufgabe stellt ein Fahrmanöver eine temporäre Handlungsfolge dar, worin unterschiedliche Fahrsituationen sequenziell ineinander überführt werden. Das Fahrmanöver selbst kann abermals aus mehreren untergeordneten Fahrmanövern bestehen. Dies lässt sich z.B. an einem Überholmanöver demonstrieren, welches aus einem Fahrstreifenwechsel

nach links, einer Vorbeifahrt und einem finalen Fahrstreifenwechsel nach rechts zusammengesetzt ist [218].

Definition 4.35 Manöver [203].
Ein Manöver ist die abstrakte Beschreibung des Verhaltens eines Teilnehmers während einer oder mehrerer Szenen.

Ferner können Szenarien gemäß [219] auf vier unterschiedlichen Detail- bzw. Abstraktionsebenen beschrieben werden:

- Funktionale Szenarien repräsentieren die im Fokus stehenden Merkmale und Eigenschaften auf semantischer bzw. sprachlicher Ebene.
- Abstrakte Szenarien greifen die sprachlich festgehaltenen Merkmale auf und formalisieren diese entlang der Beschreibung, z.B. unter Bezugnahme einer Ontologie, von Wirkzusammenhängen bzw. kausalen Effekten (engl. *Cause-Effect*).
- Logische Szenarien stellen die Szenarienbestandteile in Form von Entitäten als auch Beziehungen anhand von Parameterbereichen im Zustandsraum dar.
- Konkrete Szenarien widerspiegeln eine Instanz der logischen Szenarien mittels eines expliziten Parametersets [219].

4.8.1 Industrie- und Forschungsprojekte im Bereich des szenariobasierter Vorgehensweisen

Im Kontext des szenariobasierten Testens nimmt das Industrie- und Forschungsprojekt PEGASUS (Project for the Establishment of Generally Accepted quality criteria, tools and methods as well as Scenarios and Situations) [220] zur Freigabe und Zulassung hochautomatisierter Fahrfunktionen eine Vorreiterrolle ein. Um einen neuen Stand der Technik für die Verifikation und Validierung von automatisierten Fahrfunktionen zu definieren, werden in vier Teilprojekten verschiedene Testmethoden, Qualitätskriterien, Verkehrsszenarien, Werkzeuge, Datenbanken und Richtlinien definiert. Daraus entsteht wiederum ein szenariobasierter Prozess, welcher in einer Datenbank die relevanten logischen Szenarien verwaltet. Aus diesen logischen Szenarien werden, basierend auf Auftretenswahrscheinlichkeiten und definierten Bestehenskriterien, Testfälle abgeleitet. Anschließend wird eine Verteilung der logischen Testfälle auf verschiedene Testplattformen (MiL, SiL, HiL und ViL vgl. Abschnitt 4.7) vorgenommen sowie die Erstellung konkreter Testfälle durch Parametervariation vollzogen.

Ergänzend werden Feldtests im realen Straßenverkehr durchgeführt, um Messdaten zu erfassen. Diese Daten werden im PEGASUS-Prozess verwendet, um kritische Szenarien zu identifizieren und die Validierung zu unterstützen. PEGASUS liefert neben einem szenariobasierten Top-Down-Verifikations- und Validierungsansatz, auch eine strukturierte Sicherheitsargumentation und Möglichkeiten für die Generierung notwendiger Sicherheitsnachweise einer Gesamtfreigabeempfehlung (vgl. Abschnitt 5.1). Die in der Gesamtheit generierten Testergebnisse bilden eine zentrale Sicherheitsaussage, welche ihrerseits für eine Sicherheitsargumentation herangezogen wird [221].

Ein weiteres Industrie- und Forschungsprojekt, welches ebenfalls dem PEGASUS-Kooperationsprojekt entspringt, ist VV-Methoden (VVM) [222]. Dieses zielt darauf ab eine Erweiterung der PEGASUS-Methoden

vorzunehmen. Einer der Hauptunterschiede zwischen VVM und PEGASUS ist der zusätzliche Fokus auf die Systemarchitektur hochautomatisierter Straßenfahrzeuge. Im Hinblick darauf liegt die grundlegende Frage- und Problemstellung im VVM-Projekt darin, wie Sicherheit und gesellschaftliche bzw. gesetzliche Konformität eines hochautomatisierten oder vollautomatisierten Kraftfahrzeugs (SAE-Level 4 bzw. 5) im urbanen Umfeld verwirklicht werden kann. Prinzipiell geht es darum, einen glaubwürdigen Sicherheitsnachweis (engl. *Credible Safety Case*) entlang der Nachweisführungskette Evidenz, Argument und Behauptung zu konzipieren (vgl. Abschnitt 5.3), mittels einer kohärenten Verknüpfung der entwickelten Methoden zu begründen und auf Grundlage dessen für die Homologation freizugeben. Das Ganze erfolgt unter der Prämisse der Erreichung einer positiven Risikobilanz sowie anhand eines hierarchisch strukturierten Top-Down-Ansatzes, welcher den gesamten Lebenszyklus berücksichtigt.

Genauer genommen umfasst der Top-Down-Ansatz drei horizontal verlaufende Granularitätsebenen („Capability Layer" bezieht sich auf das erforderliche Verhalten auf Betriebsbereichs- und Fahrzeugebene, „Engineering Layer" beinhaltet das spezifizierte Verhalten auf Ebene der funktionalen und technischen Architektur, „Real World Layer" behandelt das implementierte Verhalten auf Ebene der tatsächlichen physischen Realisierung). Hierfür wird eine zusätzliche Verlagerung von hybriden, physischen und realen Testerprobungen in Richtung von Simulationsumgebungen angestrebt, wobei ein nahtloser Übergang zwischen den Tests virtueller und realer Artefakte ermöglicht werden soll.

Darüber hinaus werden konsistente organisationsübergreifende Schnittstellen für die Aufschlüsselung und den Austausch von Anforderungen, inkrementellen Tests, Sicherheitsargumentationen und -nachweisen usw. über die gesamten Lieferkette definiert. Ferner umfasst VVM unterschiedliche Methoden, wie z.B. zur Identifizierung eines Betriebsbereichs und Fahrzeugzielverhaltens, zur Miteinbeziehung einer verkehrsrechtlichen Perspektive mit Hinblick auf die Einhaltung aller relevanten gesellschaftlichen Ansprüche in Form von Gesetzen, Normen und Standards, zum Verstehen und Bewerten gefährdender Phänomene innerhalb des Verkehrsraums anhand von Kritikalitätsmetriken als auch zur systematischen Beherrschung und Reduktion des Testparameterraums auf ein handhabbares Minimum.

4.8.2 Beiträge repräsentativer Forschungsarbeiten zur Weiterentwicklung szenariobasierter Testmethoden

Auch die Forschungsarbeiten des Instituts für Technik der Informationsverarbeitung (ITIV) sowie des Forschungszentrums Informatik (FZI) befassen sich mit verschiedenartigen Ausprägungen des szenariobasierten Testens. Auf der einen Seite liefern diese Arbeiten einen wichtigen Beitrag in Bezug auf die Weiterentwicklung und das Voranschreiten szenariobasierter Vorgehensweisen. Die betrachteten Arbeiten zeigen in ihrer Gesamtheit, dass szenariobasierte Methoden in der Zwischenzeit einen unverzichtbaren Bestandteil der Absicherung automatisierter Fahrfunktionen repräsentieren.

Pfeffer et al. [211], [223], [224] entwickeln einen Prozess zur realdatenbasierten, simulationsgestützten funktionalen Absicherung hochautomatisierter Fahrfunktionen. Ausgangspunkt ist die Erkenntnis, dass klassische XiL-Testmethoden (vgl. Abschnitt 4.7) sich prinzipiell als geeignet erweisen, aber singulär keine vollständige Testabdeckung ermöglichen können. Aus diesem Grund kombinieren Pfeffer et al. reale Datenaufzeichnungen aus Fahrzeugflotten mit szenariobasierten Simulationsansätzen. Hierfür wird ein Szenario-Metamodell konzipiert, welches dynamische Manöver, Zustände und Zustandsübergänge der jeweiligen Repräsentanten eines Szenarios systematisch abstrahiert. Zudem werden die extrahierten Szenarien innerhalb von erweiterbaren Katalogen bzw. Datenbanken abgelegt, mit Bewertungsmetriken versehen

und für eine automatisierte Testfallgenerierung herangezogen. Der Vergleich von Test- und Originaldaten stellt hierbei die Validität der Simulationsergebnisse sicher.

Die Thematik der entwicklungsbegleitenden Bewertung von Fahrerassistenzsystemen mittels szenariobasierter Testansätze wird von King et al. [225], [226], [227] adressiert. Sie ziehen die Schlussfolgerung, dass bisherige szenariobasierte Vorgehensweisen hauptsächlich auf Kritikalitätsmetriken beruhen und keine systematische Überprüfung der Anforderungserfüllung zur Verfügung stellen. Im Gegensatz dazu ermöglicht der Ansatz von King et al., eine zweckmäßige Bewertung von Fahrerassistenzfunktionen in Testszenarien, welche sich ihrerseits durch parametrische Variationen charakterisieren. Dies gilt auch in Bezug auf die funktionale Anforderungserfüllung. Neben der Entwicklung eines Bewertungsschemas, welches einerseits funktionale Anforderungen und andererseits dynamische Aspekte von repräsentativen Szenarien berücksichtigt, werden auch Maßnahmen zur Reifegradbestimmung eingeführt. Dadurch wird eine effiziente Bewertung des Entwicklungsfortschritts realisiert, welche ihrerseits als Entscheidungsgrundlage für Freigabeprozesse (vgl. Abschnitt 3.1) herangezogen werden kann. In Ergänzung dazu zeigen King et al. die Übertragbarkeit der Testmethoden auf HiL- und SiL-Umgebungen auf (vgl. Abschnitt 4.7), was wiederum die Praxistauglichkeit des Konzepts unterstreicht.

Reisgys et al. [228], [229], [230] entwickeln eine Methodik zur Glaubwürdigkeitsbewertung szenariobasierter XiL-Tests. Ausgangspunkt ist die Problematik der systematischen Berücksichtigung von Unsicherheiten innerhalb simulationsbasierter Testmethoden (vgl. Anhang A.3 und A.4) – etwa in Sensormodellen oder modellbasierten Repräsentationen des Betriebsbereichs (vgl. Unterabschnitt 2.2.3). Aufgrund dessen wird ein mehrstufiger Bewertungsansatz vorgeschlagen, welcher Aspekte der Prädiktion, Plausibilisierung und statistischen Validierung umfasst. In diesem Kontext werden zuerst Unsicherheiten durch Monte-Carlo-Simulationen quantifiziert und darauf basierend Konfidenzintervalle deduziert. Im Anschluss erfolgt eine Plausibilisierung über Szenariodistanzmaße und Pass/Fail-Kriterien. Abschließend wird mittels sogenannter Barnard-Tests ein probabilistischer Vergleich zwischen XiL- und Realtestdaten vorgenommen. An dieser Stelle ist in besonderem Maße hervorzuheben, dass Reisgys et al. ihren Ansatz an realen Testfällen aus Serienentwicklungsprojekten bewerten, um anhand dessen die Praxisrelevanz und Anwendbarkeit der Vorgehensweise zu belegen.

Die Exploration und Cluster-basierte Analyse von logischen Szenarien wird von Schütt et al. [231], [232], [233], [234], [235] untersucht. Ihre Arbeiten adressieren die Herausforderung, kritische Szenarien effizient zu identifizieren, ohne den gesamten Entscheidungs- bzw. Szenarienraum simulativ abtasten zu müssen. Im Hinblick darauf wird ein sogenanntes Bayesian Optimization Framework entwickelt, welches zielgerichtet nach Bereichen hoher Kritikalität innerhalb eines vorliegenden Szenarienraums sucht. Darüber hinaus erfolgt eine Clusteranalyse unter Anwendung von Ähnlichkeitsmaßen, um redundante Szenarien zu gruppieren und zusammenzufassen. Zudem wird ein Ansatz zur Konfidenzanalyse der explorierten Bereiche konzipiert und ein systematisches Verfahren vorzunehmender Abdeckungsaussagen logischer Szenarienräume vorgeschlagen. Die Vorgehensweise von Schütt et al. steigert nicht nur die Effizienz des Testprozesses, sondern schafft auch eine quantifizierbare Grundlage für die Abdeckung sicherheitskritischer Situationen im Testkatalog automatisierter Fahrfunktionen.

Bernhard et al. [236], [237], [238] entwickeln eine adaptive Pipeline zur Auswahl von Testszenarien für Wahrnehmungsfunktionen im Bereich des automatisierten Fahrens. Im Fokus steht die Absicherung von ML-basierten Perzeptionssystemen, deren Schwächen zu prädizieren sind. Hierfür werden adaptive Sampling-Strategien mit synthetischer Bilddatengenerierung aus simulationsgestützten Rahmenwerken kombiniert. Die Zielsetzung liegt darin, durch gezieltes Abtasten besonders herausfordernde Szenarien iterativ zu identifizieren und dadurch Insuffizienzen systematisch aufzudecken. Der Ansatz erlaubt es, ML-

basierten neuronalen Netzwerken gezielt Trainingsdaten aus kritischen Szenarien einzuspeisen, um deren Robustheit im realen Feldbetrieb nachweislich zu erhöhen. Bernhard et al. validieren die Vorgehensweise umfassend anhand eines Notbremsassistenten und legen dar, dass adaptive Tests eine höhere Fehlerentdeckungsrate im Vergleich zu klassischen Random Sampling Ansätzen erzielen.

Ein Verfahren zum Clustering von Fahrsequenzen für die datenbasierte Szenarienanalyse wird von Ries et al. [239], [240], [241], [242] entwickelt. Ausgangspunkt dieser Arbeiten ist die Herausforderung, dass urbane Betriebsbereiche eine extrem hohe Varianz an Verkehrssituationen umfassen und im klassischen Sinne nicht vollständig erfasst werden können. In dieser Hinsicht schlagen Ries et al. ein modellfreies Gruppierungsverfahren vor, bei dem reale Verkehrsaufzeichnungen anfänglich zu Fahrsequenzen segmentiert und daraufhin im Hinblick auf deren semantische Ähnlichkeit gebündelt werden. Aus diesen Clustern werden wiederum charakteristische Szenarien ausgesondert, welche ihrerseits für die Validierung herangezogen werden können. Zusätzlich entwickeln Ries et al. ein Verfahren zur probabilistischen Vorhersage der Auftretenswahrscheinlichkeit einzelner Szenarien, wodurch deren quantitative Abdeckung innerhalb einer Testspezifikation evaluiert werden kann. Diese Arbeiten stellen dadurch einen wichtigen Baustein zur datengetriebenen Absicherung hochautomatisierter Fahrfunktionen im urbanen Umfeld dar.

5 Automotive-Sicherheitsentwicklung

„Tu, was du kannst, mit dem was du hast, wo immer du bist."

Theodore Roosevelt

Sowohl seitens des Automobilmarkts und dessen Endkunden als auch seitens der Gesetzgebung des Straßenverkehrs nehmen die Sicherheitsanforderungen von Kraftfahrzeugen kontinuierlich zu. Die Einführung von Fahrerassistenzsystemen und Funktionen des automatisierten Fahrens soll an dieser Stelle einen elementaren Beitrag zur Erhöhung der Verkehrssicherheit leisten. Hierbei sieht sich die Entwicklung von aktiven Sicherheits- und Fahrerassistenzsystemen hin zum unfallfreien bzw. hochautomatisierten Fahren mit facettenreichen Herausforderungen konfrontiert. Auf der einen Seite müssen die Systeme dergestalt entworfen werden, dass diese die hohen Anforderungen an Sicherheit erfüllen. Auf der anderen Seite ergibt sich die Notwendigkeit an Methoden und Maßnahmen, mit welchen profunde Aussagen über die Sicherheit dieser Systeme getätigt werden können. In diesem Kontext existieren innerhalb der Automobilindustrie Verfahrensvorschriften, Richtlinien, Normen und Standards, um die Sicherheit der in der Entwicklung befindlichen Systeme über den gesamten Produktlebenszyklus nachhaltig zu begutachten und umzusetzen. Hierfür werden im Zuge dieses Kapitels die für die vorliegende Dissertation benötigten theoretischen Grundlagen sowie ein aktueller Stand von Wissenschaft und Technik im Hinblick auf Sicherheitsentwicklung innerhalb des Automotive-Bereichs wiedergegeben.

5.1 Verkehrssicherheit und gesetzliche Grundlagen im Kontext des Straßenverkehrs

Sowohl der öffentliche als auch der individuelle Personenverkehr auf der Straße gehören zum Grundbedürfnis nach Mobilität einer modernen Gesellschaft. Hierbei erweist sich der Straßenverkehr als soziotechnisches System, welches in reziprokem Austausch mit menschlichen, gesellschaftlichen, politischen, wissenschaftlichen, ökonomischen, ökologischen als auch technologischen Einflüssen steht. In diesem Kontext repräsentiert der Aspekt der Verkehrssicherheit den unbeschadeten Transport der individuellen Teilnehmer zwischen räumlich voneinander distanzierten Start- und Zielpunkten über ein Straßennetz. Dies erfolgt unter Zuhilfenahme eines Verkehrsmittels, wie z.B. dem Kraftfahrzeug, als auch unter Berücksichtigung zeitlicher Rahmenbedingungen. Insgesamt gilt der Schutz von menschlichem Leib und Leben als oberste Prämisse der Verkehrssicherheit, woran sich an zweiter Stelle der Erhalt von Umwelt- und Sachgütern anschließt. Hierbei setzt sich die Verkehrssicherheit aus der Straßenverkehrssicherheit (Verhaltensregeln), der Straßensicherheit (Straßeninfrastruktur) sowie der Kraftfahrzeugsicherheit zusammen [143].

Die drei Säulen Straßenverkehrssicherheit, Straßensicherheit und Kraftfahrzeugsicherheit manifestieren sich auch innerhalb der Gesetzgebung des Straßenverkehrs. Dabei gelten für alle am Straßenverkehr beteiligten Akteure unterschiedliche Gesetze und Verordnungen, welche wiederum in technischen Regeln, Normen und Standards, Richtlinien als auch Empfehlungen spezifischer dargelegt werden [243].

In Deutschland beispielsweise ist das Straßenverkehrsgesetz (StVG) der geltende schematische Rechtsrahmen für den Straßenverkehr als auch entsprechender Verkehrsmittel und ordnet sich unter dem

Grundgesetz (GG) an. Dieses stützt sich am Wiener Übereinkommen von 1968 [244] und ist zudem an die Umsetzung von EU-Richtlinien und Verordnungen geknüpft. Ferner regelt das StVG die Basiselemente des Straßenverkehrsrechts und umfasst die Straßenverkehrsordnung (StVO), die Straßenverkehrszulassungsordnung (StVZO), die Fahrzeug-Zulassungsverordnung (FZV) sowie die Fahrerlaubnisverordnung (FeV) [245] (siehe Abbildung 5.1).

Innerhalb der StVO sind die allgemeinen Verkehrsregeln, Angaben zu Verkehrszeichen und Einrichtungen, exemplarisch sei hier die Richtlinie für die Anlage von Autobahnen (RAA) [246] zu nennen, als auch Bußgeldvorschriften im Sinne der Verkehrsorganisation festgehalten. In diesem Kontext werden durch die FeV Regeln für die hinreichende Befähigung und Tauglichkeit eines Kraftfahrzeugführers vorgegeben. Hinsichtlich der Inbetriebnahme bzw. Typgenehmigung von Verkehrsmitteln, wie z.B. Kraftfahrzeugen, enthalten die FZV und StVZO Anforderungen an das Fahrzeug und dessen Systeme, was zum einen die Vermeidung von Schäden der Fahrzeuginsassen und zum anderen die Gefährdungsverringerung anderer Verkehrsteilnehmer betrifft. Hierbei verweist die StVZO in der Regel auf EG-Richtlinien, welche durch UN ECE Regelungen über die Kontinentalgrenzen hinweg harmonisiert werden.

Auf Basis dieser Regelungen wird ein Kraftfahrzeug durch autorisierte und akkreditierte Prüforganisationen wie dem Technischen Überwachungsverein (TÜV) geprüft und homologiert. Zudem ist auf Gesetzesebene (siehe Abbildung 5.1) das Produktsicherheitsgesetz (ProdSG) zu beachten, welches bei Produkten, die *„im Rahmen einer Geschäftstätigkeit auf dem Markt bereitgestellt, ausgestellt oder erstmals verwendet werden“* [247], Anwendung findet. Im ProdSG sind Regelungen bezüglich Sicherheitsanforderungen von technischen Arbeitsmitteln und sogenannten Verbraucherprodukten, wozu auch Kraftfahrzeuge gehören, festgehalten. Die Markteinführung eines solchen Produkts ist nur dann gestattet, *„wenn es bei bestimmungsgemäßer oder vorhersehbarer Verwendung die Sicherheit und Gesundheit von Personen nicht gefährdet“* [247].

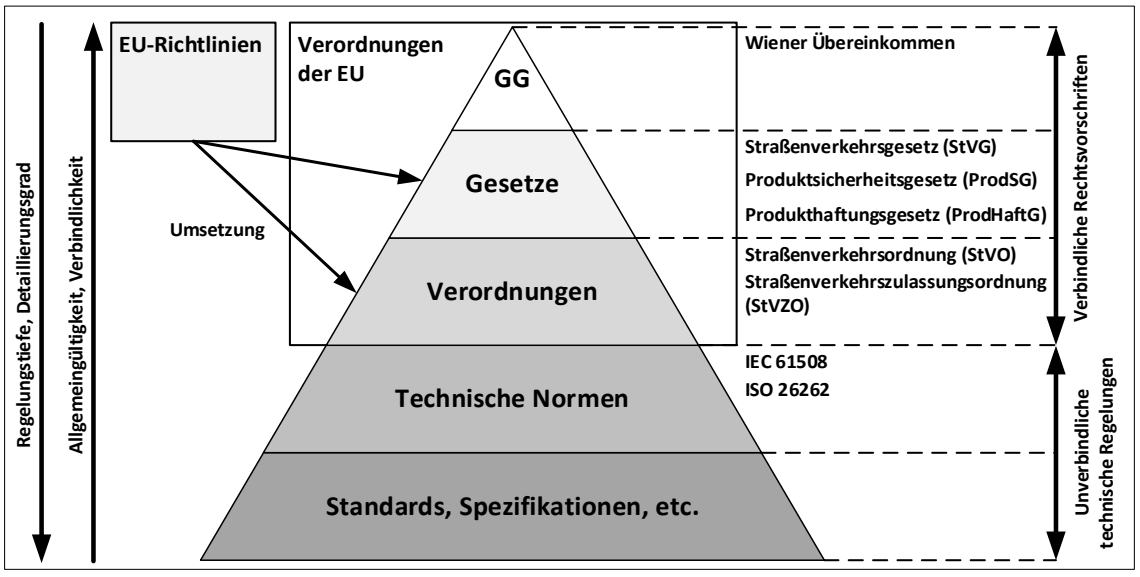


Abbildung 5.1: Rechtsordnung der deutschen Gesetzgebung im Kontext des Straßenverkehrs als hierarchische Struktur in Form einer Pyramide (in Anlehnung an [143]).

Werden durch einen Hersteller fehlerhafte Produkte im Sinne des ProdSG eingeführt, so müssen diese zurückgerufen, ersetzt oder nachgebessert werden. Im Schadensfall wird das Produkthaftungsgesetz (ProdHaftG) wirksam und der jeweilige Hersteller muss Schadensersatz leisten. Allerdings kann die Ersatzpflicht des Herstellers ausgeschlossen werden, sollte dieser nicht in der Lage gewesen sein, den Produktfehler zum Zeitpunkt der Inbetriebnahme unter Berücksichtigung von Sicherheitsnormen nach dem Stand von Wissenschaft und Technik zu identifizieren. Im Sinne der Beweislastumkehr muss der Hersteller jedoch die eindeutige Berücksichtigung des aktuellen Stands von Wissenschaft und Technik vor Gericht belegen [248].

Sowohl das ProdSG, das ProdHaftG als auch die FZV verweisen auf die Konformität des aktuellen Stands von Wissenschaft und Technik und somit einschlägigen Vorschriften und technischen Anforderungen. Diese sind auf den unteren beiden Ebenen durch technische Normen als auch Standards und Spezifikationen definiert (siehe Abbildung 5.1). Gleichwohl handelt sich hierbei um Handlungsempfehlungen, welche grundsätzlich einen rechtlichen Rahmen darstellen, aber nicht zwangsläufig umzusetzen sind. Für die Entwicklung von E/E-Systemen sind hierbei die generische Sicherheitsnorm IEC 61508 [51] und insbesondere die ISO 26262 als deren Automotive-Ableger hervorzuheben. Auf Ebene der Standards und Spezifikationen ist im Bereich der Softwareentwicklung der AUTOSAR Standard zu nennen [143].

5.2 Termini sowie Normen und Standards der Sicherheitsentwicklung

Im Kontext des Sicherheitsbegriffs sei an erster Stelle der Begriff der Verlässlichkeit (engl. *Dependability*) zu erwähnen. Dieser umschreibt im weitesten Sinne die Fähigkeit eines Systems, seinen Nutzern das beabsichtigte Integritätsniveau einer entsprechenden Dienstleistung zu erbringen. Demzufolge bildet Verlässlichkeit die von einem System zu erwartenden Eigenschaften ab, worin die Aspekte der Zuverlässigkeit, Verfügbarkeit und Sicherheit die jeweiligen Kernattribute repräsentieren [249].

Definition 5.1 Zuverlässigkeit [250], [249].
Zuverlässigkeit (engl. Reliability) kennzeichnet die Fähigkeit eines Systems während einer vorgegebenen Zeitdauer bei zulässigen Betriebsbedingungen ein gefordertes funktionsgerechtes Verhalten zu erbringen, also korrekt zu arbeiten. Demzufolge repräsentiert die Zuverlässigkeit zum gegebenen Zeitpunkt t die bedingte Wahrscheinlichkeit, dass das System ohne einen Ausfall im Intervall $[0, t]$ fehlerfrei funktioniert, sofern das System bereits zum Zeitpunkt $t = 0$ korrekt gearbeitet hat.

Hohe Zuverlässigkeit ist in Situationen erforderlich, in denen ein System ohne Unterbrechungen arbeiten soll. Somit steht beim Aspekt der Zuverlässigkeit das jeweilige Zeitintervall im Fokus, innerhalb dessen ein System korrekt funktioniert. Dahingegen bezieht sich das Attribut der Verfügbarkeit auf den Zeitpunkt, zu welchem das betrachtete System in einem funktionsfähigen Zustand zur Anwendung bereitsteht. Hierbei werden auch Instandhaltungs- und Reparaturzeiten miteinkalkuliert.

Definition 5.2 Verfügbarkeit [251], [249].
Verfügbarkeit (engl. Availability) charakterisiert die Fähigkeit eines Systems, zu einem bestimmten Zeitpunkt eine geforderte Funktion unter gegebenen Bedingungen erfüllen zu können, vorausgesetzt, dass die ggf. erforderlichen externen Hilfsmittel bereitgestellt sind. Infolgedessen spiegelt Verfügbarkeit die Wahrscheinlichkeit wider, dass das System zum gegebenen Zeitpunkt t korrekt funktioniert.

Der Aspekt der Sicherheit bezieht sich auf Ausfälle, welche Risiken[1] für menschliches Leib und Leben sowie Schäden der Umwelt zur Folge haben können.

Definition 5.3 Sicherheit [252].
Sicherheit (engl. Safety) kennzeichnet die Freiheit bzw. Abwesenheit eines unvertretbaren Risikos in Bezug auf physische Verletzung oder Schädigung der Gesundheit von Menschen als auch der Schädigung von Gütern und der Umwelt.

Es ist jedoch zu beachten, dass Sicherheit und Zuverlässigkeit im Widerspruch zueinanderstehen können. Beispielsweise ist ein vollständig passives ACC zu 100 % sicher und gleichzeitig aber zu 0 % zuverlässig bzw. verfügbar. Ein Airbag mit 100 % Zuverlässigkeit und Verfügbarkeit, welcher aber aufgrund eines Fehlers ungewollt auslöst, hat dagegen 0 % Sicherheit. Folglich muss stets ein Kompromiss zwischen Zuverlässigkeit, Verfügbarkeit und Sicherheit eingegangen werden. Grundsätzlich wird bei Systemen mit hohen Anforderungen an Zuverlässigkeit und Verfügbarkeit die Bereitstellung einer gewünschten Funktionalität priorisiert. Dafür werden auch kurzzeitig fehlerhafte Signale oder Timing-Probleme akzeptiert. Demzufolge konzentriert sich die Zuverlässigkeitsentwicklung auf diejenigen Kosten, welche durch die Ausfallzeit des Systems, Ersatzteile, Reparaturgeräte, Personal und Garantieansprüche entstehen. Weitere Aspekte sind Themen der Kundenzufriedenheit sowie die Fähigkeit eine Mission vollständig durchführen zu können. Dahingegen liegt bei der Sicherheitsentwicklung das Hauptaugenmerk darauf, Verletzungen und Schädigungen von menschlichem Leib und Leben als auch der Umwelt unter allen Umständen zu vermeiden. Daher befasst sich diese explizit mit bestimmten sicherheitskritischen und gefährlichen Systemausfallarten.

5.2.1 Funktionale Sicherheit gemäß ISO 26262

Im Kontext der Sicherheitsentwicklung repräsentiert die IEC 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer (E/E/PE)-Systeme“ [51] die internationale Referenznorm für funktionale Sicherheit. Darauf basiert wiederum die ISO 26262 „Road vehicles - Functional safety“ [50] als automobilspezifisches Derivat der IEC 61508, welche die funktionale Sicherheit von Straßenfahrzeugen zum Hauptgegenstand hat. Das Schlüsselkonzept der ISO 26262 liegt in der Eliminierung von systematischen und zufälligen Fehlern der technischen E/E-Systeme durch Sicherheitsmaßnahmen (sowohl prozessual als auch technisch) und dem nachweislichen Erreichen von funktionaler Sicherheit. Funktionale Sicherheit bezieht sich in diesem Kontext auf die Vermeidung von Schäden an Personen oder der Kraftfahrzeug- und Verkehrsumgebung, welche durch den Ausfall oder das Fehlverhalten (engl. *Malfunctioning Behavior*) eines E/E-Systems verursacht werden können. Somit stehen Gefährdungen im Fokus, welche durch Funktionsstörungen der sicherheitsbezogenen Systeme oder deren Interaktion hervorgerufen werden können. Die Sicherheit der beabsichtigten Funktion bzw. das sichere Nominalverhalten dieser Systeme wird dabei explizit nicht berücksichtigt. Solange Gefährdungen, wie z.B. UV-Strahlung, Ausstoß von Schadstoffen, Korrosion usw., nicht im direkten Zusammenhang mit dem Fehlverhalten der E/E-Systeme stehen, werden auch diese nicht näher betrachtet.

Definition 5.4 Funktionale Sicherheit [50].
Funktionale Sicherheit (engl. Functional Safety {FuSa}) ist die Freiheit von inakzeptablen Risiken basierend auf Gefährdungen, die durch Fehlfunktionen von E/E-Systemen hervorgerufen werden.

[1] Risiko (vgl. Definition 5.5)

Die ISO 26262 spezifiziert darüber hinaus einen sogenannten Sicherheitslebenszyklus, welcher sich über sämtliche Phasen der Produktentwicklung, angefangen bei der Konzeption bis hin zur Außerbetriebnahme, erstreckt und formuliert in Abhängigkeit zu den jeweiligen Phasen allgemeingültige Anforderungen sicherheitsbezogener[2] E/E-Systeme. In dieser Hinsicht sollen die Phasen, Aktivitäten und Arbeitsprodukte simultan und im wechselseitigen Austausch zu den bereits bestehenden Entwicklungs- und Produktlebenszyklusphasen basierend auf dem Referenzprozess des V-Modells durchgeführt werden. Infolgedessen sind die Aspekte der funktionalen Sicherheit eng mit den funktions- und qualitätsorientierten Entwicklungsbestrebungen als auch den daraus entstehenden Arbeitsprodukten verknüpft. Im Hinblick darauf werden diese Aktivitäten im Zuge eines übergeordneten Managements der funktionalen Sicherheit geplant und koordiniert (siehe Abbildung 5.2).

Des Weiteren werden auch die Relationen zwischen OEM und den jeweiligen Zulieferern berücksichtigt. Dementsprechend wird die Gewährleistung funktionaler Sicherheit nicht nur durch zu verrichtende Entwicklungsaktivitäten, sondern auch durch einen übergeordneten Sicherheitsmanagementprozess gemäß Teil 2 der ISO 26262 und einer sogenannten Sicherheitskultur (engl. *Safety Culture*) unter gleichzeitiger Berücksichtigung der QS, des KM sowie des PM des V-Modells (vgl. Unterabschnitt 3.2.3) maßgeblich beeinflusst.

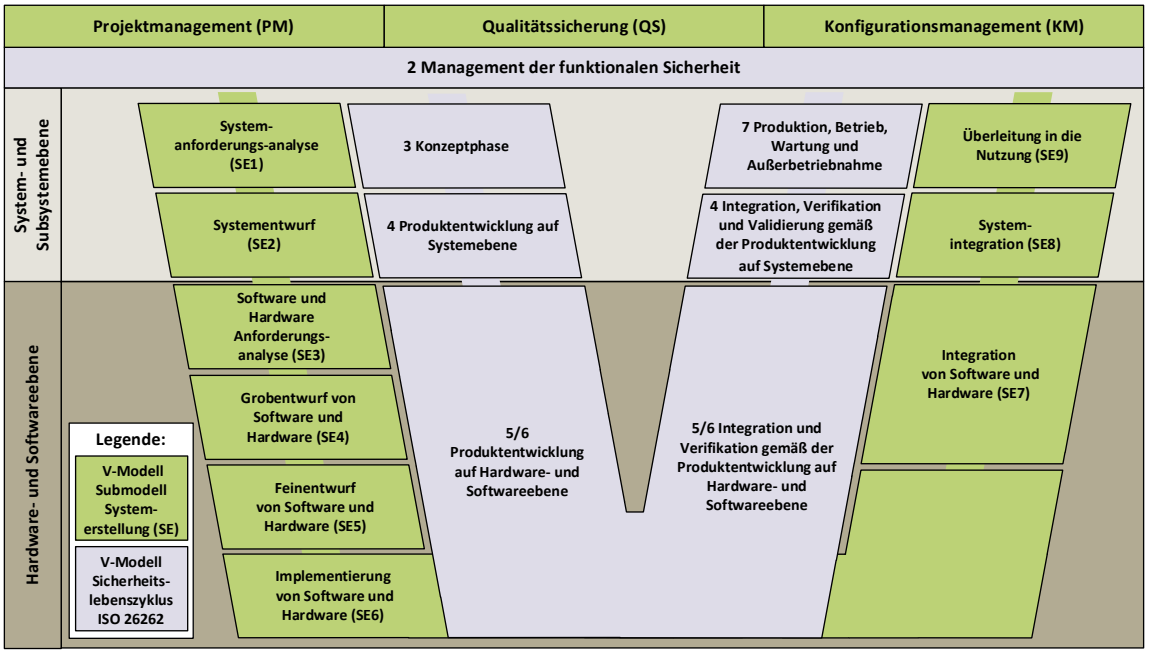


Abbildung 5.2: Einordnung der Teile 3 - 7 des Sicherheitslebenszyklus gemäß ISO 26262 V-Modell in die Phasen des V-Modell Submodell Systemerstellung (SE) unter zusätzlicher Betrachtung des übergeordneten Teil 2 „Management der funktionalen Sicherheit“ und dessen Bezug zum Projektmanagement (PM), zur Qualitätssicherung (QS) und zum Konfigurationsmanagement (KM).

[2] Die Begriffe „sicherheitsbezogen“ und „sicherheitsrelevant“ werden im Rahmen der vorliegenden Dissertation synonym verwendet.

Hinzu kommt die Erstellung eines Sicherheitsplans (engl. *Safety Plan*) und die Dokumentation für den Nachweis der jeweiligen Arbeitsprodukte als auch Rahmenbedingungen der vollständigen Sicherheitsinbetriebnahme. In diesem Zusammenhang werden vor der Freigabe für die Produktion ein Konzept aus Bestätigungsüberprüfungen (engl. *Confirmation Reviews*) aufgesetzt. Diese beruhen auf einer unabhängigen (Unabhängigkeit der Assessoren gegenüber den beteiligten Entwicklungsteams) Beurteilung darüber, ob die Ziele, wie Korrektheit, Vollständigkeit, Konsistenz, Angemessenheit und Inhalte der Arbeitsprodukte, der ISO 26262 erreicht werden.

Insgesamt besteht die ISO 26262 aus 12 Teilen. Teil 1 der ISO 26262 umfasst das Glossar und beinhaltet die relevanten Begriffe, deren Definitionen und Abkürzungen. Die Teile 3 - 7 der ISO 26262 beziehen sich auf die einzelnen Phasen des Sicherheitslebenszyklus, wobei die restlichen Abschnitte phasenunabhängig sind. Teil 8 beschreibt „Unterstützende Prozesse“, Teil 9 umfasst „Automobiles Sicherheitsintegritätsniveau (ASIL)-orientierte und sicherheitsorientierte Analysen“ und Teil 10 liefert anhand praktischer Beispiele den „Leitfaden der ISO 26262“. In Teil 11 wird ein „Leitfaden für die Anwendung der ISO 26262 auf Halbleiter“ und in Teil 12 die „Anpassung der ISO 26262 für Motorräder“ vorgestellt. Im Anhang A.5 werden die für die vorliegenden Dissertation relevanten Teile 2-7 der ISO 26262 und deren Kerninhalte zusammengefasst dargelegt.

Das Grundprinzip der ISO 26262 liegt insgesamt in der Risikominimierung eines zu entwickelnden E/E-Systems. Hierfür werden Sicherheitsziele (engl. *Safety Goal*) mit den Automotive-Sicherheitsintegritätslevel (engl. *Automotive Safety Integrity Level {ASIL}*) zur Prävention oder Minderung von Gefährdungsereignissen spezifiziert, um ein inakzeptables Risiko zu vermeiden. Ein Gefährdungsereignis entsteht aus der Kombination gefährdenden Verhaltens (z.B. ungewollte Fahrzeugbeschleunigung) und einer Betriebssituation bzw. eines Szenarios (z.B. Heranfahren an einen Zebrastreifen oder eine Ampel, Kurvenfahrt, Geradeausfahrt, Fahren bei Regen usw.). Dabei werden mögliche funktionale Fehler (z.B. Verlust der Bremsunterstützung oder fehlinterpretierter Beschleunigungswunsch), ohne auf deren Ursache einzugehen, identifiziert.

Anschließend wird analysiert, wie sich solche Fehlfunktionen auf Fahrzeugebene auswirken und wie stark der Einfluss auf die Kraftfahrzeug- und Verkehrsumgebung (Fahrer, Passagiere, Fußgänger andere Verkehrsteilnehmer etc.) ist. Diese hervorgerufenen Auswirkungen werden anhand der jeweils möglichen Betriebssituationen bzw. des Szenarios untersucht. Die Klassifizierung der Gefährdungsereignisse erfolgt anhand der Schwere (engl. *Severity*) eines möglichen Schadens, der Häufigkeit (engl. *Exposure*) der Betriebssituation bzw. des Szenarios sowie der Beherrschbarkeit (engl. *Controllability*) der jeweils innerhalb eines Gefährdungsereignisses beteiligten Akteure (siehe Tabelle 5.1). Unter Bezugnahme von statistischen Daten, Unfallanalysen sowie Erfahrungswerten basierend auf Expertenwissen erfolgt die ASIL-Klassifizierung der jeweiligen Gefährdungsereignisse.

Die ISO 26262 gliedert die Anforderungen an die Sicherheitssysteme je nach Betriebsart und möglicher Tragweite demnach in vier ASIL- und einer QM-Stufe. Dabei stellt der ASIL die notwendige Risikoreduzierung dar, welche durch eine Sicherheitsfunktion zu erzielen ist. Dabei ist zu beachten, dass QM die niedrigste und ASIL D die höchste Stufe repräsentiert. QM steht für Qualitätsmanagement und verlangt keine zusätzlichen Anforderungen im Sinne der ISO 26262, da impliziert wird, dass die Qualitätsprozesse ausreichend sind, um das identifizierte Risiko zu bewältigen. Dennoch sind auch hierfür funktionale Sicherheitsmaßnahmen durchzuführen.

Tabelle 5.1: Zuordnung der ASIL-Stufen anhand der Stufen der drei Klassifikationen Schwere, Häufigkeit und Beherrschbarkeit (entnommen aus [50]).

Klassifikation der Schwere	Klassifikation der Häufigkeit	Klassifikation der Beherrschbarkeit		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Definition 5.5 Risiko [51].
Risiko (engl. Risk) ist die Kombination aus der Eintrittswahrscheinlichkeit[3] eines Schadens und der Schwere dieses Schadens bzw. dem Schadensausmaß.

Ein Schaden umfasst dabei die Verletzung oder sonstige Schädigung von menschlichem Leib und Leben, Sachwerten oder der Umgebung [51]. Die notwendige Risikoreduzierung umfasst die *„Minderung des Risikos, die erreicht werden muss, um das tolerierbare Risiko für eine bestimmte Situation zu erreichen“* [51], welche durch einzelne oder die Verknüpfung einer Reihe unterschiedlicher Maßnahmen herbeigeführt werden kann. Das tolerierbare Risiko fußt dabei auf Wahrnehmungen und Wertvorstellungen der Gesellschaft als auch deren Akzeptanz einer bestimmten Gefahrensituation [51].

Definition 5.6 Gefahr [100].
Gefahr (engl. Danger) umfasst eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist.

Unter Anwendung von Erfahrungswerten, statistischen Auswertungen aus dem Feld und Schätzungen basierend auf Expertenwissen werden die gesellschaftlichen Wahrnehmungen der Risiken konkretisiert. Das Risiko gemäß der ISO 26262 ergibt sich aus der Häufigkeit und Aufenthaltsdauer im Gefahrenbereich, der Möglichkeit, die Gefährdung zu vermeiden als auch der Wahrscheinlichkeit des unerwünschten Ereignisses sowie potenzieller Schäden.

Definition 5.7 Gefährdung [51].
Gefährdung (engl. Hazard) repräsentiert eine potenzielle Schadensquelle, welche durch das Fehlverhalten eines E/E/PE-Systems hervorgerufen wird.

Definition 5.8 Schaden [50].
Ein Schaden (engl. Harm) bezieht sich auf die Körperverletzung oder Gesundheitsschädigung von Personen.

[3] Die Ermittlung der Eintrittswahrscheinlichkeit beruht auf statistischen Daten oder Schätzungen basierend auf Expertenwissen.

Ferner kann das tolerierbare Risiko mit dem „As Low As Reasonably Practicable“ (ALARP)-Ansatz in Bezug gesetzt werden. Dieser zielt darauf ab, Risiken durch noch vertretbare Maßnahmen so weit zu mindern, um ein vernünftigerweise praktikables Sicherheitsniveau gewährleisten zu können [253]. Demnach ist ein solches Risiko nur dann tolerierbar, wenn weitere Maßnahmen zur Risikominderung nicht durchführbar oder die Diskrepanz zwischen entstehenden Kosten im Verhältnis zur erreichten Risikoreduktion zu groß werden. Die tatsächliche Risikoreduzierung ergibt sich durch Herabsetzung des Schadensausmaßes bzw. der Schadensschwere (logarithmiert S auf der horizontalen Achse) und/oder der Eintrittswahrscheinlichkeit eines Schadens (logarithmiert H auf der vertikalen Achse) (siehe Abbildung 5.3).

Dabei liegt die tatsächliche Risikoreduzierung in der Regel unter dem Grenz- bzw. tolerierbaren Risiko, sprich dem akzeptablen Risiko (siehe Abbildung 5.3). Dieses ist im Hinblick auf das alltägliche Risiko, welchem generell eine Gesellschaft ausgesetzt ist, vergleichsweise gering.

Beim Betrieb sicherheitsrelevanter Systeme kann nicht ausgeschlossen werden, dass diese im Verlauf ihres Lebenszyklus durch Fehler, welche über Abweichungen bis hin zu Ausfällen propagieren (siehe Abbildung 5.4), die Verletzung von Sicherheitszielen und damit Gefährdungen mit Schadensfolge herbeiführen können.

Definition 5.9 Fehler [50].
Ein Fehler (engl. Fault) umfasst eine unnormale Bedingung bzw. einen nicht normalen Zustand, der zum Ausfall eines Systems, Subsystems oder einer Komponente führen kann.

Definition 5.10 Abweichung [50].
Eine Abweichung (engl. Error) kennzeichnet die Diskrepanz bzw. Nichtübereinstimmung zwischen einem berechneten, beobachteten oder gemessenen Wert oder Zustand und dem tatsächlichen, spezifizierten oder theoretisch korrekten Wert oder Zustand.

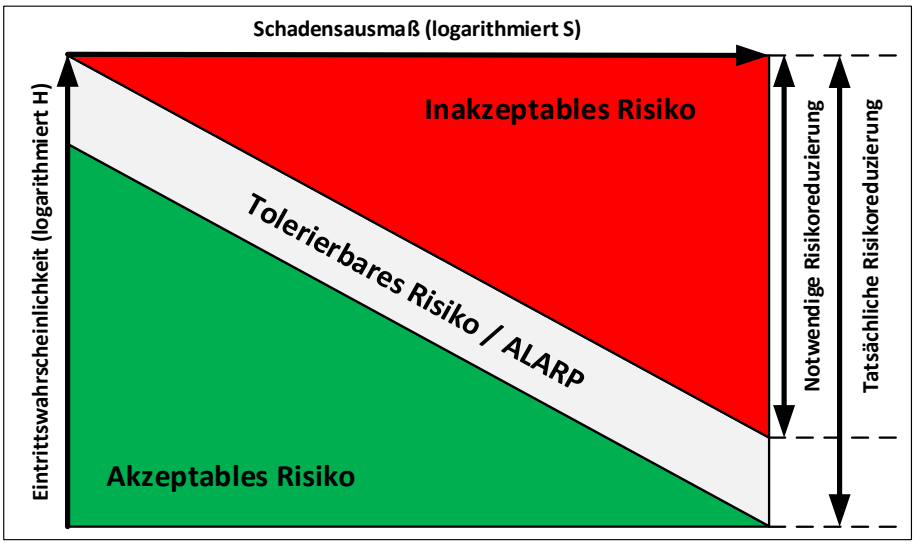


Abbildung 5.3: Allgemeine Darstellung des akzeptablen und nicht akzeptablen Risikos sowie der notwendigen und tatsächlichen Risikominimierung bezüglich des akzeptablen Risikos bzw. ALARP-Prinzips (entnommen aus [254] auf Basis von [50], [255], [51]). Die Abszisse stellt das Schadensausmaß S und die Ordinate die Eintrittswahrscheinlichkeit H logarithmiert dar.

Definition 5.11 Ausfall [50].
Im Zuge eines Ausfalls (engl. Failure) ist ein System, Subsystem oder eine Komponente nicht mehr fähig, aufgrund eines auftretenden Fehlers das ursprünglich beabsichtigte und definierte Verhalten aufzuweisen.

Im Kontext der ISO 26262 können Fehler und Ausfälle je nach ihrem Ursprung in systematische Software- und Hardwarefehler sowie zufällige Hardwarefehler unterschieden werden. Systematische Fehler und Ausfälle charakterisieren sich als deterministisch und können nur durch Verbesserung des Designs, des Produktionsprozesses, der Art und Weise des Betriebs oder anderer Einflussfaktoren ausgeräumt werden. Wesentliche Auslöser für systematische Fehler sind ein unzureichendes Design wie z.B. eine fehlerhafte Hardware- und Softwarespezifikation. Dahingegen erweisen sich zufällige Hardwareausfälle als unvorhersehbar und werden hauptsächlich durch Alterungseffekte oder Umweltfaktoren verursacht.

Für die Erreichung des notwendigen Grads an Sicherheit können unterschiedliche Ansätze und Methoden herangezogen werden. Die Fehlervermeidung (engl. *Fault Avoidance*) nutzt Maßnahmen zur Steigerung der Sicherheit im Zuge des gesamten Entwicklungsprozesses, um Fehler möglichst frühzeitig zu umgehen. In diesem Zusammenhang stehen auf der einen Seite Maßnahmen zur Fehlerverhinderung (engl. *Fault Prevention*) während der Entwurfsphase im Fokus. Hierbei handelt es sich um ein sorgfältigeres Design (Einsatz von statischer Code-Analyse, Anwendung etablierter Entwurfsverfahren und Codierungsrichtlinien beim Softwareentwurf etc.) und den Gebrauch formaler Methoden bei der Systemmodellierung [256], [50], [257]. Auf der anderen Seite haben Maßnahmen zur Fehlerbeseitigung (engl. *Fault Removal*) die Zielsetzung, die Anzahl und Schwere potenzieller Fehler im Zuge der Verifikations-, Validierungs- und Nutzungsphase des Entwicklungsprozesses zu reduzieren. Während der Entwicklung kann hierfür z.B. ein höherer Umfang an Verifikationstätigkeiten mittels entsprechender Testmethoden durchgeführt. Diese werden im Anhang A.5 beschrieben.

Eine weitere Möglichkeit zur Handhabung von Fehlern bieten Maßnahmen der Fehlerakzeptanz (engl. *Fault Acceptance*). Hierbei können zum einen Methoden der Fehlervorhersage (engl. *Fault Forecasting*) zur Bewertung des möglichen Systemverhaltens während den Konzipierungs- und Entwurfsphasen des Entwicklungsprozesses herangezogen werden. Dabei handelt es sich insbesondere um Sicherheitsanalysemethoden. Innerhalb des Automobilbereichs haben sich insbesondere die Gefahren- und Betriebsfähigkeitsanalyse (engl. *Hazard and Operability Study {HAZOP}*), die Fehlerbaumanalyse (engl. *Fault Tree Analysis {FTA}*) sowie die Fehlermöglichkeits- und -einflussanalyse (engl. *Failure Mode and Effects Analysis {FMEA}*) etabliert. Diese gehören zur Gruppe der sequenziellen und aufgrund ihrer Historie zu den traditionellen Sicherheitsanalyseverfahren, welche auf der Zuverlässigkeitstheorie basieren.

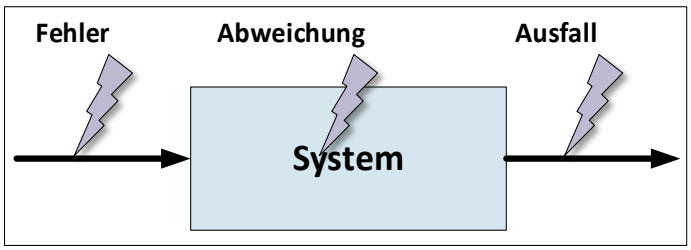


Abbildung 5.4: Propagation eines Fehlers am Systemeingang hin zu einer Abweichung innerhalb des Systems bis hin zu einem Ausfall am Systemausgang (in Anlehnung an [257]).

Auf Basis der Argumentation, dass Gefährdungen als auch Unfälle in immer umfangreicheren als auch softwareintensiveren Systemen nicht mehr rein auf Komponentenausfälle zurückgeführt werden können, entstand in den letzten 20 Jahren eine neue Klasse von Sicherheitsanalysen. Das von Leveson [258] entwickelte „System-Theoretic Process Analysis“ (STPA) beruht auf einem holistischen und systemischen Ansatz und versucht die Struktur sowie das Verhalten aller Arten von Systemen zu verstehen. Dabei wird die Thematik der Sicherheit als dynamisches regelungstechnisches Problem aufgefasst und das System anhand einer Reihe interagierender Komponenten eines Regelkreises abgebildet.

Zum anderen eröffnen Strategien der Fehlertoleranz einen weiteren Weg mit Fehlern während des Betriebs bzw. der Nutzungsphase adäquat umzugehen. Zur Erreichung der gesteckten Sicherheitsziele fordert die ISO 26262 Sicherheitsmaßnahmen und -mechanismen als auch Strategien der Fehlertoleranz, welche im Zuge des funktionalen und dem darauf aufbauenden technischen Sicherheitskonzepts zu entwerfen sind. Diese sind für das Auslösen einer angemessenen Sicherheitsreaktion bei Fehlerauftritt unabdingbar.

Definition 5.12 Sicherheitsmaßnahme [50].
Eine Sicherheitsmaßnahme (engl. Safety Measure) beschreibt eine Tätigkeit oder eine technische Lösung zur Vermeidung bzw. Beherrschung systematischer Ausfälle. Darunter fallen auch Maßnahmen zur Erkennung oder Beherrschung zufälliger Hardwareausfälle bzw. zur Minderung ihrer schädlichen Auswirkungen.

Definition 5.13 Sicherheitsmechanismus [50].
Ein Sicherheitsmechanismus (engl. Safety Mechanism) umfasst eine technische Lösung durch E/E-Funktionen oder -Elemente oder durch andere Technologien (z.B. mechanisch, hydraulisch etc.), um Fehler zu erkennen und diese zu mindern oder zu tolerieren oder einen Ausfall zu kontrollieren oder zu vermeiden, um die bestimmungsgemäße bzw. beabsichtigte Funktionalität aufrecht zu erhalten oder einen sicheren Zustand zu erreichen.

Definition 5.14 Sicherer Zustand [50].
Der sichere Zustand (engl. Safe State) beschreibt den Betriebsmodus eines Systems im Falle eines Ausfalls, ohne dass ein unangemessenes Risiko vorliegt.

Hierbei ergibt sich die Anforderung Ausfälle mit der notwendigen Performanz hinsichtlich des Timings zu detektieren und im Anschluss zu kontrollieren. Der Begriff „Fehlertoleranzzeitintervall“ (engl. *Fault Tolerant Time Interval {FTTI}*) gibt hierfür eine Orientierung. Das FTTI umfasst die minimale Zeitspanne, in der ein Fehler oder mehrere Fehler in einem System vorhanden sein können, bevor ein Gefährdungsereignis eintreten kann [50]. Nachdem ein Fehler aufgetreten ist, breitet er sich im System aus und führt zu Abweichungen, die wiederum einen Ausfall verursachen können. Einige dieser Ausfälle können in Verbindung mit entsprechenden Betriebssituationen Gefährdungsereignisse hervorrufen. Dadurch ergibt sich die Zielsetzung, Sicherheitsmechanismen zu entwerfen, welche die Fehler oder ihre Auswirkungen kontrollieren und einen sicheren Zustand herbeiführen können, bevor das Gefährdungsereignis entsteht.

5.2.2 Sicherheit der beabsichtigten Funktionalität gemäß ISO 21448

Da die Sicherheit der Nominal- bzw. Sollfunktionen nicht explizit in den Betrachtungsrahmen der ISO 26262 fällt, wurde für einen ganzheitlicheren Blick auf die Sicherheit die ISO 21448 „Safety Of The Intended Functionality“ [55] Norm aufgesetzt. Diese stellt Sicherheitsverletzungen bzw. Gefährdungen in den

Mittelpunkt, welche durch Unzulänglichkeiten wie eine unvollständige bzw. nicht ausreichend leistungsfähige Systemspezifikation bezüglich vorhergesehener, aber auch unvorhergesehener Anwendungsszenarien sowie zu erwartendem (Fehl-)[4] Gebrauch von Funktionen des automatisierten Fahrens hervorgerufen werden können. Genauer genommen geht es um die mangelnde Fähigkeit solcher Systeme, gegebene Betriebssituationen korrekt zu erfassen und sicher zu bewältigen als auch um die unzureichende Robustheit gegenüber Sensoreingangsschwankungen oder unterschiedlichen Umgebungsbedingungen. Somit handelt es sich um unsichere Betriebszustände, welche durch das entwickelte System, trotz korrekter Umsetzung aller spezifizierter Anforderungen, eingenommen und folglich zu Schäden führen können. Hinzu kommt die Betrachtung des Aspekts der Sicherheit der Fahrzeugverhaltensspezifikation in punkto sicherer Fahrverhaltensrichtlinien (engl. *Driving Policy*) [55].

Definition 5.15 Sicherheit der beabsichtigten Funktionalität [55].
Die Sicherheit der beabsichtigten Funktionalität (engl. Safety of the Intended Functionality {SotiF}) ist die Abwesenheit von inakzeptablen Risiken aufgrund von Gefährdungen, die sich aus funktionalen Unzulänglichkeiten im Hinblick auf Leistungsfähigkeit, Stabilität und Robustheit der beabsichtigten Funktionalität oder einem angemessenen vorhersehbaren Fehlgebrauch durch Personen ergeben.

Die ISO 21448 definiert eine strukturierte Vorgehensweise anhand von acht sich aneinanderreihenden Phasen bzw. Teile 5 - 13, wobei die Teile 5-11 in das V-Modell gemäß ISO 26262 eingeordnet werden können (siehe Abbildung 5.5). Der Grundsatz der ISO 21448 liegt darin, einen Nachweis über das mögliche Systemverhalten auch bei noch zu Beginn des Entwicklungsprozesses unbekannten Anwendungsszenarien wie unvorhergesehene Fahr- und Verkehrssituationen, unerwartete Wechselwirkungen der Fahrzeugsysteme und deren Kooperation mit dem menschlichen Fahrer im Kontext der Mensch-Maschine-Interaktion zu bewerkstelligen.

Dabei wird eine Argumentation der Abwesenheit eines inakzeptablen Risikos unter Festlegung von Risikoakzeptanzkriterien, z.B. die maximal zulässige Anzahl von Unfällen pro Stunde, gefordert. Die zu begründende Gesamtargumentation des tolerierbaren Risikos muss dabei auf einem oder einer Kombination des GAMAB[5]-, ALARP[6]-, MEM[7]-Ansatzes [55] sowie des Ansatzes einer positiven Risikobilanz (z.B. Restrisiko geringer als Unfallrisiko durch menschliche Fahrer im Zuge des herkömmlichen Straßenverkehrs) beruhen. Insgesamt orientiert sich die grundsätzliche Abfolge der SotiF-Prozessabschnitte an den jeweiligen Phasen der ISO 26262. Im Anhang A.6 werden die Teile 5 - 13 der ISO 21448 und deren zentralen Inhalte zusammengefasst beschrieben.

[4] Zu erwartender Miss- bzw. Fehlgebrauch kann durch übermäßiges Vertrauen in die Leistungsfähigkeit des Systems entstehen, wenn beispielsweise eine explizit für Autobahnbereiche freigegebene automatisierte Fahrfunktion durch den Anwender in urbanen Bereichen aktiviert wird.

[5] GAMAB steht für das französische „Globalement Au Moins Aussi Bon“, was „insgesamt mindestens genauso gut“ bedeutet. Nach diesem Grundsatz ist das Restrisiko (in Bezug auf die Sicherheit) eines neuen Systems nicht höher als das eines bestehenden Systems mit vergleichbarer Funktionalität oder Gefährdungen.

[6] Der „As Low As Reasonably Practicable“ (ALARP)-Ansatz zielt darauf ab, das vorhandene Restrisiko auf ein als „angemessen praktikabel“ angesehenes Niveau zu reduzieren, indem dieses gegen den hierfür benötigten Aufwand abgewogen wird.

[7] Das „Minimal Endogenous Mortality“ (MEM)-Prinzip basiert darauf, dass die Einführung eines technischen Systems die Sterberate innerhalb einer Gesellschaft nicht signifikant erhöhen sollte. Quantitative Akzeptanzkriterien für die durch ein technisches System verursachte Sterbewahrscheinlichkeit werden aus der Mindestwahrscheinlichkeit des Todes durch natürliche Ursachen abgeleitet.

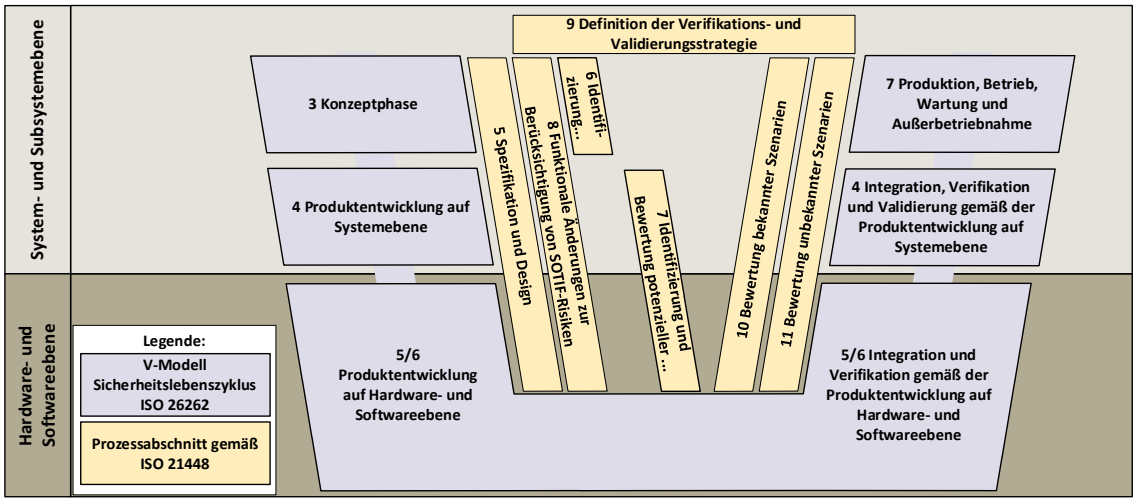


Abbildung 5.5: Einordnung der Teile 5 - 11 der ISO 21448 in die Phasen des V-Modell gemäß ISO 26262.

5.2.3 Sicherheitsbezogene Standards im Kontext des hochautomatisierten Fahrens

Im Kontext des hochautomatisierten Fahrens werden im Zuge der Normungsarbeiten unterschiedliche Standardisierungsansätze diskutiert und veröffentlicht, um die Sicherheitsthematik des hochautomatisierten Fahrens systematisch anzugehen (siehe Abbildung 5.6).

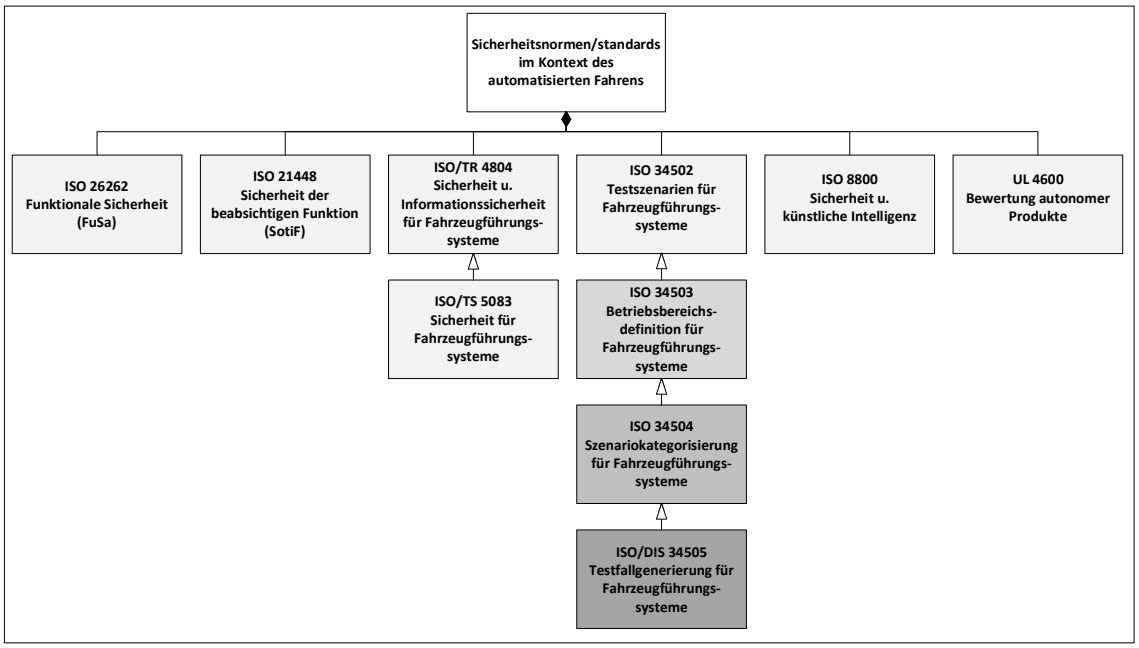


Abbildung 5.6: Automotive-Sicherheitsnormen und -standards im Kontext des automatisierten Fahrens.

Hierbei entstand 2020 aus dem von führenden Vertretern der Automobil- und Mobilitätsbranche 2019 veröffentlichten Whitepaper „Safety First for Automated Driving“ [42], der technische Bericht ISO/TR 4804 „Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation“ [259]. Die ISO/TR 4804 sieht sich als Ergänzung zu den bestehenden Normen und Veröffentlichungen und schlägt einen Rahmen sowie Leitlinien vor, welche sich auf die Sicherheit als auch auf die Informations- und Datensicherheit während der Entwicklung, Verifizierung, Validierung, Produktion und des Betriebs von automatisierten Fahrzeugführungssystemen fokussieren. Diese gelten für alle Entwicklungsbeteiligten, angefangen bei Technologie-Start-ups bis hin zu etablierten OEMs als auch Zulieferern von Schlüsseltechnologien. Erster Grundsatz der ISO/TR 4804 ist die Identifizierung und Vermeidung inakzeptabler bzw. unangemessener Risiken, welche mit dem Betrieb automatisierter Fahrzeugführungssysteme einhergehen können. Die Vermeidung unangemessener Risiken wird hierbei als wesentliche Maßnahme zur Erreichung eines akzeptablen Sicherheitsniveaus angesehen.

Diese beruht auf der Anwendung eines proaktiven und reaktiven Fahrverhaltens, der Vermeidung von Unfällen so weit wie "praktisch möglich" als auch der Vermeidung von rücksichtsloser Benachteiligung ungeschützter Verkehrsteilnehmer seien diese Radfahrer oder Fußgänger. Als zweiter Grundsatz manifestiert sich die Erreichung einer positiven Risikobilanz[8], welche beispielsweise aus Verkehrsunfallstatistiken abgeleitet und im Sinne von Risikoakzeptanzkriterien definiert werden kann. Diese Grundsätze bilden die Basis für die Ableitung der allgemeinen Sicherheitsanforderungen sowie der für die verschiedenen Funktionen des automatisierten Fahrens erforderlichen Maßnahmen über den gesamten Produktlebenszyklus einschließlich Überwachung, Durchführung von Korrekturen und Anpassungen sowie Systemupdates im Feld.

In der Zwischenzeit wurden die Inhalte der ISO/TR 4804 in Richtung einer eigenständigen technischen Spezifikation ISO/TS 5083 „Road vehicles – Safety for automated driving systems – Design, verification and validation“ [261] weiterentwickelt. Diese beschreibt einen Sicherheitslebenszyklus gemäß dem V-Modell, welcher mit einer sogenannten Konzeptuntersuchung beginnt und prozessual bis in die Phase des Betriebs hineinreicht, um Themen der Feldbeobachtung, des Änderungsmanagements, der Inspektion, Wartung und Reparatur sowie des Managements von möglichen Zwischen- und Unfällen abzudecken. Ferner handelt es sich um einen strukturierten im Sinne von sogenannten Behauptungen[9] aufgezogenen Sicherheitsnachweis, welcher systematisch auf Evidenzen[10] als auch Argumenten[11] aufbaut und darlegt, warum ein bestimmtes automatisiertes Fahrzeugführungssystem oder ein Feature davon in dessen Betrieb anhand von gerechtfertigten Risikoakzeptanzkriterien als sicher angesehen werden kann. Aspekte, wie die systematische Herleitung eines Betriebsbereichs sowie die Ableitung von Anwendungsfällen und Testszenarien werden dabei an die ISO 34503 [91] bzw. ISO 34502 „Road vehicles – Test scenarios for automated driving systems – Scenario based safety evaluation framework“ [219], ISO 34504 „Road vehicles — Test scenarios for automated driving systems - Scenario categorization“ [262] und ISO/DIS 34505 „Road vehicles — Test scenarios for automated driving systems – Scenario evaluation and test case generation“ [263] delegiert.

[8] Unter einer positiven Risikobilanz kann beispielsweise aufgefasst werden, dass die Auftretenswahrscheinlichkeit für eine Kollision, welche durch ein hochautomatisiertes Kraftfahrzeug verursacht wird, geringer ist als ein statistischer Vergleichswert von menschlichen Fahrern innerhalb eines definierten Betrachtungszeitraums [260].

[9] Behauptung (vgl. Definition 5.19)

[10] Evidenz (vgl. Definition 5.17)

[11] Argument (vgl. Definition 5.18)

Eine weitere im Zuge der ISO Standardisierungs- und Normungsarbeiten veröffentlichte Norm ist die ISO 8800 „Road vehicles - Safety and artificial intelligence“ [264]. Diese hat zur Zielsetzung, branchenspezifische Leitlinien für den Einsatz von KI und insbesondere von ML-basierten Systemen für sicherheitsrelevante Funktionen von Straßenfahrzeugen zu geben. Hierbei spezifiziert die ISO 8800 einen Rahmen für das Management der Systemsicherheit KI-basierter Funktionen, welcher mit den bestehenden Ansätzen kompatibel ist, welche derzeit in den Normen ISO 26262 und ISO 21448 definiert sind. Einerseits werden Risiken und Fehlfunktionen eines KI-Systems, die im Zusammenhang mit der funktionalen Sicherheit stehen, durch eine Interpretation der relevanten Abschnitte der ISO 26262 Teil 6 und Teil 8 [50] behandelt. Andererseits werden Risiken im Hinblick auf Leistungseinschränkungen des KI-Systems durch eine Erweiterung der Konzepte und Anleitungen der ISO 21448 abgedeckt. Darüber hinaus wird ein V-Modell basiertes Rahmenwerk einschließlich einer zirkulären und iterativen Prozessabfolge beschrieben, welches alle Lebenszyklusphasen angefangen bei der Entwicklung, über die Freigabe für den Betrieb bis hin zum Betrieb selbst behandelt. Das Ganze beruht analog zu den oben beschriebenen Normen und Standards auf einem anhand von Behauptungen aufgezogenen Sicherheitsgewährleistungsnachweis (engl. *Safety Assurance Case*) von KI-Systemen, welcher systematisch auf Evidenzen als auch Argumenten aufbaut.

Der Standard UL 4600 „Evalutation of Autonomous Products“ des American National Standards Institute (ANSI)/Underwriters Laboratories (UL) [265] befasst sich ebenfalls mit der Bewertung von automatisierten Straßenfahrzeugen. Die UL 4600 strebt an, einen systematischen Ansatz einschließlich entsprechender Aufgaben zu definieren, welche bei der Erstellung eines Sicherheitsnachweises zu berücksichtigten sind. Auch hier handelt es sich um die Erstellung eines Sicherheitsnachweises, welcher auf der Generierung von Behauptungen gründet. Dabei handelt es sich um eine robuste Kombination aus Analyse, Simulation als auch Tests für die Bereitstellung eine hinreichende Argumentation, dass ein in Betrieb zu nehmendes automatisiertes Straßenfahrzeug ein angemessenes Sicherheitsniveau erreicht.

5.3 Betriebssicherheit des hochautomatisierten Fahrens

Um die unterschiedlichen Sicherheitsthemen, sprich der funktionalen Sicherheit gemäß ISO 26262 sowie der Sicherheit der beabsichtigten Funktionalität, der Sicherheit der Fahrzeugverhaltensspezifikation und der Gebrauchssicherheit gemäß ISO 21448, bezüglich des hochautomatisierten Fahrens ganzheitlich adressieren zu können, werden diese unter den übergeordneten Begriff der Betriebssicherheit zusammengeführt (siehe Abbildung 5.7).

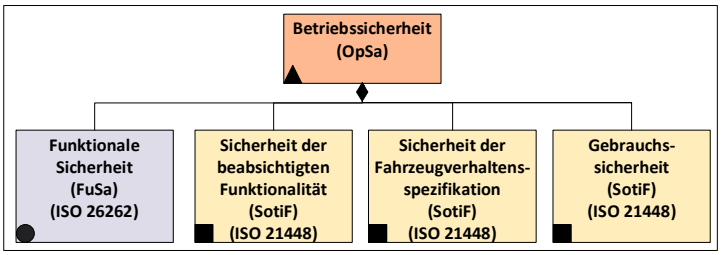


Abbildung 5.7 Hierarchische Dekomposition der Betriebssicherheit in die jeweiligen Sicherheitsthemen gemäß ISO 26262 und ISO 21448.

Definition 5.16 Betriebssicherheit.
Die Betriebssicherheit (engl. Operational Safety {OpSa}) ist die Abwesenheit eines inakzeptablen Risikos im Zusammenhang mit dem gefährdenden Verhalten des Systems hervorgerufen durch:

- *Fehlfunktionen in den an der Ausführung der Funktion beteiligten E/E-Systemen (im Sinne der **funktionalen Sicherheit gemäß ISO 26262**)* [50].
- *Unzulänglichkeiten der Leistungsfähigkeit, Stabilität und Robustheit der beabsichtigten Funktionalität selbst (im Sinne der **Sicherheit der beabsichtigten Funktion gemäß ISO 21448)*** [55].
- *Unzureichende Reaktion auf gefährdende Ereignisse in der Umgebung außerhalb der direkten Steuerung des Systems, z.B. der Bedarf das Risiko im Zusammenhang mit nicht konformem Verhalten anderer Verkehrsteilnehmer so gering wie möglich zu halten (im Sinne der **Sicherheit der Fahrzeugverhaltensspezifikation gemäß ISO 21448**)* [55].
- *Vorhersehbarer, vorsätzlicher oder versehentlicher Fehlgebrauch (engl. Misuse) des Systems sowie Unzulänglichkeiten im Hinblick auf die Mensch-Maschine-Interaktion (im Sinne der **Gebrauchssicherheit gemäß ISO 21448**)* [55].

In diesem Zusammenhang erfolgt die detaillierte Generierung des Betriebssicherheitsnachweises (engl. *Operational Safety Case*) für ein System, welches vollständig in seinen Betriebsbereich integriert ist. Dieser Nachweis wird in Übereinstimmung mit den Vorgaben des QUASAR-Handbuch (Quality Assessment of Software-Intensive System Architectures) [266] erstellt. Diese Vorgehensweise basiert auf der Anwendung der generischen Qualitätsnachweisführungskette, welche ihrerseits die vier wesentlichen Elemente der Evidenz, des Arguments und der Behauptung umfasst. Diese qualitätsorientierte Prozesskette gewährleistet eine umfassende und nachvollziehbare Dokumentation der Betriebssicherheit. Dementsprechend gliedern sich unter der generischen Betriebssicherheitsnachweiskette die Spezifikations- bzw. Liefergegenstände des zu generierenden Betriebssicherheitsnachweises an (siehe Abbildung 5.8).

Angefangen bei den Evidenzen handelt es sich einerseits um die Planungs- und Managementaktivitäten hinsichtlich der Verantwortlichkeiten und Koordinierung der Beteiligten des Entwicklungsvorhabens. Andererseits werden die Anforderungs- und Testfallspezifikation sowie der Architekturentwurf erfasst. Hinzu kommen die Verifikations-, Validierungs- und Testfallresultate des betreffenden Systems eingebettet in den jeweils definierten Betriebsbereich (siehe Abbildung 5.8).

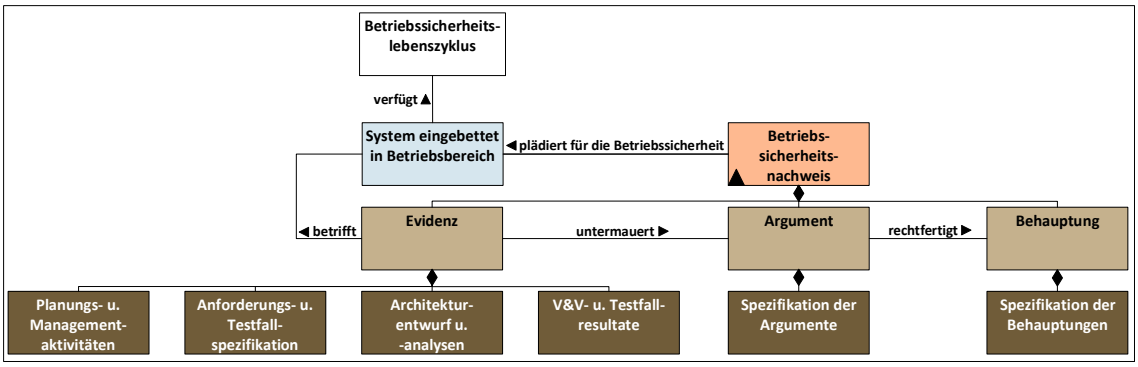


Abbildung 5.8: Hierarchischer Über- und Unterbau der Betriebssicherheitsnachweisführungskette (Evidenz, Argument und Behauptung) für ein System eingebettet in dessen Betriebsbereich.

Definition 5.17 Evidenz [266].
Beweise (engl. Evidences) sind ausreichend glaubwürdige Dokumentationen anhand von textuellen Artefakten, Diagrammen, Modellen etc. oder zu bezeugende (engl. Witnessed) bzw. zu belegende Demonstrationen mit Hilfe von Szenarien, Simulationen als auch Tests realer physischer Artefakte, welche die Argumente der Interessenvertreter bzw. Entwickler untermauern.

Das Argument wird wiederum durch die generierten Evidenzen untermauert. Unterhalb der Argumentklasse ordnet sich die Spezifikation der Argumente ein, welche wiederum die Zielvorgaben, Annahmen und herbeigeführten Entscheidungen im Entwurfsprozess repräsentieren (siehe Abbildung 5.8).

Definition 5.18 Argument [266].
Argumente (engl. Arguments) sind die eindeutigen stichhaltigen Begründungen (engl. Rationals) sowie Planungs-, Strategie-, Entwurfs- und Architekturentscheidungen (engl. Decisions) eines Interessenvertreters bzw. Entwicklers, welche die Glaubwürdigkeit (engl. Credibility) der damit verbundenen Behauptungen rechtfertigen. Anders ausgedrückt handelt es sich hierbei um glaubwürdige (engl. Credible) Begründungen einschließlich Zielvorgaben, Annahmen, Hypothesen und Einschränkungen (engl. Constraint), anhand welcher beispielsweise Assessoren nachvollziehen können, dass das System eingebettet in dessen Betriebsbereich die ihm zugewiesenen Ziele und Anforderungen angemessen erfüllt und diese selbst wiederum valide sind.

Die Behauptungen werden ihrerseits durch das Argumentationsrahmenwerk rechtfertigt. Die daraus abgeleitete Spezifikation der Behauptungen kennzeichnet sich wiederum durch zu erbringende Bestätigungsmaßnahmen[12] (engl. *Confirmation Measures*) (siehe Abbildung 5.8).

Definition 5.19 Behauptung [266].
Behauptungen (engl. Claims) sind nachweisbare Bekräftigungen (engl. Assertions) eines Interessenvertreters bzw. Entwicklers, dass das betrachtet werdende System eingebettet in dessen Betriebsbereich die ihm zugewiesenen Qualitätsziele, z.B. Betriebssicherheit, erreicht.

Insgesamt lässt sich die wesentliche Zielsetzung des Betriebssicherheitsnachweises auf eine anhand von Evidenzen untermauerte glaubwürdige Argumentation im Hinblick auf die Rechtfertigung fünf übergeordneter Behauptungen harmonisieren.

An oberster Stelle steht hierbei die Behauptung, dass das hochautomatisierte Kraftfahrzeug innerhalb seines definierten Betriebsbereichs über den gesamten Betriebssicherheitslebenszyklus frei von inakzeptablen Risiken ist. Diese können wiederum durch

- Fehlfunktionen in den an der Ausführung der Funktion beteiligten E/E-Systemen,
- Leistungseinschränkungen der beabsichtigten Funktionalität selbst,
- eine unzureichende regelkonforme und ethisch vertretbare Fahrzeugverhaltensspezifikation,
- vorhersehbaren, vorsätzlichen oder versehentlichen Fehlgebrauch als auch Unzulänglichkeiten der Mensch-Maschine-Interaktion hervorgerufen werden.

[12] Bei Bestätigungsmaßnahmen handelt es sich um eine Überprüfung, ein Audit oder ein Assessment dahingehend, dass ein Arbeitsprodukt einen ausreichenden als auch überzeugenden Nachweis der Behauptung für dessen Beitrag zur Erreichung der Betriebssicherheit liefert [50].

6 Hochautomatisierung von Kraftfahrzeugen sowie damit einhergehende Herausforderungen

„Die Welt der Zukunft wird einen immer anstrengenderen Kampf gegen die Grenzen unserer Intelligenz bringen."

Norbert Wiener

Die Regelungsmodelle der menschlichen Fahrzeugführung (vgl. Unterabschnitt 2.1.2) bieten Perspektiven, das Ego-Kraftfahrzeug sowie dessen Einbettung in die Kraftfahrzeug- und Verkehrsumgebung im Sinne des fahrzeugexternen Betriebsbereichs systematisch zu betrachten. Diese Konstellation ist gekennzeichnet durch Mensch-Maschine-, Maschine-Maschine- als auch Mensch-Mensch-Interaktionen (siehe Abbildung 6.1). Um diese verhaltensbezogenen Zusammenhänge wahrnehmen, verstehen und schließlich vermitteln zu können, müssen das Ego-Kraftfahrzeug sowie dessen rückgekoppelte Schleifen über den fahrzeugexternen Betriebsbereich erfasst werden, da diese für das situationsbedingte Verhalten maßgeblich sind. Bezugnehmend auf eine Betrachtung von Ego-Kraftfahrzeug und Betriebsbereich werden im Verlauf des nachfolgenden Kapitels die mit der Hochautomatisierung der Fahraufgabe einhergehenden Herausforderungen und Problemstellungen des zu erbringenden Betriebssicherheitsnachweises dargelegt. Des Weiteren erfolgt ein kritischer Diskurs des aktuellen Stands von Forschung, Wissenschaft und Technik sowie die Abgrenzung der im Zuge der vorliegenden Dissertation zu erstellende Konzepte und Inhalte.

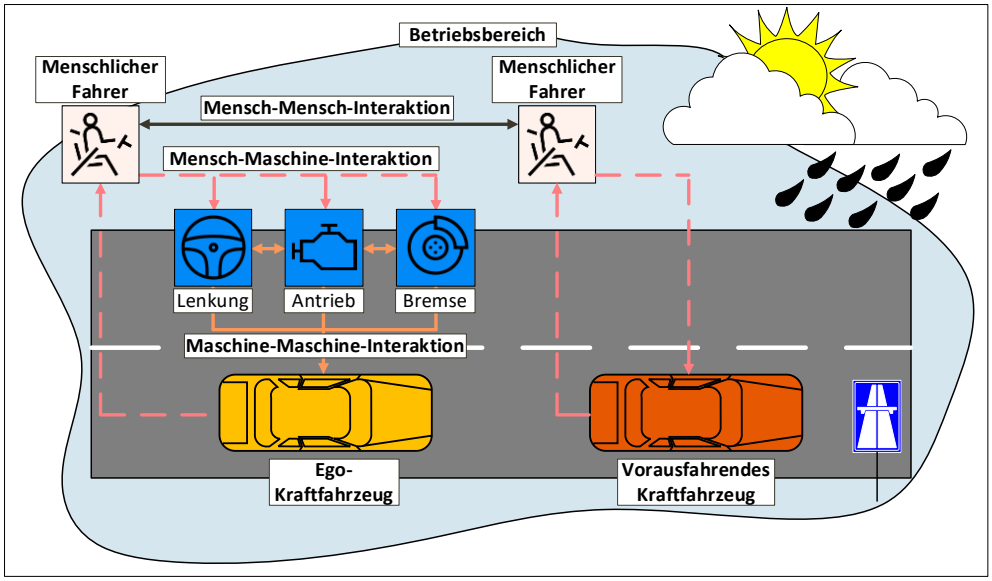


Abbildung 6.1: Ego-Kraftfahrzeug eingebettet in dessen Betriebsbereich (Autobahnabschnitt einschließlich Bedingungen wie Wind und Wetter).

6.1 Vom menschlichen Fahrer zum Fahrzeugführungssystem als Mess-, Steuerungs- und Regelungsinstanz

Vor diesem Hintergrund lässt sich der systemische Verbund menschlicher Fahrer respektive Fahrzeugführungssystem, Ego-Kraftfahrzeug sowie fahrzeugexterner Betriebsbereich (siehe Abbildung 6.1) in eine Regelkreisstruktur überführen (siehe Abbildung 6.2).

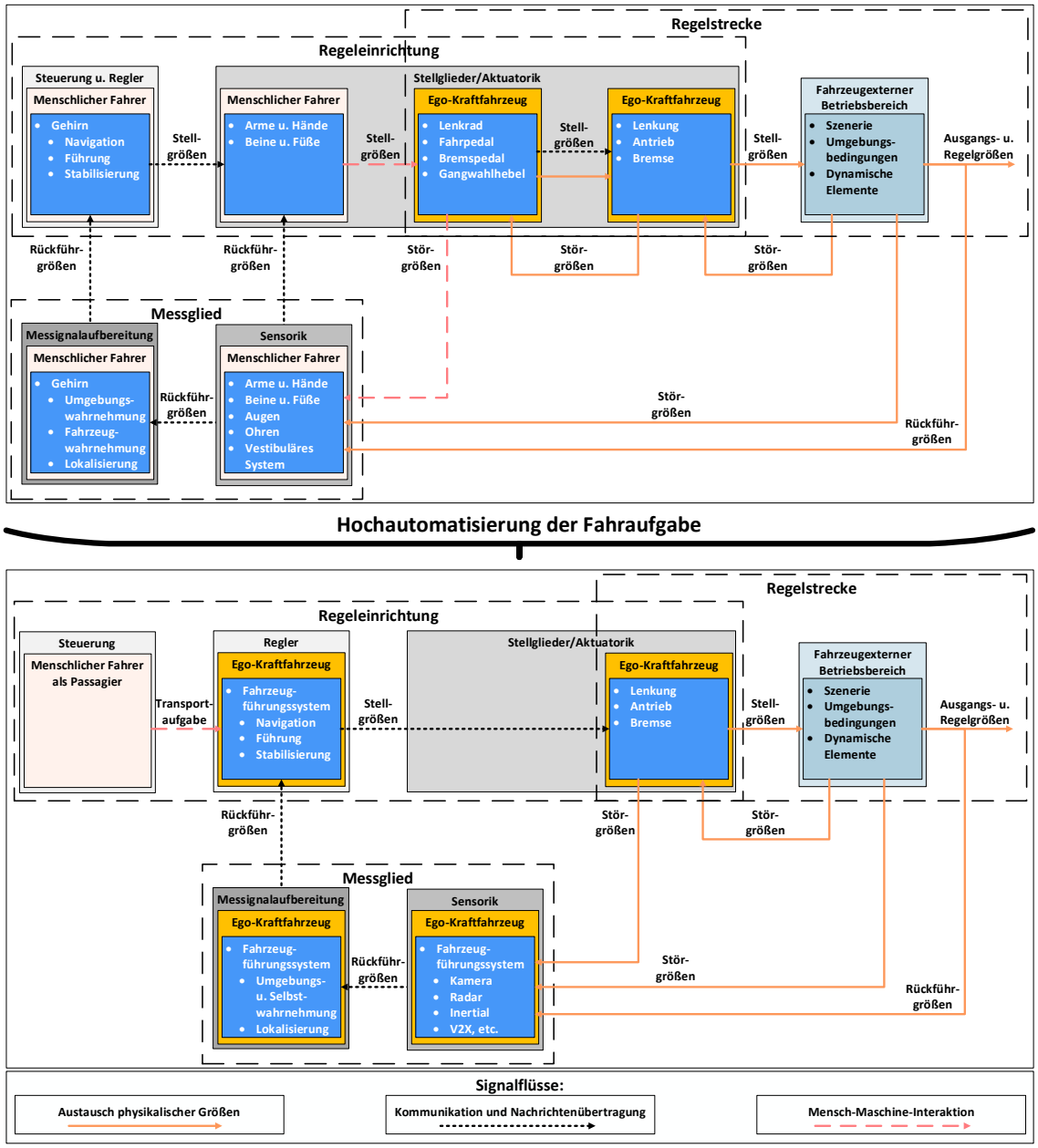


Abbildung 6.2: Übergang vom Regelkreis des menschlichen Fahrers (oben) hin zum Fahrzeugführungssystem (unten) als Mess-, Steuerungs- und Regelungsinstanz des Ego-Kraftfahrzeugs innerhalb des fahrzeugexternen Betriebsbereichs.

Menschlicher Fahrer als Mess-, Steuerungs- und Regelungsinstanz: Bezogen auf diesen Sachverhalt ist der menschliche Fahrer mit den Teilsystemen Ego-Kraftfahrzeug und fahrzeugexterner Betriebsbereich mittels zweier Schnittstellen verknüpft. Anhand der sensorischen Schnittstelle wird der Ist-Zustand der Umgebung und des Ego-Kraftfahrzeugs erfasst. Die sensorische Schnittstelle beinhaltet neben den Instrumenten im Ego-Kraftfahrzeug und den Signalisierungen aus dem fahrzeugexternen[1] Betriebsbereich (visuelle, gestikulierende sowie akustische Signale anderer Verkehrsteilnehmer, Verkehrszeichen, Ampeln, Hinweistafeln usw. bis hin zu akustischem und visuellem Feedback über die Kombiinstrumente innerhalb des Ego-Kraftfahrzeugs) auch Informationen, welche sich aus der Bewegung des Teilsystems Fahrer-Ego-Kraftfahrzeug innerhalb der Kraftfahrzeug- und Verkehrsumgebung ergeben. Über die motorische Schnittstelle, welche sich aus den Bedienelementen, sprich Lenkrad, Pedalen, Schalthebeln, Bedienknöpfen usw. zusammensetzt, wirkt dieser auf das Ego-Kraftfahrzeug als auch den fahrzeugexternen Betriebsbereich ein [64].

Innerhalb der Regeleinrichtung repräsentiert das menschliche Gehirn den Regler, welcher die Verantwortung trägt, Abweichungen zwischen Führungs- und rückgeführter Regelgrößen mit Hilfe der Messglieder zu erfassen als auch auftretende Störgrößen zu kompensieren (siehe Abbildung 6.2). Die Eingänge aus der Informationsaufnahme im Sinne der Umgebungs- und Ego-Kraftfahrzeugwahrnehmung sowie Lokalisierung werden zusammengeführt und aus deren Kombination wird eine kognitive Modellrepräsentation der realen Umwelt wie Zustände des eigenen Fahrzeugs, anderer Verkehrsteilnehmer und Objekte, Straßenverlauf etc. sowie des eigenen Handelns in dieser abgeleitet [78].

Hierbei lässt sich die Qualität der Fahrzeugführung anhand von „physikalisch vorhandenen Akzeptanzgrenzen“ (reale, physische Barrieren wie Hindernisse, Sperren, Leitplanken, Fahrbahnrand, Bordstein etc.), „Warngrenzen“ (Rotlicht einer Lichtsignalanlage, Überholverbote, und auf Seiten des Fahrzeugs Reifendruckwarnung, Abstandswarnungen etc.), „empirischen Akzeptanzgrenzen“ (Normbildung und soziale Konventionen wie z.B. das angemessene Verhalten bei der Vorbeifahrt an Kindern) sowie „forensischen Grenzen“ (Akzeptanzgrenzen wie beispielsweise die zulässige Höchstgeschwindigkeit aus Rechtsvorschriften, Normen, Verkehrsregeln etc.) spezifizieren [217]. Solange keine oder nur geringfügige Abweichungen der jeweiligen Annahmen vom tatsächlich beobachteten Ereignis in der Außenwelt auftreten, verweilt der Prozess der menschlichen Fahrzeugführung im Bereich des Unterbewusstseins. Im Normalfall sind dies Steuerungsaufgaben, welche der Fahrer aufgrund seiner Erfahrung tätigt, exemplarisch sei hier das Einlenken in eine Kurve genannt.

Erst eine Dissonanz zwischen den Modellvorstellungen und den Rückmeldungen aus dem fahrzeugexternen Betriebsbereich, wie beispielsweise der Übergang auf eine unbekannte Fahrtroute oder das Lenkverhalten des Kraftfahrzeugs bei unvorhergesehener Glätte, führt zur Transition in das Bewusstsein und der Fahrer interveniert mit Regeleingriffen. Gemäß der Drei-Ebenen-Hierarchie der Fahraufgabe nach Donges erfolgt dieser Regelungsprozess auf Navigations-, Führungs- sowie Stabilisierungsebene (vgl. Unterabschnitt 2.1.2). Auf Grundlage der dort getroffenen Entscheidungen werden Stellgrößen an die menschlichen Arme, Hände, Beine und Füße kommuniziert, welche auf Seiten des Ego-Kraftfahrzeugs mittels der Mensch-Maschine-Schnittstelle im Sinne von Lenkrad, Fahrpedal, Bremspedal und je nach Konfiguration

[1] An dieser Stelle sei darauf hingewiesen, dass das Ego-Fahrzeug gemäß der ISO 34503 [91] als Element des Betriebsbereichs aufgefasst wird. Um das Ego-Fahrzeug von der Gesamtmenge der Betriebsbereichselemente bzw. -attribute, z.B. andere Verkehrsteilnehmer, Straßen- und Witterungsverhältnisse etc. im Sinne der Szenerie, der Umgebungsbedingungen als auch der dynamischen Elemente, einfacher unterscheiden zu können, werden diese im Zuge der vorliegenden Dissertation unter dem Begriff des fahrzeugexternen Betriebsbereichs adressiert.

auch Gangwahlhebel in Form einer physischen Kraft übertragen werden (siehe Abbildung 6.2). Diese Stellgrößen werden an das Lenk-, Antriebs- und Bremssystem weitergegeben. Hier werden wiederum Drehmomente und Kräfte generiert, welche über die Schnittstelle Rad-Straßenkontakt transferiert werden.

Daraus ergibt sich das dynamische Fahrzeugverhalten anhand der Bewegungsfreiheitsgrade des Fahrzeugkörpers in Bezug zur Kraftfahrzeug- und Verkehrsumgebung als Ausgangs- und Regelgrößen der Regelstrecke. Über die Umgebung wirken wiederum Reaktionskräfte und Störgrößen wie Wind, Spurrillen, Fahrbahnneigungen, Fahrbahnunebenheiten, Schlaglöcher etc., welche entweder direkt über die Sensorik im Sinne der Augen, Ohren als auch des vestibulären Systems wahrgenommen und im Zuge der Umgebungs- und Fahrzeugwahrnehmung verarbeitet werden. Andererseits können Störgrößen über die jeweiligen Fahrzeugsysteme wie Lenkung, Antrieb sowie Bremse bis zur Mensch-Maschine-Schnittstelle propagieren (siehe Abbildung 6.2) und je nach Ausmaß bewusst oder unterbewusst durch den menschlichen Bewegungsapparat ausgeregelt werden.

Für eine bessere Bewältigung der Fahraufgabe erhält der menschliche Fahrer Unterstützung durch Fahrerassistenzsysteme (vgl. Abschnitt 2.2). Trotz dieser Systeme ruht die Verantwortung für das sichere Fahrzeugverhalten im Sinne der Einhaltung von geltenden Verkehrsregeln, der Wahrnehmung und angemessenen Reaktion auf plötzlich auftretende Situationen innerhalb der Kraftfahrzeugumgebung sowie der Beherrschung von Ausfällen oder Leistungsinsuffizienzen der jeweiligen Fahrzeugsysteme wie Antrieb, Lenkung, Bremse als auch entsprechender Fahrerassistenzsysteme wie Abstandsregeltempomat, Spurhalteassistent, Notbremsassistent usw. zu 100 % auf dem menschlichen Fahrer.

Fahrzeugführungssystem als Mess-, Steuerungs- und Regelungsinstanz: Mit der Idee der Hochautomatisierung (vgl. Unterabschnitt 2.2.2) der Fahraufgabe wird der menschliche Fahrer aus diesem Regelkreis herausgenommen und durch das hochautomatisierte Fahrzeugführungssystem ersetzt (siehe Abbildung 6.2). Dadurch kommt der menschliche Fahrer nicht mehr als Rückfallebene in Frage und agiert seitens der Regeleinrichtung innerhalb eines definierten Betriebsbereichs nur noch als Passagier bzw. Steuerung in Bezug auf die vorzugebende Transportaufgabe. Die hierfür benötigten Schnittstellen der Mensch-Maschine-Interaktion, z.B. Bedienknöpfe und -displays was die Thematik der Stellglieder angeht, werden aus Gründen der Übersichtlichkeit nicht dargestellt. Im Bereich Messglied müssen auf der einen Seite Umgebungssensoren wie z.B. Kamera, Lidar, Radar etc. eingesetzt werden, um Informationen über die jeweiligen Elemente aus dem Betriebsbereich erfassen zu können. In punkto aktueller Fahrzeugzustand wird eine Fahrzeugsensorik, wie Odometer, Beschleunigungssensoren, Drehratensensoren etc. benötigt. Ferner müssen je nach Anwendungsfall Daten über GPS, hochauflösende Karten sowie V2X-Kommunkation für die Lokalisierung herangezogen werden (siehe Abbildung 6.2).

Analog zum menschlichen Fahren müssen diese Informationen im Zuge der Messdatenaufbereitung anhand eines inneren Modells der Kraftfahrzeug- und Verkehrsumgebung sowie des eigenen Fahrzeugzustands synthetisiert werden. Das hat zur Folge, dass alle denkbaren Situationen innerhalb des fahrzeugexternen Betriebsbereichs, wie beispielsweise Straßen- und Witterungsverhältnisse, seien diese Nebel, Schnee, Rauch etc., bis hin zu unplausiblem und aggressivem Verhalten anderer Verkehrsteilnehmer sowie Sabotage, wie z.B. das widerrechtliche Entfernen der Straßenbeschilderung vor gefährlichen Streckenabschnitten, dem Fahrzeugführungssystem bekannt sein müssen, damit dieses darauf adäquat reagieren kann. Hinzu kommt analog zum menschlichen Fahren die Thematik der Einhaltung von physikalisch vorhandenen Akzeptanzgrenzen, Warngrenzen, empirischen Akzeptanzgrenzen sowie forensischen Grenzen im Sinne einer sicheren Fahrzeugverhaltensspezifikation.

Ferner muss das Fahrzeugführungssystem in der Lage sein, die Differenz zwischen dem gewünschten Ziel- und dem tatsächlichen aktuellen Systemzustand zu erfassen und wissen, wie die Konfiguration der Aktuatoren, sprich Lenkung, Antrieb und Bremse, angepasst werden kann, um den aktuellen Zustand in Richtung des gewünschten zu forcieren. Das heißt, es muss deren dynamische Input-Output-Beziehung bekannt sein und welche Art von Stimulus verwendet werden muss, um eine gewünschte Reaktion zu erhalten. Bei Soll-Ist-Abweichungen der Regelgrößen muss das Fahrzeugführungssystem folglich die Rolle der Steuerungs- und Regeleinheit übernehmen (siehe Abbildung 6.2). Nach menschlichem Vorbild kann dies auf den Ebenen Navigation (Planung der Route usw.), Führung (Planung der situationsbedingten Manöver wie Fahrstreifenwechsel, Überholen, Abbiegen etc. einschließlich Bestimmung der Fahrzeugsollpose) sowie Stabilisierung (Regelung und Berechnung der Stellgrößen als Beschleunigungs-, Brems- oder Lenkmomentanforderungen) von statten gehen (vgl. Unterabschnitt 2.1.2).

Über die Kraftfahrzeug- und Verkehrsumgebung wirken wiederum Reaktionskräfte auf die sich einstellende Fahrzeugdynamik sowie Störgrößen wie Wind, Spurrillen, Fahrbahnneigungen, Fahrbahnunebenheiten, Schlaglöcher etc. (siehe Abbildung 6.2). Zunächst müssen diese Effekte als solche identifiziert werden können. Anschließend ist zu entscheiden, an welcher Stelle diese Störgrößen kompensiert werden sollen, sei dies auf Seiten der Aktuatoren wie Lenkung, Antrieb und Bremse oder aber auf Stabilisierungsebene der Längs- und Querführung.

6.2 Herausforderungen und Problemstellungen für die System- und Sicherheitsentwicklung

Durch die Hochautomatisierung der Fahraufgabe laufen nun sämtliche Rückkopplungsschleifen, welche vorher entweder durch den menschlichen Fahrer bewältigt und/oder überwacht wurden, über einen festgelegten fahrzeugexternen Betriebsbereich auf das Fahrzeugführungssystem zu (siehe Abbildung 6.2). Ergo verschiebt sich der Verantwortungsbereich für den sicheren Betrieb eines Kraftfahrzeugs vom menschlichen Fahrer vollständig auf das hochautomatisierte Fahrzeugführungssystem. Dies gilt sowohl für die Nominalfunktion der jeweils durchzuführenden Tätigkeiten der strategischen und dynamischen Fahraufgabe (vgl. Unterabschnitt 2.1.1) als auch für die systemische Bereitstellung von Rückfallebenen im Fehlerfall.

Hinzu kommt die notwendige Implementierung von technischen und/oder organisatorischen Maßnahmen für die Kompensation von Unzulänglichkeiten der Leistungsfähigkeit, der Robustheit und des Fehlgebrauchs im Sinne der Gewährleistung der Betriebssicherheit (vgl. Abschnitt 5.3). Dieser Sachverhalt gilt für sämtliche Regelkreisbestandteile, angefangen bei der Sensorik, über die Planungs- und Regelungsalgorithmen, der Aktuatorik bis hin zu unterstützenden V2X-Infrastruktursystemen. Dadurch ergeben sich für die Automotive-System- und Sicherheitsentwicklung im Zuge der nachzuweisenden Betriebssicherheit solcher Systeme vielschichtige Herausforderungen (HF), welche sich anhand entsprechender Schlüsselbereiche gruppieren lassen:

Offener Kontext und Umweltvariabilität des Betriebsbereichs:

HF-1 Vielfalt und Volatilität von Verkehrssituationen und -szenarien aufgrund von „Open-World Problematik“ eines definierten Betriebsbereichs: Der fahrzeugexterne Betriebsbereich umfasst einen im Entwicklungsprozess spezifizierten Teil der Kraftfahrzeug- und Verkehrsumgebung, auf welchen ein hochautomatisiertes Kraftfahrzeug während des Betriebs treffen kann und von diesem sicher gehandhabt

werden muss (vgl. Unterabschnitt 2.2.3). Darunter fallen Einsatzländer, Straßentopologie, Verkehrsregeln und -zeichen, Umgebungsbedingungen wie Nebel, Schnee, Rauch etc., das Vorhandensein eines Mobilfunknetzes für V2X-Kommunikation sowie das dynamische Verhalten anderer Verkehrsteilnehmer wie Kraftfahrzeuge, Passanten oder Tiere. Des Weiteren bezieht sich Problematik des offenen Kontexts auch darauf, dass dieser während des Betriebs des hochautomatisierten Kraftfahrzeugs Änderungen in Form von neuartigen Verkehrsteilnehmern, wie z.B. E-Scootern, Verkehrsschildern, Straßenmarkierungen etc., welche zum Zeitpunkt der Entwicklungsphase noch unbekannt waren, ausgesetzt sein wird.

Dadurch kommt der Thematik der Feldbeobachtung eine neue Bedeutung zu, da das Auftreten als unbekannt bzw. als unsicher zu klassifizierende Ereignisse auch nach Inverkehrbringen der Systeme nicht ausgeschlossen werden kann. Diese funktionalen Unzulänglichkeiten müssen durch eine adäquate Betriebsbereichsüberwachung zur Laufzeit zum einen detektiert, durch Manöver minimalen Risikos, z.B. Anhalten auf dem Standstreifen, gehändelt und zum anderen durch technische Maßnahmen im Nachgang behoben werden.

HF-2 Unmöglichkeit der vollständigen Spezifikation eines definierten Betriebsbereichs infolge des Ausmaßes und der Unvorhersagbarkeit des Entscheidungs- bzw. Zustandsraums: Das Kernproblem bei der Ableitung hinreichend vollständiger Anforderungen besteht im Ausmaß des Entscheidungs- bzw. Zustandsraums im Hinblick auf den offenen Kontext eines definierten Betriebsbereichs (vgl. Unterabschnitt 2.2.3). Hierfür müssen für die jeweiligen Verkehrssituationen und -szenarien angemessene und passende Verhaltensweisen als Grundlage für den Entwurf, die Implementierung als auch die Überprüfung des hochautomatisierten Fahrzeugführungssystems spezifiziert werden. Inkonsistenzen und fehlende Fälle in den Anforderungen können konsequenterweise zu einem unangemessenen oder fehlerhaften Verhalten des hochautomatisierten Fahrzeugs führen.

Dies ist eine wesentliche Schwierigkeit beim Entwurf einer geeigneten Entscheidungslogik, aber auch von Tragweite für die Spezifikation einer Reihe fundierter Tests, bei denen das hochautomatisierte Fahrzeug systematisch mit zweckmäßigen Szenarien konfrontiert werden muss. Daraus ergibt sich auf der einen Seite der Bedarf, den Betriebsbereich durch Abstraktionen auf niedrigere Ersatzmodelle strukturell und modular herunterzubrechen. Unter diesen Umständen erfordert die Unausführbarkeit eines vollständigen Nachweises der Korrektheit im Sinne der Verifikation und Validierung quantifizierbare Metriken und Akzeptanzkriterien der verbleibenden Restrisiken.

HF-3 Statistischer und/oder formaler Nachweis der Leistungsfähigkeit und Robustheit einer positiven Risikobilanz: Bei den Fahrerassistenzsystemen ist eine komfortgetriebene Betrachtung der Auswirkungen von Leistungseinschränkungen, wie z.B. die Unfähigkeit einer Kamera, bei starkem Schneefall fehlerfrei zu sehen oder die mangelnde Robustheit der Fahrzeuglängs- und querführung gegenüber Modellunsicherheiten ausreichend, da stets auf den menschlichen Fahrer im Hinblick auf die Kompensation dieser Unzulänglichkeiten zurückgegriffen werden kann. Beim hochautomatisierten Fahren ist dies nicht mehr möglich, wodurch sich die komfortgetriebene Betrachtung der Leistungsfähigkeit und Robustheit hin zu einer hochsicherheitskritischen verschiebt. Demzufolge müssen dynamische Änderungen der Systemziele, der Funktionalität, der Struktur und des Betriebsbereichs in Echtzeit erfasst und bewältigt werden.

Darunter fallen nichtlinearen Effekte wie Totzeiten, Latenzen, zeitliche Abhängigkeiten, Trägheit, gekoppelten Feedbackschleifen, Zustandsübergänge und Kipppunkte sowohl innerhalb als auch außerhalb der Systeme. Davon sind sämtliche Regelkreisbestandteile, sprich die Sensorik, die Entscheidungslogik, die Aktuatoren sowie fahrzeugexterne V2X-Infrastruktursysteme betroffen. Verstärkt wird dieser Umstand,

wenn es darum geht ein angemessen niedriges Restrisiko zu argumentieren, welches sich aus Imperfektionen von Algorithmen des maschinellen Lernens ergibt. Die Folge ist wiederum ein zusätzlicher Validierungsaufwand mit Blick auf Zuverlässigkeit, Verfügbarkeit, Leistungsfähigkeit und Robustheit im Sinne eines statistischen und/oder formalen Nachweises der positiven Risikobilanz des Gesamtsystems (vgl. Unterabschnitt 5.2.2).

Szenariobasiertes Testen:

HF-4 Prozessuale Einbindung der Simulationsentwicklung inkl. des szenariobasierten Testens in die modellbasierte Sicherheitsentwicklung: Fahrzeugführungssysteme aber auch Fahrzeugsysteme wie Lenkung, Antrieb oder Bremse sind Kompositionen aus Mechanik, Elektronik und Software. Diese Technologien müssen im Zuge des Systementwurfs und der Systemintegration so zusammengeführt werden, dass diese gemeinsam die gewünschte Systemspezifikation bzw. Funktionalität erfüllen. Hierbei ist davon auszugehen, dass hochautomatisierte Fahrzeugführungssysteme iterativ und inkrementell überarbeitet werden müssen. Die Nachvollziehbarkeit und Rückverfolgbarkeit dieser vorgenommenen Änderungen als auch deren Folgen kann unter Bezugnahme von rein statisch beschreibenden Architektursichten und Konsistenzanalysen (vgl. Abschnitt 4.4) jedoch nicht bewerkstelligt werden.

Dies erfordert eine frühzeitige (d.h. während der Konzeptphase) Verifikation und Validierung mittels dynamischen und simulativ ausführbaren Architektursichten (vgl. Anhang A.3, A.4 sowie Abschnitt 4.7). Darunter fällt insbesondere das szenariobasierte Testen (vgl. Abschnitt 4.8) als möglicher Ausweg aus dem Testdilemma des hochautomatisierten Fahrens. Dieser Sachverhalt erfordert demnach die Errichtung der modell- und insbesondere simulationsbasierten Systementwicklung als tragende Säule der durchzuführenden Betriebssicherheitsaktivitäten. Ohne die Bereitstellung dieses Fundaments, können die agilen Vorgehensweisen im Sinne der kontinuierlichen Integration, des kontinuierlichen Testens sowie der kontinuierlichen Bereitstellung (vgl. Unterabschnitt 3.2.5) nicht zweckmäßig in den gesamten Lebenszyklus hochautomatisierter Kraftfahrzeuge eingebunden werden.

Fahrzeugzentrierter versus betriebsbereichszentrierter Sicherheitsansatz:

HF-5 Übernahme und Rückgabe der Verantwortung im Hinblick auf die Durchführung der dynamischen Fahraufgabe: Eine weitere Herausforderung ergibt sich in der angemessenen Rückgabe der Verantwortung der Fahraufgabe an den menschlichen Fahrer vor dem Verlassen eines spezifizierten Betriebsbereichs, wenn das hochautomatisierte Fahrzeugführungssystem beispielsweise nur für den Autobahnbetrieb ausgelegt wurde. Hierbei handelt es sich um sicherheitskritische Aspekte der Mensch-Maschine-Interaktion (vgl. Unterabschnitt 2.2.3) bzw. der Gebrauchssicherheit (engl. *Safety-in-Use*) hinsichtlich der Überwachung der Betriebsbereichsgrenzen zur Laufzeit als auch einer zeitnahen Wahrnehmung einer möglichen Überschreitung dieser. Was einen vorhersehbaren, vorsätzlichen oder versehentlichen Fehlgebrauch angeht, muss zudem sichergestellt werden, dass das hochautomatisierte Kraftfahrzeug beispielsweise außerhalb seines definierten Betriebsbereichs nicht dazu gebracht werden kann, trotzdem die Fahraufgabe zu übernehmen.

HF-6 Beherrschung von tatsächlichen Ausfällen sowie von systematischen als auch zufälligen Fehlern innerhalb des Fahrzeugführungssystems und der jeweiligen Fahrzeugsysteme: Auch in Anbetracht des Aspekts der funktionalen Sicherheit müssen weiterhin Sicherheitsmechanismen konzipiert werden. Die Bedingungen für ein akzeptables Restrisiko im Hinblick auf die funktionale Sicherheit sind in der ISO 26262 festgelegt (vgl. Unterabschnitt 5.2.1). Die Einhaltung dieser Norm bleibt dementsprechend eine notwen-

dige Voraussetzung für den Nachweis der Sicherheit hochautomatisierter Kraftfahrzeuge, um eine zuverlässige und fehlertolerante Implementierung zu gewährleisten. Bisher war es möglich, bei gravierenden Fehlern betroffene Systeme, Subsysteme oder Komponenten und dadurch auch Fahrerassistenzsysteme wie z.B. ein ACC im Sinne von „Fail-Safe“ komplett abzuschalten. Dadurch war es möglich die jeweiligen Systembestandteile mit einem geringeren Sicherheitsniveau und Aufwand zu entwickeln (QM und ASIL A ausreichend in Ausnahmefällen ASIL B z.B. für Notbremsfunktionen).

Da der menschliche Fahrer im Zuge der Hochautomatisierung jedoch nicht mehr als Rückfallebene in Frage kommt, entstehen wesentlich striktere sicherheitsbezogene Verfügbarkeitsanforderungen (ASIL B bis hin zu ASIL D). Dadurch dürfen Fahrzeugfunktionen wie Bremsen oder Lenken während der Fahrt keinesfalls ausfallen oder im Fehlerfall einfach abgeschaltet werden. Dieser Umstand erfordert sogenannte „Fail-Operational-Systeme“, welche auch unter dem Einfluss von Fehlern ihren Zweck ohne eine signifikante Limitierung der Gesamtfunktionalität erfüllen bzw. einen unsicheren Zustand verhindern können. Dies führt aber dazu, dass andersartige Redundanzkonzepte und folglich umfangreichere Systemarchitekturen als auch übergreifende Sicherheitskonzepte bezüglich Fehlertoleranz sowie fehleroperatives Verhalten benötigt werden. Infolgedessen kann die Implementierung von hochautomatisierten Fahrfunktionen in bestehende Fahrzeugplattformen nicht nur als sukzessive Erweiterung zu bestehenden Funktionen betrachtet werden, was wiederum zu einem erhöhten Entwicklungs- und Validierungsaufwand führt.

HF-7 Top-Down-Ableitung des Zusammenspiels auf System-Of-Systemsebene: Die Aspekte der Sicherheit der beabsichtigten Funktion, der Sicherheit der Fahrzeugverhaltensspezifikation sowie der Gebrauchssicherheit werden von der ISO 21448 zwar behandelt (vgl. Unterabschnitt 5.2.2), jedoch nur aus einer Perspektive auf die Systemebene, welche im Zusammenspiel eine Funktionalität auf Fahrzeugebene bereitstellen. Themen, wie der beabsichtigte Gebrauch anhand von Anwendungsfällen sowie die Definition und Herleitung eines Betriebsbereichs, werden lediglich als Input gefordert. Zudem wird auf eine Analyse von relevanten Regularien und rechtlichen Anforderungen aus der Straßenverkehrsgesetzgebung in der ISO 21448 nicht eingegangen, obwohl diese zunehmend an Bedeutung gewinnen und zwingend berücksichtigt werden müssen.

Der Sicherheitslebenszyklus der ISO 21448 orientiert sich am V-Modell der ISO 26262 (siehe Abbildung 5.2), welche sich mit dem Aspekt der funktionalen Sicherheit allein auf Systemebene beginnend und unter Einnahme einer fahrzeugzentrierten Perspektive auseinandersetzt (siehe Abbildung 6.3). Eine systematische Ableitung und ein Verständnis des Zusammenspiels der System-Of-Systems (Ego-Kraftfahrzeug, andere Verkehrsteilnehmer, V2X-Kommunikationssysteme etc.) innerhalb der gesamten Mobilitätsinfrastruktur und ihres Kontexts werden somit innerhalb des aktuellen Automotive-Sicherheitslebenszyklus nicht adressiert.

HF-8 Betriebsbereichszentrierte Perspektive auf das Entwicklungsvorhaben: Insgesamt fehlt eine betriebsbereichszentrierte Perspektive, worin der relevante Straßenverkehrskontext als Teil eines gesamtheitlichen System-Of-Systems-Ansatzes erfasst wird, um eine harmonische Koexistenz der beteiligten Akteure spezifizieren zu können. Dementsprechend ergibt sich eine Lücke in Bezug auf einen ganzheitlichen Betriebssicherheitslebenszyklusprozess, sprich die Ausarbeitung von Anforderungen der jeweiligen Interessenvertreter, insbesondere aus der Gesetzgebung des Straßenverkehrs (vgl. Abschnitt 5.1). Hinzu kommt das Aufsetzen eines architektonischen Rahmens einschließlich Kontext- und Umweltauswirkungen im Sinne einer systematischen Betrachtung und deduktiven Analyse des Betriebsbereichs für die Erhebung von Anforderungen an die zu entwickelnden System-Of-Systems, seien diese das Ego-Fahrzeug selbst oder aber auch unterstützende Infrastruktursysteme (siehe Abbildung 6.3).

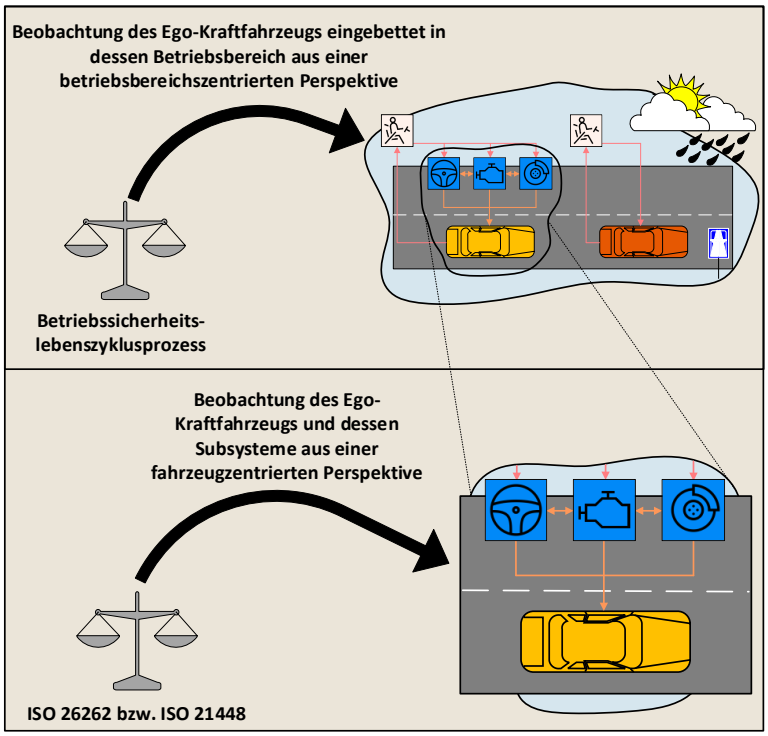


Abbildung 6.3: Betrachtung des Ego-Kraftfahrzeugs eingebettet in dessen Betriebsbereich aus einer übergeordneten betriebsbereichszentrierten Perspektive durch den Betriebssicherheitslebenszyklusprozess, wohingegen die ISO 26262 bzw. ISO 21448 das Ego-Kraftfahrzeug und dessen Subsysteme aus einer untergeordneten fahrzeugzentrierten Perspektive erfassen.

Rechtliche Rahmenbedingungen der Straßenverkehrsgesetzgebung:

HF-9 Einhaltung von Verkehrsvorschriften als auch informellen Verkehrsregeln innerhalb eines definierten Betriebsbereichs: Darüber hinaus gelten für die jeweiligen Konstellationen und Situationen innerhalb des offenen Kontexts rechtliche Anforderungen (vgl. Abschnitt 5.1) was die Einhaltung von Verkehrsvorschriften als auch informellen Verkehrsregeln (Reaktion auf dichtes Auffahren, Abschätzung des Verhaltens anderer Verkehrsteilnehmer etc.) als auch die Ausführung geeigneter Manöver (Ausweichen, Notfallabbremsung, etc.) sowie die Einhaltung von Mindestabständen unter Berücksichtigung der Fahrphysik usw. betrifft. Daraus leitet sich der Aspekt der Sicherheit der Fahrzeugverhaltensspezifikation in punkto sicherer Fahrverhaltensrichtlinien ab. Unter Berücksichtigung der geltenden Vorschriften und vorhandenen Erwartungen muss hierbei spezifiziert werden, welches Fahrzeugverhalten (Manöver, Trajektorien etc.) in welcher Situation angemessen ist. Dies bildet die Grundlage für Überlegungen in Bezugnahme auf funktionale Leistungsbeschränkungen sowie dem benötigten Level an Performanz, ergo welche Grenzen ausreichend und welche unzureichend sind.

Iterativ-inkrementelle Absicherung hochautomatisierter Fahrzeugführungsfunktionen:

HF-10 Systematische Einbindung der V-Modell basierten Sicherheitsentwicklungsaktivitäten in den zeitlich vorgegebenen Ablauf des Automotive-PEP: Im Hinblick auf den zeitlichen Ablauf des Automotive-PEPs (vgl. Abschnitt 3.1) ergibt sich eine weitere Problematik dahingehend, die Sicherheitsentwicklungsaktivitäten gemäß V-Modell (vgl. Unterabschnitt 5.2.1) strukturiert darin einzubinden. Dies ist darauf zu-

rückzuführen, dass die sequenziell Ablaufstruktur des V-Modells den Übergang in die nachfolgenden Entwicklungsphasen nur nach vollständigem Abschluss der vorangegangen vorsieht (vgl. Unterabschnitt 3.2.3). Infolgedessen entsteht die Notwendigkeit, auf der einen Seite die zeitlich und organisatorisch verteilten Entwicklungsphasen inkl. Musterstände, Fahrfreigaben etc. des PEPs sowie auf der anderen Seite die Sicherheitsentwicklungsaktivitäten gemäß V-Modell dergestalt anzupassen, so dass diese im Sinne eines ganzheitlichen Projekt- und Betriebssicherheitsplans miteinander in Einklang gebracht werden können.

HF-11 Prozessuale Unterstützung im Hinblick auf einen iterativen und inkrementellen Sicherheitsentwicklungsprozess gemäß V-Modell: Dem Sachverhalt der iterativen und inkrementellen Entwicklungsweise hochautomatisierter Fahrzeugführungssysteme wird einerseits durch die terminlich strikt zu erreichenden Freigaben und Quality Gates des PEPs (vgl. Abschnitt 3.1) und andererseits die lineare wasserfallartige Struktur des V-Modells (vgl. Unterabschnitt 3.2.3) erschwert, welche den Übergang in die nachfolgenden Entwicklungsphasen nur nach vollständigem Abschluss bzw. Durchlaufen der vorangegangen vorsehen. Dadurch entsteht das Risiko hoher Zeit- und Überarbeitungsaufwände für diejenigen Spezifikationen, welche aufgrund fehlerhafter Annahmen in der frühen Phase der Systementwicklung nur unzureichend ihren Zweck erfüllen. Dies ist darauf zurückzuführen, dass in der Praxis die Anforderungen beim Projektstart nicht vollständig erfassbar sind und erst im Verlauf der weiteren Prozessphasen vollständig, korrekt und konsistent erhoben werden können.

Hinzu kommt die Problematik immer komplexerer software-basierter Funktionalitäten, hervorgerufen durch zunehmende Automatisierung und Konnektivität (vgl. Unterabschnitt 1.1.2). Aufgrund ihres Umfangs können diese Funktionalitäten nicht mehr in Gänze ausgerollt werden, da mögliche Unzulänglichkeiten während der Integrations- und Teststufen (vgl. Unterabschnitt 3.2.3) nur unter hohem Zeitaufwand oder schlimmstenfalls gar nicht mehr nachvollzogen und behoben werden können. Dieser Sachverhalt hat zur Folge, dass gemäß des „Teile und Herrsche“-Prinzips das Entwickeln, Testen und Bereitstellen anhand von inkrementellen Teilfunktionalitäten in den Vordergrund rückt.

Das Spiralmodell nach Boehm beinhaltet ein iteratives und inkrementelles Vorgehen als Kernkonzept (vgl. Unterabschnitt 3.2.2) und verlangt dabei eine fortlaufende Risikobewertung innerhalb jeder Iteration. In hochautomatisierten Fahrzeugführungssystemen sind die potenziellen Risiken umfangreich, da sie sowohl technische als auch regulatorische Aspekte betreffen. Dies führt wiederum zu zeitaufwändigen und ressourcenintensiven Risikobewertungsprozessen, die den Entwicklungsfortschritt verzögern. Hinzu kommt der Umstand, dass in den ersten Phasen des Spiralmodells die Anforderungen unvollständig oder ungenau definiert sind. Für sicherheitskritische Systeme müssen jedoch frühzeitig präzise Sicherheitsanforderungen festgelegt werden. Diese Unsicherheit kann zu Fehlern oder unzureichenden Maßnahmen führen, die in späteren Phasen nur mit hohem Kosten- und Entwicklungsaufwand zu korrigieren sind. Des Weiteren ist für sicherheitskritische Anwendungen eine stabile, langfristige Planung essenziell, um die jeweiligen regulatorische Vorgaben erfüllen zu können. Das Spiralmodell bietet jedoch keine festen Meilensteine oder klaren Zeitpläne, was die Einhaltung externer Vorgaben, wie etwa Zulassungen oder Zertifizierungen, erschwert.

Agile Methoden und Ansätze (vgl. Unterabschnitte 3.2.4 und 3.2.5) motivieren sich aus der höheren Flexibilität von softwaregetriebenen Umfängen im Sinne der inkrementellen Auslieferung von iterativ überarbeiteten Freigaben. Durch die schrittweise Entwicklung vollständiger Inkremente, die regelmäßige Priorisierung und Anpassung der Entwicklungsressourcen, können Unsicherheiten in den frühen Phasen der Funktionsentwicklung ausgeglichen werden. Agile Vorgehensmodelle verfolgen somit einen iterativ-inkrementellen Ansatz, fokussieren sich jedoch auf die reine Erstellung von Arbeitsprodukten und versehen

deren Planung, Steuerung und Dokumentation mit einer geringeren Priorität. Dies steht wiederum im Widerspruch zur grundlegenden Strenge der Sicherheitsplanung sowie der Dokumentations- und Nachweispflicht (vgl. Abschnitt 5.3), welche für die Erreichung der Betriebssicherheit hochautomatisierter Fahrzeugführungssysteme erforderlich ist. Hier spielen die Abstimmung zwischen verschiedenen Verantwortungsbereichen und Domänen, die Planungssicherheit entlang der Lieferketten und klar definierte Entwicklungsziele eine tragende Rolle. Die schrittweise Integration von Software in Hardware und Mechatronik erfordert hierbei eindeutig festgelegte Synchronisierungspunkte. Hinzu kommt der Umstand, dass je nach Art der Systemänderung ein erneuter Zertifizierungsprozess für die Sicherheitskonformität erforderlich werden kann. Dadurch entsteht ein zunehmender Bedarf eines Sicherheitsprozesses, welcher eine kontinuierliche Bewertung und Bereitstellung von sicherheitskritischen softwarebasierten Systemen ermöglicht.

Das Multiple- respektive Agile-V-Modell repräsentiert einen potenziellen Ansatz die Welten des klassischen V-Modells und agiler Entwicklungsansätze zusammenzuführen (vgl. Unterabschnitt 3.2.6). Allerdings ist eine systematische Darlegung, inwiefern und anhand welcher Struktur die jeweiligen Sprints aufzusetzen sind, nicht vorhanden. Dadurch fehlt ein geordnetes Rahmenwerk im Sinne von dedizierten Qualitätskriterien, welche wiederum innerhalb der jeweiligen Sprints bzw. V-Modell Durchläufe zu erreichen sind. Darüber hinaus werden Iterationen und Inkremente weder systematisch zueinander in Bezug gesetzt noch mit dem Ablauf des Automotive-PEPs in Einklang gebracht. Des Weiteren wird nicht aufgezeigt, inwiefern Sicherheitsentwicklungstätigkeiten innerhalb des Multiple- bzw. Agile-V-Modells verankert werden können.

HF-12 Erfassung des dynamischen Entwicklungskontexts einschließlich vorzunehmender Annahmen, Vereinfachungen und Reduktionen: Die im Zuge des Modell- und Architekturentwurfs (vgl. Abschnitt 4.3) herbeigeführten Abstraktionen werden über den gesamten Entwicklungsprozess von verschiedenen Arten von Schlussfolgerungen, Annahmen, Hypothesen und Einschränkungen der beteiligten Interessenvertreter bzw. Akteure (Entwickler, Kunden etc.) begleitet. Hierbei geht es insbesondere um die Vermeidung von schwerwiegenden Fehlentscheidungen als auch fälschlicherweise getätigten Annahmen während des Designprozesses. Einerseits können sich die vorgenommenen Annahmen, Hypothesen und Einschränkungen im Zuge der Interpretation der grundsätzlichen Systemfunktionalität und des Systemkontexts, z.B. Lokalisierung mittels Kamerasensoren innerhalb einer schneebedeckten Fahrbahn, als ungültig erweisen. Ferner können Anforderungen falsch umgesetzt werden, weil sich der spezifizierte Kontext vom tatsächlichen Kontext zu stark unterscheidet und emergente Verhaltensweisen der Realisierung unentdeckt bleiben.

Infolgedessen ergibt sich die Notwendigkeit, die während des Entwicklungsprozesses getroffenen Annahmen, Hypothesen und Einschränkungen als solche kenntlich zu machen sowie für eine lückenlose Nachvollziehbarkeit, Rückverfolgbarkeit und Sicherheitsargumentation zu dokumentieren. Des Weiteren sind für die jeweiligen Annahmen und Modelle Gültigkeitsnachweise herauszuarbeiten. Dabei müssen Hypothesen zunächst aufgestellt und anschließend durch formale Ansätze, Simulationen und Beobachtung der realen Welt verifiziert und validiert werden. Dies erfordert eine umfassende systematische Vorgehensweise im Zusammenschluss mit Verifikations- und Validierungsaktivitäten in Bezug auf die funktionale Sicherheit, die Sicherheit der beabsichtigten Funktion einschließlich der Gebrauchssicherheit als auch der Sicherheit der Fahrzeugverhaltensspezifikation angefangen auf Betriebs- bzw. Fahrzeugebene und damit oberhalb der Systemebene. Da Betriebssicherheit eine Eigenschaft auf Fahrzeugebene ist, muss der kontinuierliche Bereitstellungsprozess von der Software- auf die Fahrzeugebene verlagert werden. Darüber hinaus sind bei sicherheitskritischen Systemen zusätzliche Entwicklungsschritte erforderlich, wie z.B. die

Gefährdungsanalyse und Risikobewertung, die Sicherheitsanalyse der Architektur, die Sicherheitsvalidierung und -zertifizierung (vgl. Abschnitt 5.2).

Kontinuierliche Gewährleistung der Betriebssicherheit im Feldbetrieb:

HF-13 Berücksichtigung der Serienphase innerhalb des Sicherheitsentwicklungsprozesses gemäß V-Modell: Bei der Entwicklung klassischer Fahrzeugsysteme wie Chassis, Lenkung, Antrieb oder Bremse liegt der Fokus weitestgehend auf dem Systementwurfs und der Systemintegration während den Entwicklungsphasen des PEPs (vgl. Abschnitt 3.1). Die Thematik des offenen Kontexts (vgl. HF-1 und HF-2) einerseits sowie die softwaregetriebene Entwicklung hochautomatisierter Fahrfunktionen andererseits, führt jedoch zu einer Verschiebung des Betrachtungsschwerpunkts innerhalb der Automotive System- und Sicherheitsentwicklung. Diese Konstellation erfordert eine zusätzliche Fokussierung und systematische Einbindung der Serienphase bzw. des Feldbetriebs. In dieser Hinsicht ergibt sich die Notwendigkeit, einen iterativen, kontinuierlichen Entwicklungs-, Integrations-, Test- und Bereitstellungszyklus zu etablieren (vgl. Unterabschnitt 3.2.5). Dieser besteht wiederum aus in die Entwurfsphasen systematisch zurückgeführten Feedbackpipelines aufgezeichneter Daten, um dann gemäß der kontinuierlichen Integration, des kontinuierlichen Testens sowie der kontinuierlichen Bereitstellung von inkrementellen OTA-Updates (vgl. Abschnitt 4.2), Anpassungen, Erweiterungen und Verbesserungen ins Feld ausgerollt zu werden.

Insgesamt führt die systematische Herausarbeitung und Strukturierung der Herausforderungen HF-1 bis HF-13 zu einer verdichteten Problemstellung, welche die besonderen Anforderungen an die System- und Sicherheitsentwicklung hochautomatisierter Fahrzeugführungssysteme transparent macht. Die daraus resultierende Problemordnung bildet einen zentralen inhaltlichen Beitrag der vorliegenden Dissertation, da sie als konzeptionelle Grundlage für den entwickelten Betriebssicherheitslebenszyklusprozess dient und dessen Zielrichtung sowie Gestaltungsentscheidungen begründet.

6.3 Lückenanalyse des Automotive Sicherheitslebenszyklus

Die etablierten Normen ISO 26262 und ISO 21448 befassen sich mit Sicherheitsrisiken, die auf klar definierten Systemgrenzen, deterministischen Ausfallursachen und technischen Fehlfunktionen basieren. Dieser Ansatz gerät bei hochautomatisierten Fahrzeugführungssystemen, welche in offenen Kontexten mit nichtlinearen und emergenten Risiken betrieben werden, an seine Grenzen. Im Folgenden werden die im vorangegangenen Abschnitt 6.2 identifizierten Schlüsselbereiche spezifischer Herausforderungen in Bezug auf die Hochautomatisierung der Fahraufgabe herangezogen, um darauf aufbauend eine sogenannte Lückenanalyse (engl. *Gap Analysis*) im Hinblick auf die jeweiligen Phasen und Teile der ISO 26262 (vgl. Unterabschnitt 5.2.1 sowie Abbildung 5.2) und ISO 21448 (vgl. Unterabschnitt 5.2.2 sowie Abbildung 5.5) durchzuführen:

Offener Kontext und Umweltvariabilität des Betriebsbereichs: Das Kernproblem bei der Ableitung hinreichend vollständiger Anforderungen ist die Ausdehnung des Entscheidungsraums in Bezug auf den offenen Kontext eines definierten Betriebsbereichs (vgl. HF-1 und HF-2). Die Undurchführbarkeit eines vollständigen Korrektheitsnachweises im Sinne von Verifikation und Validierung erfordert unter diesen Umständen quantifizierbare Metriken und Akzeptanzkriterien der Restrisiken (vgl. HF-3). Der Betriebsbereich selbst umfasst einen Teil der im Entwicklungsprozess spezifizierten Fahrzeug- und Verkehrsumgebung (vgl. Unterabschnitt 2.2.3), auf die ein hochautomatisiertes Kraftfahrzeug während des Feldbetriebs trifft und die es sicher beherrschen muss (vgl. HF-2). Aufgrund dessen ist es von zentraler Bedeutung, den

Betriebsbereich auf einem angemessenen modellbasierten Abstraktionsniveau strukturell und modular zu zerlegen:

- ISO 26262 (Teil 3 und 4 vgl. Anhang A.5): Die FuSa-Norm geht von einem klar definierten Systemkontext aus, in dem die Risiken anhand definierter Annahmen analysiert werden. In realen Fahrumgebungen bestehen jedoch Unsicherheiten, z.B. durch das unvorhersehbare Verhalten anderer Verkehrsteilnehmer oder wechselnde Umweltbedingungen. Zudem befasst sich die ISO 26262 nicht explizit mit der Definition eines Betriebsbereichs, da sie sich auf eine strenge Sicherheitsbewertung innerhalb festgelegter Betriebsgrenzen als Teil der Item Definition auf Systemebene stützt.

- ISO 21448 (Teil 5 vgl. Anhang A.6): Während die SotiF-Norm Risiken durch unbeabsichtigte Systemreaktionen berücksichtigt, fehlen methodische Ansätze für eine adäquate Modellierung und quantitative Validierung von Unsicherheiten in offenen Kontexten. Hinzu kommt, dass der SotiF-Standard sich nicht mit der Definition eines Betriebsbereichs selbst befasst, sondern diesen als Ausgangspunkt bzw. bereits vorhandenen Input in Teil 5 verlangt. Obwohl die Bedeutung der Betriebsbereichsthematik hervorgehoben wird, fehlt es an präzisen methodischen Spezifikationen für die Bestimmung und Validierung betriebsbereichsbezogener Aspekte.

Szenariobasiertes Testen: Die Beherrschung eines definierten Betriebsbereichs erfordert die Spezifikation von angemessenen und geeigneten Verhaltensweisen für die jeweiligen Verkehrssituationen und Szenarien als Grundlage für den Entwurf, die Implementierung und den Test des hochautomatisierten Fahrzeugführungssystems. Inkonsistenzen in der Spezifikation können zu unangemessenem oder fehlerhaftem Verhalten des hochautomatisierten Kraftfahrzeugs führen (vgl. HF-4):

- ISO 26262 (Teil 3 und 4 vgl. Anhang A.5): Die Testverfahren beruhen auf deterministischen Analysen und Fehlermodellen. Die FuSa-Norm bietet keine methodische Grundlage für die Validierung von sicherheitskritischen Funktionen unter expliziter Berücksichtigung von Verkehrsszenarien.

- ISO 21448 (Teil 5, 10 und 11 vgl. Anhang A.6): Die ISO 21448 erkennt szenariobasierte Tests als kritisch an, bietet jedoch derzeit keine strukturierten Anleitungen zur Definition, Auswahl, Verifizierung und Validierung geeigneter Testszenarien. Darüber hinaus fehlt es der Norm an präzisen Verfahren für unbekannte Szenarien und sie bietet keinen rigorosen Ansatz auf der Grundlage von Argumenten, um eine statistische Vollständigkeit oder Abdeckung zu erreichen.

Fahrzeugzentrierter versus betriebsbereichszentrierter Sicherheitsansatz: Entscheidend ist die Schaffung eines architektonischen Rahmens, der Kontext und Umwelteinflüsse im Sinne einer systematischen Betrachtung und deduktiven Analyse des Betriebsbereichs für die Sammlung von Anforderungen an das System-Of-Systems, sei es das betreffende Fahrzeug selbst oder unterstützende Infrastruktursysteme, einbezieht (vgl. HF-5, HF-6, HF-7 und HF-8):

- ISO 26262 (Teil 3 und 4 vgl. Anhang A.5): Die ISO 26262 befasst sich mit FuSa ausschließlich auf der Systemebene und nimmt dabei eine fahrzeugzentrierte Perspektive (siehe Abbildung 6.3).

- ISO 21448 (Teil 5, 10 und 11 vgl. Anhang A.6): Der Sicherheitslebenszyklus der ISO 21448 folgt dem V-Modell der ISO 26262 (siehe Abbildung 5.5). Allerdings behandelt die Norm SotiF-Aspekte sowie die Sicherheit der Fahrzeugverhaltensspezifikation als auch die Gebrauchssicherheit ausschließlich aus der Perspektive der Systemebene. Folglich liefert ISO 21448 keine systematische

Ableitung und kein Verständnis der Interaktion des Systems der Systeme (Ego-Kraftfahrzeug, andere Verkehrsteilnehmer, V2X-Kommunikationssysteme) innerhalb der gesamten Mobilitätsinfrastruktur im Sinne eines betriebsbereichszentrierten Sicherheitsansatzes (siehe Abbildung 6.3).

Rechtliche Rahmenbedingungen der Straßenverkehrsgesetzgebung: Rechtliche Anforderungen gelten für die jeweiligen Situationen im offenen Kontext, was insbesondere die Einhaltung von Verkehrsregeln und informellen Verkehrsregeln (Reaktion auf Auffahren, Einschätzung des Verhaltens anderer Verkehrsteilnehmer), der Durchführung geeigneter Manöver (Ausweichen, Vollbremsung) und der Einhaltung von Mindestabständen betrifft (vgl. Abschnitt 5.1). Diese Überlegungen, bewährte Praktiken, und gesetzliche Vorschriften bilden zusammen die Grundlage für zur Definition von Richtlinien für sicheres Fahrverhalten (vgl. HF-9):

- ISO 26262 (Teil 3 vgl. Anhang A.5): Die ISO 26262 berücksichtigt die gesetzlichen Anforderungen, bezieht sich aber nicht auf die Ableitung einer sicheren Fahrzeugverhaltensspezifikation.

- ISO 21448 (Teil 5 vgl. Anhang A.6): Die ISO 21448 unterstützt die Spezifikation von Richtlinien für sicheres Fahrzeugverhalten, bringt diese jedoch nicht mit den gesetzlichen Anforderungen in Einklang. Darüber hinaus adressiert sie nicht eine Analyse relevanter Vorschriften und rechtlicher Anforderungen aus dem Straßenverkehrsrecht. Daher bietet die ISO 21448 keine prozessbasierte Integration von Haftungsaspekten, Fahrer- und Fahrzeugverantwortung und länderspezifischen Vorschriften in die Sicherheitsbewertung.

Iterativ-inkrementelle Absicherung hochautomatisierter Fahrzeugführungsfunktionen: Aufgrund des wachsenden Umfangs software-basierter Fahrzeugführungsfunktionen gewinnen iterative und inkrementelle Vorgehensweisen zunehmend an Bedeutung (vgl. HF-10, HF-11 und HF-12). Diese zielen darauf ab, eine sukzessive Realisierung und kontinuierliche Weiterentwicklung unter Bezugnahme gewonnener Daten und Erkenntnisse während der Entwicklungsphase aber auch der Serienphase im Feldbetrieb voranzutreiben (vgl. HF-13):

- ISO 26262 (Teile 2 - 7 vgl. Anhang A.5): Die ISO 26262 ist vornehmlich auf ein linear sequenzielles Vorgehen anhand eindeutig definierter Entwicklungsphasen gemäß des klassischen V-Modells ausgerichtet (vgl. Abschnitte 3.2.3 und 5.2.1). Ergo finden iterativ-inkrementelle Ansätze keine explizite Berücksichtigung, wodurch Anforderungen im Hinblick auf die Absicherung kontinuierlich weiterentwickelter Systemfunktionen sowie stufenweise Teilfreigaben nicht vorgesehen sind.

- ISO 21448 (Teile 5 - 12 vgl. Anhang A.6): Auch die ISO 21448 geht von einer einmaligen und vollständigen Systemanalyse während der Entwicklungsphase aus. Dementsprechend kommt eine strukturierte Vorgehensweise im Hinblick auf eine iterativ-inkrementelle Aktualisierung der zu generierenden Arbeitsprodukte nicht zum Tragen. Insgesamt fehlen Mechanismen zum konsistenten Management von Argumentationslinien, zur Erstellung von Zwischensicherheitsnachweisen für Teilfreigaben sowie zur expliziten Verknüpfung sich verändernder Evidenzen (z. B. aktualisierte Testergebnisse, sich ändernde Betriebsbedingungen) innerhalb der Struktur des zu erstellenden Sicherheitsnachweises.

Kontinuierliche Gewährleistung der Betriebssicherheit im Feldbetrieb: Die Einführung hochautomatisierter Fahrzeugführungssysteme sorgt für eine Verlagerung umfassender Bestandteile des Sicherheits-

nachweises in die Serienphase im Sinne des Feldbetriebs. Aus diesem Grund wird die Fähigkeit, sicherheitsrelevante Veränderungen des Betriebsbereichs, des Nutzerverhaltens, der Leistungsfähigkeit, Robustheit und funktionalen Sicherheit der hochautomatisierten Fahrfunktionen kontinuierlich zu erkennen und darauf zu reagieren, ein Schlüsselfaktor (vgl. HF-13):

- ISO 26262 (Teil 7 vgl. Anhang A.5): Innerhalb der ISO 26262 liegt im Hinblick auf die Gewährleistung der funktionalen Sicherheit der Fokus überwiegend auf der Entwicklungsphase. Dies hat zur Folge, dass Anforderungen an die kontinuierliche Feldbeobachtung, Fehlererkennung und Fehlerbehebung sowie eine proaktive Anpassung sicherheitsrelevanter Funktionen im Feld nicht im Detail betrachtet werden.

- ISO 21448 (Teil 13 vgl. Anhang A.6): Die ISO 21448 befasst sich mit der Absicherung unzureichender Spezifikationen und potenzieller Restrisiken, fokussiert sich dabei aber auch auf die Entwicklungsphase. Mechanismen zur kontinuierlichen Gefahrenanalyse auf Basis von Feldbeobachtungen und zum Management neu auftretender Risiken während des Feldbetriebs (z.B. aufgrund von Änderungen der Verkehrsbedingungen oder des Nutzerverhaltens) werden nicht umfassend behandelt.

6.4 Abgrenzung zum aktuellen Stand von Wissenschaft, Forschung und Technik

Für die Bewältigung der mit der Hochautomatisierung der Fahraufgabe einhergehenden Herausforderungen und Problemstellungen entstehen innerhalb von Industrie und Forschung unterschiedlich geartete Ansätze. Dabei kristallisieren sich verschiedene Entwicklungsströmungen und -aktivitäten heraus, welche sich in Normungs- und Standardisierungsarbeiten, Industrie- und Forschungsprojekten als auch wissenschaftlichen Arbeiten und Veröffentlichungen gruppieren lassen. Nachfolgend werden die für die vorliegende Dissertation relevantesten Vertreter der jeweiligen Gruppierungen vorgestellt, eingeordnet und diskutiert.

6.4.1 Normungs- und Standardisierungsaktivitäten

Um die Limitierungen (vgl. Abschnitt 6.3) der etablierten Automotive-Sicherheitsnormen ISO 26262 und ISO 21448 im Hinblick auf die Betriebssicherheitsthematik des hochautomatisierten Fahrens anzugehen, entstand die technische Spezifikation ISO 5083 „Road vehicles – Safety for automated driving systems – Design, verification and validation“ [261] (vgl. Unterabschnitt 5.2.3). Hierbei werden die jeweiligen Aspekte der Betriebssicherheit, wie der Gebrauchssicherheit (engl. *Human Factors*) im Hinblick auf eine sichere Mensch-Maschine-Interaktion beispielsweise bei der Übernahme der Fahraufgabe einschließlich der Betrachtung eines vernünftigerweise vorhersehbaren Fehlgebrauchs als auch der Sicherheit einer regelkonformen Fahrzeugverhaltensspezifikation behandelt. Jedoch geschieht dies nicht in einem mit der ISO 26262 und ISO 21488 konsistent zusammengeführten prozessualen Gesamtansatz bzw. Betriebssicherheitsnachweis.

Des Weiteren fehlt eine zur ISO 26262 und ISO 21448 konforme systematische Top-Down-Prozessschrittabfolge, um die Entwickler der jeweiligen Sicherheitsdomänen und -aspekte zusammenzubringen. Ferner erfolgt keine Top-Down- und Bottom-Up-Betrachtung des hochautomatisierten Kraftfahrzeugs

einschließlich entsprechender Fahrzeugsysteme eingebettet in einen definierten Betriebsbereich, um die Rückkopplungs- und Regelkaskaden über den fahrzeugexternen Betriebsbereich identifizieren und absichern zu können. Zudem werden Themen, wie die systematische Herleitung eines Betriebsbereichs, als auch die Ableitung von Anwendungsfällen und Testszenarien an die ISO 34503 [91] bzw. ISO 34502 „Road vehicles – Test scenarios for automated driving systems – Scenario based safety evaluation framework“ [219] delegiert (vgl. Unterabschnitt 5.2.3). Die ISO/TS 23792 [267] definiert grundlegende Anforderungen an Autobahn-Chauffeur-Systeme, insbesondere im Hinblick auf die Einhaltung eines definierten Betriebsbereichs und die rechtskonforme Ausführung der Fahraufgabe. Sie bietet jedoch keine Methodik, wie ein Betriebsbereich systematisch definiert werden kann. Auch fehlt ein strukturierter Ansatz zur Analyse des geltenden Straßenverkehrsrechts und dessen Umsetzung anhand eines gesetzeskonformen Fahrzeugverhaltens. Dadurch entstehen im Hinblick auf das hochautomatisierte Fahren eine Vielzahl einzelner Normen, Standards und technischen Spezifikationen (siehe Abbildung 5.6), welche allerdings nicht in einen ganzheitlichen Gesamtansatz zusammengeführt werden. Diese Beschränkungen werden innerhalb des hier zu entwickelnden Betriebssicherheitslebenszyklusprozesses (vgl. Abschnitt 7.2) durch einen strukturierten und zur ISO 26262 und ISO 21448 kohärenten Prozessablauf adressiert.

Der Standard UL 4600 „Evalutation of Autonomous Products“ [265] befasst sich ebenfalls mit der Erstellung eines Sicherheitsnachweises automatisierter Systeme (vgl. Unterabschnitt 5.2.3). Es wird jedoch weder ein strukturierter Gesamtentwurfsprozess beschrieben, noch gibt es Vorgaben oder Hinweise für die Methoden, welche zur Erstellung der jeweils geforderten Arbeitsprodukte eingesetzt werden können. Insgesamt erweist es sich somit als besonders nachteilig, dass die UL 4600 keinen chronologisch ablaufenden und abschnittsweise gegliederten Sicherheitsentwicklungsprozess bereitstellt, sondern ausschließlich Bewertungskriterien der Akzeptanz eines Sicherheitsnachweises definiert.

Die ISO 8800 „Road vehicles - Safety and artificial intelligence“ [264] fokussiert sich darauf, Vorgaben und Richtlinien für den Einsatz von KI und insbesondere von ML-basierten Systemen im Kontext sicherheitsrelevante Funktionen von Straßenfahrzeugen zu definieren. Diesbezüglich beruht das Gesamtvorgehen auf einem anhand von Behauptungen aufgezogenen Sicherheitsgewährleistungsnachweis von KI-Systemen (vgl. Unterabschnitt 5.2.3). Zwar fällt die Entwicklung und Absicherung von KI-Systemen nicht explizit in den Betrachtungsrahmen der hier vorliegenden Dissertation, jedoch bestehen konkrete Analogien zwischen den Vorgehensweisen der ISO 8800 sowie dem im Verlauf dieser Arbeit zu entwerfenden Betriebssicherheitslebenszyklus hochautomatisierter Kraftfahrzeuge.

Darunter fällt der mittels Evidenzen, Argumenten und Behauptungen aufgezogene und auf dem V-Modell basierende Betriebssicherheitsnachweis (vgl. Abschnitt 7.2) einschließlich der methodisch integrierten Iterationsschleifen agiler Vorgehensweisen (vgl. Abschnitt 7.3). Demgemäß ergibt sich eine Möglichkeit für an die vorliegende Dissertation anzuknüpfende zukünftige Arbeiten, die innerhalb der ISO 8800 beschriebenen Aktivitäten nahtlos einzubetten und mit den betriebssicherheitsbezogenen Tätigkeiten zusammenzuführen. Des Weiteren bestünde analog dazu die Option, Themen der Informations- und Datensicherheit gemäß der ISO/SAE 21434 „Road vehicles – Cybersecurity engineering“ [268] in das hier aufzuziehende Gesamtkonzept einzuarbeiten.

6.4.2 Industrie- und Forschungsprojekte

Das Industrie- und Forschungsprojekt PEGASUS [220] (vgl. Abschnitt 4.8) befasst sich mit den oben erläuterten Problemstellungen und Herausforderungen (vgl. Abschnitt 6.2) am Beispiel eines SAE-Level 3 Autobahnchauffeurs für Personenkraftwagen. Dabei wird in Übereinstimmung zur vorliegenden Dissertation

die Empfehlung ausgesprochen, das Aufsetzen einer nachvollziehbaren als auch rückverfolgbaren Sicherheitsargumentation direkt zu Projektbeginn einzuleiten und die Beiträge der einzelnen Arbeitspakete zur Projektstruktur und zur Argumentationskette frühzeitig zu definieren [221]. Allerdings wird im Zuge des PEGASUS Projekts nicht aufgezeigt, inwiefern die jeweiligen Konzepte in einen ganzheitlichen modellbasierten Systementwicklungsansatz integriert werden können. Des Weiteren wird kein umfassender Bezug zu den Sicherheitsnormen ISO 26262 und ISO 21448 hergestellt.

Außerdem liegt eine detaillierte Betrachtung der Architektur des hochautomatisierten Gesamtfahrzeugs oder anderer Systeme nicht im Fokus des Projekts und wird nicht behandelt. Diese Problematik betrifft insbesondere auch das im Zuge des PEGASUS Projekts aufgesetzte 6-Schichtenmodell [269] zur Strukturierung des Betriebsbereichs eines hochautomatisierten Straßenfahrzeugs, welches ferner zur Generierung von Szenarien aus System- bzw. Domänenwissen als auch der Feldbeobachtung herangezogen wird. Dadurch werden die Elemente und Attribute eines Betriebsbereichs auf der einen Seite mit den Systemelementen der Fahrzeugarchitektur auf der anderen Seite nicht adäquat zueinander in Bezug gebracht. Diese Limitierung wird mittels der innerhalb der vorliegenden Dissertation herangezogenen Betriebsbereichsontologie angegangen (vgl. Anhang B.3).

VVM [222], welches u.a. als Nachfolger des PEGASUS-Kooperationsprojekts hervorgeht (vgl. Abschnitt 4.8), beinhaltet ein zur Betriebskonzeptphase (vgl. Abschnitt 7.2) dieser Dissertation inhaltlich vergleichbares „Operational Concept“ auf Höhe des „Capability Layers“. Allerdings ist dieses nicht anhand einer mit der ISO 26262 und ISO 21488 konsistenten prozessualen Abfolge ausgearbeitet. Das Vorgehen eines glaubwürdigen Sicherheitsnachweises ähnelt zwar dem hier zu entwickelnden Betriebssicherheitsnachweis (vgl. Abschnitt 7.2), unterscheidet sich aber dahingehend, dass der Entwicklungsablauf des Betriebssicherheitslebenszyklusprozesses der vorliegenden Arbeit auch mit dem Automotive-PEP sowie mit der agilen DevOps-Herangehensweise entlang von dedizierten Quality Gates zusammengeführt wird (vgl. Unterabschnitt 7.3.2 und 7.3.3). Weiter ist im Hinblick auf VVM anzumerken, dass der Thematik des Verhaltens als auch einer simulativ ausführbaren Verhaltensbeschreibung für eine robuste Generierung von Evidenzen dieselbe Bedeutung zugerechnet wird, wie innerhalb der vorliegenden Dissertation. Dies gilt auch bezüglich einer nachvollziehbaren Dekomposition sowie einer kontinuierlichen Validierung getroffener Annahmen, Einschränkungen, Entwurfsentscheidungen und Begründungen. Das Ganze setzt sich zudem im Hinblick auf eine iterative Entwicklungsweise fort und betrifft ebenfalls die Verknüpfung von Methoden, Artefakten, Evidenzen entlang einer strukturierten und rückverfolgbaren Argumentationskette. Jedoch wird innerhalb von VVM kein kohärenter Bezug zu einem ganzheitlichen modellbasierten Systementwicklungsansatz hergestellt, welcher den Entwurf und die Analyse funktionaler, logischer und technischer Architekturen als auch eine dazu konsistente Verhaltensbeschreibung realisiert (vgl. Abschnitt 7.4).

Neben VVM arbeitet auch die Google-Tochter Waymo an einem glaubwürdigen Sicherheitsnachweis, welcher mittels eines sogenannten Sicherheitsrahmenwerks (engl. *Safety Framework*) entwickelt wird. Der dynamische Ansatz ist ebenfalls anhand von mehreren Schichten bzw. Ebenen (engl. *Layer*) strukturiert. Hierbei zielt dieser entlang von definierten Akzeptanzkriterien auf eine hierarchisch (top-down und bottom-up) gegliederte evidenzbasierte Argumentation einschließlich eines Nachweises der Abwesenheit inakzeptabler Risiken ab, wobei die Risiken auf architekturbezogenene, verhaltens- oder betriebsbedingte Gefährdungen zurückzuführen sind. Darüber hinaus handelt es sich um einen iterativen und zirkulär ablaufenden Lebenszyklus einschließlich expliziter Betrachtung der Betriebsphase, worin die jeweiligen Aktivitäten für die Gewährleistung der Sicherheit als emergente Systemeigenschaft, als akzeptable Vorhersage und/oder retrospektive Beobachtung sowie als kontinuierlicher Vertrauenszuwachs als auch eines fortlaufenden Qualitätsverbesserungsprozesses der Sicherheitsmaßnahmen beitragen [270].

Insgesamt ist der Lebenszyklusgedanke von Waymo bezüglich einer kontinuierlichen Validierung und Konfidenzengenerierung vergleichbar mit dem hier zu entwickelnden Betriebssicherheitslebenszyklusprozess (vgl. Abschnitt 7.2). Des Weiteren herrscht hinsichtlich der Bedeutung der Thematik des Verhaltens als auch eines auf Evidenzen gestützten argumentativ aufgebauten Sicherheitsnachweises unter Berücksichtigung von Sicherheitsnormen wie der ISO 26262 und/oder ISO 21448 sowie dem aktuellen Stand von Wissenschaft und Technik weiterer Konsens. Eine der Problemstellungen und Herausforderung des Waymo-Ansatzes besteht allerdings darin, dass sich nicht alle methodisch generierten Evidenzen gleich schnell entwickeln oder den gleichen Reifegrad aufweisen. Diese Unterschiede können sich dementsprechend in den Sicherheitsargumenten selbst in Bezug auf die jeweiligen Details und/oder Granularität widerspiegeln und müssen mittels dedizierter Synchronisationspunkte aufeinander abgestimmt werden (vgl. Unterabschnitt 7.3.2 und 7.3.3). Des Weiteren wird nicht aufgezeigt, inwiefern der Sicherheitsnachweis mittels eines ganzheitlichen modellbasierten Systementwicklungsansatzes generiert werden kann (vgl. Abschnitt 7.4).

6.4.3 Auswahl veröffentlichter Arbeiten aus Industrie und Forschungseinrichtungen

Die Arbeiten von Burton et al. [271], [272], [273] stützen sich auf die Theorie komplexer Systeme und widmen sich der Zielsetzung, ein pragmatisches Rahmenwerk für das Sicherheitsmanagement automatisierter Systeme zu schaffen. Zweck des Rahmenwerks ist es, konzeptionelle Klarheit über diejenigen Faktoren zu schaffen, welche zu systemischen Fehlern führen können und sich auf die Sicherheit automatisierter Systeme auswirken. Im Fokus steht auch hier der gesamte Produktlebenszyklus einschließlich einer kontinuierlichen Beobachtung und Überprüfung im Feldbetrieb. Ferner geht es um die Entwicklung geeigneter Maßnahmen zur Minimierung oder Abschwächung der daraus resultierenden Risiken. Die dabei adressierten Interessenvertretergruppen beziehen sich auf ein breites Spektrum, angefangen bei Managern, Ingenieuren, politischen Entscheidungsträgern, Regulierungsbehörden bis hin zu Akademikern von Forschungs- und Lehreinrichtungen. Hierfür umfasst das hierarchisch strukturierte Rahmenwerk drei horizontal abgestufte Ebenen, namentlich dem „Governance Layer“ (besteht aus Anreizen und Anforderungen für Organisationen, sich durch direkte Regulierung, so genannte "Soft Law"-Ansätze oder einen Konsens in Form von nationalen und internationalen Standards an bewährte Verfahren zu halten), dem „Management Layer“ (koordiniert die Aufgaben, welche mit der Entwicklung, dem Betrieb und der Wartung der Systeme über die gesamte Lieferkette hinweg verbunden sind) sowie dem „Tasks and Technical Layer“ (umfasst Systementwurf und Sicherheitsanalyseprozess auf Produktebene). Jedoch ist das Rahmenwerk nicht dazu gedacht, bestehende Sicherheitsanalysen und -managementansätze zu ersetzen. Vielmehr bietet es eine zusätzliche Perspektive, welche es ermöglicht, die wahrgenommenen Systemgrenzen, Interessengruppen und Einflussfaktoren zu hinterfragen, um dadurch wiederum eine solidere Grundlage für das Auffinden von Lücken im derzeitigen Sicherheitsdenken zu schaffen und den Kontext für spezifischere Sicherheitsanalysen zu liefern.

In Übereinstimmung mit der vorliegenden Dissertation (vgl. Abschnitt 6.2), ziehen Burton et al. die Schlussfolgerung, dass ein fahrzeugzentrierter Ansatz bei der Entwicklung des sicheren automatisierten Fahrens nicht mehr ausreicht und im Sinne eines ganzheitlichen betriebsbereichszentrierten Ansatzes einschließlich Nutzer, Betreiber und anderen Beteiligten in einem soziotechnischen Umfeld erweitert werden muss. Darunter fällt die systematische Einbeziehung der offenen Kontextthematik eines Betriebsbereiches unter Berücksichtigung der Schwierigkeit der Definition eindeutiger Systemgrenzen. Dies gilt auch

dahingehend, Systeme mit einem akzeptablen Risikoniveau einzuführen und anschließend aktiv zu überwachen und sicherzustellen, dass Verhaltensabweichungen bzw. Diskrepanzen zwischen dem, was vorhergesagt wurde, und dem, was tatsächlich passiert, identifiziert und behoben werden können. Zum gegenwärtigen Zeitpunkt beinhaltet das Rahmenwerk eine gefestigte Struktur, um eine solide Grundlage für ein systemisches Angehen der Problemstellungen und Herausforderungen des hochautomatisierten Fahrens zu liefern. Allerdings ist das Rahmenwerk noch nicht ausgereift genug, um die jeweiligen Problemstellungen im Detail in Angriff zu nehmen und benötigt weitere Verfeinerungen respektive Überarbeitungen.

Die Notwendigkeit eines betriebsbereichszentrierten Ansatzes für die Entwicklung des hochautomatisierten Fahrens wird auch in den Buchveröffentlichungen von H.L. Ross [274], [275] hervorgehoben. H.L. Ross schlägt für die Betrachtung eines zu definierenden Betriebsbereichs für ein hochautomatisiertes Straßenfahrzeug eine Art Vogelperspektive vor, welche die jeweiligen Umweltbedingungen sowie die Elemente statischer und/oder dynamischer Charakteristik systematisch erfasst. Ferner beschreibt H.L. Ross Tätigkeiten für ein Betriebskonzept sowie ein Betriebssicherheitskonzept einschließlich einem Assessment hochautomatisierter Kraftfahrzeuge und betrachtet diese als übergeordnete Erweiterung zu den etablierten Automotive-Sicherheitsnormen ISO 26262 und ISO 21448. Jedoch fehlt eine strukturierte prozessschrittabhängige Ausgestaltung dieser Konzepte. Ferner unterstreicht er den Bedarf eines anhand von horizontalen Ebenen strukturierten modellbasierten Systementwicklungsansatzes, welcher auf jeder Hierarchieebene durch Verifikations- und Validierungstätigkeiten und somit durch Prozessiterationen kontinuierlich begleitet wird. Ein konkretes modellbasiertes Systementwicklungskonzept mit methodischer Darlegung der einzelnen ineinandergreifenden Aktivitäten wird allerdings nicht beschrieben. Es sind genau jene Limitierungen der Grundsatzarbeiten von H.L. Ross, welche durch die im Verlauf der vorliegenden Dissertationen auszuarbeitenden Entwicklungstätigkeiten des Betriebssicherheitslebenszyklus auf Prozessseite (vgl. Abschnitt 7.2) sowie die Anbindung im Hinblick auf die modellbasierte Systementwicklung (vgl. Abschnitt 7.4) auf Methodenseite im Detail adressiert werden.

Werling et al. [276] konzipieren ein sogenanntes „Safety Integrity Framework for Automated Driving“ (SIFAD). Das Rahmenwerk repräsentiert eine umfassende Methode für die Entwicklung, Freigabe und Zulassung automatisierter Fahrzeugführungssysteme der SAE-Stufe 3 (vgl. Unterabschnitt 2.2.2). Im Speziellen werden qualitative Methoden der Systementwicklung mit quantitativen Ansätzen der Statistik kombiniert, wobei die systematische Quantifizierung und Ausbreitung von Unsicherheiten und Risiken durch stochastische Monte-Carlo-Simulation im Fokus stehen (vgl. Abschnitte 4.7 und 4.8). Im Mittelpunkt von SIFAD steht die rigorose Modellierung von Unsicherheiten während des gesamten Entwicklungsprozesses, um eine positive Risikobilanz (vgl. Unterabschnitt 5.2.2) quantitativ nachweisen zu können. Im Gegensatz dazu betont der in dieser Dissertation skizzierte Betriebssicherheitsansatz einen breiteren, vertikal integrierten Sicherheitslebenszyklus, der FuSa, SotiF, konformes Fahrverhalten und Aspekte der Gebrauchssicherheit in einer konsistenten Prozessarchitektur vereint (vgl. Abschnitte 5.3 und 7.2). Während Werling et al. sich primär auf die formale Risikomodellierung und statistische Validierung von Gefahrenszenarien konzentrieren, geht das hier zu gestaltende Betriebssicherheitskonzept über die Risikobewertung hinaus und umfasst die strukturierte Ableitung, Validierung und Verifizierung operativer Betriebssicherheitsziele im gesamten System- und Betriebsbereichskontext. Eine weitere Differenzierung besteht im jeweils gewählten Abstraktionsgrad. Dahingehend fokussiert sich die Arbeit von Werling auf eine detaillierte probabilistische Modellierung von Gefährdungsszenarien, während der im Zuge der vorliegenden Dissertation vorzustellende Betriebssicherheitsansatz Themen der Skalierbarkeit, der normkonformen Prozessintegration, Nachweisbarkeit sowie Rückverfolgbarkeit betont. Allerdings besteht ein vielverspre-

chendes Integrationspotenzial des SIFADs in den hier zu entwickelnden Betriebssicherheitslebenszyklusprozess. An dieser Stelle sind die von Werling et al. entwickelten stochastischen Simulations- und Sensitivitätsanalysetechniken hervorzuheben. Diese könnten die durchzuführenden Tätigkeiten innerhalb von Teil 3-4 „Betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung“ im Hinblick auf die Bewertung von Restrisiken quantitativ verfeinern (vgl. Teil 3-4 Unterabschnitt 7.2.2). Zusätzlich könnte der systematische Umgang von SIFAD mit Unsicherheiten genutzt werden, um die Inhalte von Teil 3-4 „Betriebssicherheitsvalidierung“ weiter zu stärken (vgl. Teil 3-6 Unterabschnitt 7.2.2).

Unter dem Oberbegriff der Straßensicherheit (engl. *On-Road Safety*) beschreibt Czarnecki [277], [278] Sicherheitsanalysemethoden, welche in der Anforderungs- und frühen Entwurfsphase der Entwicklung hochautomatisierter Fahrzeugführungssysteme anzuwenden sind. Die Betriebssicherheitsthematik wird demnach als Straßensicherheit deklariert und analog zur vorliegenden Arbeit im Hinblick auf die Sicherheit des verkehrsregelkonformen Fahrzeugverhaltens, die Sicherheit der beabsichtigten Funktionalität gemäß ISO 21448 sowie die Gefahrenanalyse und Risikobewertung als Teil der funktionalen Sicherheit gemäß ISO 26262 erfasst (vgl. Abschnitt 7.2). Themen der Gebrauchssicherheit im Sinne der sicheren Mensch-Maschine-Interaktion werden allerdings ausgelassen. Einen ähnlichen Weg verfolgen auch Abdulkhaleq et al. [279], wobei diese die Thematik der Gebrauchssicherheit miteinbeziehen und die Gewährleistung der Betriebssicherheit mit Hilfe der STPA-Methode [280] entlang der hierarchisch gegliederten Fahrzeug-, System- und Komponentenebenen angehen. Eine der Beschränkungen des Ansatzes liegt mitunter darin, dass die von Abdulkhaleq et al. vorgestellte Herangehensweise nicht mit einem ganzheitlichen Systementwicklungsansatz in Bezug gesetzt wird. Darüber hinaus werden analytisch dynamische Verhaltensaspekte (vgl. Anhang A.3 und A.4) nicht adressiert.

Ähnlich verhält es sich bei dem von Grabbe et al. [281] umgesetzten systemischen FRAM- (Functional Resonance Analysis Method) Ansatz [282]. Das Ziel von FRAM besteht darin, soziotechnische Systeme in Form von Funktionen und nicht in Form von logischen Elementen zu beschreiben. Das Grundprinzip kennzeichnet sich dadurch, dass zunächst verstanden werden muss, wie ein technischer Prozess im Nominalfall bzw. fehlerfreien Fall abläuft, bevor auf Fehlfunktionen eingegangen werden kann. Diese Denkweise erweist sich isoliert betrachtet als zweckmäßig. Allerdings besteht bei FRAM die Problematik, dass die zu betrachtenden Elemente über mehrere Hierarchieebenen hinweg nicht durchgängig nachvollziehbar analysiert werden können. Dieser Sachverhalt manifestiert sich darin, dass die grafische Darstellung des FRAM-Ansatzes bei umfangreichen funktionalen Architekturen unübersichtlich wird. Dementsprechend erschwert dies den Einsatz von FRAM in Verbindung mit modellbasierten Systementwicklungsmethoden. Zudem können mit FRAM keine analytisch dynamischen Verhaltensweisen (vgl. Anhang A.3 und A.4) erfasst und bewertet werden.

Post und Davey [283] befassen sich mit der Thematik der Betriebssicherheit, lassen jedoch Themen der klassischen funktionalen Sicherheit außen vor. Ferner verwenden diese ein agiles Systementwicklungsrahmenwerk in Verbindung mit SysML und STPA. Ähnlich gehen Ahlbrecht und Betram [284] vor, welche ein modellbasiertes Systementwicklungskonzept für eine frühzeitige Sicherheitsabwägung gemäß ISO 26262 unter Anwendung von SysML und STPA präsentieren. Meyer et al. [285] stellen fest, dass sich die modellbasierte Systementwicklung innerhalb der Automobilindustrie erfolgreich als Wegbereiter für den Entwurf umfangreicher Systeme und Tests bewährt hat, die gängigen Verfahren aber weder szenariobasierte Testmethoden noch Aspekte der Sicherheit der beabsichtigten Funktionalität gemäß ISO 21448 berücksichtigten. In ihrem Beitrag wird eine erweiterte Variante des etablierten „feature-driven“ Systementwicklungsverfahrens „Compositional Unified System-Based Engineering“ (CUBE) [286] vorgestellt, welche

die Analyse von Anwendungsfällen und Szenarien miteinschließt. Mit Hilfe von SysML-Profilerweiterungen werden anwendungsfallspezifische Szenarien und die dazugehörige Verhaltens- und Systemarchitektur eines „Parkhaus-Chauffeurs“ im Sinne von strukturellen und verhaltensbezogenen SysML-Sichtenmodellen (vgl. Abschnitt 4.5) spezifiziert. Weitere damit vergleichbare Ansätze werden in [287], [288], [289] vorgestellt. Insgesamt lassen sich innerhalb der in diesem Absatz aufgezählten wissenschaftlichen Arbeiten, insbesondere Beschränkungen im Hinblick auf eine ganzheitliche Betriebssicherheitsbetrachtung identifizieren.

Kröger [290] befasst sich mit der grundlegenden gesellschaftlichen und regulatorischen Frage: „Wie sicher ist sicher genug?“ für hochautomatisierte Kraftfahrzeuge. In seiner Publikation schlägt er quantifizierbare Risikoakzeptanzkriterien vor, die auf statistischen Unfallanalysen und branchenvergleichenden Benchmarks basieren. Kröger betont zwar die soziotechnischen Dimensionen der Betriebssicherheit, sein Rahmenwerk bietet jedoch keine strukturierte Methode zur Operationalisierung dieser Risikostufen im Rahmen eines Systementwicklungsansatzes. Der Betriebssicherheitslebenszyklusprozess hier bietet einen möglichen Weg diese Lücke zu schließen (vgl. Abschnitt 7.2). Dabei werden gesellschaftliche Risikoerwartungen in explizite, überprüfbare Anforderungen an die Betriebssicherheit übersetzt, welche ihrerseits in die Lebenszyklusentwicklung und Validierungspraktiken integriert sind.

Was die Definition, Entwicklung und Überwachung eines Betriebsbereiches angeht, so verdeutlichen Mehlhorn et al. [291] die Fragmentierung der Betriebsbereichsforschung und betonen die Notwendigkeit standardisierter Taxonomien und Modellierungsmethoden. Allerdings wird auf eine prozessorientierte Integration der Betriebsbereichsthematik in den breiteren Sicherheitslebenszyklus nicht eingegangen. Der im nachfolgenden Kapitel zu gestaltende Betriebssicherheitslebenszyklusprozess nimmt darauf Bezug, indem die Betriebsbereichsmodellierung direkt in normative Sicherheitsprozesse eingebettet und so eine strukturierte operative Gefahrenanalyse und -verifizierung über den gesamten Systemlebenszyklus ermöglicht wird (vgl. Abschnitt 7.2).

Wang et al. [292] bieten eine Übersicht über die Herausforderungen, welche mit der Sicherheit der beabsichtigten Funktionalität im Sinne von SotiF (vgl. Unterabschnitt 5.2.2) hochautomatisierter Fahrfunktionen einhergehen. Dabei stehen Problemstellungen der Verifikation und Validierung im Kontext ML-basierter Systeme im Fokus. Ihr Beitrag schlägt jedoch keinen einheitlichen Betriebssicherheitslebenszyklus oder Rückverfolgbarkeitsmechanismus über System- und Betriebsbereiche hinweg vor. Das im Verlauf der vorliegenden Arbeit zu konzipierende Betriebssicherheitsrahmenwerk integriert SotiF explizit in dessen normatives Grundgerüst (vgl. Abschnitt 7.2) und bietet damit eine direkte Erweiterung der Analyse von Wang et al.

Correa-Jullian et al. [293] präsentieren eine strukturierte Vorgehensweise, was die Gefahrenanalyse von hochautomatisierten Fahrzeugflotten angeht. In dieser Hinsicht leistet ihre Arbeit einen Beitrag in Bezug auf Risiken der Mensch-Maschine-Interaktion im Kontext von hochautomatisierten Mobilitätsdienstleistungen (engl. *Mobility-as-a-Service*). Sie konzentriert sich jedoch vornehmlich auf die Identifikation von Gefährdungen, ohne einen kohärenten Rahmen für Zielformulierung, Anforderungsmanagement und Validierung über den gesamten Lebenszyklus hinweg zu bieten. Innerhalb des hier vorzuschlagenden Betriebssicherheitslebenszyklusprozesses könnte die strukturierte Gefahrenidentifizierungsmethode von Correa-Jullian et al. als ergänzender Ansatz in der Phase der operativen Gefahrenanalyse (vgl. Teil 3-4 Unterabschnitt 7.2.2) dienen, um u.a. die Risikomodellierung von Mobilitätsdienstleistungen voranzutreiben.

Ein sogenannter „Connected Dependability Cage-Ansatz“ wird von Aniculaesei et al. [294] vorgeschlagen. Dieser hebt die kontinuierliche Laufzeitüberwachung des Betriebsbereichs und Fail-Operational-Strategien über Remote-Kommandozentralen hervor. Obwohl ihr Fokus auf die Laufzeitüberwachung innovativ ist, bleibt er weitgehend reaktiv und es fehlt eine tiefe Integration in frühe Entwicklungsphasen wie Gefahrenidentifizierung, Konzeption eines Betriebssicherheitskonzepts und normative Rückverfolgbarkeit, wie sie der hier aufzusetzende Betriebssicherheitsansatz vorsieht. Eine mögliche Integration in das übergeordnete Betriebssicherheitsrahmenwerk liegt in der Erweiterung der Überwachungsebene der Serienphase hinsichtlich der Laufzeitvalidierung eines definierten Betriebsbereichs (vgl. Teil 8-7 Unterabschnitt 7.2.3).

Hanselaar et al. [295] stellen eine sogenannte „Safety Shell“ vor. Diese repräsentiert eine skalierbare und redundante Mehrkanalarchitektur, welche funktionale Insuffizienzen der Performanz und Robustheit mit Hilfe von Arbitrierungsmechanismen mindert. Der vorgestellte Architekturansatz priorisiert Verfügbarkeit und Sicherheit durch Laufzeitentscheidungen, geht aber nicht darauf ein, wie Betriebssicherheitsziele systematisch abgeleitet, überprüft und validiert werden.

Stoffel et al. [296], [297], [298] stellen eine Reihe von Beiträgen vor, die sich mit der Herausforderung der Betriebssicherheit in hochautomatisierten Fahrzeugen durch innovative Redundanz- und Fail-Operational-Strategien befassen (vgl. HF-6). Darunter fällt ein Voter-Konzept, welches serviceorientierte Architekturen nutzt, um die funktionale Integrität verteilter, über Ethernet verbundener elektronischer Steuergeräte zu gewährleisten (vgl. Abschnitt 4.2). Durch die Dezentralisierung der Fehlererkennung im Sinne von „Voter-as-a-Service“-Mechanismen überwinden Stoffel et al. die Leistungseinschränkungen herkömmlicher Lockstep-Prozessoren. Darauf basierend erweitern die Autoren den Voter-Ansatz zu einer sogenannten „On-Demand Triple Modular Redundancy“-Architektur. Die Arbeiten von Stoffel et al. konzentrieren sich hauptsächlich auf Laufzeitfehlererkennung und dynamische Rekonfigurationsmechanismen. Genau an dieser Stelle ergibt sich allerdings ein aussichtsreiches Integrationspotenzial. Insbesondere das von Stoffel et al. entwickelte Konzept der verteilten Voter und die bedarfsgesteuerten Redundanzmechanismen könnten die Laufzeitabsicherungsschicht in Bezug auf den Prozessabschnitt des Betriebssicherheitskonzepts stärken (vgl. Teil 3-5 Unterabschnitt 7.2.2).

Ein innovatives Sicherheitsrahmenwerk, welches auf der Definition, Überwachung und Funktionsdegradation von Betriebsbereichen basiert, stellen Jiang et al. [299] vor. Zentrales Element des Rahmenwerks ist ein Ansatz, welcher kausale Inferenzmodelle und fahrdynamische Stabilitätsanalysen kombiniert, um daraus Betriebsbereichsgrenzen ableiten und zur Laufzeit überwachen zu können. Diese neuartigen Echtzeit-Überwachungstechniken verfügen über ein vielversprechendes Potenzial, innerhalb des hier aufzusetzenden Betriebssicherheitskonzepts eingebettet zu werden (vgl. Teil 3-5 Unterabschnitt 7.2.2).

Um die Sicherheitsargumentation von hochautomatisierten Fahrzeugführungssystemen zu untermauern, schlagen Weissensteiner et al. [300] einen betriebsbereichsbedingten Abdeckungsansatz vor. Darunter fallen Methoden zur quantifizierbaren Betriebsbereichsabdeckung sowie eine Risikometrik, welche durch ein szenariobasiertes Sicherheitsvalidierungsrahmenwerk unterstützt wird.

Im Kontext des szenariobasierten Testens sind zudem die Forschungsarbeiten des ITIV sowie des FZI hervorzuheben (vgl. Unterabschnitt 4.8.2). Pfeffer et al. [211], [223], [224] haben maßgeblich zum szenariobasierten Testen und zur simulationsgestützten Validierung hochautomatisierter Fahrsysteme beigetragen. Im Zuge seiner Arbeiten wird ein systematischer Ansatz zur Generierung, Metabeschreibung und Kategorisierung von Fahrszenarien basierend auf realen und synthetischen Daten vorgestellt. Insbeson-

dere Pfeffers Szenario-Metamodell ermöglicht die effiziente Kodierung von Verkehrsszenarien durch tensorbasierte Darstellungen, wodurch maschinelle Lernverfahren neue und kritische Fahrsituationen erkennen können. Darüber hinaus unterstreichen die Anwendung der synthetischen Datengenerierung für das Training neuronaler Netze und die damit verbundenen Trade-off-Analysen zwischen realer und virtueller Datenqualität eine datenzentrierte Validierungsphilosophie. Insgesamt leistet Pfeffer einen umfassenden Beitrag, welcher die Repräsentativität und Diversität szenariobasierter Testfälle verbessert. Im Vergleich zum hier aufzusetzenden Betriebssicherheitsentwicklungsprozess konzentrieren sich Pfeffers Beiträge primär auf die methodische Weiterentwicklung der Szenarioidentifizierung, -klassifizierung und -abdeckungsbewertung. Pfeffers Szenario-Metabeschreibungsmodelle verfügen über das Potenzial die Abschnitte der Betriebsbereichsdefinition (vgl. Teil 3-3 Unterabschnitt 7.2.2) sowie der betriebsbereichsbedingten Gefahrenanalyse (vgl. Teil 3-4 Unterabschnitt 7.2.2) zu ergänzen, indem sie eine skalierbare, datenbasierte Grundlage für Szenario-Clustering und Neuartigkeitserkennung bieten. Darüber hinaus könnten die Methoden zur synthetischen Datengenerierung und Trade-off-Analyse für das Training von ML-Modellen die Laufzeitabsicherungs- und Validierungsaktivitäten bereichern (vgl. Teil 3-6 Unterabschnitt 7.2.2), indem sie eine robuste Erweiterung sicherheitsrelevanter Testszenarien unter verschiedenen Betriebsbereichsbedingungen ermöglichen.

Im Mittelpunkt der Arbeiten von King et al. [225], [226], [227] stehen die Extraktion logischer Szenarien aus realdatenbasierten Trajektorien sowie die Entwicklung von Methoden im Hinblick auf die szenariobasierte Reifegradabsicherung von Fahrerassistenzsystemen. Im Vergleich zum in dieser Dissertation vorzustellenden Betriebssicherheitsrahmenwerk konzentriert sich die Arbeit von King et al. vorwiegend auf spezifische technische Fortschritte bei der Szenariogenerierung, dem Szenariomanagement und der kontinuierlichen Verhaltensbewertung. Daraus ergeben sich zielführende Synergien. Kings manöverbasierte logische Szenarioextraktion könnte innerhalb der Betriebsbereichsdefinition (vgl. Teil 3-3 Unterabschnitt 7.2.2) eingesetzt werden, um die betriebsbereichsbezogene Domänenmodellierung zu bereichern und die Repräsentativität des für die Validierung der Betriebssicherheit verwendeten Szenarioraums zu erhöhen. Darüber hinaus könnte der von King et al. vorgeschlagene Ansatz zur automatisierten, kontinuierlichen Funktionsbewertung den Abschnitt der Betriebssicherheitsvalidierung (vgl. Teil 3-6 Unterabschnitt 7.2.2) stärken und so eine granulare, situationsabhängige Überwachung und Bewertung der Betriebssicherheitsgewährleistung ermöglichen.

Reisgys et al. [228], [229], [230] Arbeiten umfassen einen strukturierten Ansatz zur Bewertung der Glaubwürdigkeit von XiL-Simulationen. Besonders hervorzuheben ist ihre Methodik zur Bewertung der Simulationsglaubwürdigkeit durch Vorhersage-, Plausibilisierungs- und Validierungsschritte sowie der quantitative Umgang mit Unsicherheiten in virtuellen und realen Testumgebungen. Im Vergleich zum Betriebssicherheitslebenszyklusprozess liegt der Schwerpunkt von Reisgys' Beiträgen vorwiegend auf der Validierung simulationsbasierter Testergebnisse und der methodischen Bewertung von XiL-Umgebungen in der operativen Verifikationsphase. Genau an dieser Stelle sind vielversprechende Integrationspotenziale erkennbar. Sowohl das von Reisgys et al. entwickelte Rahmenwerk zur Unsicherheitsmodellierung als auch die Methode zur Glaubwürdigkeitsbewertung könnten insbesondere den Abschnitt der Betriebssicherheitsvalidierung (vgl. Teil 3-6 Unterabschnitt 7.2.2) unterstützen. Darüber hinaus könnte ihre szenariobasierte XiL-Teststrukturierung angepasst werden, um die Modellierung eines zu definierenden Betriebsbereichs (vgl. Teil 3-3 Unterabschnitt 7.2.2) zu vertiefen und so ein höheres Vertrauensniveau in die virtuellen Validierungsphasen zu ermöglichen.

Auch Schütt et al. [231], [232], [233], [234], [235] leisten einen umfangreichen Beitrag, was die Thematik des szenariobasierten Testens angeht. Darunter fallen Methoden zur Szenarienexploration, Clusterung,

Generierung evolutionärer Verhaltensbäume, Kritikalitätsanalyse mithilfe der Metrik „Inverse Universal Traffic Quality“ und das grafische Modellierungsrahmenwerk „Scenario Modeling Language“ (SceML). Im Vergleich zum in dieser Dissertation vorgeschlagenen Betriebssicherheitsprozess konzentrieren sich die Beiträge von Schütt et al. auf die Verfeinerung und Effizienz der szenariobasierten Validierung, wobei der Fokus auf der Optimierung der Testabdeckung und der Kritikalitätsbewertung auf der Ebene der betriebsbereichsbedingten Verifikation liegt. Die clusterbasierte Kritikalitätsanalyse und die Methoden der evolutionären Szenariogenerierung könnten den Abschnitt der betriebsbereichsbedingten Gefahrenanalyse und Risikobewertung (vgl. Teil 3-4 Unterabschnitt 7.2.2) methodisch ergänzen. Darüber hinaus könnte die Metrik der inversen universellen Verkehrsqualität in die Laufzeitvalidierung und die kontinuierliche Betriebssicherheitsüberwachung (vgl. Teil 8-7 Unterabschnitt 7.2.3) integriert werden. Das SceML-Framework bietet zudem die Möglichkeit, Betriebssicherheitsziele und -szenarien formal zu visualisieren und so die Transparenz sowie die Konsistenz der Sicherheitsargumentation über den gesamten Betriebssicherheitslebenszyklus hinweg aufrecht zu erhalten.

Im Hinblick auf die szenariobasierte Validierung von Wahrnehmungsfunktionen im Kontext des automatisierten Fahrens erarbeiten Bernhard et al. [236], [237], [238] mehrere Beiträge, wobei der Schwerpunkt auf der adaptiven Testfallauswahl, dem Szenario-Clustering und der Optimierung der Testsatzdiversität liegt. Ihre Forschung führt adaptive Sampling-Pipelines ein, um Insuffizienzen in ML-basierten Wahrnehmungsfunktionen aufzudecken. Hierunter fällt die die iterative Auswahl von Testfällen, welche die Fehlererkennung bei minimalem Ressourcenaufwand maximieren. Bernhards clusterbasierte Szenario-Diversitätsoptimierung könnte innerhalb der betriebsbereichsbedingten Gefahrenanalyse (vgl. Teil 3-4 Unterabschnitt 7.2.2) genutzt werden, um die Abdeckung sowohl nominaler als auch grenzwertiger Szenarien systematisch sicherzustellen. Darüber hinaus entspricht die Integration adaptiver Test-Feedbackschleifen der Sichtweise einer kontinuierlichen Überwachung und Validierung der Betriebssicherheit (vgl. Teil 8-7 Unterabschnitt 7.2.3) über den gesamten Produktlebenszyklus.

Ries et al. [239], [240], [241], [242] liefern eine Reihe von Beiträgen zur Extraktion, Clusterung und semantischen Analyse realer Fahrszenarien mithilfe skalierbarer datenbasierter Methoden. Ihre Arbeit umfasst die Entwicklung einer skalierbaren gitterbasierten Darstellung von Fahrszenarien. Hinzu kommt ein Ansatz in Bezug auf trajektorienbasiertes Clustering realer urbaner Fahrsequenzen sowie die Konzeption einer modellfreien Clustering-Technik für die datenbasierte Szenarioanalyse. Insbesondere schlägt Ries robuste Pipelines zur automatischen Identifizierung, Gruppierung und Analyse semantisch ähnlicher Fahrsituationen aus umfangreichen Datensätzen vor. Die skalierbaren Szenariodarstellungs- und Clustering-Techniken von Ries et al. könnten die Abschnitte der Betriebsbereichsdefinition (vgl. Teil 3-3 Unterabschnitt 7.2.2) sowie der Gefahrenmodellierung (vgl. Teil 3-4 Unterabschnitt 7.2.2) ergänzen und hierbei die systematische Ableitung kritischer Szenarien als auch die Schätzung von Szenario-Eintrittswahrscheinlichkeiten methodisch unterstützen. Darüber hinaus könnten seine semantischen Einbettungen von Fahrsequenzen zur Rückverfolgbarkeit zwischen aufgezeichneten Betriebsdaten und abgeleiteten Betriebssicherheitszielen genutzt werden und so die Betriebssicherheitsargumentation für die kontinuierliche Validierung und Überwachung (vgl. Teil 8-7 Unterabschnitt 7.2.3) stärken.

Sowohl Kallweit et al. [301], Myklebust et al. [302] als auch Munk und Schweizer [303] schlagen die Integration sicherheitsspezifischer Aspekte gemäß der ISO 26262 und/oder ISO 21448 in die agile DevOps-Methode (vgl. Unterabschnitt 3.2.5) im Sinne eines sogenannten SafeOps-Ansatzes vor. Dabei handelt es sich um die systematische Einbindung von DevOps-Prinzipien in Bezugnahme auf Automatisierung, funktionsgetriebener Entwicklung und Feldüberwachung, um die Anforderungen der ISO 26262 bzw. ISO 21448 bei der iterativen Erweiterung und Verbesserung sicherheitskritischer Produkte zu erfüllen. Einen

vergleichbaren Ansatz liefert Zeller [304], wobei es sich hierbei um den Aspekt der kontinuierlichen Bereitstellung unter Berücksichtigung aller Phasen des sicherheitstechnischen Lebenszyklus handelt. Allerdings wird eine übergreifende Betrachtung der Betriebssicherheit des hochautomatisierten Fahrens nicht adressiert. Des Weiteren wird nicht aufgezeigt, inwiefern die jeweiligen DevOps-Prinzipien in den Automotive-PEP eingearbeitet werden können.

6.5 Zusammenfassung und Einordnung der Hochautomatisierung von Kraftfahrzeugen sowie damit einhergehende Herausforderungen

Alles in allem fördern die Analyse und Bewertung des aktuellen Stands von Forschung, Wissenschaft und Technik zwei Limitierungen im Hinblick auf die Gewährleistung der Betriebssicherheit des hochautomatisierten Fahrens zu Tage. Bei ersterer handelt es sich um eine systematische Betrachtung des Ego-Fahrzeugs als Gesamtsystem eingebettet in dessen offenen Kontext, welche innerhalb des Sicherheitslebenszyklus gemäß ISO 26262 und ISO 21448 nicht prozessual adressiert wird. Die Sicherheitsnormen für das automatisierte Fahren behandeln die Problematik offener Kontexte und damit auch die Thematik eines Betriebssicherheitsnachweises hochautomatisierter Straßenfahrzeuge. Allerdings wird kein ganzheitlicher Prozess im Sinne eines Betriebssicherheitslebenszyklus aufgesetzt, welcher die unterschiedlichen Sicherheitsthemen konsistent und kohärent miteinander in Einklang bringt als auch strukturell entlang der Nachweisführungskette Evidenz, Argument sowie Behauptung zusammenführt.

Was die szenariobasierte Absicherung automatisierter Fahrfunktionen angeht, so repräsentieren die im vorangegangenen Abschnitt beschriebenen Arbeiten jeweils wertvolle Einzellösungen. Ansätze wie die adaptive Testfallauswahl für Wahrnehmungsfunktionen (Bernhard [236]), der semantische Vergleich von Fahrsequenzen mittels Einbettungsmethoden (Ries [239]), die clusterbasierte Kritikalitätsanalyse (Schütt [231]), das Szenario-Metamodell (Pfeffer [211]), die szenariobasierte Reifegradbestimmung (King [225]) und die Bewertung der Simulationsglaubwürdigkeit in XiL-Umgebungen (Reisgys [228]) bieten ein umfassendes Set an Werkzeugen für die Szenariogenerierung, Priorisierung, Testeffizienz und Interpretierbarkeit (vgl. Unterabschnitt 4.8.2). Jedoch zeigt der szenariobasierte Fokus dieser Beiträge auch die Grenzen einer rein domänenspezifischen Betrachtung. Ohne Integration in einen normativen, prozessorientierten Rahmen ist ihre Operationalisierung im Kontext der Automotive Sicherheitsentwicklung eingeschränkt. Das in dieser Dissertation vorzuschlagende Prozessrahmenwerk für Betriebssicherheit trägt diesem Bedarf Rechnung, indem es ein vertikal integriertes, zielorientiertes Vorgehensmodell bietet, das von der initialen Konzeptentwicklung bis zur Laufzeitüberwachung reicht.

Die zweite Limitierung charakterisiert sich durch eine Diskrepanz zwischen der V-Modell basierten Sicherheitsentwicklung einerseits und agilen Methoden andererseits. Dieser Umstand bezieht sich auch auf den prozessualen Ablauf des PEPs sowie die hierfür bestehenden Vorgehensmodelle und Methoden (vgl. Abschnitt 3.1 und 3.2). Dabei handelt es sich um die sequenzielle und strikt top-down ablaufende Herangehensweise des klassischen V-Modells, bei der Anforderungen zu Projektbeginn vollständig definiert und dokumentiert werden müssen. Dieses Vorgehen ist innerhalb des dynamischen Entwicklungskontexts hochautomatisierter Fahrfunktionen sowie im Hinblick auf die Realisierung des Multiple-V-Modellansatzes gemäß der VDA „Reifegradabsicherung für Neuteile“ (vgl. Unterabschnitt 3.2.6) nicht umsetzbar. Softwarebasierte Fahrzeugführungssysteme sowie Absicherungsmaßnahmen und szenariobasiertes Testen erfordern eine flexible Reaktion auf Änderungen, welche in der wasserfallartigen Ablaufstruktur des V-

Modells nicht integriert werden können. Im Speziellen geht es dabei um die Betrachtung analytisch dynamischer Verhaltensaspekte (vgl. Anhang A.3 und A.4).

Dies manifestiert sich darin, dass das Bewusstsein im Hinblick auf die Bedeutung und Relevanz dynamisch analytischer Verhaltensaspekte einschließlich szenariobasiertes Testen für das hochautomatisierte Fahren innerhalb der Community der modellbasierten Automotive-Sicherheitsentwicklung begrenzt ist. Insgesamt gibt es derzeit keinen gesamtheitlichen Entwicklungsansatz, welcher die Generierung eines modellbasierten Betriebssicherheitsnachweises entlang der Säulen Prozess, modellbasierte Methode, Modellierungssprache und Modellierungswerkzeug ermöglicht (vgl. Abschnitt 4.3). Aufgrund dessen können der Entwurf und die Analyse funktionaler, logischer und technischer Architekturen als auch eine dazu konsistente dynamisch analytische Verhaltensbeschreibung nicht realisiert werden. Zudem wird die Thematik des Treffens von Annahmen, welche sich über den gesamten Modellierungsvorgang erstreckt, innerhalb der Automotive-Sicherheitsentwicklung methodisch nicht adäquat berücksichtigt. Dabei handelt es sich um eine modellbasierte Generierung eines Betriebssicherheitsnachweises entlang der Nachweisführungskette Evidenz, Argument und Behauptung. Außerdem erschwert die späte Validierung Iterationen sowie inkrementelle Anpassungen während der Entwicklung und im Betrieb.

Agile Methoden verfügen über die notwendige Flexibilität im Sinne eines iterativ-inkrementellen Entwurfs, welcher dem dynamischen Charakter des Entwicklungskontexts gerecht werden kann. Dies fördert eine Kultur, in der die Mitglieder der verschiedenen Teams, wie Entwicklung, Test und Betrieb, eng zusammenarbeiten und ihr Wissen durch kontinuierliches Feedback miteinander teilen. Allerdings stoßen agile Herangehensweisen bei sicherheitskritischen Systemen an ihre Grenzen. Die starke Fokussierung auf inkrementelle Änderungen und das Fehlen eines strukturierten, durchgängigen Top-Down- respektive Bottom-Up-Ansatzes führen zu Schwierigkeiten bei der Einhaltung der jeweiligen Sicherheitsnormen und damit der Gewährleistung der Betriebssicherheit. Ein hybrider Ansatz, welcher die Vorteile des sicherheitsbezogenen V-Modells einerseits und agiler Methoden andererseits kombiniert, bietet einen möglichen Lösungsweg. So könnten einerseits die Planbarkeit und Verbindlichkeit des V-Modells und andererseits die Anpassungsfähigkeit, Handlungsschnelligkeit und Effizienz agiler Ansätze genutzt werden. Erst dadurch würde sich ein flexibles Prozessmodell mit kontinuierlichem Feedback ergeben, welches in der Lage ist, das V-Modell im Sinne des Multiple-V-Ansatzes (vgl. Unterabschnitt 3.2.6) in den PEP zu integrieren und bezogen auf die Betriebssicherheitsentwicklung des hochautomatisierten Fahrens umzusetzen.

7 Agiler Betriebssicherheitslebenszyklusprozess

„Immer versucht. Immer gescheitert. Egal. Noch mal versuchen. Nochmal scheitern. Besser scheitern."

Samuel Barclay Beckett

Die Hochautomatisierung der Fahraufgabe und der daraus herrührende Sachverhalt des offenen Kontexts resultiert in signifikanten Änderungen des Umfangs bzw. Geltungsbereichs sicherheitsrelevanter Tätigkeiten innerhalb der Automotive-Sicherheitsentwicklung von E/E-Systemen. Eine systematische Betrachtung des Ego-Fahrzeugs als Gesamtsystem eingebettet in dessen offenen Kontext wird im Sicherheitslebenszyklus gemäß ISO 26262 und ISO 21448 nicht adressiert (vgl. Abschnitt 6.2). Dies gilt auch für die derzeitigen sich in Entwicklung befindenden Sicherheitsnormen für das automatisierte Fahren (vgl. Unterabschnitt 6.4.1). Dadurch fehlt zum aktuellen Zeitpunkt ein ganzheitlicher Sicherheitsentwicklungsansatz bezüglich der Gewährleistung der unterschiedlichen Sicherheitsthemen im Sinne der Betriebssicherheit hochautomatisierter Kraftfahrzeuge einschließlich unterstützender Infrastruktursysteme innerhalb eines definierten Betriebsbereichs. Demzufolge wird im nachfolgenden Kapitel ein ganzheitlicher Betriebssicherheitslebenszyklusprozess entworfen. Abschließend wird dieser unter Berücksichtigung von agilen Scrum- und DevOps-Prinzipien (vgl. Unterabschnitt 3.2.4 und 3.2.5) mit dem Automotive-PEP (vgl. Abschnitt 3.1) verknüpft und finalisiert.

7.1 Diskussion möglicher Lösungswege und Ableitung prozessualer Anforderungen für einen übergreifenden Betriebssicherheitsnachweis

Die in Kapitel 6 systematisch dargestellten Herausforderungen (vgl. Abschnitt 6.2 HF-1 bis HF-13), die daraus abgeleitete Lückenanalyse im Hinblick auf die Normen ISO 26262 und ISO 21448 (vgl. Abschnitt 5.2) sowie die Abgrenzung zum aktuellen Stand von Wissenschaft und Technik (vgl. Abschnitt 6.4) zeigen auf, dass das bestehende Sicherheitsnormensystem im Automobilbereich signifikante Erweiterungspotenziale im Hinblick auf die Absicherung hochautomatisierter Fahrzeugführungssysteme aufweist. Insbesondere die betriebssicherheitsbezogenen Aspekte der Definition und Modellierung offener Kontexte bzw. Betriebsbereiche (vgl. HF-1), die explizite Operationalisierung betrieblicher Risiken (vgl. HF-2) sowie kontinuierliche Validierungsmechanismen im Feldbetrieb (vgl. HF-13) sind in den bisherigen Normungsansätzen nicht durchgängig verankert. Auch die systematische Berücksichtigung einer iterativ-inkrementellen Nachweisführung (vgl. HF-11) im Sinne agiler Vorgehensweisen erfordert eine vertiefte methodische Einbettung.

Vor diesem Hintergrund lassen sich im Grundsatz drei separate Lösungswege zur Weiterentwicklung des Automotive Sicherheitslebenszyklus diskutieren:

a. Erweiterung der bestehenden Teile der ISO 26262 und ISO 21448 durch spezifische Zusatzerläuterungen und Empfehlungen zur Betriebssicherheit.

b. Separate fragmentarische Behandlung betriebsbereichsrelevanter Themen in Form von unabhängigen Zusatznormen (z.B. ISO 34502, ISO 34503, ISO 5083, UL 4600 vgl. Unterabschnitt 5.2.3).

c. Gestaltung eines dedizierten Entwicklungsstrangs innerhalb eines adaptierten Prozessmodells für die übergreifende Gewährleistung der Betriebssicherheit.

Im Hinblick auf das Vorangehende bietet Lösung (a) den Vorteil einer schrittweisen Weiterentwicklung der bestehenden Normen. Allerdings besteht das Risiko, dass das Ausbleiben hierarchischer und strukturbezogener Prozessanpassungen zu widersprüchlichen Erweiterungen führt. Dahingegen ermöglicht Ansatz (b) eine vertiefte Auseinandersetzung mit einzelnen domänenspezifischen Gesichtspunkten, kann jedoch aufgrund mangelnder Prozessintegration die bestehende Fragmentierung der jeweiligen Entwicklungs- und Sicherheitsaspekte verstärken. Lösung (c) umfasst die Konzeption eines erweiterten Lebenszyklusprozesses, welcher einerseits auf etablierten Normenbestandteilen aufbaut und andererseits neue Anforderungen konsistent einbettet.

Auf Grundlage der oben aufgezeigten Lösungswege sowie der Abwägung möglicher Vor- und Nachteile, charakterisiert sich Lösungsweg (c) als die zielführendste Option. Im Zentrum dieses Vorschlags steht die Einführung einer eigenständigen Betriebskonzeptphase. Diese zusätzliche Phase bietet das Potenzial,

- Betriebsbereichsmodelle, Erwartungen der involvierten Interessenvertreter und betriebliche Szenarien frühzeitig prozessorientiert einzubetten (vgl. HF-1, HF-2 und HF-4),
- Anforderungen aus einem offenen, dynamischen Betriebsumfeld methodisch zu erfassen und systematisch zu strukturieren (vgl. vgl. HF-1, HF-2, HF-7 und HF-8),
- Verhaltenserwartungen im rechtlich-normativen Kontext bereits in der Initialisierungsphase abzusichern (vgl. HF-9),
- sowie die Systementwicklung auf ein robustes, kontextreflexives Betriebssicherheitskonzept auszurichten (vgl. HF-3, HF-5, HF-6 und HF-13).

Demgegenüber verfügen Teil 2 (Management der funktionalen Sicherheit vgl. Unterabschnitt 5.2.1 und Anhang A.5) und Teil 7 (Produktion, Betrieb, Wartung, Außerbetriebnahme vgl. Unterabschnitt 5.2.1 und Anhang A.5) der ISO 26262 bereits über eine hohe strukturelle Reife im Umgang mit Management- und Betriebsfragen. Ihre Weiterentwicklung im Sinne der Betriebssicherheit erfordert daher keine Neustrukturierung, sondern gezielte inhaltliche Ergänzungen: etwa durch die Einführung betriebsbereichsbezogener Kennzahlen (engl. *Key Performance Indicators {KPIs}*), kontinuierliche Felddatenrückführungen (vgl. HF-13) oder Kriterien für Betriebssicherheitsupdates sowie Mechanismen zur modularen Evidenzwiederverwendung und Reifegradargumentation (vgl. HF-10 und HF-11). Das hierbei beabsichtigte Vorgehen ermöglicht es, vorhandene prozessuale Stärken weiter zu nutzen und gezielt dort zu erweitern, wo neue Herausforderungen und Potenziale im Umgang mit offenen Betriebskontexten entstehen. Durch diese integrative Herangehensweise wird ein konsistenter Nachweisweg ermöglicht, der entlang der Argumentationslinie Evidenz, Argument und Behauptung die Anforderungen der Betriebssicherheit abdeckt und in einem normkonformen Lebenszyklusprozess operationalisiert.

Um die erforderlichen Eigenschaften eines übergreifenden Betriebssicherheitslebenszyklusprozesses zu definieren, werden im weiteren Verlauf dedizierte Anforderungen aus den Problemstellungen und Herausforderungen innerhalb der Automotive System- und Sicherheitsentwicklung (vgl. Abschnitt 6.2) sowie der Lückenanalyse des Automotive Sicherheitslebenszyklus (vgl. Abschnitt 6.3) abgeleitet.

Für die erfolgreiche Etablierung eines modellbasierten Betriebssicherheitsentwicklungsansatzes ist die Akzeptanz der Anwender von im Kontext der Automotive System- und Sicherheitsentwicklung essenziell. Von besonderer Relevanz sind hierbei die nahtlose Integration in bestehende Vorgehensmodelle, die Modularisierung sicherheitsrelevanter Themen sowie die Einbindung in den Gesamtentwicklungsprozess unter Berücksichtigung von Evidenzführung und Argumentationslogik. Diese definieren den Rahmen für die durchzuführenden Aktivitäten und gewährleisten eine systematische, transparente und normkonforme Entwicklung:

AF-1 Errichtung einer betriebsbereichszentrierten Entwicklungsperspektive
Der Betriebssicherheitslebenszyklusprozess soll die Einnahme einer betriebsbereichszentrierten Entwicklungsperspektive beginnend auf System-Of-Systemsebene etablieren und dabei das V-Modell der ISO 26262 als Grundgerüst verwenden, um eine systematische Abstimmung und Integration mit der ISO 26262, der ISO 21448 als auch künftigen Standards zu gewährleisten.
Adressierte Herausforderungen: HF-7, HF-8

AF-2 Transparente Sicherheitsargumentation entlang der Nachweisführungskette
Der Betriebssicherheitslebenszyklusprozess soll der Nachweisführungskette "Evidenz → Argument → Behauptung" folgen, um eine transparente Sicherheitsargumentation zu unterstützen.
Adressierte Herausforderungen: HF-12

AF-3 Betriebskonzeptphase als Wegbereitung für nachgelagerte Sicherheitsaktivitäten
Der Betriebssicherheitslebenszyklusprozess soll eine modulare Betriebsbereichskonzeptphase enthalten, die vor- und nachgelagerte Sicherheitsaktivitäten systematisch vorbereitet.
Adressierte Herausforderungen: HF-7, HF-8

AF-4 Rahmen für übergreifende Sicherheitsthemen
Der Betriebssicherheitslebenszyklusprozess soll einen integrierten Rahmen für übergreifende Sicherheitsthemen (funktionale Sicherheit, Sicherheit der beabsichtigten Funktionalität, regelkonformes Fahrverhalten, Gebrauchssicherheit) schaffen.
Adressierte Herausforderungen: HF-3, HF-5, HF-6, HF-9

Nur eine widerspruchsfreie und eindeutige Darlegung im Hinblick darauf, welche Funktionen in welchen Kontexten erwartet werden, ermöglicht die frühzeitige Identifikation von Risiken und zweckmäßige Ableitung von Anforderungen. Die präzise Definition von Anwendungsfällen bildet hierfür eine geeigneten Start- bzw. Ausgangspunkt des Entwicklungsvorhabens:

AF-5 Anwendungsfälle auf Basis von Nutzer- und Interessenvertreterzielsetzungen
Der Betriebssicherheitslebenszyklusprozess soll die Definition von Anwendungsfällen auf Basis von Nutzer- und Betreiberzielen als Startpunkt des Entwicklungsvorhabens ermöglichen.
Adressierte Herausforderungen: HF-7, HF-8

AF-6 Anwendungsfalldefinition unter Berücksichtigung der Interaktionsbedarfe und Systemgrenzen
Der Betriebssicherheitslebenszyklusprozess soll die Berücksichtigung der Interaktionsbedarfe mit Infrastruktur, Nutzern, Verkehrsteilnehmern und rechtlichen Vorgaben fördern sowie eine modulare Anwendungsfalldefinition inkl. der Systemgrenzen und Automatisierungsgrade realisieren.
Adressierte Herausforderungen: HF-1, HF-2, HF-7, HF-8, HF-9

Ein ganzheitlicher Betriebssicherheitsprozess setzt die systematische Berücksichtigung der Zielsetzungen, Rollen und rechtlichen Verpflichtungen aller relevanten Interessenvertreter voraus. Dazu gehören Hersteller, Betreiber, Gesetzgeber sowie Normungs- und Zulassungsstellen. Ohne diese frühzeitige Kontextintegration kann keine tragfähige und rechtskonforme Betriebssicherheitsstrategie entwickelt werden:

AF-7 Systematische Identifikation der relevanten Interessenvertreter
Der Betriebssicherheitslebenszyklusprozess soll die systematische Identifikation der relevanten Interessenvertreter (z.B. Hersteller, Betreiber, Gesetzgeber) sowie die Dokumentation der Interessenvertreteranforderungen ermöglichen.
Adressierte Herausforderungen: HF-8, HF-9

AF-8 Analyse des regulatorischen Kontexts
Der Betriebssicherheitslebenszyklusprozess soll die Analyse des regulatorischen Kontexts in Abhängigkeit des zu definierenden Betriebsbereichs sowie der Verhaltenserwartungen vorantreiben.
Adressierte Herausforderungen: HF-9

Der Betriebsbereich stellt die maßgebende Referenz für die Gestaltung und Bewertung der zu realisierenden Betriebssicherheitsfunktionen dar. Somit ist die Fähigkeit zur strukturierten und analytisch dynamischen Modellierung dieses Kontexts die Grundvoraussetzung, um Szenarien, Risiken und systemische Leistungsgrenzen im Entwicklungsprozess adäquat adressieren zu können:

AF-9 Taxonomisch strukturierte Spezifikation des Betriebsbereichs
Der Betriebssicherheitslebenszyklusprozess soll die taxonomisch strukturierte Spezifikation des Betriebsbereichs inklusive Umgebungsinteraktionen sowie auszugrenzender Randfälle ermöglichen.
Adressierte Herausforderungen: HF-1, HF-2, HF-7, HF-8

Die systematische Identifikation, Bewertung und Reduktion betriebsbereichsbezogener Risiken muss sowohl klassische Fehlfunktionen als auch verhaltensbedingte, emergente oder missbräuchliche Risiken im offenen Kontext berücksichtigen, um eine akzeptable Restunsicherheit nachweisbar machen zu können:

AF-10 Übergreifende betriebsbereichsbezogene Gefährdungsanalyse und Risikobewertung
Der Betriebssicherheitslebenszyklusprozess soll eine Gefährdungs- und Risikoanalyse in Bezug auf klassischen E/E-Fehlfunktionen aber auch im Hinblick auf unzureichende Funktionsleistungen, Fehlgebrauch und emergentes Verhalten bereitstellen.
Adressierte Herausforderungen: HF-1, HF-2, HF-3, HF-7, HF-8, HF-9

AF-11 Restrisikoargumentation entlang von Betriebssicherheitszielen
Der Betriebssicherheitslebenszyklusprozess soll eine quantifizierbare Restrisikoargumentation entlang von Betriebssicherheitszielen inkl. Szenarien, Systemverhalten und Interessenvertretertoleranzen ermöglichen.
Adressierte Herausforderungen: HF-3, HF-4

Für die Beherrschung und Reduktion der identifizierten Risiken und Gefährdungen werden technische, funktionale und ggf. organisatorische Maßnahmen benötigt. Hierunter fällt der systematische Entwurf von betriebssicherheitsbezogenen Mechanismen im Sinne robuster, nachvollziehbarer und fail-operational fähiger Strategien, was den Umgang mit Fehlfunktionen, Funktionsinsuffizienzen und kritischen Situationen innerhalb des definierten Betriebsbereichs angeht:

AF-12 Übergreifende Konzeption von Betriebssicherheitsmaßnahmen
Der Betriebssicherheitslebenszyklusprozess soll die Definition von absichernden Strategien inklusive degradierter Betriebszustände auf System-Of-Systemsebene realisieren und die Spezifikation sicherer ethisch konformer Fahrzeugverhaltensrichtlinien vorantreiben.
Adressierte Herausforderungen: HF-3, HF-5, HF-6, HF-9

Die Wirksamkeit und Nachvollziehbarkeit der umgesetzten Betriebssicherheitsmaßnahmen und -funktionen erfordert frühzeitige Verifikations- und Validierungsaktivitäten bekannter als auch unbekannter Szenarien. Dabei sind Rückführbarkeit und Argumentationsstärke zentrale Qualitätsmerkmale:

AF-13 Frühzeitige modellbasierte Betriebssicherheitsvalidierung
Der Betriebssicherheitslebenszyklusprozess soll eine frühzeitige modellbasierte Verifikation und Validierung der Betriebssicherheitsstrategien und -maßnahmen prozessual verankern.
Adressierte Herausforderungen: HF-4, HF-11

AF-14 Umfang und Nachvollziehbarkeit der Betriebssicherheitsvalidierung
Der Betriebssicherheitslebenszyklusprozess soll Updates und kontextuelle Änderungen in die Verifikations- und Validierungsaktivitäten miteinbeziehen und die Ergebnisse nachvollziehbar und rückverfolgbar mit den Betriebssicherheitszielen, Betriebsbereichselementen und Interessenvertretervorgaben verknüpfen.
Adressierte Herausforderungen: HF-4, HF-11, HF-12

Im Verlauf des Entwicklungsprozesses müssen Anwendungsfälle, Betriebsbereichselemente und Szenarien stufenweise auf System-, Subsystem- und Komponentenebene heruntergebrochen werden. Diese Verfeinerung erlaubt eine systematische Zuweisung von Anforderungen, Nachweisen und Testaktivitäten entlang der gesamten Entwicklungstiefe. Voraussetzung dafür ist eine modulare und konsistente Rückverfolgbarkeit über alle Granularitätsebenen hinweg:

AF-15 Granularitätsebenenabhängige Top-Down Verfeinerung
Der Betriebssicherheitslebenszyklusprozess soll die nahtlose Verfeinerung und durchgängige Zuordnung von Anwendungsfällen, Betriebsbereichselementen und Szenarien entlang von Granularitätsebenen umsetzen.
Adressierte Herausforderungen: HF-7, HF-8

Auch nach Inverkehrbringen eines Systems darf die Betriebssicherheit nicht als abgeschlossen gelten. Aus diesem Grund ist eine kontinuierliche Laufzeitüberwachung und Rückführung von Felddaten sowie die adaptive Umsetzung von Absicherungsstrategien notwendig, um neue Risiken rechtzeitig erkennen aber auch angemessen adressieren zu können:

AF-16 Feldbeobachtung, Einflussanalyse und datenbasierte Rückführung
Der Betriebssicherheitslebenszyklusprozess soll die Spezifikation von Mechanismen für Feldbeobachtung, Einflussanalyse und datenbasierte Rückführung aus dem Feldbetrieb als integralen Prozessbestandteil etablieren.
Adressierte Herausforderungen: HF-13

AF-17 Langfristig nachvollziehbares Evidenzmanagement

Der Betriebssicherheitslebenszyklusprozess soll ein mehrversionsfähiges und langfristig nachvollziehbares Evidenzmanagement umfassen, wobei durchzuführende Updates valide Sicherheitsbewertungen und ggf. Revalidierungen auslösen.
Adressierte Herausforderungen: HF-12, HF-13

Im Zuge rasant wachsender Funktionsumfänge und immer kürzer werdender Entwicklungszyklen gewinnt der Aspekt eines iterativ-inkrementellen Betriebssicherheitsnachweises zunehmend an Bedeutung. Dieser Umstand erfordert frühzeitige Teilsicherheitsnachweise, eine systematische Argumentation von Zwischenfreigaben sowie die Zulassung von Rückkopplungen im Sinne einer agilen, flexiblen aber auch strukturierten Vorgehensweise:

AF-18 Erstellung iterativ-inkrementeller Betriebssicherheitsnachweise
Der Betriebssicherheitslebenszyklusprozess soll die Erstellung iterativ-inkrementeller Betriebssicherheitsnachweise und Zwischenfreigaben unterstützen und diese an definierte Qualitätskriterien, Risikoschwellen und Interessenvertreterwartungen entlang des Automotive PEPs koppeln.
Adressierte Herausforderungen: HF-10, HF-11, HF-13

AF-19 Modulare Freigaben und zyklusbasierte Änderungsschleifen
Der Betriebssicherheitslebenszyklusprozess soll Wiederverwendung von Teilsicherheitsnachweisen und modulare Freigaben erlauben sowie zyklusbasierte Änderungsschleifen der Betriebssicherheitsanforderungen und Validierungspläne unterstützen.
Adressierte Herausforderungen: HF-10, HF-11, HF-13

Zusammengefasst bildet der abgeleitete Anforderungskatalog das methodische Fundament des im Rahmen dieser Dissertation zu entwickelnden Betriebssicherheitslebenszyklusprozess. Er übersetzt die mit der Hochautomatisierung der Fahraufgabe einhergehenden Herausforderungen in konkrete, phasenbezogene und überprüfbare Prozessanforderungen, um in den nachfolgenden Abschnitten einen möglichen Lösungsweg zur Schließung der identifizierten Lücken der Normen ISO 26262 und ISO 21448 aufzuzeigen.

7.2 Vertikale Sicherheitslebenszykluserweiterung

Um die unterschiedlichen Sicherheitsthemen, sprich der funktionalen Sicherheit gemäß ISO 26262 (vgl. Unterabschnitt 5.2.1) sowie der Sicherheit der beabsichtigten Funktionalität, der Sicherheit der Fahrzeugverhaltensspezifikation und der Gebrauchssicherheit gemäß ISO 21488 (vgl. Unterabschnitt 5.2.2), ganzheitlich adressieren zu können, wurden diese im Hinblick auf den übergeordneten Begriff der Betriebssicherheit zusammengeführt (vgl. Abschnitt 5.3). Auf Grundlage dessen wird im Hinblick auf AF-1, AF-3 und AF-4 die erste Stufe der Dimensionserweiterung des Sicherheitslebenszyklusprozesses entlang der vertikalen Achse des ISO 26262 V-Modells vorgenommen. Prinzipiell zielt die Dimensionserweiterung darauf ab, den Ansatz, welcher insbesondere innerhalb der Sicherheitsintegritätsnorm ISO 26262 zur Vermeidung systematischer Fehler angewendet wird, auf die offene Kontextthematik gemäß HF-1 und HF-2 sowie die daraus abgeleiteten Aspekte der Betriebssicherheit gemäß HF-3, HF-9, HF-5 und HF-6 zu übertragen und einen ganzheitlichen Betriebssicherheitslebenszyklusprozess zu gestalten. Hierbei wird eine zusätzliche Betriebskonzeptphase oberhalb der ursprünglichen Konzeptphase der ISO 26262 aufgesetzt (siehe schraffierter Bereich Abbildung 7.1), wodurch sich das ursprüngliche Nummerierungsschema der Phasen bzw. Teile der ISO 26262 (siehe Abbildung 5.2) um „1“ erhöht.

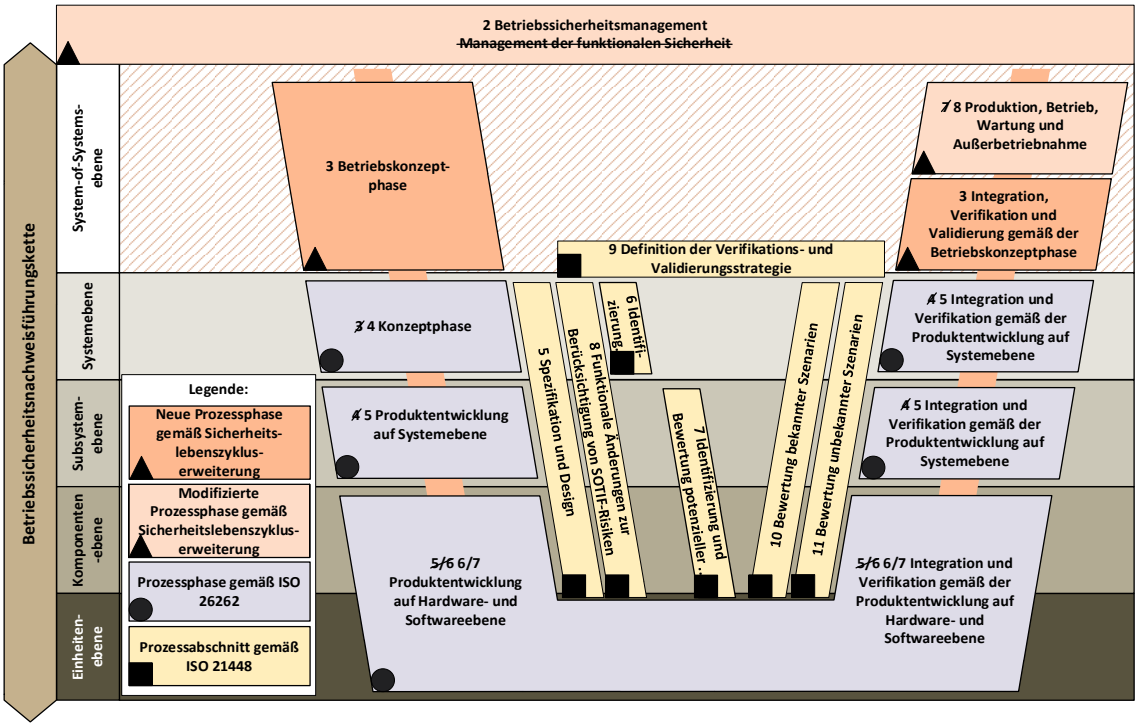


Abbildung 7.1: Um Betriebskonzeptphase (orange schraffiert) bzw. System-Of-Systemsebene vertikal erweitertes V-Modell der ISO 26262 bzw. ISO 21448.

Darüber hinaus werden unterhalb des hierarchischen Überbaus der Betriebskonzeptphase die ISO 26262 und ISO 21488 in einen systematisch strukturierten Bezug zueinander gesetzt (siehe Abbildung 7.1). Des Weiteren werden oberhalb des erweiterten V-Modells die Planungs- und Managementaktivitäten gemäß dem „Betriebssicherheitsmanagement“ erfasst, wobei das ursprüngliche „Management der funktionalen Sicherheit“ hinsichtlich der ganzheitlichen Betriebssicherheit erweitert wird (siehe oberer Randbereich Abbildung 7.1). Zudem wird die Erstellung eines nachvollziehbaren Betriebssicherheitsnachweises angestrebt, um die Erreichung der Betriebssicherheit zu belegen und das Gesamtprodukt für die Produktion und den Betrieb freigeben zu können. Insgesamt erfolgt die Generierung des Betriebssicherheitsnachweises gemäß AF-2 entlang der Qualitätsnachweisführungskette Evidenz, Argument und Behauptung (vgl. Abschnitt 5.3). Diese ebenenübergreifende Nachweisführungskette begleitet dementsprechend sämtliche Prozessphasen (siehe linker Randbereich Abbildung 7.1).

Insgesamt stützt sich die vertikale Erweiterung des Sicherheitslebenszyklus auf die im Rahmen der Promotion erarbeitete und publizierte Grundlage „Extending the Automotive Safety Life Cycle Towards Operational Safety of Automated Driving“ [305], welche einen wesentlichen methodischen Impuls für die nachfolgende Ausgestaltung liefert. In diesem Zusammenhang reguliert der an dieser Stelle eingeführte Betriebssicherheitslebenszyklusprozess den Betriebssicherheitslebenszyklus des Systems eingebettet in dessen Betriebsbereich. Des Weiteren beschreibt der Betriebssicherheitslebenszyklusprozess die jeweiligen Phasen, Abschnitte und Schritte im Sinne des „WAS“, welche wiederum benötigt werden, um einen strukturierten Betriebssicherheitsnachweis aufsetzen zu können (siehe Abbildung 7.2).

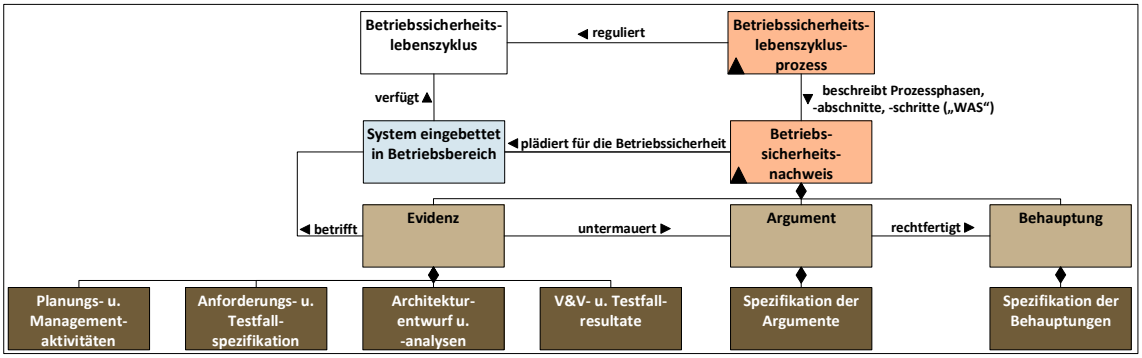


Abbildung 7.2: Eingeführter Betriebssicherheitslebenszyklusprozess als hierarchischer Überbau der Betriebssicherheitsnachweis-führungskette (Evidenz, Argument und Behauptung siehe Abbildung 5.8) für ein System eingebettet in dessen Betriebsbereich.

7.2.1 Teil 2 Betriebssicherheitsmanagement

Für die nachfolgende Konzeption des Teil 2 „Betriebssicherheitsmanagement“ wird der strukturelle und inhaltliche Aufbau von Teil 2 „Management der funktionalen Sicherheit“ gemäß der ISO 26262 herangezogen (vgl. Unterabschnitt 5.2.1 und Anhang A.5). Die darin enthaltenen Prozessabschnitte „2-5 Allgemeines Sicherheitsmanagement“, „2-6 Projektbezogenes Sicherheitsmanagement“ und „2-7 Sicherheitsmanagement mit Blick auf Produktion, Betrieb, Wartung und Außerbetriebnahme“ werden gemäß des Aspekts der ganzheitlichen Betriebssicherheit in „2-5 Allgemeines Betriebssicherheitsmanagement“, „Teil 2-6 Projektbezogenes Betriebssicherheitsmanagement“ sowie „2-7 Betriebssicherheitsmanagement in Bezug auf Produktion, Betrieb, Wartung und Außerbetriebnahme“ umbenannt (siehe Abbildung 7.3). An dieser Stelle sei darauf hingewiesen, dass die wesentlichen Inhalte von Teil 2 „Management der funktionalen Sicherheit“ gemäß der ISO 26262 übernommen und bedarfsgerecht im Sinne der Betriebssicherheit sowie der Sicherheit der beabsichtigten Funktionalität gemäß ISO 21448 modifiziert werden.

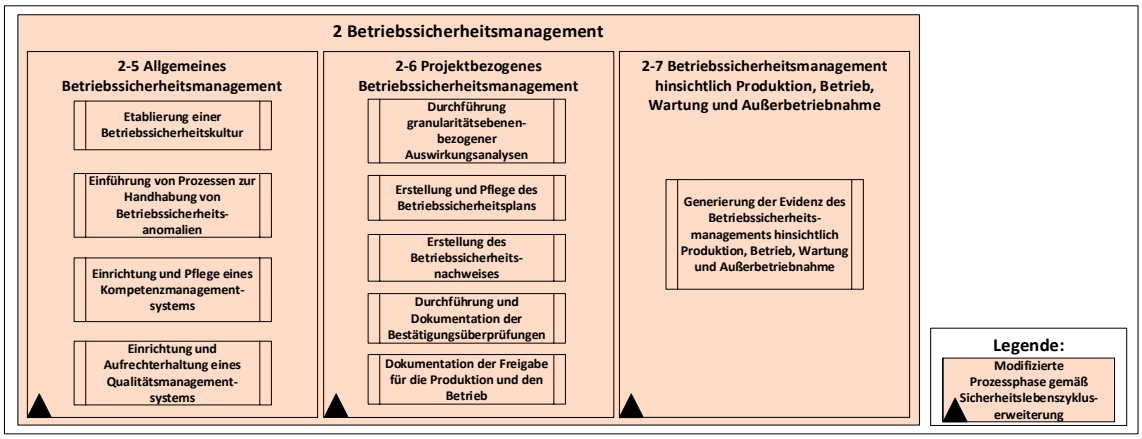


Abbildung 7.3: Modifizierte Prozessphasen und -schritte gemäß Teil 2 „Betriebssicherheitsmanagement“ des eingeführten Betriebssicherheits-lebenszyklusprozesses.

Hierfür werden in Analogie zur normativen Struktur der Sicherheitsnormen ISO 26262 und ISO 21448 die jeweiligen Zielvorgaben, Prozesstätigkeiten und Arbeitsprodukte (engl. *Work Product {WP}*) der im Hinblick auf die Betriebssicherheit zusätzlichen Managementaktivitäten beschrieben, wobei die modifizierten Aktivitäten als unterstrichen hervorgehoben werden.

Teil 2-5 Allgemeines Betriebssicherheitsmanagement

2-5.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) eine Betriebssicherheitskultur, welche die effektive Erreichung der Betriebssicherheit inkl. der funktionalen Sicherheit und der Sicherheit der beabsichtigten Funktionalität unterstützt und eine effektive Kommunikation mit den jeweils involvierten Entwicklungsdisziplinen fördert, zu etablieren und aufrecht zu erhalten;

b) Prozesse zur Sicherstellung einer angemessenen Lösung identifizierter Betriebssicherheitsanomalien einzuführen und zu pflegen;

c) ein Kompetenzmanagementsystem einzurichten und zu pflegen, um sicherzustellen, dass die Kompetenz der beteiligten Personen ihren Verantwortlichkeiten entspricht;

d) ein Qualitätsmanagementsystem zur Unterstützung der Betriebssicherheit inkl. der funktionalen Sicherheit und der Sicherheit der beabsichtigten Funktionalität einzurichten und aufrecht zu erhalten;

2-5.2 Allgemein durchzuführende Prozesstätigkeiten

Die durchzuführenden Tätigkeiten werden unverändert aus Teil 2 der ISO 26262 übernommen und lediglich um den Begriff der Betriebssicherheit sowie der Sicherheit der beabsichtigten Funktionalität ergänzt. Für inhaltliche Details hierzu sei auf Teil 2 der ISO 26262 [50] verwiesen.

2-5.3 Arbeitsprodukte

2-5.3.1 Organisationsspezifische Vorgaben und Prozesse für die Betriebssicherheit inkl. der funktionalen Sicherheit und Sicherheit der beabsichtigten Funktionalität gemäß 2-5.2 bzw. ISO 26262:2-5.4.2-5.4.6/5.5.1

2-5.3.2 Evidenz eines Kompetenzmanagementsystems gemäß 2-5.2 bzw. ISO 26262:2-5.4.4/5.5.2

2-5.3.3 Evidenz eines Qualitätsmanagementsystems gemäß 2-5.2 bzw. ISO 26262:2-5.4.5-5.4.6/5.5.3

2-5.3.4 Bericht der identifizierten Betriebssicherheitsanomalien gemäß 2-5.2 bzw. ISO 26262:2-5.4.3/5.5.4

Teil 2-6 Projektbezogenes Betriebssicherheitsmanagement

2-6.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) die Zuweisung der Rollen und Verantwortlichkeiten im Zusammenhang mit den Betriebssicherheitsaktivitäten zu definieren;

b) Auswirkungsanalysen auf System-Of-Systems-, System-, Subsystem-, Komponenten- oder Einheitenebene durchzuführen, um Änderungen und deren Einflussnahme auf die Betriebssicherheit, die funktionale Sicherheit sowie die Sicherheit der beabsichtigten Funktionalität zu evaluieren;

c) zugeschnittene (engl. *tailored*) bzw. angepasste Betriebssicherheitsaktivitäten festzulegen und Begründungen für diese Anpassungen sowie deren Überprüfung bereitzustellen;

d) die (verteilten) Betriebssicherheitsaktivitäten zu planen;

e) die Koordination und Verfolgung des korrekten Fortschreitens der Betriebssicherheitsaktivitäten gemäß dem Betriebssicherheitsplan inkl. der untergeordnete Pläne für die funktionale Sicherheit und die Sicherheit der beabsichtigten Funktionalität während des gesamten Betriebssicherheitslebenszyklusprozesses sicherzustellen;

f) einen glaubwürdigen, verständlichen und rückverfolgbaren Betriebssicherheitsnachweis zu erstellen und die Erfüllung der Betriebssicherheit zu belegen;

g) im Rahmen von Betriebssicherheitsassessments und Bestätigungsüberprüfungen zu beurteilen, ob die Entwicklungsgegenstände und bereitgestellten Arbeitsprodukte (System-Of-Systems, Systeme, Subsysteme, Komponenten oder Einheiten) die Betriebssicherheit erreichen;

h) am Ende der Entwicklungsphase die Entscheidung dahingehend herbeizuführen, ob die Entwicklungsgegenstände (System-Of-Systems, Systeme, Subsysteme, Komponenten oder Einheiten) auf Basis der Nachweise der erreichten Betriebssicherheit für die Produktion und den Betrieb freigegeben werden können;

2-6.2 Allgemein durchzuführende Prozesstätigkeiten

Die nachfolgenden Prozesstätigkeiten beziehen sich auf die jeweiligen Aktivitäten gemäß Teil 2 der ISO 26262 sowie Teil 12 der ISO 21448 und werden nur an dedizierten Stellen explizit hinsichtlich der Thematik der ganzheitlichen Betriebssicherheit inkl. der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität ergänzt. Vertiefende Details im Hinblick auf die jeweiligen Tätigkeiten, sind innerhalb von Teil 2 der ISO 26262 [50] bzw. Teil 12 der ISO 21448 [55] zu finden.

Im Zuge des projektbezogen Betriebssicherheitsmanagements werden Auswirkungsanalysen (engl. *Impact Analysis*) auf System-Of-Systems-, System-, Subsystem-, Komponenten- oder Einheitenebene durchgeführt, um Modifikationen und deren Auswirkungen auf die Betriebssicherheit, die funktionale Sicherheit sowie die Sicherheit der beabsichtigten Funktionalität zu bewerten. Hierbei ist festzustellen, ob es sich bei dem Produkt um eine Neuentwicklung, eine Änderung oder eine Wiederverwendung eines bestehenden Produkts mit einer veränderten Umgebung bzw. einem veränderten Betriebsbereich handelt. Im Falle einer Änderung des Betriebsbereichs eines System-Of-System, Items, Systems oder einer Komponente erfolgt die Auswirkungsanalyse auf der jeweiligen Granularitätsebene, um die vorzunehmenden Änderungen zu ermitteln und deren Einfluss auf die Betriebssicherheit zu erfassen. Darunter fallen auch die Ermittlung und Beschreibung der durchzuführenden Maßnahmen in Abhängigkeit von den Auswirkungen der Änderungen. Dies gilt auch im Falle der Wiederverwendung bereits existierender System-Of-Systems, Items, Systeme, Komponenten oder Einheiten.

Hinzu kommt die Festlegung und Planung zugeschnittener Betriebssicherheitsaktivitäten mit entsprechenden Begründungen sowie die Koordination und Verfolgung des Fortschritts dieser Aktivitäten gemäß dem Betriebssicherheitsplan, welcher wiederum um untergeordnete Pläne für die funktionale Sicherheit und die Sicherheit der beabsichtigten Funktionalität ergänzt wird. Hierunter fallen die Durchführung von projektunabhängigen Entwicklungstätigkeiten und Verfahren, die Definition und Planung von zugeschnittenen Analyse-, Integrations-, Verifikations- und Validierungstätigkeiten, die Terminplanung für die Bestätigungsüberprüfungen sowie das Audit und Assessment. Im Falle einer verteilten Entwicklung müssen sowohl der Kunde als auch der Lieferant einen Betriebssicherheitsplan für die jeweiligen Betriebssicherheitsaktivitäten festlegen.

Der Betriebssicherheitsnachweis wird gemäß dem Betriebssicherheitsplan erstellt und charakterisiert sich dadurch, eine nachvollziehbare Argumentation für die Erreichung der Betriebssicherheit zu liefern. Das Betriebssicherheitsmanagement umfasst darüber hinaus die Verantwortung dahingehend, die Durchführung der jeweils erforderlichen Bestätigungsmaßnahmen sicherzustellen. In Abhängigkeit der ASIL-Bewertung werden diese Maßnahmen mit ausreichender Unabhängigkeit in Bezug auf Ressourcen, Management und Freigabeautorität umgesetzt. Die Bestätigungsmaßnahmen[1] umfassen sogenannte Bestätigungsüberprüfungen, ein Betriebssicherheitsaudit sowie ein Betriebssicherheitsassessment.

Die Freigabeempfehlung für die Produktion und den Betrieb darf nur genehmigt werden, wenn ausreichende Nachweise inkl. der Berichte der Bestätigungsmaßnahmen vorliegen, welche wiederum ein Vertrauen in Bezug auf die Erreichung der Betriebssicherheit gewährleisten. Zum Zeitpunkt der Produktionsfreigabe müssen eine Baseline für die eingebettete Software, einschließlich der Kalibrierungsdaten, sowie eine Basislinie für die Hardware verfügbar sein und dokumentiert werden.

2-6.3 Arbeitsprodukte

2-6.3.1 Auswirkungsanalyse auf System-Of-Systems-, System-, Subsystem-, Komponenten- oder Einheitenebene gemäß 2-6.2 bzw. ISO 26262:2-6.4.3/6.4.4/6.5.1/6.5.2

2-6.3.2 Betriebssicherheitsplan gemäß 2-6.2 bzw. ISO 26262:2-6.4.5-6.4.13/6.5.3

2-6.3.3 Betriebssicherheitsnachweis gemäß 2-6.2 bzw. ISO 26262:2-6.4.8/6.5.4

2-6.3.4 Bericht der Bestätigungsmaßnahmen gemäß 2-6.2 bzw. ISO 26262:2-6.4.9-6.4.12/6.5.5 und ISO 21448-12.5

2-6.3.5 Bericht der Freigabe für die Produktion und den Betrieb gemäß 2-6.2 bzw. ISO 26262:2-6.4.13/6.5.6 und ISO 21448-12.5

Teil 2-7 Betriebssicherheitsmanagement hinsichtlich Produktion, Betrieb, Wartung und Außerbetriebnahme

2-7.1 Zielvorgaben

[1] Bei Bestätigungsmaßnahmen handelt es sich um eine Überprüfung, ein Audit oder ein Assessment dahingehend, dass ein Arbeitsprodukt im Sinne der Vollständigkeit, Korrektheit und Konsistenz einen ausreichenden sowie überzeugenden Nachweis der Behauptung für dessen Beitrag zur Erreichung der Betriebssicherheit unter Berücksichtigung der Ziele und Anforderungen der Betriebssicherheitslebenszyklusprozesses sowie der ISO 26262 und ISO 21448 liefert [50].

Die Zielvorgaben der Klausel sind:

a) die Verantwortlichkeiten der Organisationen und Personen festzulegen, welche für die Erreichung und Aufrechterhaltung der Betriebssicherheit in Bezug auf Produktion, Betrieb, Wartung und Außerbetriebnahme verantwortlich sind;

2-7.2 Allgemein durchzuführende Prozesstätigkeiten

Die nachfolgenden Prozesstätigkeiten beziehen sich wiederum auf die jeweiligen Aktivitäten gemäß Teil 2 der ISO 26262 und werden nur an dedizierten Stellen explizit im Hinblick auf die Thematik der ganzheitlichen Betriebssicherheit inkl. der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität ergänzt. Vertiefende Details im Hinblick auf die jeweiligen Tätigkeiten, sind innerhalb von Teil 2 der ISO 26262 [50] zu finden.

Die Entwicklungsbeteiligten und involvierten Organisationen müssen Personen benennen, welche einerseits die Verantwortung tragen und andererseits über die Befugnis verfügen, die Betriebssicherheit der Entwicklungsgegenstände (System-Of-Systems, Systeme, Subsysteme, Komponenten oder Einheiten) in Bezug auf Produktion, Betrieb, Wartung und Außerbetriebnahme zu erreichen und aufrechtzuerhalten.

Des Weiteren werden zusätzliche Prozesse eingeführt und aufrechterhalten, um die Betriebssicherheit in Bezug auf Produktion, Betrieb, Wartung und Außerbetriebnahme zu erreichen und über den gesamten Betriebssicherheitslebenszyklusprozess sicherzustellen. Dies umfasst Prozesse zur Felduberwachung in Bezug auf die Betriebssicherheit inkl. der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität (vgl. Teil 8-5). Falls sich die jeweiligen Entwicklungsgegenstände (System-Of-Systems, Systeme, Subsysteme, Komponenten oder Einheiten) während der Produktion, des Betriebs, der Wartung oder der Außerbetriebnahme ändern, wird die Freigabe für die Produktion bzw. den Betrieb unter Bezugnahme von Auswirkungsanalysen aktualisiert.

2-7.3 Arbeitsprodukte

2-7.3.1 Evidenz eines Betriebssicherheitsmanagements hinsichtlich Produktion, Betrieb, Wartung und Außerbetriebnahme gemäß 2-7.2 bzw. ISO 26262:2-7.4.2/7.5.1

7.2.2 Teil 3 Betriebskonzeptphase

Für die Betriebskonzeptphase werden im weiteren Verlauf sieben eigenständige Prozessabschnitte bzw. Teile definiert und ausgearbeitet, welche abschließend einen nahtlosen Übergang in die jeweiligen Prozessphasen, -abschnitte als auch -schritte der ISO 26262 und ISO 21448 ermöglichen (siehe Abbildung 7.4 respektive Abbildung B.1 und Abbildung B.2). Die Top-Down Grundstruktur wird dabei aus dem grundsätzlichen Prozessablauf der ISO 26262 (siehe Abbildung A.7) übernommen und auf sieben dedizierte Themenbereiche übertragen. In dieser Hinsicht basieren die im weiteren Verlauf spezifizierten Inhalte der jeweiligen Prozessabschnitte auf dem aktuellen Stand der Wissenschaft und Technik (vgl. Abschnitt 6.4), den identifizierten Herausforderungen und Problemstellungen im Zuge der Hochautomatisierung der Fahraufgabe (vgl. Abschnitt 6.2), der Lückenanalyse der Automotive Sicherheitsstandards (vgl. Abschnitt 6.3) sowie den daraus abgeleiteten prozessualen Anforderungen (vgl. Abschnitt 7.1):

- **Teil 3-1 Anwendungsfalldefinition:** Die erforderlichen Inhalte der Anwendungsfalldefinition (vgl. AF-5 und AF-6) werden aus den Grundlagen szenariobasierter Vorgehensweisen und Testprozessreferenzen abgeleitet (vgl. Abschnitt 4.8). Dabei wird auf der einen Seite die Charakteristik der Anwendungsfalldefinition als Startpunkt der modellbasierten Systementwicklung (vgl. Abschnitt 4.3) und auf der anderen Seite deren übergeordnete Rolle in Bezug auf das szenariobasierte Testen als Grundpfeiler der Absicherung hochautomatisierter Fahrfunktionen genutzt (siehe Abbildung 4.12).

- **Teil 3-2 Identifikation und Analyse der Interessenvertreter:** Der Abschnitt der Interessenvertreteridentifikation und Analyse (vgl. AF-7 und AF-8) beruht einerseits auf den gesetzlichen Grundlagen im Kontext des Straßenverkehrs (vgl. Abschnitt 5.1). Andererseits erfolgt das Hinzuziehen des Architekturparadigmas (vgl. Abschnitt 4.2) sowie der Konzepte des Systemanliegens und Interessenvertreter im Kontext der Modellierungs- und Architekturrahmenwerke der Automotive-Systementwicklung (vgl. Abschnitt 4.6).

- **Teil 3-3 Betriebsbereichsdefinition und -analyse:** Was die Inhalte der Betriebsbereichsdefinition und -analyse angeht (vgl. AF-9), so gründen diese auf der im Grundlagenteil identifizierten Signifikanz des Betriebsbereichs bei der Automatisierung der Fahraufgabe (vgl. Unterabschnitt 2.2.3). Des Weiteren wird auf der im Rahmen der Promotionsarbeiten entwickelten und publizierten Betriebsbereichsontologie [306] aufgebaut (vgl. Anhang B.3). Diese Ontologie bildet einen zentralen Baustein des gesamten Betriebskonzeptansatzes, da sie eine formal strukturierte, eindeutig interpretierbare und methodisch anschlussfähige Repräsentation des Betriebsbereichs bereitstellt. Im Bereich der Generierung, Priorisierung und Interpretierbarkeit betriebsbereichsbezogener Szenarien wird auf den Forschungsarbeiten des ITIV und FZIs aufgebaut (vgl. Unterabschnitt 4.8.2).

- **Teil 3-4 Betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung:** Der Abschnitt der betriebsbereichsbedingten Gefahrenanalyse und Risikobewertung (vgl. AF-10 und AF-11) leitet sich zum einen aus den grundsätzlichen Gefährdungsanalysen als zentraler Bestandteil der bestehenden Automotive Sicherheitsnormen ISO 26262 (vgl. Unterabschnitt 5.2.1 sowie Anhang A.5) und ISO 21448 (vgl. Unterabschnitt 5.2.2 sowie Anhang A.6) ab. Zum anderen wird das Safer Complex Systems Framework von Burton et al. [271] herangezogen, um systemische Ursachen, Konsequenzen und erschwerende Risikofaktoren von Gefährdungssituationen identifizieren zu können. Des Weiteren kommen die ITIV- bzw. FZI-Forschungsarbeiten von Schütt [231], Reisgys [228], Bernhard [236] und Ries [239] zum Tragen (vgl. Unterabschnitt 4.8.2), um die Kritikalität, das Ausmaß der Unsicherheiten, die Auftrittswahrscheinlichkeiten sowie die Abdeckung sicherheitskritischer Szenarien und Gefährdungssituationen bewerten zu können.

- **Teil 3-5 Betriebssicherheitskonzept:** Die notwendigen Inhalte des Betriebssicherheitskonzepts (vgl. AF-12) beruhen auf der eingeführten Perspektive und Konsolidierung der fragmentarischen Aspekte der funktionalen Sicherheit, der Sicherheit der beabsichtigten Funktionalität, der Sicherheit der Fahrzeugverhaltensspezifikation sowie der Gebrauchssicherheit im Sinne der Mensch-Maschine-Interaktion unter dem Oberbegriff der Betriebssicherheit (vgl. Abschnitt 5.3).

- **Teil 3-6 Betriebssicherheitsvalidierung:** Die durchzuführenden Tätigkeiten der Betriebssicherheitsvalidierung (vgl. AF-13 und AF-14) gründen auf den etablierten Verifikations- und Validierungsaktivitäten der ISO 26262 (vgl. Anhang A.5 und A.7). Diese werden um den Aspekt bekannter und unbekannter Szenarien gemäß der ISO 21448 erweitert (Anhang A.6) und im Hinblick

szenariobasierter Vorgehensweisen konsolidiert (vgl. Abschnitt 4.8). Im Speziellen sind die Arbeiten von Pfeffer [211], Reisgys [228] und King [225] hervorzuheben (vgl. Unterabschnitt 4.8.2), welche einen Beitrag zur robusten Erweiterung sicherheitsrelevanter Testszenarien als auch deren Glaubwürdigkeit und Bewertung leisten.

- **Teil 3-7 Granularitätsebenenabhängige Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs:** Der Abschnitt der granularitätsebenenabhängigen Verfeinerung (vgl. AF-15) wird aus dem systemischen Grundsatz der hierarchischen Dekomposition abgeleitet (vgl. Abschnitt 4.1) und auf die Aspekte der Anwendungsfalldefinition, Betriebsbereichsdefinition und Szenarienbeschreibung ausgeweitet. Dadurch wird insbesondere in Bezug auf die szenariobasierten Vorgehensweisen (Unterabschnitt 4.8.2) eine normative bzw. prozessorientierte Plattform geschaffen.

Hierfür werden wiederum die jeweiligen Zielvorgaben, Prozesstätigkeiten und Arbeitsprodukte der im Zuge dieser Dissertation entwickelten Prozessabschnitte bzw. Prozessklauseln der Betriebskonzeptphase dargelegt (siehe Abbildung 7.4).

Teil 3-1 Übergeordnete Interessenvertreterzielsetzung und Anwendungsfalldefinition

3-1.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) die Anwendungsfälle sowie deren Übergänge ineinander aus der Perspektive der Benutzer bzw. Kunden mit einem hohen Abstraktionsgrad bzw. geringen Detaillierungsgrad auf oberster Granularitätsebene zu definieren;

b) den grundsätzlichen Zweck des Entwicklungsvorhabens bzw. des zu entwickelnden Produkts bzw. Systems[2], hier System-Of-Systems, die Features auf Basis der Kundenbedürfnisse sowie der involvierten Akteure zu definieren und zu beschreiben;

c) die Erwartungen bzw. Annahmen in welcherlei Art das zu entwickelt werdende Produkt oder System im Sinne eines System-Of-Systems vom Anwender bedient wird, das erwünschte Verhalten als auch der Funktionsumfang, welche als Nutzen für welche Art von Anwender zur Verfügung gestellt werden, darzulegen;

d) einen modularen Rahmen für die Kategorisierung
    - der funktionalen Systemgrenzen und Einschränkungen einschließlich des Automatisierungsgrads,
    - der beabsichtigten Einsatzumgebung,
    - der zu erwartenden Bedingungen,
    - der relevanten Situationen innerhalb welcher die Features bzw. Benutzerfunktionen bereitgestellt werden,

    zu instanziieren und die letztendliche Automatisierungsaufgabe zu identifizieren;

[2] Es sei anzumerken, dass innerhalb der Dissertation hauptsächlich der allgemeine Systembegriff eines technischen Produkts verwendet wird. Dieser kann sich jeweils auf ein System-Of-Systems, System, Subsystem, eine Komponente oder eine Einheit beziehen (vgl. Abschnitt 4.1).

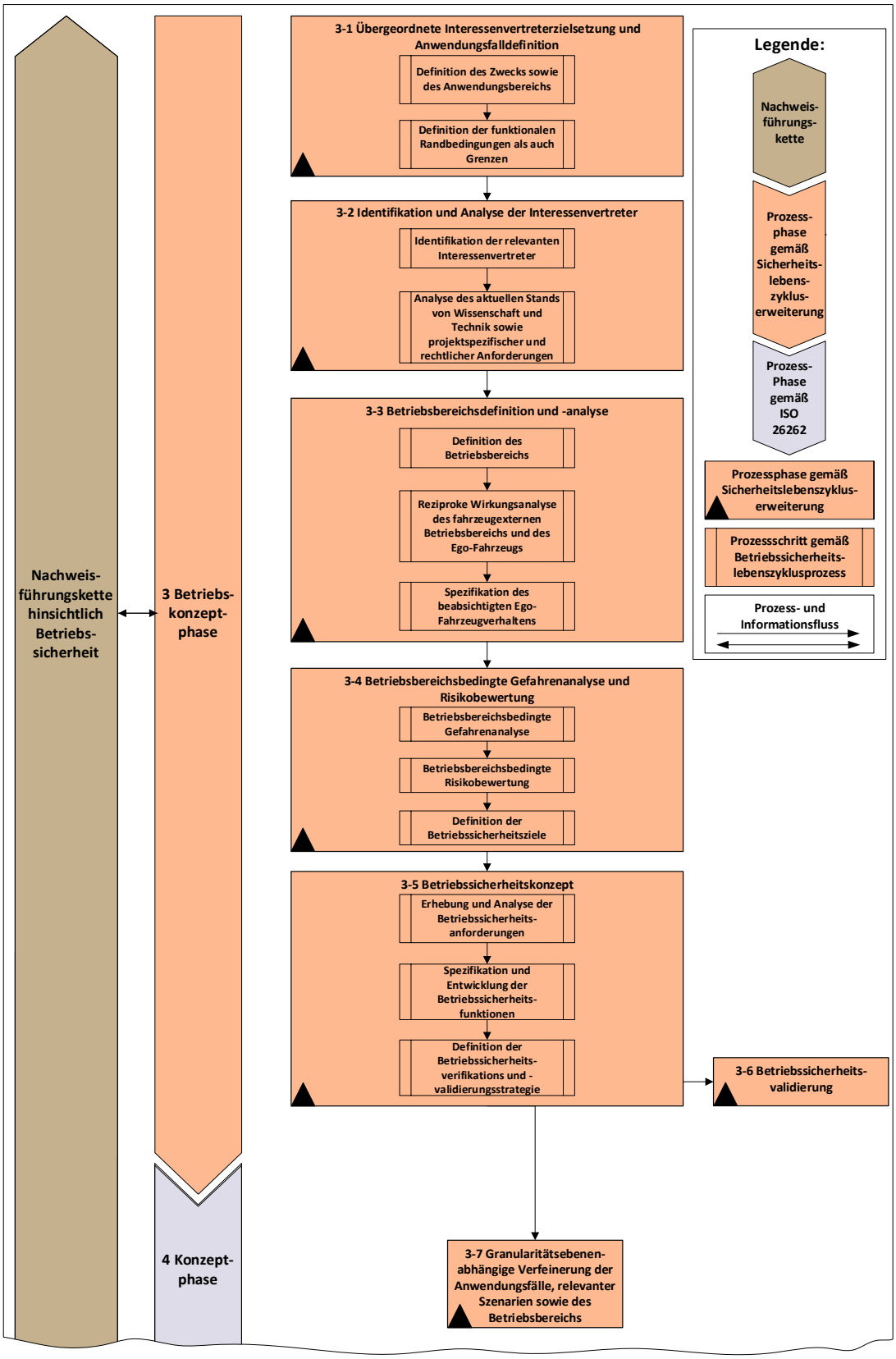


Abbildung 7.4: Detailliertes Top-Down-Prozessablaufdiagramm der Teil 3 Betriebskonzeptphase des eingeführten Betriebssicherheitslebenszyklusprozesses.

e) ein der gegebenen Granularitäts- und Abstraktionsebene angemessenes Verständnis der spezifizierten Anwendungsfälle zu fördern, damit die Aktivitäten in den nachfolgenden Phasen durchgeführt werden können.

Allgemein durchzuführende Prozesstätigkeiten

Die Anwendungsfalldefinition (engl. *Use Case Definition*) repräsentiert die Initiierung des gesamten Entwicklungsvorhabens und spiegelt im Sinne der Anforderungsentwicklung auf oberster Granularitätsebene den Ausgangspunkt für alle weiteren sicherheitstechnischen Entwicklungsaktivitäten wider. Ferner gibt diese den Entwicklungsrahmen bzw. -umfang vor und wird als Referenz für ein einheitliches Verständnis sowie einen gemeinsamen Entwicklungskontext herangezogen. Hierbei zielt die Anwendungsfalldefinition darauf ab, die Kundenanforderungen und -bedürfnisse an das zu entwickelnde System-Of-Systems anhand von spezifischen Anwendungsfällen zu formalisieren und strukturiert zu erfassen. Diese beinhalten eine Beschreibung des Funktionsumfangs und des gewünschten Verhaltens, ohne dabei auf spezifische Details einzugehen. Dabei wird der grundsätzliche Zweck des zu entwickelnden System-Of-Systems, beispielsweise der hochautomatisierte Transport von Personen und Gütern auf der Straße, identifiziert und herausgestellt. Zudem erfolgt eine erste grobe Definition der Systemgrenzen sowie die Ableitung der beabsichtigten Umgebung des System-Of-Systems einschließlich der Zielländer. Darunter fallen abstrakte Aspekte wie Region, beispielsweise Deutschland, in Frage kommende Typen des befahrbaren Bereichs, wie Autobahnen, Landstraßen etc., sowie das Transportmittel, z.B. ein Personenkraftwagen, sowie mögliche Umgebungsbedingungen wie Wetter, Tages- und Nachtzeiten bis hin zu unterstützenden Infrastruktursystemen. Die dabei vorgenommenen Annahmen und Einschränkungen sind entsprechend der Spezifikation der Argumente festzuhalten.

Darüber hinaus werden die Anwendungsfälle um den Automatisierungsgrad unter Berücksichtigung von Features wie „Folge vorausfahrendem Fahrzeug hochautomatisiert“, „Folge Fahrspur hochautomatisiert“, „Führe Spurwechsel hochautomatisiert aus“ usw. ergänzt (vgl. Abschnitt 4.8). Dieses Vorgehen erfolgt aus Kunden bzw. Anwenderperspektive. Es umfasst, welches verkehrstypische Verhalten die Anwender und andere beteiligte Akteure, beispielsweise Fußgänger, Radfahrer, vorausfahrende Fahrzeuge etc. innerhalb der jeweiligen Situationen von dem zu entwickelnden System-Of-Systems zu erwarten haben und welche Beweggründe sich für das erwartete Verhalten ergeben. Somit wird festgelegt, welcher Akteur welche Rollen und Aufgaben innerhalb welcher Umgebung übernimmt. In diesem Zusammenhang stellen die abstrakt beschriebenen Funktionalitäten und Aspekte der beabsichtigten Einsatzumgebung einen modularen Rahmen für die nachfolgenden Prozessabschnitte zur Verfügung, um darin im Sinne der Interessenvertreteridentifikation und Betriebsbereichsdefinition weiter präzisiert werden zu können. Folglich sind auch hier die deduzierten Annahmen und Einschränkungen für eine begründbare und stichhaltige Argumentation zu dokumentieren.

3-1.2 Arbeitsprodukte

3-1.2.1 Anwendungsfalldefinition gemäß 0

Teil 3-2 Identifikation und Analyse der Interessenvertreter

3-2.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) die relevanten Interessenvertreter wie Hersteller-, Zulieferer-, und Betreiberorganisationen, Endnutzer, Gesetzgeber, Behörden sowie ggf. weitere Institutionen des Entwicklungsvorhabens zu identifizieren;

b) unter Berücksichtigung unternehmensbezogener, organisatorischer und projektspezifischer Rahmenbedingungen übergeordnete Anforderungen bezüglich des Entwicklungsvorhabens bzw. des zu entwickelnden Produkts respektive System-Of-Systems zu erheben;

c) auf Grundlage von

- relevanten behördlichen Gesetzen,
- relevanten Verordnungen und Richtlinien wie Straßenverkehrsgesetz, Produktsicherheits- und Produkthaftungsgesetz, Zulassungsvorschriften, Typgenehmigungen, Straßenverkehrsordnungen etc.,
- relevanten national und international gültigen Normen, Standards und Spezifikationen,
- den aktuellen Stand von Wissenschaft und Technik,

den rechtlichen Kontext des Entwicklungsvorhabens zu identifizieren und zu analysieren;

d) die auf Basis der gültigen Gesetze, behördlichen Vorgaben und Richtlinien, Normen und Standards sowie des aktuellen Stands von Wissenschaft und Technik übergeordneten Anforderungen bzgl. des Entwicklungsvorhabens bzw. des zu entwickelnden Produkts respektive System-Of-Systems zu erheben;

3-2.2 Allgemein durchzuführende Prozesstätigkeiten

Unter Bezugnahme der beabsichtigten Funktionalität sowie der festgelegten Systemgrenzen der spezifizierten Anwendungsfälle, exemplarisch sei hier der hochautomatisierte Transport von Personen mittels eines Personenkraftwagens auf deutschen Autobahnen genannt, werden zunächst die relevanten Interessenvertreter wie Hersteller-, Zulieferer-, und Betreiberorganisationen, Endnutzer, Gesetzgeber, Behörden sowie ggf. weitere Institutionen des Entwicklungsvorhabens identifiziert. Daraus leitet sich der Entwicklungskontext der zu entwerfenden und daraufhin zu betreibenden System-Of-Systems ab. Die Definition dieses Kontexts beinhaltet die Strategie, die Planung, die Agenda, den Umfang sowie den Ablauf der nachfolgenden Analyse- und Argumentationsaktivitäten. Auf Grundlage dessen werden die verschiedenen Gesichtspunkte und Perspektiven der involvierten Interessenvertreter auf das Entwicklungsvorhaben überprüft. Anschließend werden unter Berücksichtigung unternehmensbezogener, organisatorischer, projektspezifischer sowie regulatorischer Rahmenbedingungen die übergeordneten Anforderungen, Annahmen, Hypothesen und Einschränkungen erhoben.

Von besonderer sicherheitstechnischer Relevanz erweisen sich die länderspezifischen produktbezogenen Gesetze, Richtlinien und Standards, sprich der jeweils geltende rechtliche Kontext und dessen Perspektive auf das Entwicklungsvorhaben. Darunter fallen Verordnungen und Richtlinien wie Straßenverkehrsgesetze, Produktsicherheits- und Produkthaftungsgesetze, Zulassungsvorschriften und Typgenehmigungen sowie Straßenverkehrsordnungen (vgl. Abschnitt 5.1). Hierbei ist insbesondere die Straßenverkehrsordnung hervorzuheben, worin es um die Einhaltung der Verkehrsregeln, die Vermeidung kritischer Verkehrssituationen und Unfällen unter Berücksichtigung von unterschiedlichen Straßen- und Witterungsverhältnissen geht.

Um die gesetzlichen und regulatorischen Vorgaben zu erfüllen, werden diese zunächst analysiert, per Top-Down-Ansatz in deren Grundprinzipien zerlegt und anschließend systematisch als verbindliche

Anforderungen für die spätere Systemspezifikation festgehalten. Dieses Vorgehen kennzeichnet sich insbesondere durch vorzunehmende Deduktionsschritte, welche sich in Annahmen, Hypothesen und Einschränkungen äußern und wiederum im Sinne der Spezifikation der Argumente erfasst werden müssen. Des Weiteren wird auf Basis der Sorgfaltspflicht der aktuelle Stand von Wissenschaft und Technik, der von der Gesellschaft erwartbare Nutzen unter Gewährleistung der Betriebssicherheit, sowie die Einhaltung anerkannter ggf. ethischer Normen und Standards mitberücksichtigt. Dabei ist die Nachvollziehbarkeit und Rückverfolgbarkeit der jeweiligen Anforderungen sowie deren konkrete Umsetzung essenziell für den Nachweis der Produktkonformität.

3-2.3 Arbeitsprodukte

3-2.3.1 Spezifikation der projektbezogenen Anforderungen gemäß 3-2.2

3-2.3.2 Spezifikation der behördlichen Anforderungen gemäß 3-2.2

Teil 3-3 Betriebsbereichsdefinition und -analyse

3-3.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) den Betriebsbereich einschließlich der Verknüpfung und Querbeziehungen der Elemente, Bausteine, Parameterbereiche sowie möglichen Situationen und Bedingungen mit dem benötigten Detaillierungsgrad unter Berücksichtigung der Anwendungsfälle als auch Perspektiven der Interessenvertreter auf oberster Granularitätsebene zu instanziieren und zu definieren;

b) die nichtrelevanten Betriebsbereichselemente sowie nichtrelevante Kombinationen, Parameterbereiche, Situationen als auch Bedingungen auszuschließen und damit die Grenzen des definierten Betriebsbereichs festzulegen;

c) den definierten Betriebsbereich mit Hinblick auf die möglichen Interaktionen und Auswirkungen, welche durch das mögliche Systemverhalten und den festgelegten Funktionsumfang sowie der anzuwendenden und einzuhaltenden Gesetze und Regularien hervorgerufen werden können, zu analysieren;

d) auf Grundlage der Betriebsbereichsanalyse das elementare beabsichtigte Nominalverhalten und Fähigkeiten der zu entwickelnden oder zu nutzenden System-Of-Systems zu spezifizieren und unter Berücksichtigung der Betriebsbereichsinstanziierung Szenarien zur Erfüllung der Anwendungsfälle abzuleiten;

3-3.2 Allgemein durchzuführende Prozesstätigkeiten

Auf Autobahnen, Landstraßen innerhalb und außerhalb geschlossener Ortschaften oder auf Parkanlagen ergeben sich jeweils in Abhängigkeit der Umgebungsbedingungen wie Wind, Regen, Schneefall, Sonneneinstrahlung etc. sowie der Verkehrsteilnehmer differenzierte Anforderungen an das Verhalten der zu entwickelnden System-Of-Systems. Für den Betriebssicherheitsnachweis muss daher zuerst ein zweckmäßiges Verständnis der jeweiligen Betriebsbedingungen und den dadurch abgesteckten Systemgrenzen geschaffen werden (vgl. Unterabschnitt 2.2.3). Um eine gemeinsame Konversationsbasis unter den beteiligten Interessenvertretern zu schaffen, wird für die Betriebsbereichsdefinition eine Betriebsbereichstaxonomie (ISO 34503 [91], PEGASUS Schichtenmodell [269],

ASAM OpenODD [307] etc.) herangezogen. Ferner erfolgt die Betriebsbereichsdefinition mit unterschiedlichem Detaillierungsgrad. Dieser wird im Zuge der Betriebskonzeptphase und in Abhängigkeit der Anwendungsfälle so gewählt, dass die nachfolgenden Analyseaktivitäten und die Entwicklung des Betriebssicherheitskonzepts ermöglicht werden. Somit kann es in der Phase des Betriebskonzepts beispielsweise ausreichen, lediglich anzugeben, dass Fahrbahnmarkierungen zum Betriebsbereich gehören. Im Laufe der nachgelagerten Prozessphasen (Konzeptphase, Produktentwicklung auf Systemebene oder Produktentwicklung auf Hardware- und Softwareebene siehe Abbildung B.1 und Abbildung B.2) wird die Betriebsbereichsdefinition modular weiter ausdetailliert (vgl. Teil 3-7). Hierbei wird dann je nach Bedarf die exakte Breite, Länge, die farblichen Bestandteile, der Zustand usw. der Fahrbahnmarkierungen beschrieben, um damit z.B. die benötigten Fähigkeiten einer Kameraeinheit darlegen zu können. Die Betriebsbereichsdefinition muss infolgedessen so erweiterbar sein, dass neue Attribute oder Details systematisch hinzugefügt werden können.

Des Weiteren kann der Betriebsbereich aus unterschiedlichen Perspektiven der jeweils beteiligten Interessenvertreter (lokale Behörden, Regulierungsbehörden, Dienstleister, Hersteller, Entwickler oder Lieferanten von Komponenten und Teilkomponenten) spezifiziert werden. Eine Stadtverwaltung kann z.B. eine Betriebsbereichsdefinition als Teil einer Beschaffungsspezifikation für einen hochautomatisierten Mobilitätsdienst aufsetzen, während ein Fahrzeughersteller eine Betriebsbereichsdefinition entwickelt, um die Fähigkeiten und funktionalen Grenzen eines hochautomatisierten Kraftfahrzeugs entsprechenden Zulassungsbehörden zu vermitteln und den Betriebssicherheitsnachweis zu erbringen.

Ausgangspunkt für die Betriebsbereichsdefinition bilden die in der Anwendungsfalldefinition festgelegte und abstrakt beschriebene Einsatzumgebung (Zielländer, Regionen, Art und Gestalt des fahrbaren Bereichs, wie z.B. Autobahn, Landstraße, Stadtverkehr etc.) sowie die darin zu erwartenden Umgebungsbedingungen. Dabei werden Attribute wie das zu erwartet werdende Terrain und zugehörige ortsabhängige Merkmale wie Gefälle, Steigungen, Krümmungen, Zustand und Beschaffenheit des Fahrbahnbereichs etc. als Bestandteile des Betriebsbereichs festgesetzt oder davon ausgeschlossen. Analog gilt dies auch für die betriebliche Infrastruktur, wie die Verfügbarkeit und Platzierung des fahrbaren Bereichs, Navigationshilfen (Fahrbahnmarkierungen, erweiterte Beschilderung), Verkehrsmanagementeinrichtungen (Ampeln, Vorfahrtsschilder, Fahrlicht), Sperrzonen, besondere Straßennutzungsregeln (zeitabhängige Fahrspurwechsel), Baustellen, Mautstellen als auch das Vorhandensein von unterstützender Infrastruktur, Karten- und Wetterdaten usw. Zudem werden Umwelt- und Wetterbedingungen wie Oberflächentemperatur, Lufttemperatur, Luftdichte, Wind, Sicht, Niederschlag, Vereisung, Beleuchtung etc. in die Spezifikation mitaufgenommen oder davon exkludiert. Hinzu kommen dynamische Objekte im Sinne von zu erwartenden Verkehrsteilnehmern wie Last- und Personenkraftwägen, Einsatzkräfte, Radfahrer, Passanten, Tiere bis hin zu möglichen Gegenständen wie Steine, Hölzer, Plastiktüten, Radkappen, Reifenüberreste, verlorengegangene Ladungen etc. Die dabei vorgenommenen Systemabgrenzungen müssen im Sinne von Annahmen, Randbedingungen und Einschränkungen argumentiert werden.

Daraufhin erfolgt eine Betriebsbereichsanalyse der möglichen Verhaltensmuster und Einflussgrößen der spezifizierten Betriebsbereichselemente. Für eine qualitative und/oder quantitative Auswertung werden die Auftretenswahrscheinlichkeiten, z.B. unter Anwendung des Vorgehens von Ries [239] (vgl. Unterabschnitt 4.8.2), Unsicherheiten und Verteilungen der möglichen Umgebungsbedingungen wie Sonnenschein, Wind, Nebel, Regen etc. beispielsweise anhand von Wetteraufzeichnungen ermittelt und über die systematische Variation beispielsweise gemäß King [225] (vgl. Unterabschnitt 4.8.2)

deren Einfluss analysiert. Ferner können Monte-Carlo-Simulationen (vgl. Abschnitt 4.8) mit verschiedenen Parametern durchgeführt werden, um den Sichtbarkeitsbereich anhand von unterschiedlichen Beleuchtungsniveaus zu erfassen und abzugrenzen. Zudem werden die dynamische Interaktion sowie die Verknüpfungen und Querbeziehungen zwischen dem und/oder den hochautomatisiertem Ego-Fahrzeugen und dessen Anwendern, möglichen Infrastruktursystemen sowie dem restlichen fahrzeugexternen Teil des Betriebsbereichs im Sinne statischer und dynamischer Objekte systematisch erfasst. Dies resultiert in der Ableitung der betriebsbereichsbezogenen Szenarien, wobei gemäß dem Ansatz von Pfeffer [211] (vgl. Unterabschnitt 4.8.2) die extrahierten Szenarien innerhalb von erweiterbaren Katalogen abgelegt und mit Bewertungsmetriken versehen werden können.

Auf Grundlage dieser möglichen Verhaltensmuster und Einflussgrößen der spezifizierten Elemente werden die notwendigen Fähigkeiten (engl. *Capabilities*) für die zu entwickelnden System-Of-Systems abgeleitet. Darunter fallen Fähigkeiten wie relevante statische und dynamische Objekte wahrzunehmen, das zukünftige Verhalten relevanter Objekte vorherzusagen, die Ego-Fahrzeugverhaltensintention an andere Verkehrsteilnehmer zu kommunizieren sowie den Anwendern oder Fahrgästen die Kommunikation und Interaktion mit dem Ego-Fahrzeug oder ggf. mit Tele-Operatoren zu ermöglichen. Hierbei werden erste Entwurfsentscheidungen dahingehen getroffen, welche dieser Fähigkeiten von welchem zu entwickelnden oder zu nutzenden System-Of-Systems übernommen werden sollen, seien diese die hochautomatisierten Ego-Fahrzeuge oder unterstützende Infrastruktursysteme bis hin zu intelligenten Verkehrsleitsystemen. Diese Entwurfsentscheidungen werden wiederum durch getroffene Annahmen, berücksichtigte Randbedingungen und vorgenommen Einschränkungen argumentiert und begründet.

3-3.3 Arbeitsprodukte

3-3.3.1 Betriebssicherheitsdefinition gemäß 3-3.2

Teil 3-4 Betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung

3-4.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) die Gefährdungen und ihre Auswirkungen, welche sich aus dem beabsichtigten Nominalverhalten, den Fähigkeiten, dem Fehlverhalten sowie des vorhersehbaren, vorsätzlichen oder versehentlichen Missbrauchs der zu entwickelnden oder zu nutzenden System-Of-Systems innerhalb des definierten Betriebsbereichs ergeben können, systematisch zu ermitteln;

b) die Risiken, welches sich aus dem gefährdenden Verhalten des festgelegten Funktionsumfangs ergeben, sowie die jeweiligen Szenarien innerhalb welcher das gefährdende Verhalten zu Schäden führen kann, systematisch hinsichtlich ihrer potenziellen Schadenshöhe und der Wahrscheinlichkeit ihres Eintretens zu ermitteln und zu bewerten;

c) die Betriebsbereichsparameterräume, welche die Bedingungen definieren, unter denen das Nominalverhalten als auch das Fehlverhalten des zu entwickelnden oder zu nutzenden System-Of-Systems als gefährdend angesehen wird, festzulegen;

d) eine Argumentation der Abwesenheit eines inakzeptablen Risikos unter Festlegung von Risikoakzeptanzkriterien aufzubauen sowie quantitative und messbare Kriterien für die Akzeptanz von

Risiken zu definieren und die Rechtfertigung für die gewählten Risikoakzeptanzkriterien zu formulieren;

e) Betriebssicherheitsziele, welche sich auf die Vermeidung oder Verminderung der gefährdenden Ereignisse beziehen, um ein inakzeptables Risiko zu vermeiden, zu spezifizieren.

3-4.2 Allgemein durchzuführende Prozesstätigkeiten

Für die betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung werden die im Zuge der Betriebsbereichsanalyse und Systemverhaltensbeschreibung abgeleiteten Situationen sowie Szenarien (vgl. Teil 3-3) herangezogen. Dabei werden potenzielle Gefährdungssituationen und Risiken, welche sich aus dem beabsichtigten Nominalverhalten, dem Fehlverhalten sowie des vorhersehbaren, vorsätzlichen oder versehentlichen Missbrauchs der zu entwickelnden oder zu nutzenden System-Of-Systems ergeben können, in einem frühzeitigen Stadium der Betriebssicherheitsentwicklung ermittelt. Dies beinhaltet auch mögliche Infrastruktursysteme, welche das hochautomatisierte Ego-Fahrzeug mit den benötigten Kontextinformationen versorgen und unterstützen. Die frühzeitige Gefahrenanalyse trägt als Begründungsbasis dazu bei, die Kompatibilität der Betriebsbereichselemente untereinander sicherzustellen. Darüber hinaus bietet diese in Form von Annahmen, Randbedingungen und Einschränkungen die Grundlage von Entwicklungsstrategien sowie Entwurfsentscheidungen und erleichtert eine vollständige Gefahrenanalyse während der späteren Konzeptphase (siehe Abbildung B.1 bzw. Abbildung B.2). Hierfür werden Methoden wie HAZOP, STPA, FMEA oder FTA eingesetzt und um Checklisten, Unfalldatenbanken, Unfallstatistiken, Feldstudien etc. ergänzt. Zudem kann der Safer Complex Systems Frameworks von Burton et al. [271] hinzugezogen werden, um potenzielle Unfallursachen, Folgen und verschärfende Risikofaktoren zu identifizieren. Darüber hinaus bietet es sich an, auf die ITIV- bzw. FZI-Forschungsarbeiten von Schütt [231], Reisgys [228], Bernhard [236] und Ries [239] zurückzugreifen (vgl. Unterabschnitt 4.8.2). Diese stellen ein umfangreiches Set an Methoden und Werkzeugen zur Verfügung, um die Kritikalität, das Ausmaß der Unsicherheiten, die Auftrittswahrscheinlichkeiten sowie die Abdeckung sicherheitskritischer Szenarien und Gefährdungssituationen quantitativ evaluieren zu können.

Hauptquelle möglicher Automationsrisiken repräsentiert das fahrende hochautomatisierten Ego-Kraftfahrzeug. Dieses wird im Hinblick auf Gefährdungssituationen, welche aufgrund mangelnder Performanz, Stabilität und Robustheit bezüglich unbekannter, ungewöhnlicher oder die unerwartete Kombination von auslösenden Bedingungen und Ereignissen aus dem fahrzeugexternen Betriebsbereich hervorgerufen werden können, untersucht (siehe Abbildung 7.5).

Insbesondere handelt es sich hierbei um Unzulänglichkeiten bei der Erkennung und Klassifizierung statischer und dynamischer Objekte, die unzureichende Prädiktion der jeweiligen Trajektorien und Fehlinterpretation der gegebenen Verkehrssituationen. Ferner werden unangemessene Fahrzeugverhaltensweisen, welche infolge mangelhafter Fahrzeugverhaltensspezifikationen sowie Defiziten bei der Interpretation und Umsetzung der Straßenverkehrsordnung mit Blick auf die Interaktion mit anderen Verkehrsteilnehmern auftreten können, in Betracht gezogen. Dies beinhaltet auch unerwartetes bzw. nichtkonformes Verhalten der anderen Verkehrsteilnehmer. Hinzu kommen Risiken und Gefährdungen, welche sich im Zuge des Verlassens des definierten Betriebsbereichs und die Interaktion sowie Übergabe der Fahrzeugführung an den menschlichen Fahrer oder beispielsweise einem Tele-Operator ergeben können. Zudem werden mögliche Gefährdungssituationen, welche auf Abweichungen, Fehler, Ausfälle oder Fehlverhalten der Fahrzeug- und Infrastruktursysteme zurückzuführen sind, analysiert.

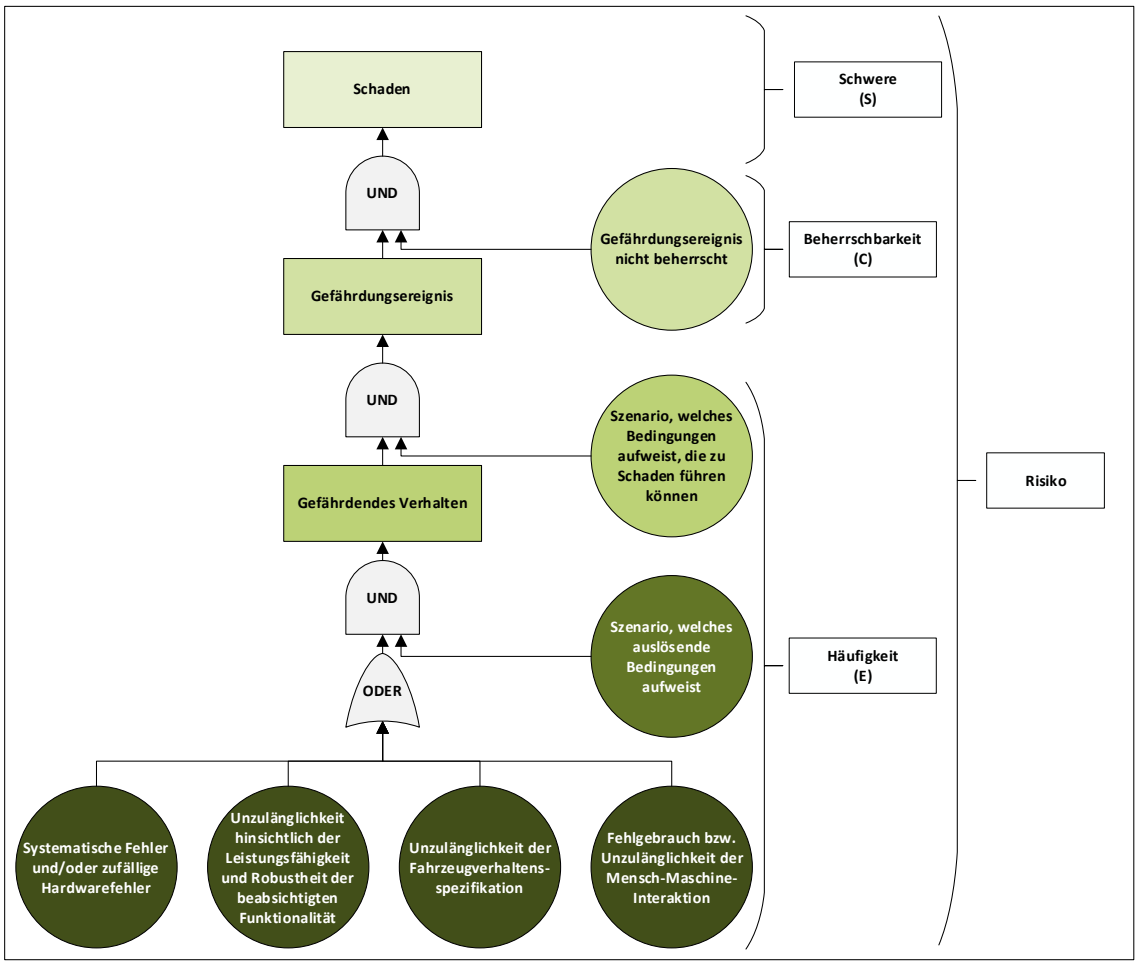


Abbildung 7.5: Qualitativer bottom-up verlaufender Fehlerbaum bezüglich möglicher Ursachen und Effekte eines Schadens als Top-Ereignis während des Betriebs eines oder mehrerer hochautomatisierter Ego-Kraftfahrzeuge.

Genauer genommen erfolgt die Gefahrenanalyse unter Berücksichtigung des beabsichtigten Fahrzeugnominalverhaltens in Abhängigkeit der physikalischen Bewegungsfreiheitsgrade und Betriebsbereichsparameterbereiche wie Geschwindigkeiten, minimaler Abstände etc. In Richtung der Fahrzeuglängsachse können gefährdende Verhaltensweisen wie zu hohe, zu niedrige, ungewollte oder oszillierende Beschleunigungen oder Verzögerungen entstehen. Diese können wiederum Gefährdungsereignisse wie Heckkollisionen als auch Seitenaufpralle mit anderen Fahrzeugen, ein instabiles oder ein nicht mehr lenkbares Fahrzeug durch blockierende Räder bis hin zu Fußgänger- und Fahrradunfällen hervorrufen. Seitens der Fahrzeugquerachse können durch zu hohe, zu niedrige, ungewollte oder oszillierende Querbeschleunigungen und Gierrate um die Fahrzeughochachse Gefährdungsereignisse wie eine unzureichende Stabilitätskontrolle des Fahrzeugs im Sinne von zu starkem Unter- und Übersteuern bei Kurvenfahrt oder das ungewollte Verlassen der Fahrspur und damit potenzielle Kollisionen mit dem Gegenverkehr entstehen.

Daraufhin werden die identifizierten Risiken anhand von Gefährdungsereignissen und deren Abläufe hinsichtlich ihrer potenziellen Schadenshöhe sowie der Wahrscheinlichkeit ihres Eintretens eingestuft. Genauer genommen erfolgt dies anhand der Schwere (engl. *Severity {S}*) eines möglichen Schadens, der Häufigkeit (engl. *Exposure {E}*) des Szenarios, welches zu einem möglichen Schaden führen

kann, sowie der Beherrschbarkeit (engl. *Controllability {C}*) der jeweils in einem Gefährdungsereignis beteiligten Akteure (siehe Abbildung 7.5). Unter Bezugnahme von statistischen Daten, Unfallanalysen sowie Erfahrungswerten wird dann basierend auf Expertenwissen die ASIL-Klassifizierung der jeweiligen Gefährdungsereignisse durchgeführt (vgl. Unterabschnitt 5.2.1).

Zudem wird eine systematische Argumentation der Abwesenheit eines inakzeptablen Risikos unter Festlegung von Risikoakzeptanzkriterien, z.B. die maximal zulässige Anzahl von Unfällen pro Stunde, aufgebaut sowie quantitative und messbare Kriterien für die Akzeptanz von Restrisiken definiert und eine Rechtfertigung für die gewählten Risikoakzeptanzkriterien formuliert. Dies erfolgt unter Bezugnahme von behördlichen und industriellen Regularien, Unfallstatistiken, Verkehrsanalysen und -daten als auch dem aktuellen Stand von Wissenschaft und Technik.

Die zu begründende Gesamtargumentation des tolerierbaren Risikos kann dabei auf einem oder einer Kombination des GAMAB[3]-, ALARP[4]-, MEM[5]-Ansatzes [55] sowie des Ansatzes einer positiven Risikobilanz (z.B. Restrisiko geringer als Unfallrisiko durch menschliche Fahrer im Zuge des herkömmlichen Straßenverkehrs) beruhen. Im Anschluss werden implementierungsneutrale Betriebssicherheitsziele, welche sich auf die Vermeidung oder Verminderung der gefährdenden Ereignisse beziehen und damit ein akzeptables Restrisiko gewährleisten sollen, spezifiziert. Dies beinhaltet u.a. die Beschreibung der anwendbaren Bedingungen und Zustände eines minimalen Risikos sowie die Argumentation, warum diese in Form von dokumentierten Behauptungen sicher sind. Ferner wird die Verantwortung für die Erfüllung der jeweiligen Betriebssicherheitsziele auf das hochautomatisierte Kraftfahrzeug oder aber auf den fahrzeugexternen Betriebsbereich im Sinne der Betreiber, Anwender, Verkehrsteilnehmer als auch der möglicherweise involvierten unterstützenden Infrastruktursysteme, intelligenten Verkehrsleitsysteme etc. zugewiesen.

Abschließend ist die betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung einschließlich der Betriebssicherheitsziele zu verifizieren. Dabei soll sichergestellt werden, dass die Auswahl der Betriebssituationen und Gefahrenidentifikation einschließlich der Infrastruktur- und Ego-Kraftfahrzeugkonfiguration, angemessen ist. Des Weiteren ist die Übereinstimmung mit der Betriebsbereichsdefinition zu gewährleisten und die Konsistenz sowie die akzeptable Abdeckung der Gefährdungsereignisse nachzuweisen. Ferner ist die Übereinstimmung der Betriebssicherheitsziele mit den zugewiesenen ASILs sowie den Gefährdungsereignissen darzulegen.

3-4.3 Arbeitsprodukte

3-4.3.1 Bericht der betriebsbereichsbedingten Gefahrenanalyse und Risikobewertung gemäß 3-4.2

3-4.3.2 Spezifikation der Betriebssicherheitsziele und -anforderungen gemäß 3-4.2

[3] GAMAB steht für das französische „Globalement Au Moins Aussi Bon“, was „insgesamt mindestens genauso gut“ bedeutet. Nach diesem Grundsatz ist das Restrisiko (in Bezug auf die Sicherheit) eines neuen Systems nicht höher als das eines bestehenden Systems mit vergleichbarer Funktionalität oder Gefährdungen.

[4] Der „As Low As Reasonably Practicable“ (ALARP)-Ansatz zielt darauf ab, das vorhandene Restrisiko auf ein als „angemessen praktikabel“ angesehenes Niveau zu reduzieren, indem dieses gegen den hierfür benötigten Aufwand abgewogen wird.

[5] Das „Minimal Endogenous Mortality“ (MEM)-Prinzip basiert darauf, dass die Einführung eines technischen Systems die Sterberate innerhalb einer Gesellschaft nicht signifikant erhöhen sollte. Quantitative Akzeptanzkriterien für die durch ein technisches System verursachte Sterbewahrscheinlichkeit werden aus der Mindestwahrscheinlichkeit des Todes durch natürliche Ursachen abgeleitet.

3-4.3.3 Verifikationsbericht der betriebsbereichsbedingten Gefahrenanalyse und Risikobewertung gemäß 3-4.2

Teil 3-5 Betriebssicherheitskonzept

3-5.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) Strategien, Schutzmaßnahmen, Einschränkungen und Kenngrößen im Sinne von Betriebssicherheitsfunktionen auf Betriebsbereichsebene
   - für eine geeignete und rechtzeitige Erkennung und Beherrschung relevanten Fehl- und gefährdenden Verhaltens in Übereinstimmung mit den Betriebssicherheitszielen,
   - zur Erreichung der erforderlichen Fehlertoleranz oder zur angemessenen Minderung von Auswirkungen relevanten Fehl- und gefährdenden Verhaltens durch Maßnahmen innerhalb des Betriebsbereichs,

   zu spezifizieren;

b) das funktionale oder degradierte funktionale Verhalten innerhalb des Betriebsbereichs in Übereinstimmung mit den Betriebssicherheitszielen zu spezifizieren;

c) Kriterien und Strategien für die Verifikation und Validierung des Betriebssicherheitskonzepts festzulegen;

3-5.2 Allgemein durchzuführende Prozesstätigkeiten

Grundsätzlich leiten sich aus der betriebsbereichsbedingten Gefahrenanalyse und Risikobewertung drei Kernhandlungsfelder für den Betriebssicherheitsnachweis ab. Zunächst ist dies die durch Evidenzen und Argumente rechtfertigte Behauptung der Fähigkeit von Unfallvermeidung und Regelkonformität seitens aller Verkehrsszenarien und -situationen innerhalb eines definierten Betriebsbereichs. Hinzu kommt die Behauptung der nachweislichen Einhaltung der gebotenen Sorgfalt u.a. durch Anwendung und Berücksichtigung von etablierten Managementaktivitäten, Prozessen, Standards, Methoden einschließlich einschlägiger Top-Down- und Bottom-Up-Analysen sowie des aktuellen Stands von Wissenschaft und Technik. Darüber hinaus ist der Nachweis bzw. die Behauptung einer positiven Risikobilanz, beispielsweise die Unterschreitung des Unfall- oder Gefährdungsrisikos für Fahrzeuginsassen und andere Verkehrsteilnehmer hervorgerufen durch den herkömmlichen Straßenverkehr bzw. den menschlichen Fahrer, zu erbringen.

Um die hierfür spezifizierten Betriebssicherheitsziele zu erfüllen, werden im Zuge des Betriebssicherheitskonzepts Betriebssicherheitsmaßnahmen hinsichtlich der hochautomatisierten Ego-Fahrzeuge, aber auch des fahrzeugexternen Betriebsbereichs im Sinne konstruktiver und bauartbedingter Maßnahmen sowie organisatorischen oder schulischen Instruktionen im Hinblick auf die involvierten Akteure entwickelt. Hinzu kommt die systematische Absicherung von unterstützenden Infrastruktursystemen. Im Speziellen geht es darum, inakzeptable Risiken in Richtung von akzeptablen Risiken systematisch zu reduzieren (siehe Abbildung 7.6).

Das Betriebssicherheitskonzept selbst wird entlang zweier Entwicklungspfade aufgesetzt. Die innerhalb der beiden Entwicklungspfade jeweils definierten Betriebssicherheitsfunktionen bilden wiederum den systematischen Übergang in die Konzeptphase und damit auf der einen Seite die Item Definition gemäß ISO 26262 respektive die Spezifikation und das Design der jeweiligen Funktionalitäten gemäß ISO 21448 auf der anderen Seite (siehe Abbildung B.1 und Abbildung B.2).

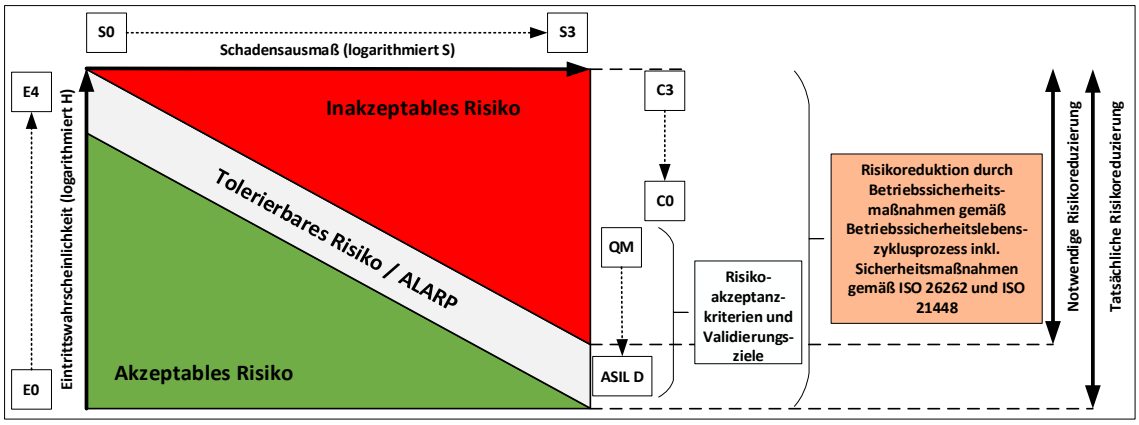


Abbildung 7.6: Konkretisierung der allgemeinen Darstellung des akzeptablen und nicht akzeptablen Risikos (siehe Abbildung 5.3) sowie der Risikominimierung gemäß des konzipierten Betriebssicherheitslebenszyklusprozesses.

Betriebssicherheitskonzept im Hinblick auf das Ego-Kraftfahrzeug:

Im Zuge des ersten Pfades erfolgt die Betriebssicherheitsentwicklung, was das hochautomatisierte Ego-Kraftfahrzeug angeht. Hierfür werden als erstes die dynamischen Betriebsbereichselemente aus einer Black-Box-Perspektive sozusagen beobachtet und das jeweilige Verhalten anhand von physikalischen Gesetzen im Sinne der Bewegungsfreiheitsgrade betrachtet.

Darüber hinaus sind Kontextanalysemethoden einzusetzen, um das hochautomatisierte Fahrzeug und dessen Umgebung dergestalt miteinander in Bezug zu setzen, damit ersichtlich wird, welche Elemente des fahrzeugexternen Teils des Betriebsbereichs unter welchen Gegebenheiten eine adäquate Fahrzeugreaktion erfordern. Auf Grundlage dessen sowie unter Bezugnahme der in den Anwendungsfällen beschriebenen Features wie „Folge vorausfahrendem Fahrzeug hochautomatisiert“, „Folge Fahrspur hochautomatisiert“, „Führe Spurwechsel hochautomatisiert aus“ wird dann systematisch das beabsichtigte Nominalverhalten sowie die notwendigen Fahrmanöver des Ego-Fahrzeugs spezifiziert.

In erster Linie geht es darum, die Kombinatorik der jeweiligen Zustände (Anfahren, Anhalten, stationäre Geradeausfahrt, Kurvenfahrt etc.) sowie deren Übergänge (von Geradeausfahrt zur Kurvenfahrt, von trockener Fahrbahn zu nasser Fahrbahn usw.) festzulegen. Ferner wird daraus das elementare Fahrzeugverhalten bzw. die an die Situation angepasste Fahrdynamik (beschleunigen, verzögern und lenken) deduziert. Für eine einheitliche und harmonisierte Konversationsbasis erfolgt dies anhand standardisierter Begriffe aus der ISO 8855 [308]. Diese Aktionen und Ereignisse werden zudem um transiente (beispielsweise die aktuelle Transportmission) sowie permanente (regulatorische als auch gesellschaftliche Rahmenbedingungen und Anforderungen aus der Analyse der Interessenvertreter vgl. Teil 3-2) Ziele und Werte ergänzt. Darunter fallen Einsatzregeln sowie Erwartungen für die Interaktion mit der Umgebung und anderen Aspekten des operativen Zustandsraums, einschließlich Verkehrsgesetze, soziale Normen und Signalisierungs- und Verhandlungsverfahren mit anderen Verkehrsteilnehmern (sowohl automatisierte Fahrzeuge sowie herkömmliche mit menschlichen Fahrern, einschließlich expliziter Signalisierung sowie impliziter Signalisierung der Intention des Ego-Fahrzeugverhaltens).

Die Herleitung der Verhaltensspezifikation kennzeichnet sich dabei durch das Treffen von Annahmen und Hypothesen, welche ausdrücklich als solche kenntlich gemacht und für nachfolgende Nachweis- und Argumentationsschritte dokumentiert werden müssen. Aus der dynamischen Abfolge der Aktionen und Events der statischen sowie dynamischen Betriebsbereichselemente werden wiederum die Szenarien zur Erfüllung der jeweiligen Anwendungsfälle (vgl. Teil 3-3) abgeleitet. Jede in den Gesetzestexten und Regularien beschriebene Verkehrssituation sowie jedes Betriebsbereichselement, welches ein spezifisches Verhaltensmuster der Entwicklungsgegenstände (Ego-Kraftfahrzeug und/oder unterstützendes Infrastruktursystem) als Reaktion darauf erfordert bzw. hervorruft, wird hierbei durch mindestens ein Szenario abgedeckt. Zudem werden die ermittelten Situationen und Szenarien durch Verkehrsstatistiken aus Fahrdaten im realen Straßenverkehr ergänzt. Dadurch lässt sich die Wahrscheinlichkeit ihres Auftretens und die Verteilung ihrer Eigenschaften in der realen betrieblichen Straßenumgebung beschreiben.

Des Weiteren werden die Betriebssicherheitsziele in Bezug auf das präventive und regelkonforme Fahrverhalten betrachtet. Diese bilden die Basis für eine sichere Fahrzeugverhaltensspezifikation bzw. Fahrverhaltensrichtlinien in Übereinstimmung mit den jeweils geltenden Verkehrsvorschriften und -regeln, so dass sich die hochautomatisierten Kraftfahrzeuge derart verhalten, wie es die verschiedenen Teilnehmer des Straßenverkehrs erwarten können. Somit werden für die Planung, Umsetzung und Überwachung einer gesetzeskonformen, proaktiven, reaktiven, aber auch unfallfreien (so weit wie praktikabel möglich) Fahrzeugverhaltensspezifikation die jeweils benötigten Betriebssicherheitsfunktionen spezifiziert. Hierfür werden auf Grundlage der Analyse der Straßenverkehrsordnung (vgl. Teil 3-2) sowie anhand von Unfallanalysen, physikalischen Gesetzen, konstruktiven Beschränkungen etc. KPIs sowie Grenz- bzw. Schwellenwerte für quantifizierbare und damit validierbare Fahrverhaltensmuster abgeleitet und mit Blick auf Annahmen, Hypothesen, Randbedingungen und Einschränkungen argumentiert. Dabei handelt es sich um Abstands- und Geschwindigkeitskorridore in Abhängigkeit der Straßentypen und -abschnitte (Autobahn, Landstraßen, innerstädtisch etc.) sowie unter Berücksichtigung der Witterungsverhältnisse und Sichtbedingungen als auch der involvierten Verkehrsteilnehmer. Für die situationsbedingten Verhaltensweisen werden überdies systematisch nachvollziehbare und rückverfolgbare „Wenn-dann-Regeln“ abgeleitet. Ein wichtiger Aspekt ist dabei das Vorhandensein alternativer Handlungsweisen. In Anbetracht dessen wird u.a. auch auf strafrechtliche Wertungen zurückgegriffen, um eine quantitative und qualitative Gewichtung der potenziell gefährdeten Güter zu bestimmen. Die Gewichtung dient dazu, im Falle einer notwendigen Notfallreaktion aus mehreren Trajektorien Optionen die adäquateste auswählen zu können.

Hierbei wird auch das benötigte Leistungsniveau der Aus- und Durchführung dieser Verhaltensmuster spezifiziert. Beispielsweise sollte ein hochautomatisiertes Kraftfahrzeug eine Kollision vermeiden, indem es zum einen ein geeignetes Notfallmanöver (Vollbremsung und/oder Ausweichen) und zum anderen dieses auch mit einer angemessenen Leistungsfähigkeit der Verzögerung und Querbeschleunigung ausführt, welche die Straßenreibung, die Szenenkonfiguration und andere relevante Bedingungen berücksichtigt. Ferner muss sichergestellt werden, dass während dieses Manövers die Lenk- und Bremsfähigkeit, sprich die Beherrschbarkeit erhalten bleibt. Mit zunehmender Geschwindigkeit nimmt einerseits die Sicherheitsintegrität ab und andererseits steigt die Kritikalität der jeweiligen Situationen an. Dementsprechend werden geschwindigkeits- und reaktionszeitabhängige Toleranzbereiche vorgegeben, die quantifizierbare Abweichungen, z.B. von der vorgeschriebenen Fahrspur, erlauben. Falls das hochautomatisierte Kraftfahrzeug diesen Schwellenwerten zu nahekommt, muss sichergestellt werden, dass beispielsweise die Geschwindigkeit verringert wird.

Für die relevanten Sicherheitsschwellen werden Maßnahmen bzw. Strategien zur kontinuierlichen Beobachtung und Aufzeichnung entwickelt. Weichen diese Werte plötzlich, sporadisch oder auch kontinuierlich über einen Zeitraum stärker vom nominalen Wert ab, so kann dies auf unterschiedliche Ursachen zurückzuführen sein. Auf der einen Seite kann es sich um Unzulänglichkeiten einer ausreichenden Performanz, Stabilität und Robustheit gegenüber fahrzeuginternen sowie fahrzeugexternen Unsicherheiten im Sinne der Sicherheit der beabsichtigten Funktionalität handeln. Hierfür werden die Betriebssicherheitsziele des beabsichtigten Nominalverhaltens inkl. der spezifizierten Fähigkeiten des Ego-Kraftfahrzeugs für die Bereitstellung der jeweiligen Anwendungsfälle und kundenerlebbaren Funktionen herangezogen.

Gemäß der ASIL-Klassifizierung und Akzeptanzkriterien der Betriebssicherheitsziele werden Maßnahmen und Strategien festgelegt, um die jeweiligen Fahrzeugfähigkeiten, wie z.B. relevante statische und dynamische Objekte wahrzunehmen, die spezifizierte Fahrzeugverhaltensplanung korrekt auszuführen etc., mit einer ausreichenden Performanz, Stabilität sowie Robustheit anhand von Betriebssicherheitsfunktionen auszulegen. Für eine angemessene Reaktion auf unerwartete bzw. unbekannte Situationen, welche entweder im Entwicklungsprozess übersehen oder aber durch neuartige Verkehrsteilnehmer o.Ä. hervorgerufen werden können, werden Überwachungs- und Degradationskonzepte aufgesetzt, welche das Überführen in einen Zustand minimalen Risikos (z.B. Anhalten auf dem Standstreifen) ermöglichen und unter zu erfüllenden Prämissen dessen sicheres Verlassen wiederum koordinieren. Darauf bezugnehmend kann beispielsweise ein Laufzeitobjekt des definierten Betriebsbereichs instanziiert werden, um diesen während des Betriebs im Sinne der funktionalen Systemgrenzen zu beobachten.

Aber auch infolge von zufälligen (Alterungseffekte, Verschleiß etc.) und systematischen Fehlern kann es im Hinblick auf die funktionale Sicherheit (vgl. Unterabschnitt 5.2.1) zu Ausfällen der notwendigen Basisfunktionalitäten kommen. Aufgrund der Hochautomatisierung der Fahraufgabe und des Wegfalls des menschlichen Fahrers als Rückfallebene im Fehlerfall, kann auf solche Ereignisse nicht mehr mit „Fail-Safe“-Mechanismen reagiert werden. Folglich werden hierfür „Fail-Operational“-Redundanzkonzepte und -funktionen in Übereinstimmung mit den definierten Betriebssicherheitszielen und Verfügbarkeitsanforderungen spezifiziert. Diese Betriebssicherheitsfunktionen umfassen demnach die Erkennung und Einnahme sicherer Betriebsmodi, die Durchführung sicherer Zustandsübergänge aber auch Maßnahmen zur Feststellung, ob die situativ geforderte Funktionalität auch unter Einfluss von Fehlern, Abweichungen und Ausfällen erbracht und im Falle der Nichterbringung die sichere Degradation bis hin zur Einnahme eines sicheren Zustands vollzogen werden kann.

Betriebssicherheitskonzept im Hinblick auf den fahrzeugexternen Betriebsbereich:

Entlang des zweiten Pfades läuft die Betriebssicherheitsentwicklung im Hinblick auf den fahrzeugexternen Betriebsbereich ab. Dies umfasst Betriebssicherheitsmaßnahmen und -funktionen was die physische Infrastruktur, Aktivitäten von Nutzern und Betreibern, unterstützende Infrastruktursysteme bis hin zu intelligenten Verkehrsleitsystemen mit zugehörigen Diensten betrifft. Zählt die physische Infrastruktur zu den relevanten Faktoren der Betriebssicherheitsargumentation, so werden hierfür konstruktive bzw. gestalterische Maßnahmen wie Zäune, Absperrungen, Leitplanken, Beschilderungen, Markierungen, Kennzeichnungen, Signalisierungen sowie organisatorische Einschränkungen für Passanten, Radfahrer oder andere Verkehrsteilnehmer beispielsweise für Fahrbahnbereiche, worin ausschließlich hochautomatisierte Kraftfahrzeuge betrieben werden dürfen, spezifiziert.

Des Weiteren werden auf Grundlage der Betriebssicherheitsziele in Bezug auf das Verlassen des definierten Betriebsbereichs sowie der sicheren Übergabe der Verantwortung der Fahrzeugführung an den jeweiligen Anwender Bedienkonzepte im Sinne der Gebrauchssicherheit spezifiziert. Dabei handelt es sich um Überwachungsmaßnahmen zur rechtzeitigen Erkennung der Betriebsbereichsgrenzen und der Bereitschaft des menschlichen Fahrers oder Tele-Operators, die Fahraufgabe zu übernehmen. Für den Fall, dass die Übernahme nicht rechtzeitig erfolgen kann, werden Strategien zur sicheren Überführung in einen Zustand minimalen Risikos entwickelt. Zudem werden Betriebssicherheitsfunktionen aufgesetzt, welche die sichere Aktivierung und Deaktivierung der hochautomatisierten Fahrfunktionen koordinieren und einen vorhersehbaren, vorsätzlichen oder versehentlichen Fehlgebrauch, beispielsweise eine Aktivierung außerhalb des zugelassenen Betriebsbereichs, unterbinden. Des Weiteren werden je nach Anwendungsfall Betriebssicherheitsmaßnahmen, welche bisher durch die Verpflichtungen von Fahrern und Haltern (Überwachung der Fahrzeugbeladung, des Fahrzeugzustands, der Beleuchtungsanlage, des Reifenzustands, des Reifenluftdrucks usw.) gewährleistet wurden, in die Fahrzeugspezifikation mitaufgenommen.

Sind unterstützende Infrastruktur- oder intelligente Verkehrsleitsysteme für die Koordinierung von Fahrzeugflotten sowie die damit verbundenen Dienste wie Karten-, Unfall- und Wetterdaten, V2X-Kommunikation, die Lokalisierung über GPS bis hin zur Übermittlung von Fahranweisungen an das hochautomatisierte Kraftfahrzeug von Tele-Operatoren über das Mobilfunknetz Bestandteil der gesamtheitlichen Betriebssicherheitsargumentation, so werden auf Grundlage der hierfür abgeleiteten Betriebssicherheitsziele zweckmäßige Betriebssicherheitsmaßnahmen und -funktionen spezifiziert. Dabei sind die Betriebssicherheitsfunktionen in Übereinstimmung mit den ASIL-Klassifizierungen und Akzeptanzkriterien sowie Leistungsfähigkeitsanforderungen Sinne von zeitlichen Aspekten wie Latenz, Kommunikationstotzeiten etc. als auch der Stabilität und Robustheit (Sicherheit der beabsichtigten Funktion) sowie der notwendigen Verfügbarkeit und Redundanz (funktionale Sicherheit) für einen sicheren Gesamtbetrieb auszulegen. Dies umfasst auch die eventuelle Einnahme sicherer Zustände im Falle von Degradationen der Leistungsfähigkeit oder Ausfällen der jeweiligen System-Of-Systems.

Spezifikation der Verifikations- und Validierungsstrategie:

Daraufhin wird die Verifikations- und Validierungsstrategie einschließlich der Validierungsziele, Erfüllungskriterien und Metriken in Bezug auf die Betriebssicherheit definiert. Diese deckt das gesamte vorgesehene Betriebskonzept einschließlich aller Bestandteile und Maßnahmen ab, welche für die Erreichung der Betriebssicherheit als relevant erachtet werden. Im Rahmen dessen werden Testpläne und Strategien der notwendigen Bewertung der potenziell gefährdenden Situationen und Szenarien, die ausreichende Abdeckung des relevanten Szenarienraums, die erforderlichen Evidenzen (z.B. Analyseergebnisse, Prüfberichte, spezielle Untersuchungen, aber auch das entworfene Betriebssicherheitskonzept selbst) sowie die jeweiligen Verfahren zur Generierung der Evidenzen festgelegt. Für jeden einzelnen Testfall wird die Zielsetzung gemäß der Betriebssicherheitsargumentation quantifiziert (z.B. Kriterien für Testabschluss, -abbruch und -wiederaufnahme). Darüber hinaus werden für die gesamte Teststrategie objektive Metriken für den Testabschluss und die Testqualität definiert. Dies gilt auch für ggf. vorzunehmende Änderungen sowie deren Auswirkungen im Zuge der Feldbeobachtung.

Zu den möglichen Verfahren gehören Analysen der spezifizierten Anforderungen, Analysen externer und interner Schnittstellen sowie funktionaler Abhängigkeiten, Generierung und Analysen von Äquivalenzklassen auslösender Umgebungsbedingungen und Anwendungsfälle, Analysen von kritischen

Szenarien etc. Zudem werden Methoden wie beispielsweise FMEA, FTA, das szenariobasierte Testen, Simulationen, Realfahrten, Langzeittests von Fahrzeugflotten usw. zur Durchführung der Analysen selektiert. Ferner wird die Eignung der gewählten Verifikations- und Validierungsmethoden argumentiert. Insgesamt geht es hierbei um die nachvollziehbare evidenzbasierte Argumentation sowie die Behauptung dahingehend, ob und wie die Validierungsziele im Sinne der ASIL-Bewertungen und Risikoakzeptanzkriterien erfüllt werden.

Abschließend ist das Betriebssicherheitskonzept im Hinblick auf dessen Konsistenz und Einhaltung der Betriebssicherheitsziele zu verifizieren. Ferner ist dessen Eignung in Bezugnahme auf die Minderung und/oder Vermeidung gefährdender Verhaltensweisen anhand von Evidenzen darzulegen.

3-5.3 Arbeitsprodukte

3-5.3.1 Betriebssicherheitskonzept gemäß 3-5.2

3-5.3.2 Verifikationsbericht des Betriebssicherheitskonzepts gemäß 3-5.2

Teil 3-6 Betriebssicherheitsvalidierung

3-6.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) das Betriebssicherheitskonzept, in Bezug auf dessen Konsistenz und Übereinstimmung mit den Betriebssicherheitszielen sowie dessen Fähigkeit inakzeptable Risiken und Gefährdungen zu mindern oder zu vermeiden, zu überprüfen;

b) die Beherrschung aller definierten, essenziellen Gefährdungsszenarien und damit die Erreichung der Validierungsziele, nachzuweisen;

c) Analysen zur Nachweiserbringung, dass die Betriebssicherheitsfunktionen geeignet respektive wirksam sind, die spezifizierten Betriebssicherheitsziele unter Berücksichtigung der Gefährdungsursachen zu erfüllen, durchzuführen;

d) den Nachweis,
   - dass die Betriebssicherheitsziele und Akzeptanzkriterien mit ausreichender Konfidenz erfüllt werden
   - und das Betriebssicherheitskonzept angemessen ist, die notwendige Unterschreitung des Gesamtrestrisikos im Hinblick auf bekannte und insbesondere unbekannte Gefährdungsszenarien und damit die geforderte Betriebssicherheit zu erreichen,

   zu erbringen;

e) etwaige Korrekturen, welche im Zuge einer kontinuierliche Feldbeobachtung nach der Inverkehrbringung zu implementieren sind, zu verifizieren und zu validieren;

3-6.2 Allgemein durchzuführende Prozesstätigkeiten

Die Hersteller und/oder Betreiber eines Betriebskonzepts für den hochautomatisierten Personenverkehr auf der Straße müssen den jeweiligen Zulassungsbehörden oder internen und externen Auditierungen sowie Assessments den Nachweis erbringen, dass die für den gesamten Betriebsbereich relevanten Risiken und Gefährdungen identifiziert wurden und ein konsistentes Betriebssicherheitskonzept hierfür als Evidenz zur Vermeidung oder Reduktion dieser Risiken auf ein

akzeptables Niveau eingeführt wird. Diese nachvollziehbare und rückverfolgbare Argumentation wird durch einen Verifikations- und Validierungsprozess begleitet, welcher durch zu generierende Evidenzen bestätigt, dass die jeweiligen Entwicklungsgegenstände (hochautomatisiertes Kraftfahrzeug, unterstützendes Infrastruktursystem etc.) die gesetzlichen Anforderungen sowie Verkehrsvorschriften erfüllen und keine inakzeptablen Risiken für die Anwender und andere Verkehrsteilnehmer bergen.

Hierunter fällt die gesamtheitliche Überprüfung der Betriebssicherheitsfunktionen, welche je nach Entwurfsentscheidung sowohl auf Seiten des hochautomatisierten Ego-Kraftfahrzeugs als auch auf Seiten unterstützender Infrastruktursysteme implementiert werden können. Hinzu kommt die Beurteilung der Anwendbarkeit, Handhabbarkeit und Benutzerfreundlichkeit sowie notwendiger Instruktionen, Trainings, Ausbildungen und Regelungen im Hinblick auf deren Wirksamkeit. Dies betrifft auch konstruktive Maßnahmen innerhalb der Straßeninfrastruktur wie Signalisierungen, Anzeigen, Hinweise, Ampeln, Barrieren etc.

Genauer genommen werden im Zuge des Verifikationsprozesses die Anforderungen und Betriebssicherheitsziele im Hinblick auf Konsistenz sowie auf vollständige und korrekte Umsetzung bzw. Erfüllung überprüft. Darunter ist u.a. die glaubwürdige und gerechtfertigte Behauptung des korrekten Verhaltens der Betriebssicherheitsfunktionen unter Beachtung gültiger Normen, Standards, Vorschriften und Gesetze im Rahmen der spezifizierten Grenzen und Kennzahlen aufzufassen. Dieser Schritt stellt sicher, dass bekannte Szenarien abgedeckt sind und die jeweiligen System-Of-Systems sich wie erwartet verhalten. Die Verifikation kann zu Änderungen und Verbesserungen des funktionalen Entwurfs führen, welche wiederum neue Verifikationsanforderungen nach sich ziehen. Dieses Vorgehen erhöht die Effektivität des Betriebssicherheitskonzepts, indem bekannte unsichere Szenarien systematisch angegangen und deren Vorhandensein angemessen reduziert wird. Der Verifikationsprozess wird mittels einer Reihe von Methoden durchgeführt. Darunter fällt das Testen von Prototypen einschließlich der Kombination von Tests auf dem Prüfgelände, Simulationen sowie Realfahrten als auch die Verwendung formaler Methoden, wie FTA, FMEA, STPA etc. Darüber hinaus erweisen sich die Ansätze und Vorgehensweisen von Pfeffer [211], Reisgys [228] und King [225] als zielführende Ergänzung (vgl. Unterabschnitt 4.8.2), was die Glaubwürdigkeit und Bewertung von sicherheitsrelevanten Testszenarien angeht.

Dahingegen wird im Rahmen des Validierungsprozesses bewertet, ob die vorgesehenen Anwendungsfälle erfüllt werden, die Anforderungen sich als adäquat erweisen und damit kein unangemessenes Unfallrisiko verursacht wird. Die Validierung zielt daher darauf ab, eine statistische evidenzbasierte Argumentation aufzubauen, um die Behauptung der Gewährleistung der Betriebssicherheit sowohl in bekannten als auch in unbekannten Szenarien mit ausreichender Konfidenz zu bestätigen. Hierbei ist eine Nachweisführung auf Basis von Evidenzen zu erbringen, dass in die Vollständigkeit und Richtigkeit der Gesamtspezifikation vertraut werden kann. Dieser Sachverhalt betrifft auch das sichere und risikomindernde Verhalten in kritischen Verkehrs- und Unfallsituationen oder unter widrigen Umgebungsbedingungen im realen Straßenverkehr. Ferner gilt dies auch für das sichere Verlassen des Betriebsbereichs, das gesetzeskonforme und so weit wie praktisch umsetzbar unfallfreie Nominalverhalten als auch die Erfüllung der Risikoakzeptanzkriterien und -metriken. Bei der Validierung werden die zu überprüfenden System-Of-Systems in Szenarien oder Situationen getestet, denen diese nach deren Freigabe mit hoher Wahrscheinlichkeit im Straßenverkehr ausgesetzt sein werden. Diese Testszenarien werden in validierten virtuellen (Simulation vordefinierter Szenarien) Umgebungen oder aber im Zuge von Realfahrten durchgeführt.

Zusätzlich werden spontane bzw. unerwartete Situationen und Szenarien untersucht (Tests auf offener Straße oder Simulation zufällig generierter Szenarien). Des Weiteren spielen langfristige Feldversuche eine maßgebende Rolle, um die Annahmen, Hypothesen, Randbedingungen und Einschränkungen über den definierten Betriebsbereich einschließlich des Verhaltens anderer Verkehrsteilnehmer, zu validieren. Während der finalen Testfahrten innerhalb des definierten Betriebsbereichs dürfen keine Betriebssicherheitsziele verletzt oder ggf. erforderliche Testfahrerübernahmen ausgelöst werden. Darüber hinaus werden sicherheitskritische Parameterbereiche, welche sich aus den Betriebssicherheitszielen ableiten, sowie die Verletzung von Redundanzanforderungen überprüft. Die Extrapolation der Ergebnisse der Testfahrten auf das verbliebene Gesamtrestrisiko erfolgt mittels Extremwertanalyse, Simulation und Unfalldaten. Analog zur Verifikation kann auch die Validierung notwendige und zwingend erforderliche Änderungen am Gesamtentwurf des Betriebskonzepts nach sich ziehen. Eine gültige statistische Aussage und Nachvollziehbarkeit setzt voraus, dass bei jeder Überarbeitung des Entwurfs diejenigen Validierungstests wiederholt werden, welche sich im Zuge durchzuführender Auswirkungsanalysen als notwendig und hinreichend charakterisieren.

3-6.3 Arbeitsprodukte

3-6.3.1 Spezifikation der Betriebssicherheitsvalidierung gemäß 3-6.2

3-6.3.2 Betriebssicherheitsvalidierungsbericht gemäß 3-6.2

Teil 3-7 Granularitätsebenenabhängige Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs

3-7.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) die Anwendungsfälle, relevante Szenarien als auch den definierten Betriebsbereich in Abhängigkeit und passend zum Abstraktionsgrad der gegebenen Granularitätsebene (System-Of-Systems-, System-, Subsystem-, Komponenten- oder Einheitenebene) modular zu verfeinern, um die notwendigen Aktivitäten innerhalb der jeweiligen Prozessschritte der ISO 26262 sowie der ISO 21448 konsistent und systematisch zu unterstützen.

3-7.2 Allgemein durchzuführende Prozesstätigkeiten

Im Hinblick auf die jeweiligen Sicherheitsentwicklungsphasen und deren Granularitätsebenen entstehen unterschiedliche Kriterien des notwendigen Detaillierungsgrads der definierten Anwendungsfälle, Betriebsbereichselemente und daraus abgeleiteten Szenarien. Somit werden je nach Bedarf und Abhängigkeit der phasenbezogenen Entwicklungsaktivitäten die spezifizierten Anwendungsfälle, Betriebsbereichselemente bzw. -attribute und Szenarien per deduktivem Top-Down-Prinzip unter Anwendung von Taxonomien systematisch verfeinert und ausdetailliert. Somit kann es in der Phase des Betriebskonzepts beispielsweise ausreichen, lediglich anzugeben, dass Kraftfahrzeuge im Sinne von anderen Verkehrsteilnehmern zum definierten Betriebsbereich gehören.

Im Laufe der nachgelagerten Prozessphasen (Konzeptphase, Produktentwicklung auf Systemebene oder Produktentwicklung auf Hardware- und Softwareebene siehe Abbildung B.1 und Abbildung B.2) werden die Kraftfahrzeugattribute konkretisiert. Hierbei werden u.a. die zu erwartenden Abmessun-

gen etc. beschrieben, um damit beispielsweise die benötigten Kriterien eines Objekterkennungsalgorithmus spezifizieren zu können. Analog dazu erfolgt die Szenarienbeschreibung zu Beginn der Betriebskonzepthase mittels funktionaler Szenarien, welche einen möglichen Weg zur Erfüllung der definierten Anwendungsfälle auf oberster Granularitätsebene darstellen. Die funktionalen Szenarien werden im weiteren Verlauf anhand von logischen Szenarien präzisiert, bis diese abschließend in konkrete Szenarien überführt werden (vgl. Abschnitt 4.8). Dieses Vorgehen erfolgt im Zusammenspiel mit der Konkretisierung der Anwendungsfälle und der jeweils betroffenen Betriebsbereichselemente.

3-7.3 Arbeitsprodukte

3-7.3.1 Spezifikation der Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs gemäß 3-7.2

7.2.3 Teil 8 Produktion, Betrieb, Wartung und Außerbetriebnahme

Für die nachfolgende Konzeption des Teil 8 „Produktion, Betrieb, Wartung und Außerbetriebnahme“ wird wiederum der strukturelle und inhaltliche Aufbau von Teil 7 „Produktion, Betrieb, Wartung und Außerbetriebnahme“ gemäß der ISO 26262 herangezogen (vgl. Unterabschnitt 5.2.1). Die darin enthaltenen Nummerierungen der Prozessabschnitte „7-5 Planung für Produktion, Betrieb, Wartung und Außerbetriebnahme“, „7-6 Produktion“ und „7-7 Betrieb, Wartung und Außerbetriebnahme“ werden gemäß der Eingliederung von Teil 3 Betriebskonzeptphase (vgl. Abschnitt 7.2) um „1“ auf „8-5“, „8-6“ bzw. „8-7“ erhöht (siehe Abbildung 7.1 und Abbildung 7.7). Ihre Weiterentwicklung im Sinne der Betriebssicherheit erfordert keine Neustrukturierung, sondern gezielte inhaltliche Modifikationen (als unterstrichen hervorgehoben) im Sinne der Einführung betriebsbereichsbezogener KPIs sowie einer kontinuierliche Felddatenrückführung und Kriterien für Betriebssicherheitsupdates (vgl. AF-16 und AF-17).

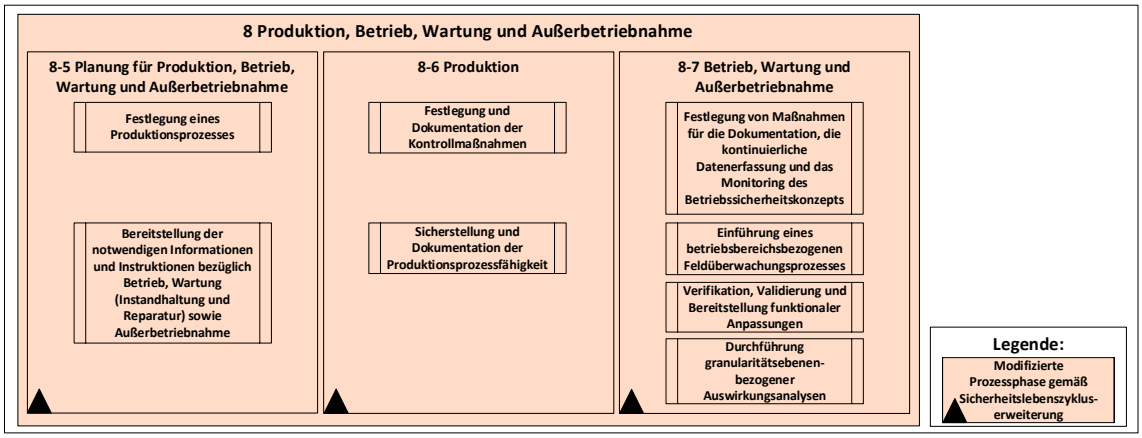


Abbildung 7.7: Modifizierte Prozessphasen und -schritte gemäß Teil 8 „Produktion, Betrieb, Wartung und Außerbetriebnahme“ des eingeführten Betriebssicherheitslebenszyklusprozesses.

Teil 8-5 Planung für Produktion, Betrieb, Wartung und Außerbetriebnahme

8-5.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) einen Produktionsprozess für betriebssicherheitsrelevante Systeme, Subsysteme, Komponenten oder Einheiten festzulegen, welche für den Einbau in Kraftfahrzeugen und/oder unterstützenden Infrastruktursystemen vorgesehen sind;

b) die notwendigen Informationen und Instruktionen zu Betrieb, Wartung (Instandhaltung und Reparatur) sowie Außerbetriebnahme für die jeweiligen Anwendergruppen bereitzustellen, welche mit den betriebssicherheitsrelevanten System-Of-Systems, Systemen, Subsystemen, Komponenten oder Einheiten interagieren. Dadurch soll sichergestellt werden, dass die Betriebssicherheit über den gesamten Betriebssicherheitslebenszyklus gewährleistet ist.

8-5.2 Allgemein durchzuführende Prozesstätigkeiten

Die nachfolgenden Prozesstätigkeiten beziehen sich auf die jeweiligen Aktivitäten gemäß Teil 7 der ISO 26262 und werden nur an dedizierten Stellen explizit mit Blick auf die Thematik der ganzheitlichen Betriebssicherheit inkl. der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität ergänzt. Zusätzliche Details im Hinblick auf die jeweiligen Tätigkeiten, sind innerhalb von Teil 7 der ISO 26262 [50] zu finden.

Was die Informationen und Instruktionen des Betriebs angeht, so werden die Bedienkonzepte in punkto Handhabbarkeit der Mensch-Maschine-Interaktion dergestalt ausgelegt (vgl. Unterabschnitt 2.2.3), dass diese die menschlichen Anwender nicht überfordern und eine sichere Annäherung an das hochautomatisierte Kraftfahrzeug und eines sicheren Zugangs zu diesem ermöglichen. Dies beinhaltet auch Maßnahmen und Strategien, welche nach der Einnahme eines Zustands minimalen Risikos greifen sowie vorgeben, wie und unter welchen Voraussetzungen dieser wieder verlassen werden kann. Darunter fallen auch Anleitungen für planmäßige, aber auch außerplanmäßige Wartungs- und Servicearbeiten sowie der Interaktion mit dem zu schulenden Wartungspersonal.

Hinzu kommen Schulungskonzepte und Instruktionen der jeweiligen Anwender und Betreiber, was die korrekte Bedienung der Mensch-Maschine-Schnittstellen, Auslösung von Nothalt- oder Notruffunktionen sowie Anweisungen für die Handhabung von Zwischenfällen und die Absicherung von Unfallstellen angeht. Dies beinhaltet auch das Aufsetzen und Abstimmen von Interaktionskonzepten (Beschreibungen, Dokumentationen, Abbildungen etc. zur Identifizierung, Deaktivierung, Freigabe oder Bergung des hochautomatisierten Ego-Kraftfahrzeugs, Feststellung der Anwesenheit von Fahrgästen, Evakuierung von Fahrgästen, Brandbekämpfung usw.) für den Umgang mit Einsatzkräften (Ersthelfer, Polizei, Feuerwehr etc.) vor Ort.

8-5.3 Arbeitsprodukte

8-5.3.1 Betriebssicherheitsrelevanter Inhalt des Produktionsplans gemäß 8-5.2 bzw. ISO 26262:7-5.4.1.1-5.4.1.3/5.5.1

8-5.3.2 Betriebssicherheitsbezogene Inhalte des Produktionslenkungsplans, einschließlich des Prüfplans gemäß 8-5.2 bzw. ISO 26262:7-5.4.1.5-5.4.1.6/5.5.2

8-5.3.3 Spezifikation der Herstellbarkeitsanforderungen gemäß 8-5.2 bzw. ISO 26262:7-5.4.1.7/5.5.3

8-5.3.4 Bericht der Produktionsprozessfähigkeit gemäß 8-5.2 bzw. ISO 26262:7-5.4.2.2/5.5.4

8-5.3.5 Betriebssicherheitsrelevanter Inhalt des Wartungsplans gemäß 8-5.2 bzw. ISO 26262:7-5.4.3.1-5.4.3.3/5.5.5

8-5.3.6 Betriebssicherheitsrelevanter Inhalt der Wartungsinstruktionen gemäß 8-5.2 bzw. ISO 26262:7-5.4.3.3/5.5.6

8-5.3.7 Betriebssicherheitsrelevanter Inhalt der dem Nutzer zur Verfügung gestellten Informationen gemäß 8-5.2 bzw. ISO 26262:7-5.4.3.4/5.5.7

8-5.3.8 Betriebssicherheitsrelevanter Inhalt der Instruktionen für die Außerbetriebnahme gemäß 8-5.2 bzw. ISO 26262:7-5.4.3.5/5.5.8

8-5.3.9 Spezifikation der Anforderungen des Betriebs, der Wartung und der Außerbetriebnahme gemäß 8-5.2 bzw. ISO 26262:7-5.4.3.6/5.5.9

8-5.3.10 Betriebssicherheitsrelevanter Inhalt der Rettungsdienstanweisungen gemäß 8-5.2 bzw. ISO 26262:7-5.4.3.7/5.5.10

Teil 8-6 Produktion

8-6.1 Zielvorgaben

Die Zielvorgabe der Klausel ist:

a) die Betriebssicherheit während der Produktionsphase (nach der Produktionsfreigabe) durch den jeweiligen Hersteller oder die für den Produktionsprozess von System-Of-Systems, Systemen, Subsystemen, Komponenten oder Einheiten verantwortlichen Personen oder Organisationen (Betreiber, Fahrzeughersteller, Lieferant, Unterlieferant usw.) sicherzustellen;

8-6.2 Allgemein durchzuführende Prozesstätigkeiten

Die durchzuführenden Tätigkeiten werden unverändert aus Teil 7 der ISO 26262 übernommen und lediglich um den Begriff der Betriebssicherheit sowie der Sicherheit der beabsichtigten Funktionalität ergänzt. Für inhaltliche Details hierzu sei auf Teil 7 der ISO 26262 [50] verwiesen.

8-6.3 Arbeitsprodukte

8-6.3.1 Bericht über Kontrollmaßnahmen gemäß 8-6.2 bzw. ISO 26262:7-6.4.1.1-6.4.1.2/6.4.1.5/6.5.1

8-6.3.2 Bericht der Produktionsprozessfähigkeit gemäß 8-6.2 bzw. ISO 26262:7-6.4.1.3-6.4.1.4/6.5.2

Teil 8-7 Betrieb, Wartung und Außerbetriebnahme

8-7.1 Zielvorgaben

Die Zielvorgaben der Klausel sind:

a) die Betriebssicherheit während der Betriebs-, Wartungs- (Instandhaltungs- und Reparatur-) und Stilllegungsphase des Betriebssicherheitslebenszyklus zu gewährleisten;

b) Maßnahmen für die Dokumentation, die kontinuierliche Datenerfassung und das Monitoring des Betriebssicherheitskonzepts auf System-Of-Systemsebene als auch der Sicherheitskonzepte auf System-, Subsystem-, Komponenten- und Einheitenebene im Feld festzulegen;

c) granularitätsebenenübergreifende Auswirkungsanalysen gemäß 2-6.2 auch während des Betriebs im Feld durchzuführen;

d) funktionale Anpassungen bei Bedarf zu verifizieren, zu validieren und bereitzustellen;

8-7.2 Allgemein durchzuführende Prozesstätigkeiten

Die nachfolgenden Prozesstätigkeiten beziehen sich auf die jeweiligen Aktivitäten gemäß Teil 7 der ISO 26262 sowie Teil 13 der ISO 21448 und werden nur an dedizierten Stellen hinsichtlich der Thematik der ganzheitlichen Betriebssicherheit inkl. der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität ergänzt. Zusätzliche Beschreibungen im Hinblick auf die jeweiligen Tätigkeiten, sind innerhalb von Teil 7 der ISO 26262 [50] bzw. Teil 13 der ISO 21448 [55] zu finden.

Während der Einführung und des Betriebs des hochautomatisierten Kraftfahrzeugs einschließlich der möglichen Kooperation mit Infrastruktursystemen ist eine kontinuierliche Überwachung im Feld unerlässlich. Demnach werden die im Zuge des Betriebssicherheitskonzepts spezifizierten Sicherheitsschwellen, Toleranzbereiche sowie weitere Metriken einschließlich getroffener Annahmen, welche sich z.B. auf Beinahe-Crashs beziehen, während des gesamten Feldbetriebs aufgezeichnet[6] und analysiert. Dieses Vorgehen erfolgt des Weiteren in Übereinstimmung zum Abstraktionsgrad der jeweiligen Granularitätsebenen, worin die ebenenbezogenen Sicherheitskonzepte (System-Of-Systemsebene, Systemebene sowie Hardware- und Softwareebene) einem fortlaufenden Monitoring unterzogen werden. Die Analyse der Daten wird nach Szenario, Geografie und anderen Betriebsbereichsattributen segmentiert, um die statistische Aussagekraft der Messungen zu erhöhen. Falls die Daten auf höhere Risiken als erwartet hindeuten, neuartige Betriebsbereichselemente hinzukommen, die Verkehrsregeln sich ändern, Softwarebugs sowie zufällige Hardwareausfälle sich manifestieren oder gar Zwischen- und Unfälle eintreten, werden erforderliche Korrekturmaßnahmen im Rahmen eines Änderungsmanagements per granularitätsebenenübergreifender Auswirkungsanalyse umgesetzt und dokumentiert.

Zu Beginn des Betriebssicherheitslebenszyklus (vgl. Teil 2-6) aber auch im Falle von durchgeführten Änderungen während des Feldbetriebs ist eine Auswirkungsanalyse auf System-Of-Systems-, System-, Subsystem-, Komponenten- und Einheitenebene durchzuführen. Bei einer Änderung des Betriebsbereichs eines System-Of-System, Items, Systems oder einer Komponente wird die Auswirkungsanalyse auf der jeweiligen Granularitätsebene durchgeführt, um die vorzunehmenden Änderungen adäquat zu ermitteln und deren Einfluss auf die Betriebssicherheit zu beschreiben. Dies gilt auch für die Ermittlung und Beschreibung der durchzuführenden Betriebssicherheitsmaßnahmen in Abhängigkeit von den Auswirkungen der Änderungen.

Darunter fallen beispielsweise technische Änderungen an der Fahrzeugflotte oder dem betroffenen Infrastruktursystem sowie die mögliche Einschränkung des definierten Betriebsbereichs. Zudem wird vorgegeben, wie die funktionalen Anpassungen bzw. Änderungen vorzunehmen sind, sei dies durch

[6] Es wird hier davon ausgegangen, dass für die Gewährleistung des Datenschutzes die entsprechenden Datenverwaltungspraktiken angewendet werden. Auf dies und weitere Themen der Informations- und Datensicherheit wird aber im Zuge der vorliegenden Dissertation nicht weiter eingegangen.

OTA-Updates oder im Rahmen von Werkstattbesuchen. Diese Updates betreffen auch die jeweiligen Regelungen für Wartungen, Services etc. sowie Aktualisierungen der Instruktionen und eventueller Schulungsprogramme sowie bei Bedarf die Aufklärung der Anwender, Einsatzkräfte usw. über den gesamten Produktlebenszyklus. Zusätzlich wird dieser Vorgang durch Regressionstests im Sinne eines dem Problemfall zugeschnittenen Verifikations- und Validierungs- und Freigabeprozesses begleitet, worin u.a. darzulegen ist, welche sicherheitsrelevanten Systembestandteile und Komponenten überhaupt betroffen und ob die vorgenommenen Änderungen in Übereinstimmung mit der Spezifikation umgesetzt sind. Ferner ist die grundsätzliche Behauptung, dass die Betriebssicherheit durch die Aktualisierungen positiv beeinflusst wird und keine neuen inakzeptablen Risiken auftreten können anhand von Evidenzen zu argumentieren.

8-7.3 Arbeitsprodukte

8-7.3.1 Betriebsbereichsbezogener Feldüberwachungsprozess gemäß 8-7.2 bzw. ISO 26262:7-7.4.1.1/7.5.1 und ISO 21448-13.5

7.2.4 Hierarchische Strukturierung des Betriebssicherheitsnachweises

Im Zuge der Sicherheitslebenszykluserweiterung wird wiederum ein strukturierter Unterbau der Qualitäts- bzw. Betriebssicherheitsnachweiskette benötigt, welcher in direktem Zusammenhang zu den jeweiligen Tätigkeiten der Betriebssicherheitsentwicklung einschließlich der Aktivitäten im Hinblick auf die funktionale Sicherheit als auch der Sicherheit der beabsichtigten Funktionalität steht (siehe Abbildung B.1 und Abbildung B.2). Dementsprechend gliedern sich unter der generischen Betriebssicherheitsnachweiskette die Spezifikations- bzw. Liefergegenstände des zu generierenden Betriebssicherheitsnachweises als Gesamtarbeitsprodukt (2-6.3.3) an (siehe Abbildung 7.8).

In diesem Zusammenhang werden die Planungs- und Managementaktivitäten (vgl. Abschnitt 7.2) gemäß der Betriebssicherheit (OpSa), der funktionalen Sicherheit (FuSa) sowie der Sicherheit der beabsichtigten Funktionalität (SotiF) als Evidenzen erfasst. Dabei handelt es sich einerseits um die jeweils durchzuführenden Auswirkungsanalysen sowie die spezifische Planung der Betriebssicherheitsaktivitäten inkl. der Planung der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität (siehe Tabelle B.1).

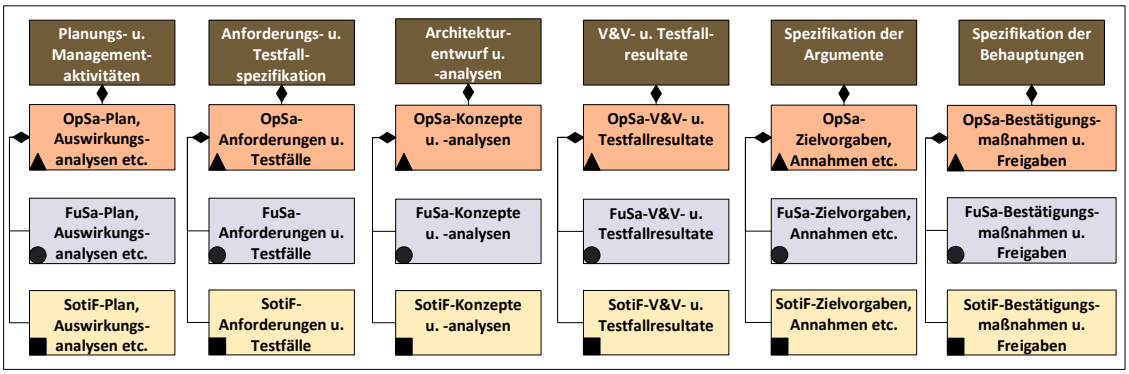


Abbildung 7.8: Strukturierter hierarchischer Unterbau der Betriebssicherheitsnachweisführungskette für ein System eingebettet in dessen Betriebsbereich (siehe Abbildung 7.2).

In Bezugnahme auf die Evidenzen handelt es sich darüber hinaus um die Anforderungs- und Testfallspezifikation, wobei diese angefangen bei der Spezifikation der behördlichen und projektbezogenen Anforderungen über die Betriebssicherheitsziele bis hin zu den Hardware- und Softwaresicherheitsanforderungen entlang der jeweiligen Betriebssicherheitslebenszyklusprozessphase erhoben und verfeinert werden. Hinzu kommen die Verifikations- und Validierungsstrategien einschließlich der jeweiligen Testfallspezifikation (siehe Tabelle B.2).

Seitens der Evidenzen manifestiert sich zudem der Architekturentwurf als zentraler Aspekt, welcher wiederum aus den Sicherheitskonzepten und -analysen der Betriebssicherheit, der funktionalen Sicherheit gemäß ISO 26262 als auch der Sicherheit der beabsichtigten Funktionalität gemäß ISO 21448 im Sinne der zu erbringenden Liefergegenstände bzw. Arbeitsprodukte besteht. Darunter fallen außerdem die identifizierten Betriebssicherheitsgefährdungen, und Szenarien, welche ihrerseits anhand von Gefährdungen bezüglich der funktionalen Sicherheit als auch der Sicherheit der beabsichtigten Funktionalität einschließlich sogenannter auslösender Bedingungen[7] konkretisiert werden. Zudem werden die ASIL-Bewertungen und Akzeptanzkriterien der Betriebssicherheit erfasst, welche entsprechend der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität konkretisiert werden. Des Weiteren sind die dabei getroffenen Annahmen im Hinblick auf Häufigkeit, Schwere und Kontrollierbarkeit sowie Risikoakzeptanzkriterien innerhalb der jeweiligen Arbeitsprodukte zu dokumentieren (siehe Tabelle B.3).

Hinzu kommen die Verifikations-, Validierungs- und Testfallresultate als Evidenzen. Hierbei handelt es sich um Arbeitsprodukte im Hinblick auf die Betriebssicherheit, welche um jene der funktionalen Sicherheit als auch der Sicherheit der beabsichtigten Funktionalität vervollständigt werden (siehe Tabelle B.4). Die Spezifikation der Behauptungen kennzeichnet u.a. durch zu erbringende Bestätigungsmaßnahmen inkl. der Freigabeempfehlungen der Betriebssicherheit, der funktionalen Sicherheit sowie der Sicherheit der beabsichtigten Funktionalität (siehe Tabelle B.5).

7.3 Horizontale Sicherheitslebenszykluserweiterung

Im weiteren Verlauf werden die im Zuge der vorliegenden Dissertation aufgesetzte Betriebskonzeptphase sowie die Prozessphasen und -abschnitte der ISO 26262 bzw. ISO 21448 (siehe Abbildung 7.1) per Top-Down-Prinzip links entlang der vertikalen Achse gruppiert und im Sinne eines ganzheitlichen V-Modells für die Betriebssicherheitsentwicklung zusammengezogen, wobei die betriebssicherheitsbezogene Farbgebung (orange) im Hinblick auf sämtliche Sicherheitsaspekte übertragen wird (siehe Abbildung 7.9). In Bezug auf HF-10 wird der PEP (vgl. Abschnitt 3.1) oben entlang der horizontalen Achse des Betriebssicherheits-V-Modells angeordnet. Hierbei handelt es sich um eine prozessübergreifende Anpassung, um die zeitlich und organisatorisch verteilten Entwicklungsphasen (inkl. Musterstände, Fahrfreigaben etc.) des PEPs sowie die Betriebssicherheitsentwicklungsaktivitäten dergestalt anzupassen, so dass diese im Sinne eines ganzheitlichen Projekt- und Betriebssicherheitsplans miteinander in Einklang gebracht werden können (vgl. AF-19). Darunter wird die Serienphase im Sinne des Betriebs, der Wartung und der Außerbetriebnahme unter Berücksichtigung von HF-13 angeordnet. Dadurch lässt sich die Ausdehnung des Betrachtungsschwerpunkts im Sinne einer verstärkten Fokussierung und systematischen Einbindung der Serienphase bzw. des Feldbetriebs adressieren.

[7] Auslösebedingungen sind spezifische Aspekte, Merkmale oder Gegebenheiten innerhalb eines Szenarios, welche als Auslöser für eine nachfolgende Systemreaktion dienen, die entweder zu einem gefährdenden Verhalten oder zur Unfähigkeit, einen vernünftigerweise vorhersehbaren indirekten Fehlgebrauch zu verhindern oder zu erkennen und abzuschwächen, beiträgt [55].

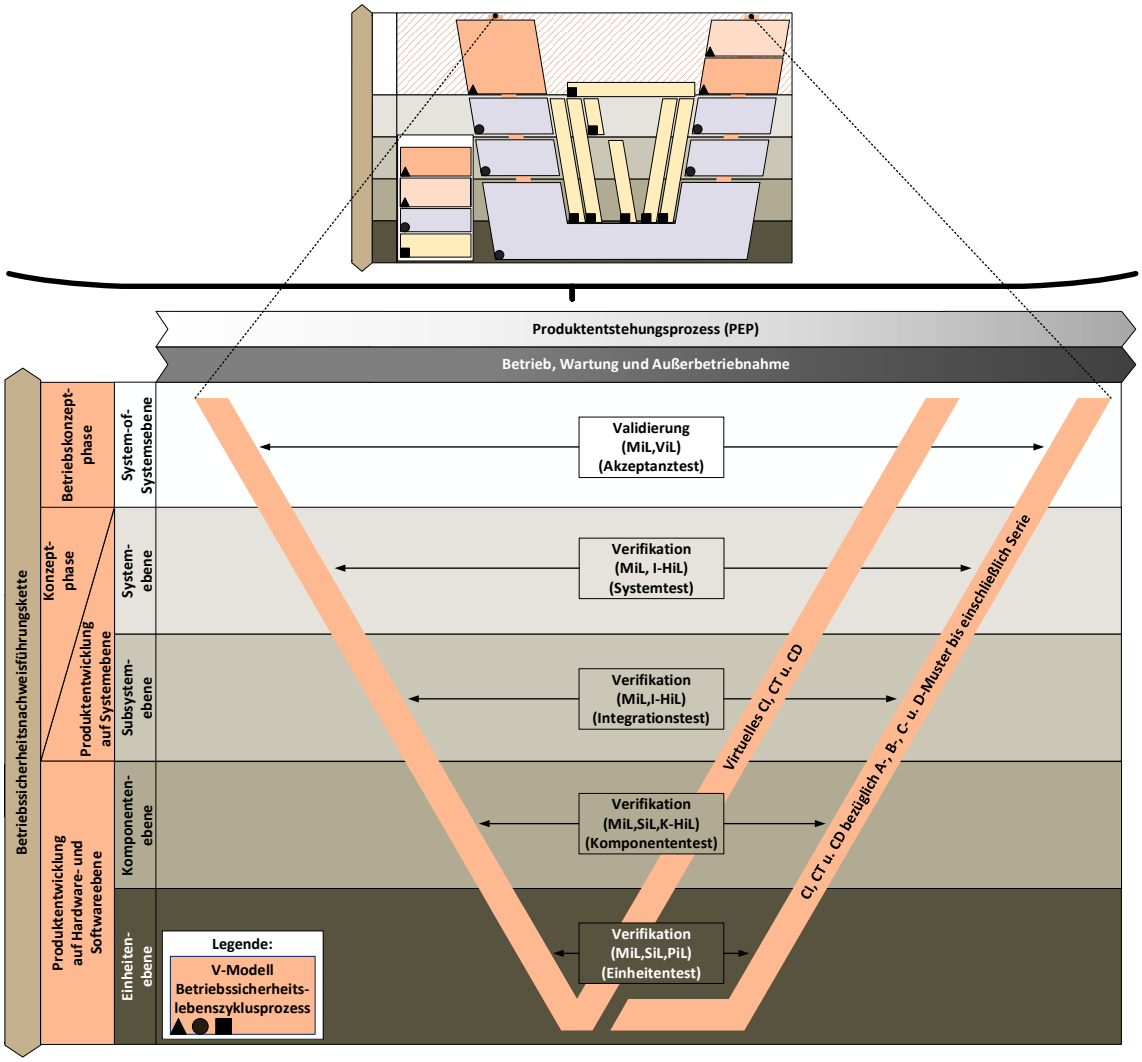


Abbildung 7.9: Im Hinblick auf die Einführung eines virtuellen Integrationsschenkels inkl. CI, CT und CD horizontal erweitertes V-Modell des Betriebssicherheitslebenszyklusprozesses (siehe Abbildung 7.1).

Im Anschluss daran wird der rechte Integrations- und Testschenkel des ursprünglichen V-Modells um einen zusätzlichen Schenkel für die Einbettung der virtuellen und kontinuierlichen Integration (CI), dem Test (CT) sowie der Bereitstellung (CD) ergänzt (siehe Abbildung 7.9). Dies ermöglicht eine frühzeitige Verifikation und Validierung mittels dynamischen und simulativ ausführbaren Architektursichten (vgl. Anhang A.3 und A.4) und gestattet die Errichtung der modell- und insbesondere simulationsbasierten Systementwicklung (vgl. Abschnitt 4.3) als tragende Säule der durchzuführenden Betriebssicherheitsaktivitäten über sämtliche Granularitätsebenen hinweg. Zudem wird der ursprünglich alleinstehende rechte Schenkel einerseits mit den Musterständen, den Fahrfreigaben sowie mit der Serienfreigabe des PEPs und andererseits mit der Serienphase gekoppelt.

Der linke Schenkel der Entwurfsphase wird über die XiL-Absicherungs- bzw. Teststufen inkl. dem szenariobasierten Testen im Sinne eines granularitätsebenenübergreifenden MiL-Ansatzes (vgl. Abschnitt 4.7 und 4.8) mit den beiden rechten Schenkeln der virtuellen als auch realen Integrationsphase verknüpft. An dieser Stelle sei explizit hervorzuheben, dass jene horizontale Verzahnung sowohl während des PEPs als

auch im Verlauf der Serienphase dauerhaft aufrechterhalten wird (siehe Abbildung 7.9). Die dadurch entstehende prozessuale Basis dient wiederum als Befähigungsprogramm einer kontinuierlichen Beobachtung sowie einer kontinuierlichen Bereitstellung von inkrementellen Updates, Anpassungen, Erweiterungen und Verbesserungen während des Feldbetriebs.

7.3.1 Iterativ-inkrementelle Betriebssicherheitsreifegradabsicherung

Um den strukturbedingten Konflikt bzw. Widerspruch des V-Modells und des PEPs auf der einen Seite und der agilen Vorgehensweisen im Sinne der iterativ-inkrementellen Entwicklung inkl. CI, CT und CD auf der anderen Seite aufzulösen (vgl. HF-11), bedarfs es weiterer schrittweiser Anpassungen prozessualer Natur (vgl. AF-18). Zur Sicherstellung der Produktqualität wird im Hinblick auf das Multiple-V-Modell der VDA parallel zum PEP eine Reifegradabsicherung entlang von Meilensteinen durchgeführt (vgl. Unterabschnitt 3.2.6). Grundsätzlich erweist sich dieser Ansatz als aussichtsreich, die Konzepte des klassischen V-Modells und agiler Entwicklungsansätze zusammenzuführen.

Was allerdings fehlt, ist die systematische Verankerung der Betriebssicherheitsentwicklungstätigkeiten im Sinne einer fortlaufenden Betriebssicherheitsreifegradabsicherung während des PEPs aber auch im Verlauf des Serienbetriebs im Feld. Allgemein basiert die Bewertung des Reifegrads auf festgelegten Indikatoren, für die wiederum ein spezifischer Satz an Mess- und Bewertungskriterien definiert werden muss. Im Hinblick darauf könnten die jeweiligen Phasen bzw. Arbeitsprodukte des V-Modells für die Betriebssicherheitsentwicklung als Mess- und Bewertungskriterien herangezogen werden. Jedoch unterbindet der binäre Charakter des klassischen V-Modells im Sinne von „Phase abgeschlossen“ versus „Phase nicht abgeschlossen“ die Einbeziehung dieses Vorgehens (vgl. Unterabschnitt 3.2.3).

Aufgrund dessen werden an dieser Stelle vier Betriebssicherheitsreifegradstufen bzw. -level (engl. *Operational Safety Maturity Level {OpSa-ML}*) definiert, um einerseits die binäre Ausprägung der jeweiligen Phasen und Arbeitsprodukte entzerren zu können. Andererseits bietet die vierteilige Abstufung des Betriebssicherheitsreifegrads den Vorteil, entlang der Integrationsphasen des PEPs direkt auf die A-,B-,C- und D-Musterstände inkl. der Fahrfreigabe-Level (FFG-L1-4) bezogen werden zu können (vgl. Abschnitt 3.1). Der OpSa-ML wird wiederum direkt auf die zu erbringenden Arbeitsprodukte der jeweiligen Phasen des Betriebssicherheitslebenszyklusprozesses bzw. der hierarchischen Evidenzstrukturierung des Betriebssicherheitsnachweises zurückgeführt (vgl. Unterabschnitt 7.2.4).

Der jeweilige Betriebssicherheitsreifegrad dient somit als Indikator dafür, in welchem Umfang und mit welcher Qualität die Arbeits- oder Teilarbeitsprodukte die Anforderungen an die Betriebssicherheit bereits erfüllen. Die dafür notwendigen Inhalte der Arbeitsprodukte ergeben sich wiederum aus den Zielvorgaben und Anforderungen der jeweiligen Phase der Betriebssicherheitsentwicklung (vgl. Abschnitt 7.2). An erster Stelle handelt es sich dabei um die Betriebssicherheitsreifegradstufen in Bezug auf die Entwurfsphasen gemäß dem linken Schenkel des Betriebssicherheits-V-Modells (siehe Tabelle 7.1).

Tabelle 7.1: Betriebssicherheitsreifegradstufen in Bezug auf die Entwurfsphasen.

Betriebs-sicherheits-reifegradstufe	Kurzbeschreibung	Definition der Betriebssicherheitsreifegradstufe gemäß den Entwurfsphasen entlang des linken Betriebssicherheits-V-Modell Schenkels (siehe Abbildung 7.9) (Anforderungs- und Testfallspezifikation sowie Architekturentwurf siehe Tabelle B.2 und Tabelle B.3)

OpSa-ML1	Initialer Entwurf und Grundstruktur verfügbar	• Inhaltstruktur ist verfügbar und Teilinhalte sind dokumentiert • Fehlende Inhalte sind als solche ausgewiesen
OpSa-ML2	Kerninhalte verfügbar	• Erforderliche Kerninhalte (Zielvorgaben) sind dokumentiert • Verständlichkeit der Kerninhalte inkl. der Referenzen ist sichergestellt • Kerninhalte sind für die nachfolgende Durchführung der Verifikationsprüfung[8] vollständig aufbereitet
OpSa-ML3	Inhalte vollständig und verifiziert	• Arbeitsprodukt ist hinsichtlich des gesamten Betrachtungsgegenstands vollständig • Nachvollziehbarkeit und Rückverfolgbarkeit sowohl innerhalb des Arbeitsprodukts selbst als auch im Hinblick auf zu Bezug nehmende Arbeitsprodukte ist bestätigt • Verifikationsüberprüfung bestanden (keine kritischen Befunde (engl. *Findings*) offen)
OpSa-ML4	Bestätigungsüberprüfungen bestanden und Inhalte freigegeben für die Serie	• Bestätigungsüberprüfung ist erfolgreich bestanden • Erforderliche Maßnahmen zur Behebung etwaiger Befunde aus der Bestätigungsüberprüfung sind umgesetzt • Bericht der Bestätigungsmaßnahmen für die vollständige Gesamtversion des Arbeitsprodukts ist vorhanden (keine wesentlichen Befunde offen) • Baseline des Arbeitsprodukts ist verfügbar • Arbeitsprodukt ist für die Serie freigegeben und als solches innerhalb des Betriebssicherheitsnachweises referenziert

Hinzu kommen die Betriebssicherheitsreifegradstufen in Bezug auf die Integrationsphasen gemäß den beiden rechten Schenkeln des Betriebssicherheits-V-Modells (siehe Tabelle 7.2).

Tabelle 7.2: Betriebssicherheitsreifegradstufen in Bezug auf die Integrationsphasen.

Betriebssicherheitsreifegradstufe	Kurzbeschreibung	Definition der Betriebssicherheitsreifegradstufe gemäß den Integrationsphasen entlang der beiden rechten Betriebssicherheits-V-Modell Schenkel (siehe Abbildung 7.9) (V&V-Aktivitäten und Testfallresultate siehe Tabelle B.4)
OpSa-ML1	Initialer Entwurf und Grundstruktur verfügbar	• Arbeitsprodukt ist vorhanden und erhält im Sinne des A-Musters die Fahrfreigabe für Teststrecken (FFG-L1)
OpSa-ML2	Kerninhalte verfügbar	• Kerninhalte (Zielvorgaben) des Arbeitsprodukts für die Experten- und Dauerlauf-Straßenfahrfreigabe (FFG-L2) im Sinne des B-Musters sind implementiert

[8] Eine Verifikationsprüfung (engl. *Verification Review*) ist eine Tätigkeit, die in Form von Expertenrunden, Walkthroughs oder Inspektionen durchgeführt wird, um sicherzustellen, dass das Ergebnis oder Arbeitsprodukt einer Entwicklungsphase bzw. -aktivität die Projektanforderungen und/oder technischen Anforderungen hinsichtlich Korrektheit und Vollständigkeit erfüllt [50].

		• Test- und Validierungsberichte beinhalten die Resultate, welche für das FFG-L2 erforderlich sind • Bericht der Toolqualifizierung[9] der eingesetzten Werkzeuge für Modellierungs- und Simulationsumgebungen, Messdatenauswertung etc. ist vorhanden • Nicht umgesetzte bzw. nicht implementierte Betriebssicherheitsmechanismen sind durch organisatorische und/oder technische Ersatzmaßnahmen[10] abgedeckt
OpSa-ML3	Inhalte vollständig und verifiziert	• Betriebssicherheitskonzepte inkl. der FuSa- und SotiF-Sicherheitskonzepte sind im Hinblick auf das C-Muster bzw. die allgemeine Straßenfahrfreigabe (FFG-L3) vollständig implementiert und verifiziert • Organisatorische und/oder technische Ersatzmaßnahmen werden nicht mehr benötigt • Test- und Validierungsberichte beinhalten die Resultate, welche für das FFG-L3 erforderlich sind • Bericht der Toolqualifizierung aller qualifizierungsrelevanter Werkzeuge ist vorhanden
OpSa-ML4	Bestätigungsüberprüfungen bestanden und Inhalte freigegeben für die Serie	• Betriebssicherheitskonzepte inkl. der FuSa- und SotiF-Sicherheitskonzepte sind im Hinblick auf das D-Muster bzw. die Serienfahrfreigabe (FFG-L4) vollständig implementiert und verifiziert • Test- und Validierungsberichte beinhalten die Resultate, welche für das FFG-L4 erforderlich sind • Arbeitsprodukt ist für die Serie freigegeben und als solches innerhalb des Betriebssicherheitsnachweises referenziert

Zuletzt erfolgt die Zuordnung der Betriebssicherheitsreifegradstufen in Bezug auf die Planungs- und Managementaktivitäten inkl. der zu generierenden Behauptungen des Betriebssicherheitsnachweises (siehe Tabelle 7.3).

Tabelle 7.3: Betriebssicherheitsreifegradstufen in Bezug auf das übergreifende Betriebssicherheitsmanagement.

Betriebs-sicherheits-reifegradstufe	Kurzbeschreibung	Definition der Betriebssicherheitsreifegradstufe gemäß dem übergreifenden Betriebssicherheitsmanagement (siehe Abbildung 7.1) (Planungs- und Managementaktivitäten sowie Behauptungen siehe Tabelle B.1 und Tabelle B.5)

[9] Wenn ein Software-Tool im Betriebssicherheitslebenszyklus zur Entwicklung eines Systems oder seiner Hardware- oder Software-Komponenten eingesetzt wird und die durchzuführenden Aktivitäten auf die einwandfreie Funktion des Werkzeugs angewiesen sind, ist eine Toolqualifizierung (engl. *Tool Qualification*) erforderlich. Diese umfasst u.a. die Dokumentation der Angaben zur Identifikation des Tools, des Tool Confidence Levels, des maximalen ASIL für sicherheitskritische Fehler, der Qualifikationsumgebung, den angewandten Methoden und deren Ergebnissen sowie mögliche Einschränkungen oder identifizierte Fehlfunktionen [50].

[10] Organisatorische Ersatzmaßnahmen im Rahmen des FFG-L2 umfassen beispielsweise spezielle Trainings für Testfahrer, um sicherzustellen, dass Testfahrten ausschließlich von geschultem Personal durchgeführt werden dürfen. Technische Ersatzmaßnahmen umfassen beispielsweise die eingeschränkte Aktivierung einer Notbremsfunktion, die Bremsvorgänge nur mit einer limitierten Negativbeschleunigung ausführen darf.

OpSa-ML1	Initialer Entwurf und Grundstruktur verfügbar	• Grundstruktur des Betriebssicherheitsplan ist vorhanden • Grobterminierung der Audits und Assessments ist vorhanden • Rollen, Verantwortlichkeiten sowie organisationsspezifische Vorgaben und Prozesse für die Betriebssicherheit sind etabliert • Notwendige Auswirkungsanalysen sind durchgeführt
OpSa-ML2	Kerninhalte verfügbar	• Vorläufiger Betriebssicherheitsplan ist vorhanden • Vorläufige Audits und Assessments sind durchgeführt
OpSa-ML3	Inhalte vollständig und verifiziert	• Vollständiger Betriebssicherheitsplan ist vorhanden • Bewertbare Zusammenfassung des Betriebssicherheitsnachweises ist vorhanden • Vollständiges Audit und Assessment ist durchgeführt • Bericht der Bestätigungsmaßnahmen ist vorhanden • Festgestellte Befunde sind bewertet und im Bedarfsfall mit Maßnahmen versehen • Prognose zum Abschluss aller noch offenen Punkte bis zum Produktionsstart ist positiv
OpSa-ML4	Bestätigungsüberprüfungen bestanden und Inhalte freigegeben für die Serie	• Notwendige Maßnahmen zur Behebung der für die Produktion und den Betrieb festgestellten Befunde sind umgesetzt • Abschlussüberprüfung und Abschlussassessment sind finalisiert • Betriebsbereichsbezogener Feldüberwachungsprozess ist etabliert • Bericht der Freigabe des vollständigen Betriebssicherheitsnachweises für die Produktion und den Betrieb ist vorhanden

Die Charakteristik der zuvor definierten Betriebssicherheitsreifegradabstufungen erweist sich wiederum als geeignet, um einen direkten Zusammenhang zwischen diesen Abstufungen und den Sprints bzw. Iterationen des agilen Scrum-Ansatzes herzustellen (vgl. Unterabschnitt 3.2.4). Diesbezüglich wird jeder Betriebssicherheitsreifegradabstufung eine Iteration zugeteilt. Vor diesem Hintergrund besteht die Zielsetzung darin, im Rahmen der Durchführung der Sprints beziehungsweise Iterationen einerseits die angestrebten Arbeitsprodukte zu erstellen und andererseits den jeweils erforderlichen Betriebssicherheitsreifegrad zu erreichen. Jede erfolgreich abgeschlossene Iteration führt zu einem kontinuierlichen Anstieg des Betriebssicherheitsreifegrads, der schließlich in der Erreichung des OpSa-ML4 mündet (dargestellt durch horizontal dunkler werdenden Farbverlauf siehe Abbildung 7.10).

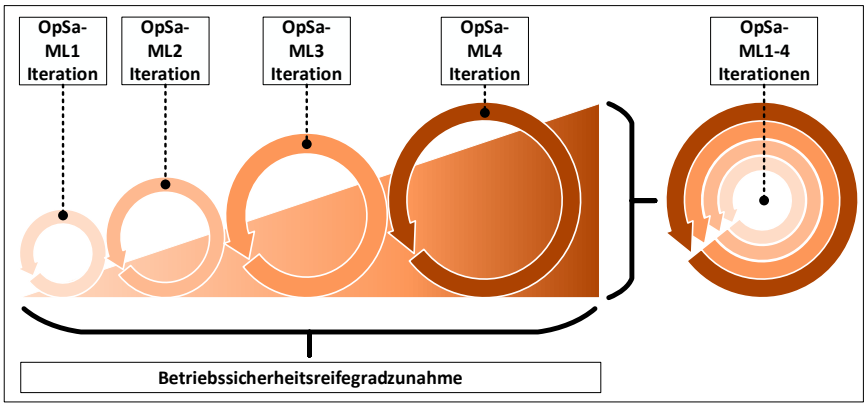


Abbildung 7.10: Betriebssicherheitsreifegradzunahme entlang der vierstufigen OpSa-ML Iterationen.

Darüber hinaus werden, unter erneuter Bezugnahme auf den Scrum-Ansatz (vgl. Unterabschnitt 3.2.4), die im Rahmen der eingeführten OpSa-ML Iterationen zu erstellenden Arbeitsprodukte auf den Aspekt des Inkrements ausgerichtet. Im Hinblick darauf wird an der Stelle ein systematischer Zusammenhang von Iteration, Inkrement, Betriebssicherheitsreifegrad und Arbeitsprodukt respektive Teilarbeitsprodukt hergestellt. Demzufolge werden die jeweiligen Inkremente durch wiederholte Iterationen und die Durchführung der jeweiligen Prozessphasen erzeugt. Diese Inkremente stellen ein Arbeits- oder Teilarbeitsprodukt dar. Für den Fall, dass die Inkremente mit einem entsprechenden Betriebssicherheitsreifegrad bereits vorliegen, so werden diese iterativ überarbeitet, um die nächste Stufe zu erreichen (siehe Abbildung 7.11).

Der Betriebssicherheitsreifegrad fungiert dabei als eine Art Gate, das einerseits die Qualität des erzeugten Inkrements bewertet und andererseits dessen Weitergabe bei Erfüllung der Reifegradkriterien ermöglicht. Auf diese Weise wird eine iterativ-inkrementelle Absicherung des Betriebssicherheitsreifegrads realisiert (siehe Abbildung 7.11).

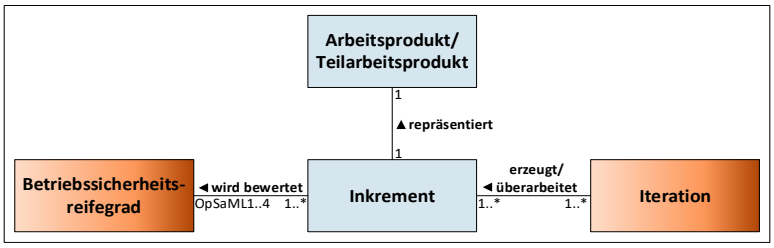


Abbildung 7.11: Hergestellter Zusammenhang von Arbeitsprodukt/Teilarbeitsprodukt, Betriebssicherheitsreifegrad, Inkrement und Iteration.

7.3.2 Multiple-SafeDevOps-V-Modell für die Betriebssicherheitsentwicklung

Die Einführung der iterativ-inkrementellen Betriebssicherheitsreifegradabsicherung ermöglicht es im Hinblick auf AF-18 und AF-19, die Freigaben gemäß des PEPs sowie die Iterationen und Inkremente im Kontext agiler Vorgehensweisen sowohl in einen systematischen Bezug zueinander als auch zum Betriebssicherheits-V-Modell zu setzen (vgl. Unterabschnitt 7.3.1). Zu diesem Zweck wird zuerst eine Konkretisierung des Arbeitsprodukts in Richtung der granularitätsebenenbezogenen Freigabe vorgenommen, was durch einen zunehmend dunkler werdenden Top-Down-Farbverlauf visualisiert wird. Diese Betrachtungsweise

wird ebenfalls auf den Aspekt des Inkrements angewendet, wobei dieses als Verfeinerung des allgemeingültigen Systems[11] eingebettet in dessen Betriebsbereich agiert (siehe Abbildung 7.12).

Die dadurch entstehende Systematik ermöglicht eine konsistente Integration des Betriebssicherheits-V-Modells auf der einen Seite und des agilen Scrum-Ansatzes auf der anderen Seite, um HF-11 adressieren zu können. Der Entwicklungsablauf des Betriebssicherheitslebenszyklusprozesses basiert somit auf zwei Ausführungsformen: der sequenziellen und der iterativ-inkrementellen. Die sequenzielle Ausführung ist durch eine klassisch lineare Abfolge der Aktivitäten gekennzeichnet. Im Gegensatz dazu werden bei der iterativen Ausführung die jeweiligen Betriebssicherheitsaktivitäten innerhalb derselben Prozessphase oder Granularitätsebene so lange wiederholt, bis der angestrebte Betriebssicherheitsreifegrad erreicht ist.

Dabei wird jeder Iteration bzw. jedem Sprintdurchlauf eine Teststufe zugeordnet. Begleitet wird dies durch die ebenenübergreifende Betriebssicherheitsnachweisführungskette im Sinne von Evidenz, Argument und Behauptung. Vor diesem Hintergrund wird in den frühen Entwicklungsphasen der MiL-Ansatz systematisch integriert, wobei dieser bis zum Serienbetrieb im Rahmen szenariobasierter Tests Anwendung findet. Der Prozess wird abhängig von Bedarf und Verfügbarkeit durch Musterstände, einschließlich hybrider sowie physischer Prototypen, ergänzt (PiL, SiL, HiL, ViL vgl. Abschnitte 4.7 und 4.8). Dadurch ergibt sich ein zunehmend höherer Detaillierungsgrad sowie ein erweiterter Umfang der Verifikations- und Validierungstätigkeiten, welche ihrerseits in Einklang mit dem jeweils zu erreichenden Betriebssicherheitsreifegrad stehen (siehe Abbildung 7.13). Hervorzuheben ist, dass eine Phase oder Granularitätsebene den angestrebten Betriebssicherheitsreifegrad nur dann erreichen kann, wenn sowohl alle Elemente der jeweiligen Ebene als auch alle Integrationsbestandteile der darunterliegenden Phasen den vorgesehenen Reifegrad erfüllen. Der ansteigende Reifegrad führt letztlich zur vollständigen Bearbeitung und Erreichung der jeweiligen V-Modell-Phase, wie es im klassischen Ansatz vorgesehen ist. Der Weg dorthin wird jedoch durch mehrere Iterationen bzw. Sprints umgesetzt.

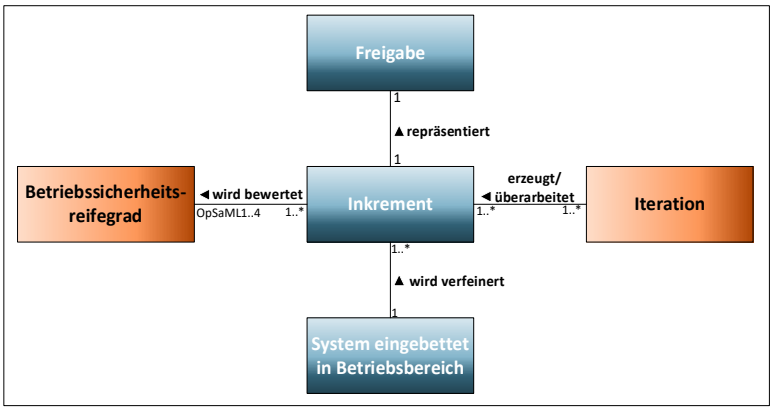


Abbildung 7.12: Im Hinblick auf Abbildung 7.11 konkretisierter Zusammenhang von Inkrement, Betriebssicherheitsreifegrad, Freigabe, Iteration und System eingebettet in Betriebsbereich im Kontext des Betriebssicherheitslebenszyklusprozesses gemäß V-Modell.

[11] Es ist anzumerken, dass in der vorliegenden Dissertation primär der allgemeine Systembegriff im Kontext eines technischen Produkts verwendet wird. Dieser Begriff kann ein System-Of-Systems, ein System, ein Subsystem, eine Komponente oder eine Einheit umfassen (vgl. Abschnitt 4.1).

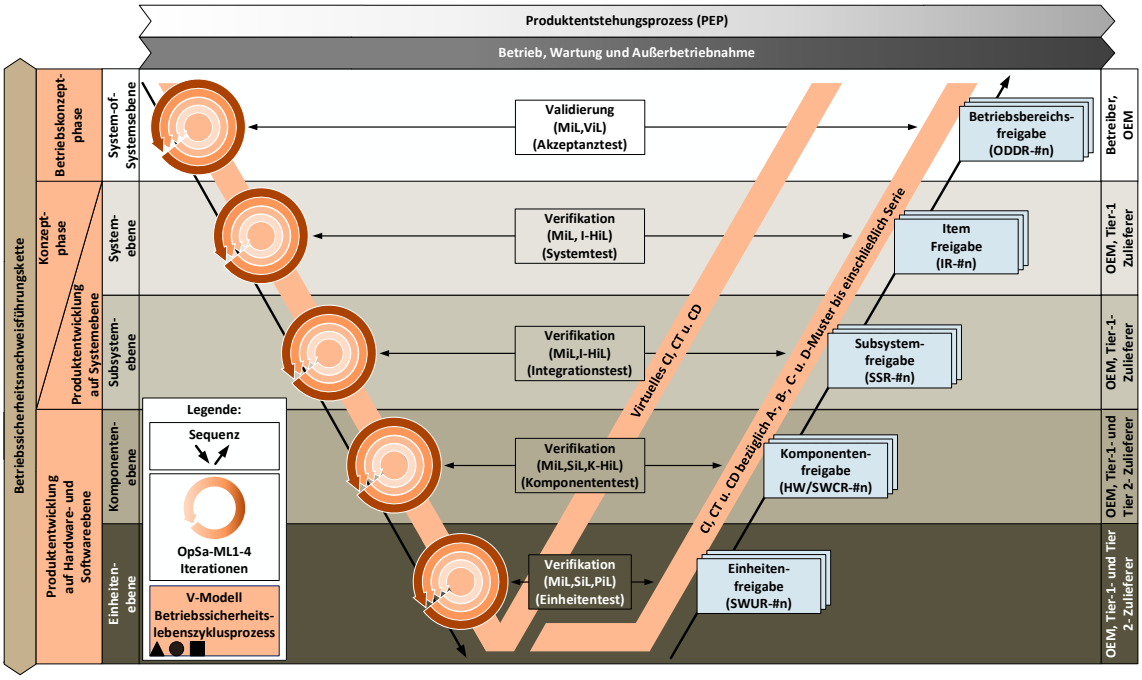


Abbildung 7.13: Durch Iterationen und inkrementelle Freigaben „agilisiertes“ V-Modell des eingeführten Betriebssicherheitslebenszyklusprozesses (siehe Abbildung 7.9).

Ein weiterer Vorteil der betriebssicherheitsgerichteten Reifegradabstufungen liegt darin, dass die darunterliegenden Phasen beziehungsweise Granularitätsebenen nicht auf den vollständigen Abschluss der übergeordneten Ebenen warten müssen. Für den Übergang in die nächste darunterliegende Phase genügt der OpSa-ML1 der darüberliegenden Ebene als Input. Gleichzeitig erfordert es bei den Iterationen kein vollständiges Durchlaufen aller Phasen, da diese stets auf den jeweils zu erreichenden Betriebssicherheitsreifegrad ausgerichtet sind. Dadurch können klar definierte und abgestufte Arbeitspakete erstellt und zugeteilt werden. Die prozessuale Integration von Sprints bzw. Iterationen ermöglicht die Überwachung des aktuellen Entwicklungsstands und ermöglicht ein zeitnahes Eingreifen bei auftretenden Schwierigkeiten.

Abschließend kombiniert die inkrementelle Ausführung eine oder mehrere Iterationen, um am Ende jedes Zyklus ein System-Of-Systems, System, Subsystem, eine Komponente oder eine Einheit zu generieren, das im Hinblick auf den jeweils angestrebten Betriebssicherheitsreifegrad verifiziert ist und nach erfolgreicher Durchführung des jeweiligen Testverfahrens freigegeben wird. Jede Phase auf dem rechten Schenkel endet somit mit einer Freigabe für die darüberliegende Ebene. Darunter fallen die Softwareeinheitenfreigabe (SWUR-#n), die Hardware- bzw. Softwarekomponentenfreigabe (HW/SWCR-#n), die Subsystemfreigabe (SSR-#n), die Item Freigabe (IR-#n) sowie die Betriebsbereichsfreigabe inkl. der Fahrzeugfreigabe (ODDR-#n) (siehe Abbildung 7.13).

Hierbei ermöglicht das schrittweise bzw. inkrementelle Hinzufügen neuer Funktionalität eine stufenweise Integration der neu erstellten und/oder überarbeiteten Realisierungsbausteine. Dies hat den Vorteil, dass mögliche Fehlerursachen leichter aufgedeckt werden können, da technische Insuffizienzen mit hoher Wahrscheinlichkeit auf die neu hinzugefügten oder veränderten Bestandteile zurückzuführen sind. Diesbezüglich können die verschiedenen Rollen der Hersteller und Zulieferer auf drei Gruppen verteilt werden (vgl. Abschnitt 3.1). Die erste und dem Endprodukt am nächsten stehende Gruppe sind die OEMs, deren Aufgaben die Anforderungsspezifikation und Entwicklung des Betriebskonzepts evtl. in Zusammenarbeit

mit Betreiberorganisationen, die Integration von Systemen und Funktionen sowie die Validierung inkl. der Durchführung von Tests des gesamten Aufbaus sind. Zur zweiten Gruppe gehören die Tier-1-Zulieferer, welche für die Entwicklung von Steuergeräten und Anwendungssoftware verantwortlich sind. Die Tier-2-Lieferanten liefern schließlich die notwendige Hardware (z.B. Mikrocontroller und Speicherchips) als auch die Basissoftware und Betriebssysteme. Folglich können diese Gruppierungen der jeweiligen Phase bzw. Granularitätsebene zugeordnet werden (siehe rechter Randbereich Abbildung 7.13).

Insgesamt wird das iterativ-inkrementelle Vorgehen im Sinne eines für die Betriebssicherheitsentwicklung angepassten Scrum-Rahmenwerks (vgl. Unterabschnitt 3.2.4) umgesetzt. Dabei repräsentieren die Zielvorgaben der Prozessabschnitte des Betriebssicherheitslebenszyklusprozesses (vgl. Abschnitt 7.2) sowie der jeweils zu erreichende Betriebssicherheitsreifegrad (siehe Tabelle 7.1, Tabelle 7.2 und Tabelle 7.3 Unterabschnitt 7.3.1) das Produkt Backlog (siehe Abbildung 7.14).

Die daraus abgeleiteten Zielvorgaben werden im Zuge der Sprint-Planung im Sinne des Betriebssicherheitsplans als Sprint-Backlog terminlich und organisatorisch festgelegt sowie koordiniert. Im Anschluss daran werden die OpSa-ML Iterationen bzw. Sprints durchgeführt, woraus wiederum die Arbeitsprodukte und Freigaben (siehe Tabelle B.1, Tabelle B.2, Tabelle B.3, Tabelle B.4 und Tabelle B.5) des Betriebssicherheitslebenszyklusprozesses als Inkremente hervorgehen (siehe Abbildung 7.14).

Durch die Verknüpfung der ebenenbezogenen OpSa-ML Iteration mit der zugehörigen Teststufe lassen sich SafeDevOps- bzw. V-Zyklen für jede Granularitätsebene ableiten. Dadurch wird das nahtlose Ineinandergreifen von iterativen Entwicklungs- und Testprozessen ermöglicht. Der Zusammenschluss aus strukturierten SafeDevOps- bzw. V-Zyklen je Granularitätsebene bildet so die Grundlage für ein durchgängiges und modulares Vorgehen (siehe Abbildung 7.15).

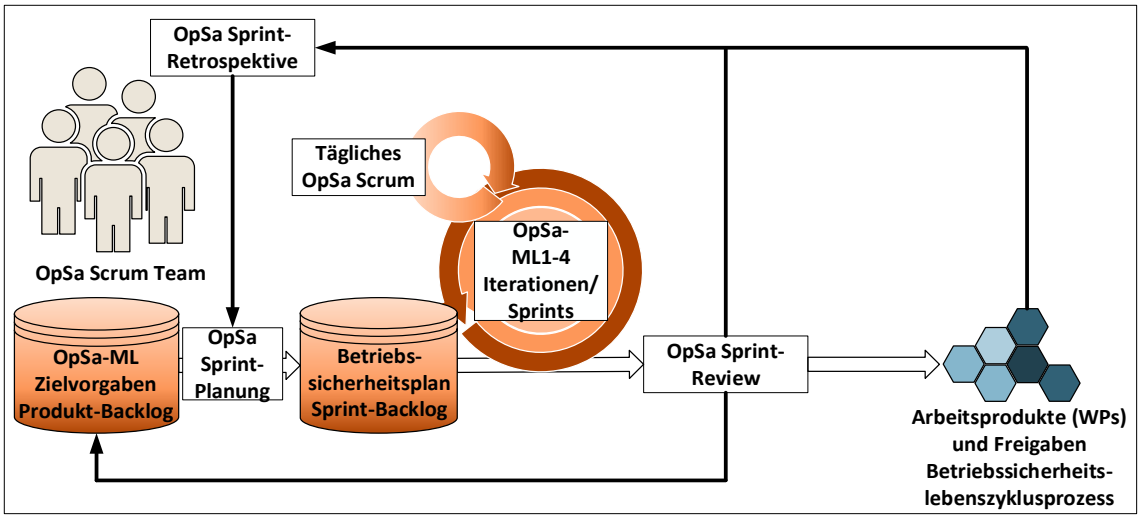


Abbildung 7.14: Anpassung des Scrum-Rahmenwerks (siehe Abbildung 3.5) für die Betriebssicherheitsentwicklung.

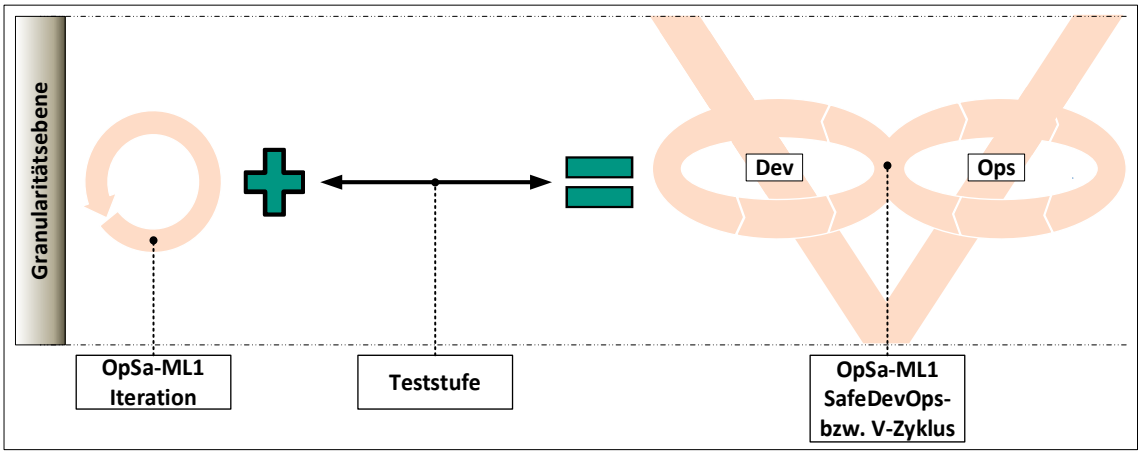


Abbildung 7.15: Ebenenbezogener SafeDevOps- bzw. V-Zyklus als Kombination aus OpSa-ML Iteration und Teststufe.

Dementsprechend ergibt sich durch die Skalierung der V- bzw. SafeDevOps-Zyklen über die Granularitätsebenen hinweg ein Multiple-SafeDevOps-V-Modell. In diesem Kontext wird ein iterativer und kontinuierlicher Entwicklungs-, Integrations-, Test- und Bereitstellungszyklus im Sinne der Bewältigung von HF-13 vorgeschlagen. Dieser integriert systematisch Feedbackpipelines, welche auf Erkenntnissen aus der Feldbeobachtung basieren, in die Entwurfsphasen der jeweiligen Phasen bzw. Granularitätsebenen zurück. Diese datenbasierten Erkenntnisse werden genutzt, um eine kontinuierliche Integration, ein kontinuierliches Testen sowie eine kontinuierliche Bereitstellung von inkrementellen Anpassungen, Erweiterungen und Verbesserungen zu ermöglichen. Die Maßnahmen werden sowohl entlang des PEPs als auch während des Betriebs zyklisch umgesetzt und ausgerollt (siehe Abbildung 7.16).

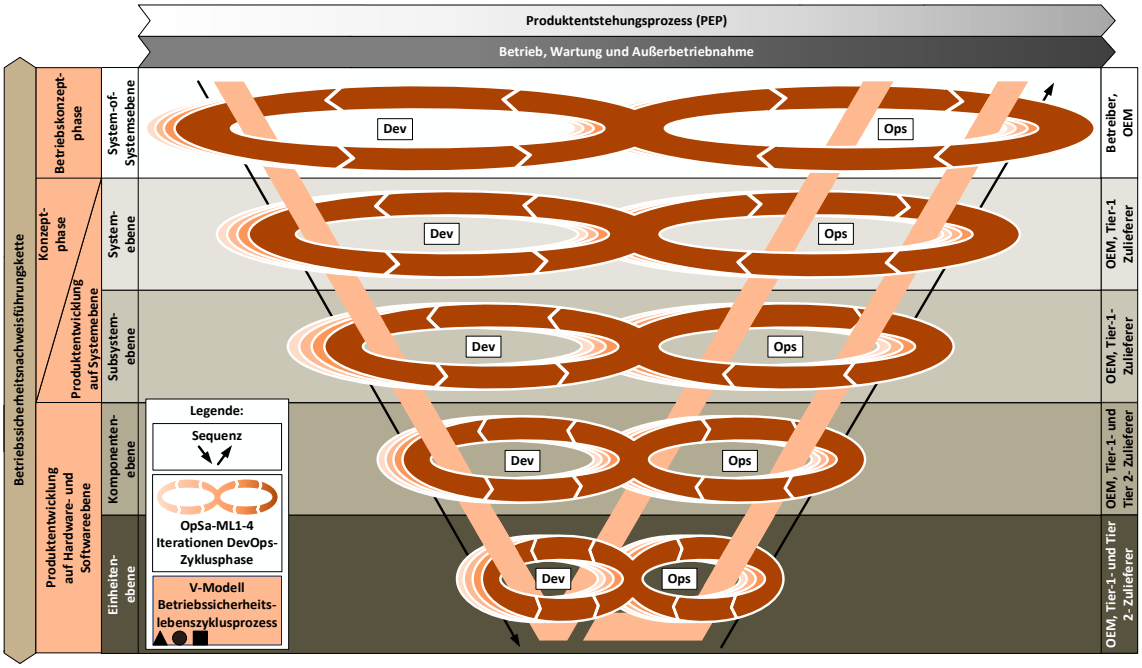


Abbildung 7.16: Multiple-SafeDevOps-V-Modell des Betriebssicherheitslebenszyklusprozesses.

Über alle Ebenen hinweg betrachtet, lässt sich das Gesamtvorgehen entlang eines übergeordneten Safe-DevOps-Zyklus zusammenfassen. Während des PEPs erfolgt im Dev-Zyklus ein iteratives Kontinuum entlang der aufeinander folgenden Schritte der Betriebssicherheitsplanung, des Betriebssicherheitsentwurfs, der Betriebssicherheitsimplementierung sowie der Betriebssicherheitsintegration und -verifikation. Anschließend wird ein nahtloser Übergang zur Betriebssicherheitsvalidierung, -freigabe und -bereitstellung vollzogen, sowohl für die virtuellen als auch die realen Bereitstellungsphasen, wobei insbesondere die jeweiligen Musterstände und Fahrfreigaben berücksichtigt werden. Daraufhin werden die während des Feldbetriebs gewonnenen Erkenntnisse aus der Betriebssicherheitsfeldbeobachtung sowie der Betriebssicherheitsdiagnose und -analyse in den Dev-Zyklus zurückgeführt und eingearbeitet (siehe Abbildung 7.17).

Während des Serienbetriebs nach dem PEP zeichnet sich der übergeordnete SafeDevOps-Zyklus dadurch aus, dass der Dev-Zyklus die Entwicklungstätigkeiten und -schritte umfasst, die sich auf die jeweiligen, granularitätsebenenabhängigen Anpassungen beziehen (vgl. Teil 3-7). Im Gegensatz dazu fokussiert der rechte Ops-Zyklus die Aktivitäten im Sinne der granularitätsebenenabhängigen Feldüberwachung sowie die retrospektive Auswirkungsanalyse (vgl. Teil 8-7). Je nach Umfang der Änderung, sei diese die Einführung einer erweiterten Funktionalität bzw. eines neuen Features, die Behebung von Software Bugs oder anders gearteter Verbesserungen im Hinblick auf die Betriebssicherheit, so werden die jeweiligen Entwurfs-, Integrations-, Verifikations- und Validierungsaktivitäten des Betriebssicherheitslebenszyklus bedarfsgerecht darauf zugeschnitten. An dieser Stelle ist jedoch zu beachten, dass für alle Änderungen die nachweislich fortlaufende Gewährleistung der Betriebssicherheit erbracht werden muss. Bezogen auf diesen Sachverhalt muss stets das ganzheitliche Zusammenspiel von System-of-Systems, Systemen, Subsystemen sowie Hardware- und Softwarekomponenten und -einheiten berücksichtigt werden.

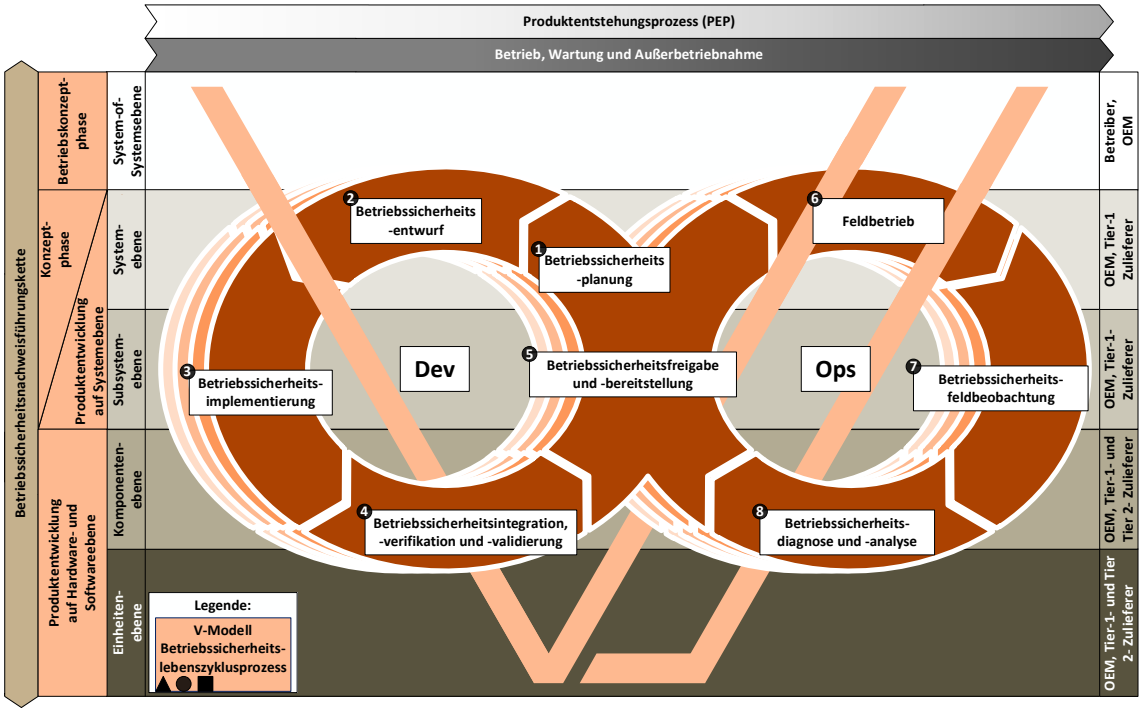


Abbildung 7.17: Übergeordnete DevOps-Zyklen des Multiple-SafeDevOps-V-Modells.

7.3.3 Ablauf des Betriebssicherheitslebenszyklusprozesses entlang des Produktentstehungsprozesses

Die Anwendung der stufenweisen Betriebssicherheitsreifegradabsicherung (vgl. Unterabschnitt 7.3.1) schafft eine strukturierte Verbindung zwischen den zeitlich sowie organisatorisch getrennten Entwicklungsphasen des PEPs – einschließlich Musterständen und Fahrfreigaben – und den sicherheitsorientierten Aktivitäten des Multiple-SafeDevOps-V-Modells (vgl. Unterabschnitt 7.3.2). Dies schafft die Basis für einen kohärenten Betriebssicherheitsplan (vgl. Unterabschnitt 7.2.1), welcher sowohl die Projekt- als auch die Betriebssicherheitsanforderungen im Sinne der Adressierung von HF-10, HF-13 bzw. HF-11 gemäß AF-19 organisiert.

Um im Entwicklungsprozess einerseits ebenenübergreifende Abhängigkeiten und andererseits die Auswirkungen der jeweiligen Spezifikationen frühzeitig analysieren und bewerten zu können, wird jede Entwurfsiteration durch eine Verifikation auf der jeweiligen granularitätsebenenabhängigen MiL-Teststufe begleitet. Das Resultat ist die phasenbezogene Erreichung des erforderlichen Betriebssicherheitsreifegrads sowie die ebenenbezogene Betriebsbereichsfreigabe ODDR0.1 für das geplante Inkrement (siehe Schritt 1 Abbildung 7.18). Die in der darüberliegenden Phase generierten Arbeitsprodukte erhalten den Betriebssicherheitsreifegrad OpSa-ML1 und dienen ihrerseits als Übergangsmarkierung bzw. Input für die nachfolgende Phase. Dort wird nach demselben Vorgehen eine OpSa-ML1-Entwurfsiteration durchgeführt, gefolgt von der Verifikation, mit welcher wiederum die Item Freigabe IR0.1 angestrebt wird (siehe Schritt 2 Abbildung 7.18).

Im Anschluss daran kommt insbesondere der zusätzlich errichtete rechte Schenkel des Multiple-SafeDevOps-V-Modells zum Tragen. Darauf Bezug nehmend verläuft der rechte Schenkel der virtuellen Integration inkl. kontinuierlicher Test und kontinuierliche Bereitstellung angefangen auf der jeweils im Fokus stehenden Granularitätsebene bis hin zur obersten auf Höhe der Betriebskonzeptphase. Die generierten Bestandteile gemäß der Item Freigabe IR0.1 werden virtuell integriert und in die darübergelegene Betriebskonzeptphase überführt. Die Verifikation Anforderungen erfolgt durch einen systematischen Bottom-Up- und Top-Down-Vergleich der verifizierten Anforderungen, einschließlich der zugehörigen Annahmen, Hypothesen, Randbedingungen und Einschränkungen aus vorherigen Phasen, mit den umgesetzten Anforderungen der aktuellen Phase (siehe Schritt 3 Abbildung 7.18). In jedem OpSa-ML ist festgelegt, welche Dokumente und Artefakte die verifizierte Ausgabe darstellen (vgl. Unterabschnitt 7.2.4 und 7.3.1). Diese bestehen aus Entwicklungs- und Reifegradabsicherungsartefakten sowie den verifizierten Anforderungen der jeweiligen Phase. Diese Arbeitsprodukte und Inkremente sind das Ergebnis der Entwicklungs- und Qualitätssicherungsaktivitäten der aktuellen Phase und dienen als Eingabe für den entsprechenden OpSa-ML als Gate.

Zusätzlich werden die verifizierten Anforderungen der vorherigen Phase und die umgesetzten Anforderungen der aktuellen Phase berücksichtigt. Die Verifikation der Arbeitsprodukte erfolgt anhand der Reifegradabsicherungsdokumentationen, während die Anforderungen durch einen Vergleich der verifizierten Anforderungen der vorherigen Phase mit den umgesetzten Anforderungen der aktuellen Phase überprüft werden, um Vollständigkeit, Konsistenz, Korrektheit und Rückverfolgbarkeit sicherzustellen. Jede Phase definiert die erforderlichen Arbeitsprodukte und den Zielreifegrad im Rahmen des OpSa-MLs, wobei diese aus den Ergebnissen der vorherigen Phasen inkl. der darin erreichten OpSa-MLs stammen. Zudem wird angegeben, in welcher Phase jedes Arbeitsprodukt erstellt und gegebenenfalls angepasst wurde.

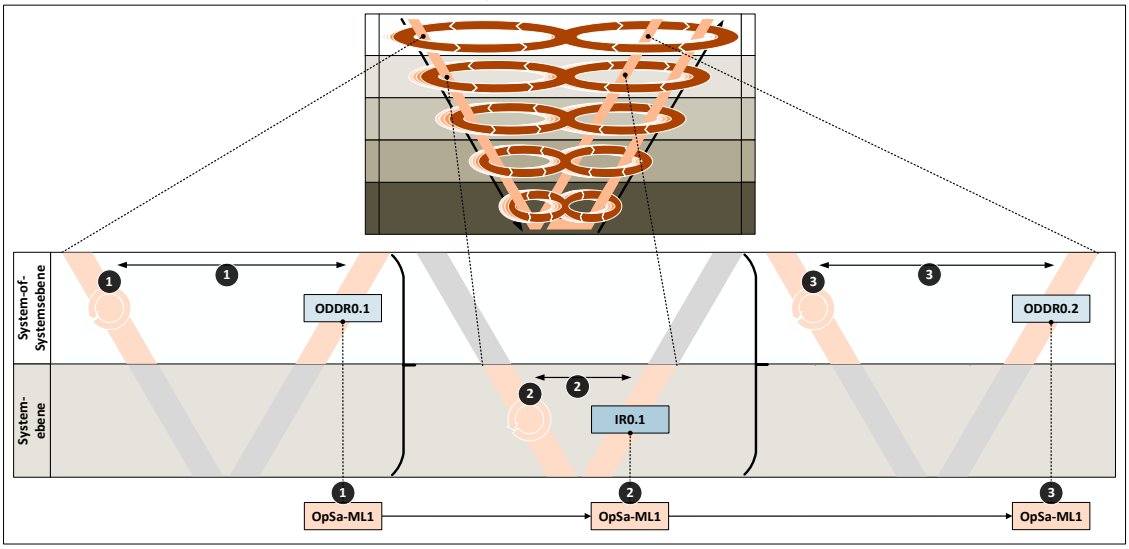


Abbildung 7.18: Ablauf des stufenweisen und iterativ-inkrementellen Entwurfs, der Integration sowie der Verifikation und Validierung im Rahmen des Multiple-SafeDevOps-V-Modells.

Das Ergebnis ist eine iterativ-inkrementelle Erweiterung und Verfeinerung im Hinblick auf die Betriebsbereichsfreigabe ODDR0.2 (siehe Schritt 3 Abbildung 7.18). Der Vorteil der frühzeitigen Verifikation und Validierung liegt in der frühen Bewertung des integrierten Verhaltens, was die spätere Testfallgenerierung und die Definition der Integrations- und Freigabestufen während der realen Integrationsphase fördert. Dieses Vorgehen wird auf sämtliche Phasen des Multiple-SafeDevOps-V-Modells übertragen und gewährleistet die Bereitstellung von evidenzbasierten Argumenten auf jeder Granularitätsebene unter Berücksichtigung vorgenommener Verfeinerungsschritte. Entsprechende Befunde im Sinne von Unzulänglichkeiten bzw. Diskrepanzen zwischen dem erforderlichen, dem spezifizierten sowie dem virtuell bis hin zum in der Realität implementierten Produkt- oder Systemverhalten werden den jeweils betroffenen Prozessphasen zugeordnet und lösen je nach Problemstellung wiederum iterative Entwicklungsaktivitäten bzw. Iterationsschleifen aus, um die jeweils festgestellten Defizite anhand von Maßnahmen zu beheben.

Ferner können dadurch zu verwendende bzw. bereits existierende Komponenten, wie z.B. Radar- oder Lidarsensoren aus einer niedrigeren Granularitätsebenen hinsichtlich der zugrundeliegenden Annahmen, möglicher Unzulänglichkeiten und Konsequenzen für die Validierung etc. analysiert werden. Die jeweiligen Spezifikationen können dann mit Blick auf die zugehörigen Aspekte (z.B. Reflexionskoeffizienten, Vorhandensein metallischer Strukturen innerhalb des Betriebsbereichs usw.) verfeinert werden. Auf Grundlage dessen können wiederum Entwurfsentscheidungen auf einer höheren Granularitätsebene getroffen werden. Die Gesamtbewertung des OpSa-MLs wird aus der Zusammenführung der Einzelbewertungen innerhalb der jeweiligen vertikalen Phasen bzw. Granularitätsebenen abgeleitet, wobei jene dem niedrigsten Wert eines Einzelkriteriums entspricht. Somit bestimmt der niedrigste Betriebssicherheitsreifegrad der darunter liegenden Ebenen den maximal erreichbaren OpSa-ML der darüber liegenden Ebenen in Bezug auf die Integration. Daraus ergeben sich verbindliche Synchronisationspunkte und Absprachen zwischen den Ebenen sowie den jeweils involvierten Entwicklungsbeteiligten (Betreiber, OEM, Tier-1 und Tier-2), die für die Planung der Integrationsstufen und Freigaben maßgebend sind.

Der schrittweise Ablauf der V- bzw. SafeDevOps-Zyklen kann folglich mit den zeitlich und organisatorisch verteilten Entwicklungsphasen des PEPs in Einklang gebracht werden. Hierfür werden entlang der vertikalen Achse die Prozessphasen des im Zuge der vorliegenden Dissertation aufgesetzten Betriebssicherheitslebenszyklusprozesses (Betriebskonzeptphase, Konzeptphase, Produktentwicklung auf Systemebene, Produktentwicklung auf Hardware- und Softwareebene) per Top-Down-Prinzip gruppiert und angeordnet. Darunter folgt die Freigabeplanung der jeweiligen Betriebssicherheitslebenszyklusphasen. An dieser Stelle sei darauf hingewiesen, dass die zu Beginn überwiegend sequenzielle Abarbeitung der Phasen spätestens zum Zeitpunkt der Technologieentwicklung in einen synchronen oder asynchronen Ablauf übergeht. Die Orientierung und Organisation der beteiligten Interessenvertreter und Disziplinen werden dann durch die terminierten Synchro- und Prüfpunkte bzw. Freigaben geschaffen (siehe Abbildung 7.19 respektive Abbildung 7.20).

Der Gesamtprojektplan des PEPs umfasst verschiedene Entwicklungsphasen und basiert auf einem Stage-Gate Ansatz, worin übergeordnete RGA-MS mit dazu adäquaten Liefergegenständen spezifiziert werden (vgl. Abschnitt 3.1). Daraus ergibt sich der Bedarf, die Entwicklungsabfolge des Betriebssicherheitslebenszyklusprozesses in Einklang mit dem Automotive-PEP zu bringen. Dabei stehen einerseits die notwendige Strenge in der Betriebssicherheitsplanung sowie die Einhaltung der Dokumentations- und Nachweispflichten im Fokus, während andererseits durch die iterativ-inkrementelle Entwicklung, die regelmäßige Priorisierung und Anpassung der Entwicklungsressourcen die erforderliche Flexibilität und Effizienz sichergestellt werden kann. Das oben beschriebene stufenweise Vorgehen wird sowohl auf den gesamten PEP mit Schwerpunkt E/E-Entwicklung als auch auf die Phasen des Betriebs, der Wartung und der Außerbetriebnahme übertragen. Zu diesem Zweck wird im Folgenden eine ganzheitliche Betrachtung der PEP-Entwicklungsphasen – von der Produktstrategie- und Technologieentwicklung über die Fahrzeugentwicklung bis hin zu Produktions- und Verkaufsstart – ergänzt durch die Phasen des Betriebs, der Wartung und der Außerbetriebnahme vorgenommen.

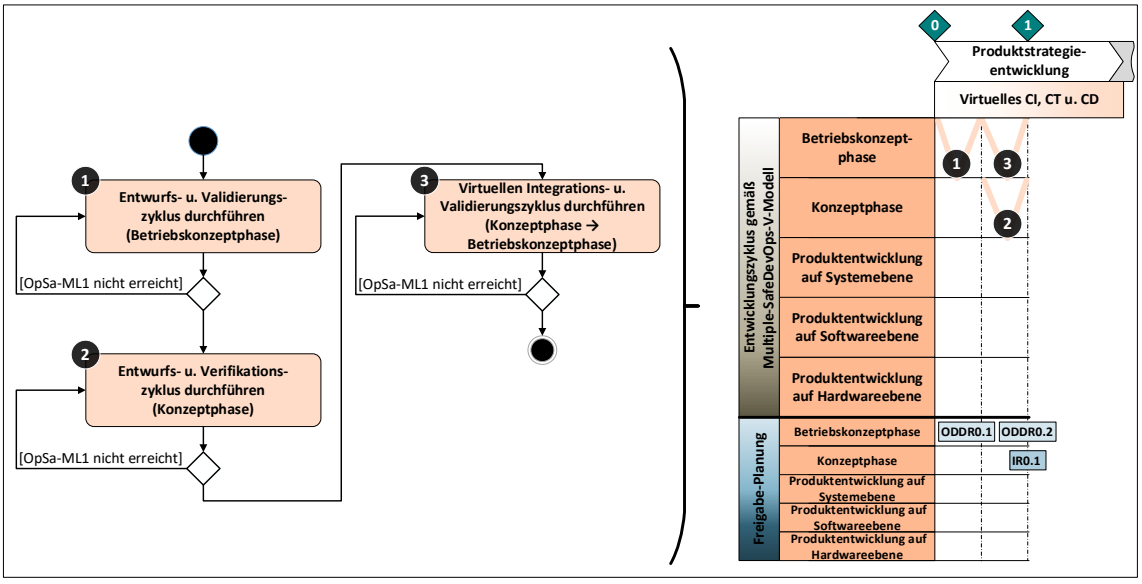


Abbildung 7.19: Einordnung des stufenweisen und iterativ-inkrementellen Entwurfs, der Integration sowie der Verifikation und Validierung im Rahmen der V- bzw. SafeDevOps-Zyklen in die Produktentwicklungsphase des PEPs.

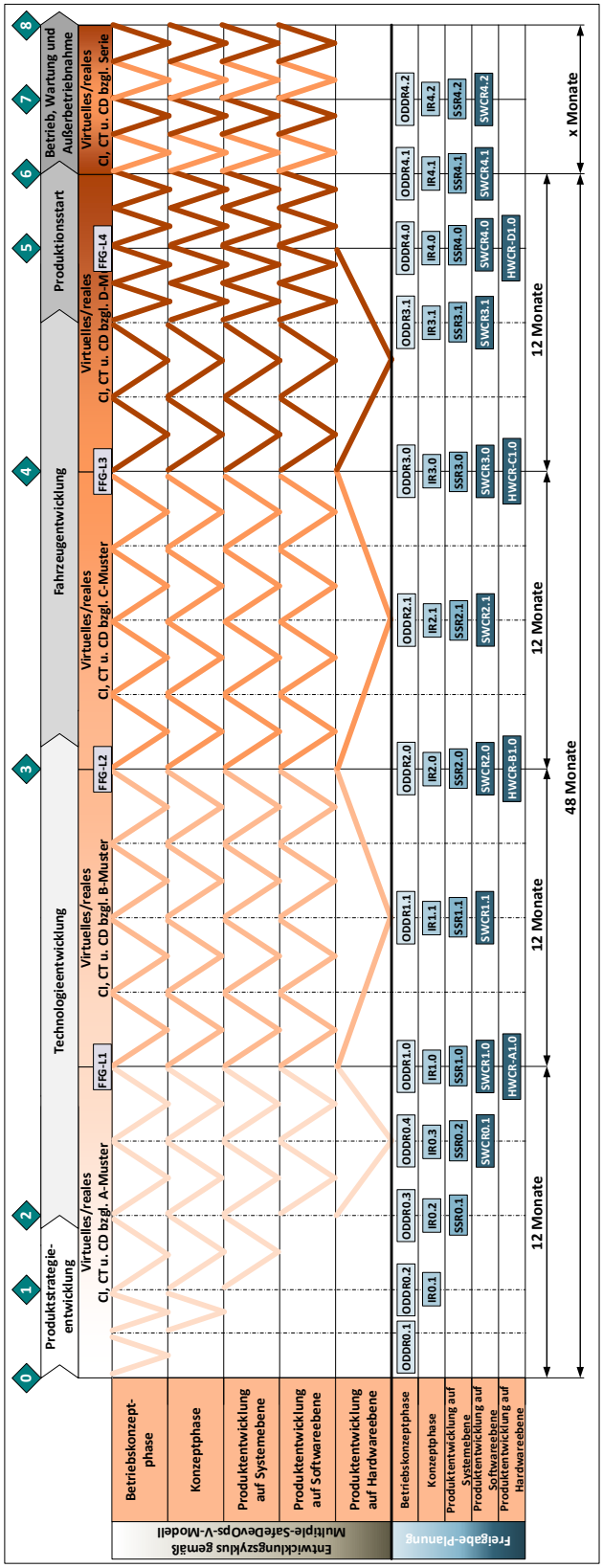


Abbildung 7.20: Zusammenführung der vertikal verlaufenden Phasen des Betriebssicherheitslebenszyklusprozesses und der horizontalverlaufenden Phasen des PEPs unter zusätzlicher Berücksichtigung des Betriebs, der Wartung und Außerbetriebnahme (in Anlehnung an [104]).

Des Weiteren werden entlang der Phasen die Musterstände und Fahrfreigabelevel (FFG-L) sowie die RGA-MS 0-7 (vgl. Abschnitt 3.1) als auch zusätzliche RGA-MS 8 und 9 im Hinblick auf Betrieb, Wartung und Außerbetriebnahme angeordnet (siehe Abbildung 7.20). Der grundsätzliche Entwicklungsablauf orientiert sich wiederum am Multiple-SafeDevOps-V-Modell. Im Absicherungsprozess wird für jede Testebene eine inkrementelle ebenenbezogene Freigabe[12] durchgeführt. Diese erfolgen in festen Zyklen entsprechend des Betriebssicherheitsplans. Dieser beschreibt, wann welche System-Of-Systems, Systeme, Subsysteme und Komponenten inkl. der Einheiten in welchem Betriebssicherheitsreifegrad zu Verfügung stehen müssen, wobei dieser wiederum durch das Scrum-Rahmenwerk im Zuge der Detailumsetzung verfeinert wird (siehe Abbildung 7.14).

Ziel ist es, den geplanten Betriebssicherheitsreifegrad bzw. den inkrementellen Funktionshub zu bestätigen und das jeweilige Element für die weitere Nutzung freizugeben. Im Verlauf der 48 Monate des PEP bis zur Serienproduktion wird das Multiple-SafeDevOps-V-Modell mehrfach zyklisch durchlaufen, wobei die einzelnen Entwicklungsstränge sowohl synchron als auch asynchron zueinander verlaufen. Deren Synchronisierung basiert wiederum auf verbindliche Absprachen der jeweiligen Entwicklungsbeteiligten gemäß den definierten Freigabeumfängen sowie dedizierter Musterstände zu definierten Zeitpunkten innerhalb des PEPs bis hin zur Freigabe und kontinuierlichen Integration von Updates, Anpassungen etc. während des Betriebs im Feld (siehe Abbildung 7.20).

Dadurch entsteht ein Kontinuum an V- bzw. SafeDevOps-Zyklen, welches sich sowohl über die jeweiligen Granularitätsebenen bzw. Betriebssicherheitsentwicklungsphasen auf der vertikalen Achse als auch über die Phasen des PEP einschließlich Betrieb, Wartung und Außerbetriebnahme erstreckt. Vor diesem Hintergrund sei darauf hingewiesen, dass zwischen den Musterfreigaben eine beliebige Anzahl an Inkrementen bzw. Zwischenfreigaben geplant und umgesetzt werden können. Deren Planung sowie Skalierung ist im Kontext des jeweiligen Gesamtprojektplans auf die Bedürfnisse und Randbedingungen der Entwicklungsbeteiligten zuzuschneiden. Im Zuge der vorliegenden Dissertation wird exemplarisch von jeweils einer Zwischenfreigabe mit Erreichung des A-Musterstands ausgegangen (siehe Abbildung 7.20).

Der Übergang in darunter- bzw. darübergelegene Prozessphasen wird wiederum durch definierte RGA-MS vorgegeben und koordiniert. Hierbei repräsentieren die RGA-MS Kontrollpunkte, welche einerseits das Ende und andererseits den Beginn einer bestimmten Entwicklungsphase markieren. Darüber hinaus dienen diese als Synchronisationspunkte der verschiedenen Prozessschritte, beteiligten Interessenvertreter als auch der involvierten Domänen und Disziplinen. Gleichzeitig wird eine enge Koordination zwischen den Verantwortungsbereichen und Domänen angestrebt, um Planungssicherheit entlang der Lieferketten sowie die Verfolgung eindeutig definierter Entwicklungsziele und Synchronisationspunkte zu gewährleisten.

Im Hinblick auf die jeweiligen RGA-MS müssen klar definierte Indikatoren bzw. Qualitätskriterien, sogenannte Liefergegenstände, erbracht werden, bevor der RGA-MS erreicht bzw. passiert werden kann. Die granularitätsebenenübergreifende Aggregation aller Arbeitsprodukte repräsentiert einen expliziten Betriebssicherheitsreifegrad und ermöglicht es, den Projektfortschritt zu identifizieren, zu überwachen und zu bewerten. Die Gesamtbewertung des OpSa-MLs ergibt sich aus der Zusammenführung der Einzelbewertungen innerhalb der jeweiligen vertikalen Phasen und entspricht dem niedrigsten Wert eines Einzelkriteriums. Am Ende einer Phase muss demnach der Betriebssicherheitsreifegrad im Sinne einer definierten Erhöhung der Funktionalität virtuell und/oder physisch verifiziert und validiert werden, um den

[12] Es sei anzumerken, dass aufgrund von Darstellungsgründen die Softwareeinheitenfreigaben (SWUR-#n siehe Abbildung 7.13) mit den Softwarekomponentenfreigaben zusammengefasst werden (SWCR-#n siehe Abbildung 7.20).

spezifischen RGA-MS zu erreichen. Vor diesem Hintergrund leiten sich die Liefergegenstände bzw. Evidenzen, Argumente, Behauptungen und Anforderungen aus den geforderten Arbeitsprodukten der jeweiligen Prozessschritte des Betriebssicherheitslebenszyklus einschließlich ISO 26262 sowie ISO 21448 ab (vgl. Unterabschnitt 7.2.4) und werden durch PEP-typische Liefergegenstände ergänzt (siehe Abbildung 7.20).

In dieser Hinsicht erfolgt die Einordnung der im Zuge des Betriebssicherheitslebenszyklusprozesses in Ergänzung zu erbringenden Liefergegenstände innerhalb von RGA-MS 0 – 7 gemäß [104], wobei die zusätzlichen Liefergegenstände als unterstrichen hervorgehoben werden. RGA-MS 8 und 9 repräsentieren gänzlich neu hinzukommende RGA-MS einschließlich der Liefergegenstände im Hinblick auf den im Verlauf der vorliegenden Dissertation konzipierten Betriebssicherheitslebenszyklusprozess:

- **Produktstrategieentwicklung:**
    - **RGA-MS 0 – Innovationsfreigabe für Serienentwicklung:**
        - Definition der grundsätzlichen Vermarktungs- und Produktstrategie
        - Spezifikation der groben Zielsetzung, Zeit- und Budgetvorgabe
        - Auswirkungsanalyse auf System-Of-Systems-, System-, Subsystem-, Komponenten- oder Einheitenebene
        - Spezifikation des Betriebssicherheitsplans einschließlich der Pläne für die funktionale Sicherheit als auch die Sicherheit der beabsichtigten Funktionalität
    - **RGA-MS 1 – Anforderungsmanagement für Vergabeumfang (3 Monate):**
        - Bestätigung der Plausibilität des Produkt-Business-Cases
        - Vorläufige/frühzeitige (virtuelle) Betriebssicherheitsverifikation und -validierung
    - **RGA-MS 2 – Festlegung der Lieferkette und Vergabe der Umfänge (3 Monate):**
        - Vorauswahl und Nominierung von Lieferanten für Systeme, Subsysteme, Komponenten und ggf. Einheiten für die Technologieentwicklungsphase
        - Dokumentation machbarer und bewerteter Lösungen für das Betriebs- bzw. Betriebssicherheitskonzept

  Die Produktstrategieentwicklung (vgl. Abschnitt 3.1) wird durch RGA-MS 0 eingeleitet (siehe Abbildung 7.20). Hierbei beruhen die Liefergegenstände „Auswirkungsanalyse auf System-Of-Systems-, System-, Subsystem-, Komponenten- und Einheitenebene“ sowie die „Spezifikation des Betriebssicherheitsplans“ auf den Betriebssicherheitsmanagementaktivitäten (vgl. Unterabschnitt 7.2.1). Ein weiterer Aspekt ist die Unklarheit, Mehrdeutigkeit und ggf. Widersprüchlichkeit der Kundenbedürfnisse, Ziele sowie Anforderungen zu Beginn des Entwicklungsvorhabens. Infolgedessen werden die jeweiligen Arbeitsprodukte bzw. Liefergegenstände für die Erreichung von RGA-MS 1 anhand von mehreren Inkrementen (z.B. Betriebsbereichsversion ODDR0.1 rein für Autobahnen, welche im zweiten Schritt im Sinne von Betriebsbereichsversion ODDR0.2 um

Autobahnauffahrten erweitert wird oder aber die inkrementelle Weiterentwicklung eines hochautomatisierten Längsführungsanwendungsfalls um einen hochautomatisiertes Querführungsanwendungsfall) erzeugt. Demzufolge werden die Liefergegenstände so lange überarbeitet, bis der notwendige OpSa-ML1 erreicht und die aufgedeckten Unklarheiten, Widersprüchlichkeiten etc. in einer für alle Entwicklungsbeteiligten akzeptablen Art und Weise ausgeräumt sind. Somit erhält die Betriebssicherheitsverifikation und -validierung das Prädikat „vorläufig", da es sich hauptsächlich um virtuelle simulations- und szenariobasierte MiL-Aktivitäten handelt (vgl. Abschnitt 4.7 und 4.8). RGA-MS 2 repräsentiert einerseits den Abschluss der Produktstrategieentwicklung und andererseits den Übergang in die Technologieentwicklung.

- **Technologieentwicklung:**
    - **RGA MS 3 – Freigabe technische Spezifikation (18 Monate):**
        - Spezifikation des Serienentwicklungskonzepts einschließlich Anforderungen und Funktionen für Produkt und Produktion
        - Verifikationsbericht technischer, zeitlicher und kommerzieller Zielsetzungen und deren realisierbarer Lösungen
        - Betriebssicherheitsnachweis auf Grundlage des B-Musterstands (OpSa-ML2)

Im Zuge der Technologieentwicklung (vgl. Abschnitt 3.1) werden die weiteren Entwicklungsphasen des Betriebssicherheitslebenszyklusprozesses initiiert (siehe Abbildung 7.20). Angefangen bei der Konzeptphase, über die Produktentwicklung auf Systemebene bis hin zur Produktentwicklung auf Hardware- und Softwareebene werden V- bzw. SafeDevOps-Entwicklungszyklen durchlaufen, um die jeweiligen Freigaben auf den unterschiedlichen Ebenen zu generieren. Hierbei ist anzumerken, dass Tätigkeiten wie beispielsweise die Betrachtung und Anpassung aufgrund ebenenübergreifenden Abhängigkeiten auf Basis der jeweiligen Software- und Hardwarefreigaben auf den übergeordneten Entwicklungsphasen (in sequenzieller Abfolge Betriebskonzept-, Konzeptphase und Produktentwicklung auf Systemebene siehe Abbildung 7.20) weitergeführt werden.

Die Bestätigung der initialen Version (A-Muster) des Betriebssicherheitsnachweises beruht auf virtuellen sowie szenariobasierten Integrations- sowie Verifikations- und Validierungsaktivitäten (MiL vgl. Abschnitt 4.7 und 4.8). Dieser Vorgang wird je nach Bedarf sowie Vorhandensein durch A-Musterstände einschließlich hybrider als auch physischer Prototypen unterstützt (SiL, PiL, HiL, ViL vgl. Abschnitt 4.7 und 4.8), was sich wiederum in einem zunehmenden Detaillierungsgrad bzw. erweiterten Inhalt der Verifikations- und Validierungstätigkeiten manifestiert. Dabei werden die jeweiligen Entwicklungspfade gleichgeschaltet und OpSa-ML1-Freigaben im Hinblick auf das A-Muster inkl. FFG-L1 generiert. Weiteres Charakteristikum der Synchronisation ist die Durchführung von phasenübergreifenden Top-Down- und Bottom-Up-Analysen entlang der vertikalen Achse.

Den Abschluss der Technologieentwicklung und damit den Übergang in die Fahrzeugentwicklungsphase bildet RGA-MS 3. Im Zuge dessen werden sämtliche Entwicklungsstränge für die B-Muster Gesamtfreigabe inkl. FFG-L2 und damit den B-Muster Betriebssicherheitsnachweis synchronisiert. Dementsprechend werden die jeweils notwendigen Verifikations- und Validierungsaktivitäten über alle Entwicklungsphasen hinweg durchgeführt und aufeinander abgestimmt

(siehe Abbildung 7.20). Das Grundprinzip besteht darin, zunächst Tests auf niedrigeren Ebenen (Einheiten, Komponenten, Subsysteme) durchzuführen, bevor die Integration und Tests auf höheren Ebenen (System, System-Of-Systems) abgewickelt werden. Daraus abgeleitete Maßnahmen und Änderungen werden innerhalb der jeweiligen Entwicklungsstränge umgesetzt, was sich wiederum in Freigabeversionen mit OpSa-ML2 manifestiert. Die Verifikation und Validierungstätigkeiten basieren hierbei wiederum auf drei Säulen: Virtuell (analytisch durch Simulation bzw. MiL), hybrid (Kombination von Simulationen und physisch vorhandenen Komponenten bzw. HiL) und physisch (Tests auf Prüfständen und Fahrzeugen bzw. ViL) (vgl. Abschnitt 4.7 und 4.8).

- **Fahrzeugentwicklung:**
    - **RGA-MS 4 – Produktionsplanung abgeschlossen (12 Monate):**
        - Bestätigung der Herstellbarkeit und Machbarkeit
        - Bestätigung der Serienlieferanten und Beginn der Auftragsvergabe
        - Bestätigung des gesamten Zielkatalogs
        - Abschluss der Detailentwicklung aller Systeme, Subsysteme und Komponenten
        - Evidenz des Betriebssicherheitsmanagements bezüglich Produktion, Betrieb, Wartung und Außerbetriebnahme
        - Betriebssicherheitsrelevanter Inhalt des Produktionsplans, des Produktionslenkungsplans, des Prüfplans
        - Spezifikation der Herstellbarkeitsanforderungen
        - Betriebssicherheitsrelevanter Inhalt des Wartungsplans, der Wartungsinstruktionen, der dem Nutzer zur Verfügung gestellten Informationen, der Instruktionen für die Außerbetriebnahme sowie der Rettungsdienstanweisungen
        - Betriebssicherheitsnachweis auf Grundlage des C-Musterstands (OpSa-ML3)

Während der Fahrzeugentwicklung (vgl. Abschnitt 3.1) wird der Produktreifegrad insbesondere auf den Hardware- sowie Softwareentwicklungssträngen mittels entsprechender V- bzw. Safe-DevOps-Zyklen und Freigaben vorangetrieben (siehe Abbildung 7.20). Analog zur Technologieentwicklung werden parallel dazu auf den übergeordneten Phasen ebenenübergreifende Wechselwirkungen unter Bezugnahme der jeweiligen Software- und Hardwarefreigaben analysiert und ggf. Anpassungen durchgeführt.

In Abhängigkeit der jeweils benötigten Evidenzen und Betriebssicherheitsargumentationen werden Simulationen mit zunehmendem Detaillierungsgrad und erweitertem Inhalt durchgeführt. Diese repräsentieren virtuelle Verifikations- und Validierungsmethoden, welche wiederum Behauptungen argumentativ bestätigen, dass die Anforderungen und Spezifikationen erfüllt und/oder zweckmäßig sind. Hierbei unterliegt der Vorgang einer iterativ-inkrementellen Herangehensweise, worin Simulationsmodelle sukzessive durch physische Komponenten ersetzt bzw. erweitert werden. Im Laufe des Entwicklungsprozesses findet nach und nach eine Verlagerung

von virtuellen zu physischen Testumgebungen statt, um den erforderlichen Betriebssicherheitsreifegrad schrittweise zu erhöhen. Im Hinblick darauf müssen die für die hybriden bzw. physischen Verifikations- und Validierungsaktivitäten aufgebauten B-Musterstände eine Reproduktion der virtuellen Repräsentationen sein. Nur wenn dies der Fall ist, können Test- und Simulationsergebnisse korreliert und die Modelle für weitere Simulationsschleifen validiert werden. Je genauer die Simulationsergebnisse mit den physischen Testergebnissen übereinstimmen, desto höher ist deren Aussagekraft auf der einen Seite und desto geringer ist das Risiko unerwünschter kosten- und zeitintensiver Nachbesserungen auf der anderen Seite.

Ferner sind im Rahmen von RGA-MS 4 betriebssicherheitsrelevante Inhalte sowie der Nachweis des Betriebssicherheitsmanagements, des Managements der funktionalen Sicherheit als auch der Sicherheit der beabsichtigten Funktionalität hinsichtlich Produktion, Betrieb, Wartung und Außerbetriebnahme abzuliefern. Hinzu kommen ergänzende PEP-typische Liefergegenstände.

Für den Abschluss der Fahrzeugentwicklungsphase (vgl. Abschnitt 3.1) werden in Bezug auf das C-Muster inkl. FFG-L3 wiederum sämtliche Entwicklungsstränge synchronisiert und die jeweils notwendigen Verifikations- und Validierungsaktivitäten über alle Entwicklungsphasen hinweg durchgeführt. Die jeweiligen Freigaben repräsentieren dabei den Abschluss der Detailentwicklung. Es folgen zusätzliche inkrementelle Verfeinerungen im Sinne weiterer Softwarefreigaben (siehe Abbildung 7.20).

- **Produktionsstart:**
    - **RGA-MS 5 – Serienwerkzeugfallende Teile und Serienanlagen verfügbar (9 Monate):**
        - Montage unter seriennahen Herstellungsprozessbedingungen
        - Verifikation der Serienwerkzeuge und des Vorserienherstellungsprozesses
        - Abschluss der Gesamtfahrzeugintegration
        - Bericht der Produktionsprozessfähigkeit
    - **RGA-MS 6 – Produktionsprozess- und Produktfreigabe (3 Monate):**
        - Bestätigung der Herstellbarkeit und Taktzeiten unter vorgegebenen Serienbedingungen bei der Produktion und den Zulieferern
        - Bestätigung der Erreichung der Entwicklungsziele mit Vorserienfahrzeugen und ggf. Vorserieninfrastruktursystemen
        - Betriebssicherheitsnachweis auf Grundlage des D-Musterstands (OpSa-ML4)
        - Abschluss der Betriebsbereichsintegration
        - Endgültiger Betriebssicherheitsnachweis
        - Bericht der Bestätigungsmaßnahmen
        - Bericht über die Kontrollmaßnahmen sowie über die Produktionsprozessfähigkeit

- Bericht der Freigabe für die Produktion und den Betrieb
- Etablierung des betriebsbereichsbezogenen Feldüberwachungsprozesses

Zu Beginn des Produktionsstarts (vgl. Abschnitt 3.1) erfolgt für das D-Muster inkl. FFG-L4 die Synchronisierung aller Entwicklungsstränge als auch die Durchführung der jeweiligen Verifikations- und Validierungsaktivitäten über alle Entwicklungsphasen hinweg (siehe Abbildung 7.20). Im weiteren Verlauf wird der Softwarestand für den Beginn der Produktion bzw. SOP aufgesetzt. Daraufhin wird die finale Synchronisierung aller Entwicklungsstränge als auch die abschließende ebenenübergreifende Betriebssicherheitsverifikation und -validierung im Sinne des Serienentwicklungsstands durchgeführt. Diese mündet im endgültigen Betriebssicherheitsnachweis, welcher durch Audit- und Assessmentberichte im Zuge von RGA-MS 6 bestätigt wird. Diese und weitere PEP-spezifische Liefergegenstände ermöglichen letztendlich die Freigabe für die Produktion und den Betrieb.

- **Betrieb, Wartung und Außerbetriebnahme:**
  - **RGA-MS 7 – Projektabschluss, Verantwortungsübergabe an Serie, Start Requalifikation (3 Monate):**
    - Auslieferung und Übergabe an Kunden bzw. Betreiber
  - **RGA-MS 8 – Freigabe Update bzw. Anpassung (x Monate):**
    - Anpassung des Betriebssicherheitsnachweises
    - Bericht Verifikations- und Validierungsergebnisse und/oder ggf. Bericht der Bestätigungsmaßnahmen für die Anpassung
    - Bericht der Freigabe für die Anpassung
    - Auslieferung und Bereitstellung der Anpassungen bzw. des Updates
  - **RGA-MS 9 – Außerbetriebnahme (x Monate):**
    - Bericht der ordnungsgemäßen Außerbetriebnahme

Zum Abschluss des Produktionsstarts erfolgt im Rahmen von RGA-MS 7 die Auslieferung und Übergabe an die Betreiber bzw. Kunden und ergo der Übergang in die Phase des Betriebs, der Wartung sowie der Außerbetriebnahme (vgl. Abschnitt 3.1). Während des Betriebs im Feld findet eine kontinuierliche Datenerfassung und das Monitoring des Betriebssicherheitskonzepts auf System-Of-Systemsebene einschließlich der Sicherheitskonzepte auf System-, Subsystem-, Komponenten- oder Einheitenebene statt (vgl. Teil 8-7). Sollten aufgrund von detektierten Anomalien, Störungen, Software-Bugs o.Ä. Aktualisierungstrigger ausgelöst werden, neuartige Betriebsbereichselemente hinzukommen, die Verkehrsregeln sich ändern oder gar Zwischen- und Unfälle eintreten, werden notwendige Änderungen im Rahmen eines ebenenübergreifenden Anpassungsmanagements abgeleitet und durchgeführt. Des Weiteren wird festgelegt, wie die Anpassungen und funktionalen Änderungen vorzunehmen sind, sei dies durch OTA-Updates oder im

Rahmen von Werkstattbesuchen. Das gesamte Vorgehen geht analog zu den Entwicklungsphasen von statten, worin die jeweiligen auf den Problemfall zugeschnittenen als auch aufeinander synchronisierten V- bzw. Safe-DevOps-Zyklen durchlaufen werden (siehe Abbildung 7.20).

Sämtliche Änderungen an den Betriebssicherheitsartefakten werden verifiziert sowie validiert und durch Bestätigungsmaßnahmen des Betriebssicherheitsnachweises im Hinblick auf die durchzuführenden Anpassungen wiederum mit dem erforderlichen OpSa-ML4 freigeben (siehe Abbildung 7.20). Je nach Umfang bzw. Tragweite der Anpassungen können für die Freigabe auch stichhaltige Verifikations- und Validierungsergebnisse und -berichte ausreichen, wodurch Bestätigungsmaßnahmen nicht explizit erbracht werden müssen. Die Argumentation hierfür erfolgt mittels der durchgeführten granularitätsebenenübergreifenden Auswirkungsanalysen (vgl. Teil 8-7). Deren Ergebnis entscheidet auch darüber, mit welchem Betriebssicherheitsreifegrad der V- bzw. SafeDevOps-Zyklus wiederum gestartet wird, z.B. OpSa-ML3 (siehe Abbildung 7.20). Zum Abschluss von RGA-MS 8 erfolgt dann die Auslieferung bzw. Bereitstellung der inkrementellen Anpassung. Im Zuge des Betriebs können je nach Bedarf und Notwendigkeit folglich weitere Anpassungen im Sinne einer kontinuierlichen Integration mittels zusätzlicher RGA-MS (vergleichbar mit RGA-MS 8) durchgeführt werden. Der gesamte Betriebssicherheitslebenszyklusprozess endet schließlich mit RGA-MS 9 und dem Bericht der ordnungsgemäßen Außerbetriebnahme und Entsorgung (siehe Abbildung 7.20).

7.4 Modell- und simulationsbasierter Betriebssicherheitsentwicklungsansatz

Da im Zuge der Hochautomatisierung der Fahraufgabe die kundenerlebbaren Funktionen selbst von Sicherheitsrelevanz sind, werden die Grenzen zwischen Sicherheits- und Systementwicklung aufgeweicht und erfordern eine enge Integration beider Disziplinen (vgl. HF-4). Demzufolge müssen die Themen der Betriebssicherheit in einem modellbasierten Systementwicklungsansatz behandelt werden. Hierfür wird im weiteren Verlauf die notwendige Säule der Modellierungsmethode (vgl. Abschnitt 4.3) im Sinne des SPES-Modellierungsrahmenwerks (vgl. Abschnitt 4.6) herangezogen und mit dem Betriebssicherheitslebenszyklusprozess (vgl. Abschnitt 7.2) zusammengeführt.

Vor diesem Hintergrund werden einerseits die Granularitätsebenen und andererseits die Entwurfs- und Dekompositionsschleifen sowie die Integrations-, Verifikations- und Validierungsschleifen des SPES-Modellierungsrahmenwerks in direkten Zusammenhang mit dem Entwicklungsablauf des Multiple-SafeDevOps-V-Modells gesetzt. Dadurch erfolgt eine vollständige Integration der SafeDevOps-Zyklen entlang der vier Sichtweisen auf jeder Granularitätsebene. Gleichzeitig werden diese Zyklen über die Schenkel des V-Modells vertikal verbunden (Abbildung 7.21).

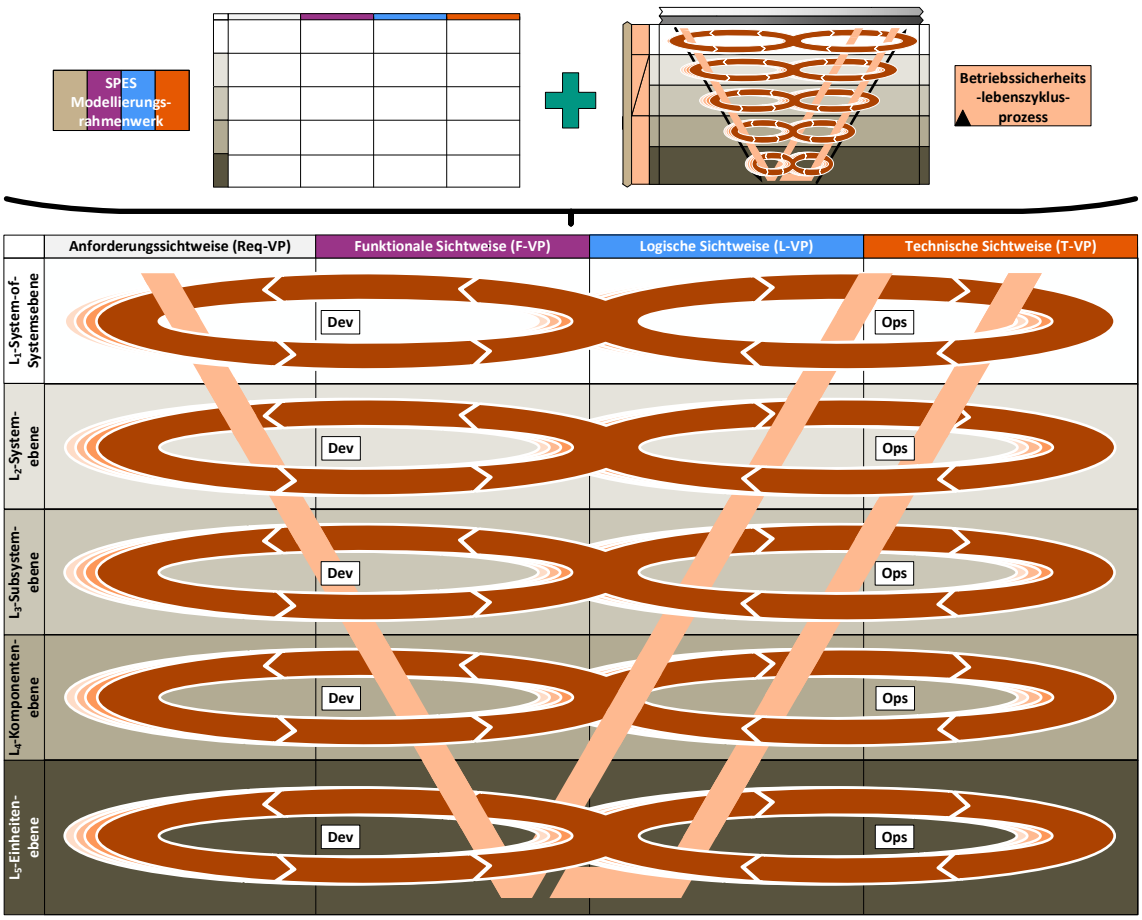


Abbildung 7.21: Zusammenführung des SPES-Modellierungsrahmenwerks sowie des Multiple-SafeDevOps-V-Modells unter Berücksichtigung der L_1-L_5-Granularitätsebenen bzw. der vertikal hierarchisch gegliederten Prozessphasen.

7.4.1 Zickzackförmiger Top-Down- und Bottom-Up-Entwicklungsablauf

Infolgedessen bilden die Granularitätsebenen und Sichtweisen des SPES-Modellierungsrahmenwerks den äußeren Rahmen, welcher wiederum die Grenzen eines zweidimensionalen Entwicklungsraums bzw. -matrix definiert. Angefangen im linken oberen Matrixfeld verläuft die modellbasierte Betriebssicherheitsentwicklung im Sinne des Systementwurfs bzw. der Synthese über die jeweiligen Sichtweisen hinweg grundsätzlich von links nach rechts sowie unter Anwendung des Top-Down-Prinzips entlang der Granularitätsebenen. Im Gegensatz dazu werden die Integrations-, Verifikations- und Validierungsaktivitäten in umgekehrter Reihenfolge vollzogen, sprich von rechts nach links sowie unter Berücksichtigung des Bottom-Up-Prinzips. Daraus ergibt sich eine bidirektionaler zickzackförmiger Entwicklungsablauf, welcher durch die SafeDevOps-Zyklen begleitet und vernetzt wird (siehe Abbildung 7.22).

Folglich durchläuft das zu entwickelnde System-Of-Systems, System, Subsystem, Komponente bis hin zur Einheit mehrere Zyklen. Der bidirektionale zickzackförmige Entwicklungsablauf ist allerdings nicht strikt über sämtliche Granularitätsebenen und Sichtweisen fest vorgegeben. Je nach Problemstellung können unterschiedliche Entwicklungspfade durchlaufen werden. Dadurch kann das Modellierungsrahmenwerk durch Tailoring auf das durchzuführende Projekt sowie die zugrundeliegende Organisations- und Unternehmensstruktur zugeschnitten werden.

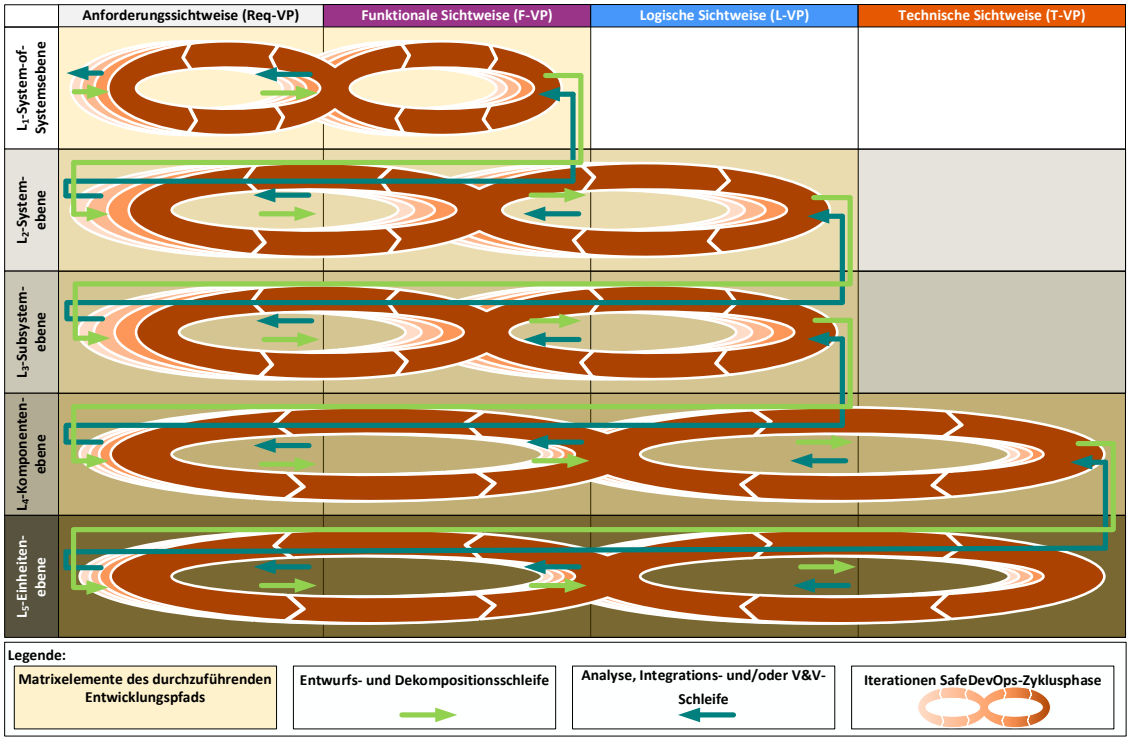


Abbildung 7.22: Matrix bzw. zweidimensionaler Entwicklungsraum des SPES-Modellierungsrahmenwerks inkl. der Einbettung der zugeschnittenen SafeDevOps-Zyklusphasen des Betriebssicherheitslebenszyklusprozesses.

Die Entwürfe sowie die Spezifikationen der darüberliegenden L_n-Granularitätsebene definieren demnach die Anforderungen für die nächste daruntergelegene L_{n+1}-Granularitätsebene. Je nach Entwicklungsvorhaben und Projektkontext markiert der Übergang in die nächste darunterliegende L_{n+1}-Granularitätsebene auch die Übergabe einer oder mehrerer System-Of-Systems-, System-, Subsystem-, Komponenten- oder Einheitenspezifikationen an andere interne Organisationseinheiten und Domänen oder aber an externe Organisationsgruppen und Zulieferer. Zudem werden an dieser Nahtstelle die jeweiligen Anforderungen zwischen den involvierten Interessenvertretern im Sinne des Lasten- und Pflichtenhefts verhandelt und abschließend festgelegt. Des Weiteren erfolgt beim Übergang von der interdisziplinären Subsystem- auf die disziplinspezifische Komponentenebene auch die Zuweisung von Teilaufgaben an die jeweiligen Entwicklungsdisziplinen Mechanik, E/E-Hardware und Software (siehe Abbildung 7.22).

Die Voraussetzung für die Bottom-Up-Integration ist wiederum die Verfügbarkeit von verifizierten Entwürfen bzw. Spezifikationen aus der nächsttieferen L_{n+1}-Granularitätsebene. In dieser Hinsicht kann die kontinuierliche Integration sowohl aus einer virtuellen als auch aus einer physisch manifestierten Perspektive betrachtet werden. Die virtuelle Integration korreliert mit dem System-Of-Systems-, System- und Subsystementwurf, indem verfügbare Komponenten, Einheiten und ihre Spezifikationen in das modellbasierte Gesamtgebilde integriert werden. Eine weitere Perspektive der virtuellen Integration bezieht sich auf die durchzuführenden Simulationsaktivitäten. Aus einer physisch geprägten Perspektive erfasst die Integration die Kombination von Hardware und Software zu einem mechatronischen bzw. cyber-physischen Gesamtsystem. Für sämtliche Perspektiven der Integration wird die Funktionalität mit einem definierten Betriebssicherheitsreifegrad (d.h. das funktionale Wachstum von Hardware und Software sowohl virtuell als auch physisch) zu einem definierten Zeitpunkt gefordert. Dies ermöglicht eine systematische sowie strukturierte Verifikation und Validierung der jeweiligen Betrachtungseinheit.

Eine konforme Realisierung des Entwicklungsgegenstands liegt somit dann vor, wenn die Verifikationsaktivitäten gezeigt haben, dass das spezifizierte Verhalten Teil des implementierten Verhaltens ist. Diese Konformitätsprüfungen reichen von Konsistenzprüfungen bis hin zu formalen Nachweisen und Evidenzen. Durch diese gesamtheitliche und systematische Vorgehensweise wird zum einen der Nachweis bzw. die Behauptung erbracht, dass die jeweiligen Teilspezifikationen der unteren L_{n+1}-Granularitätsebene die Anforderungen der sich darüber befindenden L_n-Granularitätsebene im Sinne der Verifikation erfüllen. Die Überprüfung ist allerdings nur in dem Maße schlüssig, inwieweit das erforderliche Verhalten auch explizit gemacht werden konnte. Unerwünschtes implementiertes, aber nicht spezifiziertes Verhalten oder erforderliches Verhalten, welches innerhalb der Spezifikation fehlt, kann daher nicht erfasst werden. Um mit diesen zusätzlichen Verhaltensmengen umgehen zu können, werden die im Zuge des Entwurfsprozesses getroffenen Annahmen, Hypothesen und Einschränkungen herangezogen.

Für die getroffenen Annahmen und festgelegten Einschränkungen muss somit im Zuge der Validierungsaktivitäten eine Evidenz für deren Vertretbarkeit, Konsistenz, Widerspruchsfreiheit und Gültigkeit erbracht werden (vgl. HF-12). Dabei wird die Legitimität der Hypothesen, Annahmen und Einschränkungen durch formale Ansätze, Simulation und Beobachtung der realen Welt überprüft (vgl. Abschnitt 4.7 und 4.8). Da bei den Modellen des Betriebsbereichs nicht davon ausgegangen werden kann, dass diese das reale bzw. tatsächliche Verhalten exakt wiedergeben, sondern nur annähernd, muss die robuste Erfüllung der verhaltensbezogenen Anforderungen nachgewiesen werden. Das bedeutet, dass die jeweiligen L_1-System-Of-Systems, L_2-Systeme, L_3-Subsysteme, L_4-Komponenten und L_5-Einheiten auch bei vernünftigen Variationen des realen Kontextverhaltens zweckmäßig funktionieren müssen. Diese Variationen können unterschiedlich interpretiert werden: Sensorrauschen, nicht modellierte Störungen (z.B. Temperaturschwankungen), Variationen physikalischer Parameter (z.B. Gewicht oder Größe einer technischen Komponente, welche von der Spezifikation abweicht) oder konservativ eingeschränkte Modellierungsfehler, d.h. Abweichungen zwischen Modellverhalten und tatsächlichem physikalischen Verhalten.

Ferner werden einige Parameterwerte in der Software erst spät im Entwicklungsprozess instanziiert und sind daher in den frühen Phasen des Entwurfsprozesses, in denen modellbasierte Verfahren angewendet werden, noch unbekannt. Dementsprechend müssen auch diese offenen Parameter im Zuge der Verifikations- und Validierungsaktivitäten berücksichtigt werden. Ein weiterer Aspekt besteht darin, das Unbekannte im Sinne noch nicht getesteter Kontexte zu untersuchen. Da Unbekanntes nicht zielgerichtet entdeckt werden kann, werden die jeweiligen Realisierungen der L_1-System-Of-Systems, L_2-Systeme, L_3-Subsysteme, L_4-Komponenten und L_5-Einheiten innerhalb der Zufälligkeit des offenen Kontexts Betriebsbereichs betrachtet. Dabei können beispielsweise stochastische Methoden (Markov-Ketten, Bayes‘sche Netze etc.), Monte-Carlo-Simulationen sowie experimentelle Designmethoden eingesetzt werden (vgl. Abschnitt 4.8).

Das eigentliche Ziel bei der Entwicklung ist demzufolge, eine hinreichend explizite Repräsentation des relevanten Teils der Realität zu erreichen, um über die Gültigkeit der erzielten Lösung der jeweiligen Betrachtungseinheit in akzeptabler Art und Weise argumentieren zu können. Damit wird deutlich, dass Validierungsaspekte auf jeder Granularitätsebene vorhanden sind, genauer gesagt, dass die Validierung eng mit jedem Schritt der horizontalen Konkretisierung, aber auch vertikalen Dekomposition verbunden ist. Somit werden die im Zuge der vorgenommenen Anforderungs- und Entwurfsdekomposition getroffenen Annahmen, Einschränkungen sowie Entwurfsentscheidungen im Hinblick auf die durchgeführten Modelldeduktionen, -allokationen und -verfeinerungen frühzeitig validiert.

Validität bzw. Gültigkeit bedeutet, dass die verwendeten Artefakte geeignet sind, die von den Interessengruppen gewünschten Eigenschaften in hinreichender Weise zu beschreiben. Dies umfasst insbesondere

Robustheit, Konsistenz und eine akzeptable Korrektheit unterhalb eines bestimmten Schwellenwerts für das Restrisiko. Dabei ist zu berücksichtigen, dass eine formale Vollständigkeit aufgrund der Offenheit des Kontexts nie vollständig erreicht werden kann. Diese Validierungsschleifen werden, beispielsweise unter Anwendung von Regressionstests, solange durchgeführt, bis die jeweiligen Entwürfe die erforderlichen Verifikations- und Validierungsergebnisse im Sinne einer robusten Basis liefern, so dass die nachfolgenden Aktivitäten der funktionalen, logischen und technischen Sichtweise der darunterliegenden L_{n+1}-Granularitätsebene eingeleitet werden können. Darunter fällt auch die Bereitstellung von Metriken zur Hypothesenprüfung und Evidenzgenerierung auf jeder Granularitätsebene für die Validierung vor der Freigabe und die Überprüfung sowie Aufrechterhaltung der Gültigkeit nach der Freigabe für den Feldbetrieb.

7.4.2 Systemmodellartefakte des modell- und simulationsbasierten Betriebssicherheitsnachweises

Der eingeführte Betriebssicherheitslebenszyklusprozess übernimmt hierbei die Rolle der Prozesssäule, reguliert den Betriebssicherheitslebenszyklus eines Systems eingebettet in dessen Betriebsbereich und beschreibt die notwendigen Anforderungen im Sinne des „WAS“ für die Generierung eines umfassenden Betriebssicherheitsnachweises als Gesamtliefergegenstand. Der Betriebssicherheitsnachweis belegt seinerseits die Betriebssicherheit eines Systems eingebettet in dessen Betriebsbereich und wird entlang der Nachweisführungskette Evidenz, Argument und Behauptung strukturiert. Daraus ergeben sich wiederum die Spezifikationen der Planungs- und Managementaktivitäten, der Anforderungs- und Testfallspezifikation, des Architekturentwurfs und der Architekturanalysen, der Verifikations-, Validierungs- und Testfallresultate, der Argumente sowie der Behauptungen als untergeordnete Arbeitsprodukte bzw. Liefergegenstände (siehe Abbildung 7.23). Die Gesamtheit der Spezifikationen und Architekturentwürfe, d.h. der Betriebssicherheitsnachweis, wird innerhalb des Systemmodellkonstrukts (vgl. Abschnitt 4.6) als Datenbank im Sinne der „Single Source of Truth" integriert. Das SPES-Modellierungsrahmenwerk beschreibt die Abfolge der jeweiligen Aktivitäten zur Generierung des oder der Systemmodelle, sprich das „WIE“.

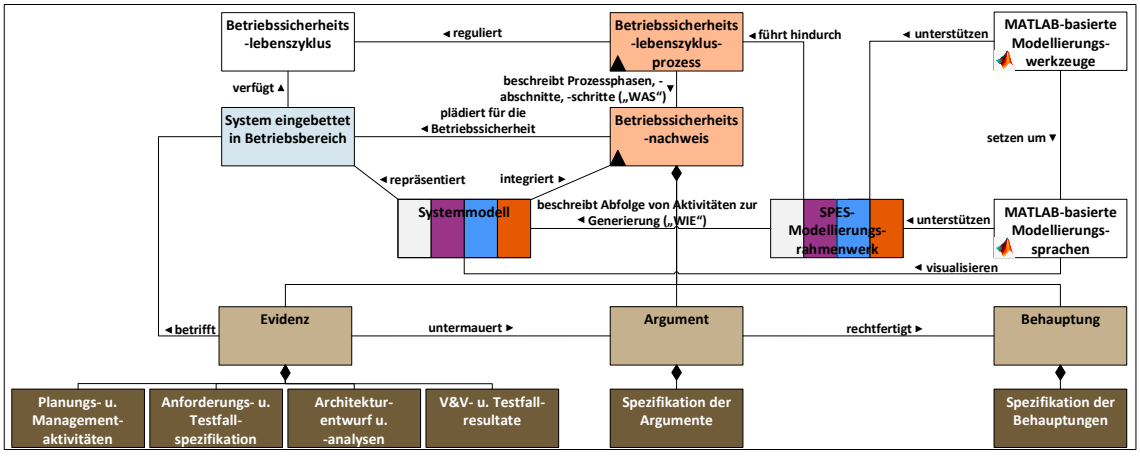


Abbildung 7.23: Zusammenhang der Säulen der modellbasierten Systementwicklung (Betriebssicherheitslebenszyklusprozess, SPES-Modellierungsrahmenwerk, MATLAB Modellierungssprache und -werkzeug) sowie die Integration des Betriebssicherheitsnachweises in das Systemmodell als Datenbank.

Insgesamt geht es darum, im Hinblick auf eines oder mehrerer Systeme eingebettet in deren Betriebsbereich, über den gesamten Betriebssicherheitslebenszyklus nachweisbasiert für deren Betriebssicherheit plädieren zu können. Der gesamte Vorgang wird durch ein oder mehrere Modellierungssprachen und -werkzeuge im Sinne der Mathworks Entwicklungsumgebungen MATLAB Simulink [175], System Composer [177] und Stateflow [176] unterstützt (siehe Abbildung 7.23). Allerdings sei hier explizit anzumerken, dass die Generierung von Systemmodellen unter Anwendung des SPES-Modellierungsrahmenwerks auch mit Hilfe anderer Modellierungssprachen und -werkzeugen, wie z.B. der SysML (vgl. Abschnitt 4.5), realisiert werden kann. Jedoch müssen die aufgeführten Limitierungen (vgl. Abschnitt 4.7), insbesondere was die Thematik analytisch dynamischer und/oder regelkreisbasierter Verhaltensweisen angeht (vgl. Abschnitt 4.4), mit Abhilfemaßnahmen (engl. *Workaround*) angegangen werden.

Das Systemmodellkonstrukt erfasst einerseits die modellbasierte Darstellung des jeweiligen Entwicklungsgegenstands mittels unterschiedlicher Ausprägungen der jeweiligen Formalismen, welche als eine Kombination von strukturbezogenen und analytischen Architekturmodellen im Hinblick auf die SPES-Architektursichtweisen ausgedrückt werden. Ein weiterer integraler Zweck des Systemmodells besteht darin, den Architekturentwurf eines Systems zu ermöglichen, welches seinerseits dessen Anforderungen erfüllt, und die nachvollziehbare sowie rückverfolgbare Zuordnung der Anforderungen zu den System-Of-Systems, Systemen, Subsystemen, Komponenten und Einheiten (Hardware oder Software) zu unterstützen. Infolgedessen werden die der SPES-Anforderungssichtweise zugehörigen Planungs-, Behauptungs-, Argument-, Anforderungs-, Testfall- und Anwendungsfallartefakte als weitere Bestandteile des Systemmodells aufgefasst. Dadurch agiert das Systemmodell als Informationsquelle bzw. Datenbank und integrierender Rahmen der wesentlichen Artefakte bzw. Modelle (siehe Abbildung 7.24).

Darunter fallen der Architekturentwurf, die Anforderungs- und Testfallspezifikation, die Anwendungsfallspezifikation sowie die Spezifikationen der Pläne, Strategien, Argumente und Behauptungen (siehe Abbildung 7.24). Die innerhalb der SPES-Anforderungssichtweise zu erfassenden Planungs-, Behauptungs-, Argument-, Anforderungs-, Testfall- und Anwendungsfallartefakte werden ihrerseits durch entsprechende Elemente detailliert. Die Anforderungsartefakte bestehen wiederum aus Businessanforderungen (engl. *Business Requirement {BReq}*), welche in Richtung von Interessenvertreteranforderungen (engl. *Stakeholder Requirement {SHReq}*) konkretisiert, die ihrerseits abermals in technische Anforderungen (engl. *Technical Requirement {TReq}*) präzisiert werden (siehe Abbildung 7.25).

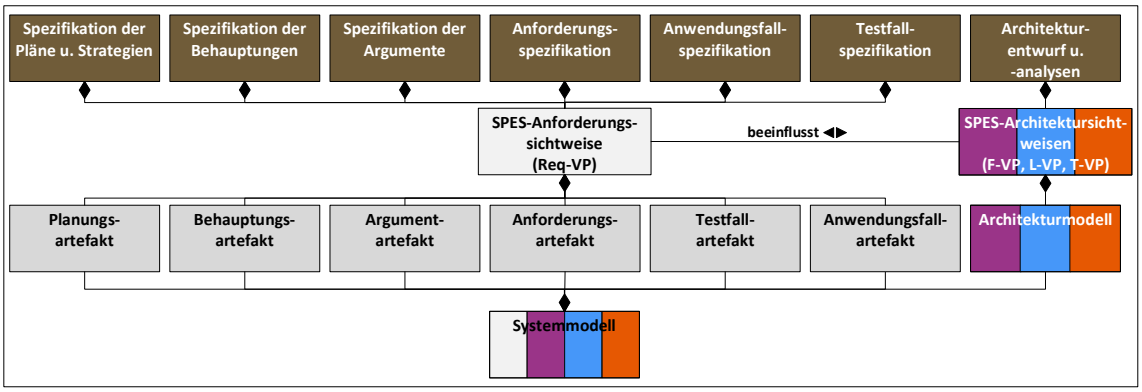


Abbildung 7.24: Dekomposition und über Generalisierungen hergestellter Zusammenhang der Spezifikationen und des Entwurfs im Hinblick auf die SPES-Sichtweisen und die Integration der Artefakte in das Systemmodell als Datenbank.

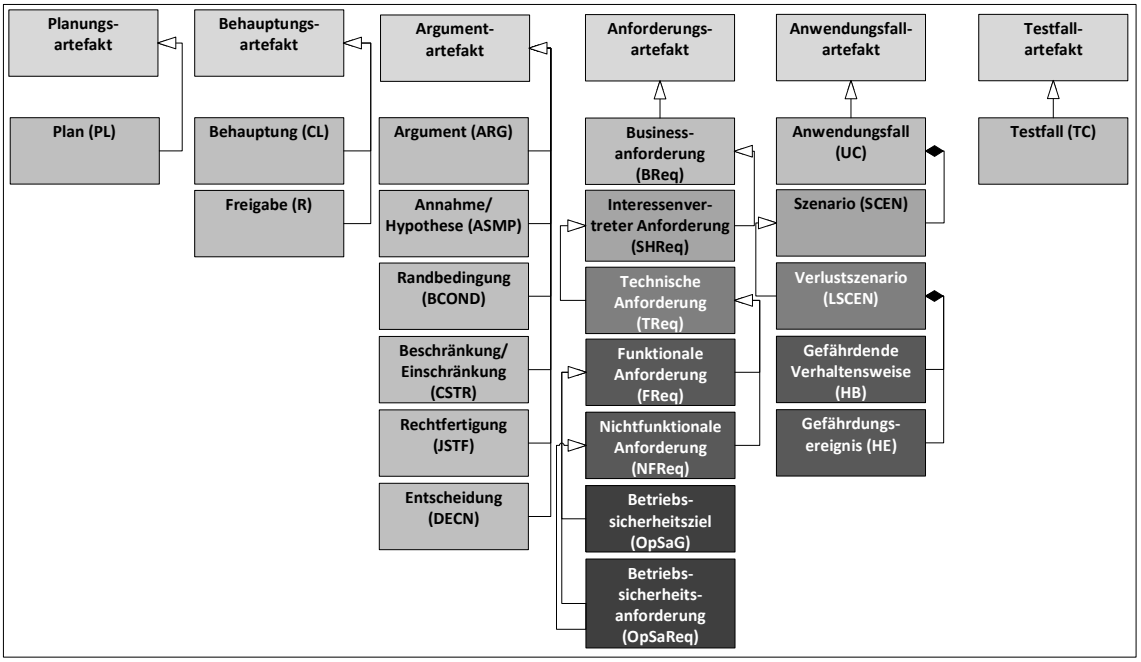


Abbildung 7.25: Artefakte der Spezifikation der Planungs- und Managementaktivitäten, Behauptungen, Argumente, Anforderungen sowie der Anwendungs- und Testfälle.

Die technischen Anforderungen lassen sich nochmals anhand von funktionalen (engl. *Functional Requirement {FReq}*) und nichtfunktionalen Anforderungen (engl. *Non-functional Requirement {NFReq}*) unterscheiden. Hinzu kommt deren jeweilige Verfeinerung in Richtung von Betriebssicherheitszielen (engl. *Operational Safety Goal {OpSaG}*) und Betriebssicherheitsanforderungen (engl. *Operational Safety Requirement {OpSaReq}*). Die Argumentartefakte kennzeichnen sich ihrerseits durch Argumente (engl. *Argument {ARG}*), Annahmen/Hypothesen (engl. *Assumption {ASMP}*), Randbedingungen (engl. *Boundary Condition {BCOND}*), Beschränkungen bzw. Einschränkungen (engl. *Constraint {CSTR}*), Rechtfertigungen (engl. *Justification {JSTF}*) sowie Entscheidungen (engl. *Decision {DECN}*). Was die Anwendungsfallartefakte angeht, so werden diese durch Anwendungsfälle (engl. *Use Case {UC}*), Szenarien (engl. *Scenario {SCEN}*), Verlustszenarien (engl. *Loss Scenario {LSCEN}*), gefährdende Verhaltensweisen (engl. *Hazardous Behaviour {HB}*) sowie durch mögliche Gefährdungsereignisse (engl. *Hazardous Event {HE}*) konkretisiert. Demgemäß werden die Pläne (engl. *Plan {PL}*), Behauptungen (engl. *Claim {CL}*), Freigaben (engl. *Release {R}*) und Testfälle (engl. *Test Case {TC}*) bedarfsgerecht unter den jeweiligen Variablen erfasst und dokumentiert (siehe Abbildung 7.25).

Die zu entwickelnden Architekturmodelle gemäß des SPES-Modellierungsrahmenwerks werden in funktionale (F) und logische Architekturmodelle (L) sowie in technische Architekturmodelle (T) separiert, um jeweils die funktionalen, logischen und technischen Architekturen abbilden zu können (vgl. Abschnitt 4.2). Allerdings steht und fällt die erfolgreiche Durchführung der jeweiligen SafeDevOps-Zyklen mit der Möglichkeit, simulative Verifikations- und Validierungsaktivitäten frühzeitig durchführen zu können. Dieser Sachverhalt steht zudem in einem engen Verhältnis im Hinblick auf das Tätigen von Annahmen, Einführen von Einschränkungen sowie deren kontinuierliche Verifikation, Validierung respektive Falsifikation, insbesondere was die offene Kontextproblematik des hochautomatisierten Fahrens angeht. Hinzu kommt die Thematik der Gewinnung eines systematischen Verständnisses sowie die Transparenz herbeigeführter Strategie- und Entwurfsentscheidungen (vgl. HF-12).

Demnach wird eine kohärente Verhaltensbeschreibung entwickelt, die mit den funktionalen, logischen und technischen Architekturen harmoniert. Dadurch werden die grundlegenden Systemaspekte – Funktion, Verhalten sowie logische und technische Architektur (vgl. Abschnitt 4.2) – in einen konsistenten Zusammenhang gebracht (siehe Abbildung 7.26). Die funktionalen, logischen und technischen Architekturmodelle werden den strukturellen Sichtenmodellen zugeordnet, wohingegen sich die funktional, logisch und technisch spezifischen Verhaltensmodelle je nach Ausprägung und Analysegegenstand einerseits als verhaltensbezogene Sichtenmodelle und/oder als analytisch statische bzw. dynamische Verhaltensmodelle erweisen (vgl. Abschnitt 4.4). Dabei handelt es sich um eine durchgängige Abdeckung funktionaler, logischer und technischer Merkmale der Fahrzeug- und ggf. Infrastrukturarchitekturen eingebettet in deren Betriebsbereich sowie um eine dazu komplementäre, nahtlose und ausführbare funktional, logisch und/oder technisch spezifische Verhaltensmodellierung. Zusammen mit einer integrierten Verhaltensmodellierung lassen sich daraus ausführbare Architekturen unterschiedlichen Konkretisierungsgrads entwerfen. Hierbei wird eine Trennung zwischen dem funktional spezifischen Verhaltensmodell (FB) sowie dem logisch (LB) und/oder technisch spezifischen Verhaltensmodell (TB), welche jeweils das zu untersuchende Verhalten konkretisieren, vorgenommen (siehe Abbildung 7.26).

Im Zuge der integrierten Simulationsausführung innerhalb des modellbasierten Architekturentwicklungswerkzeuges wird sowohl die Visualisierung der Simulationsergebnisse als auch deren Weiterverarbeitung unter Hinzunahme definierter Metriken realisiert, was sich wiederum als eine notwendige Voraussetzung für die integrierte Variantenbewertung sowie für mögliche iterative Modellverbesserungen manifestiert. Allerdings ist sicherzustellen, dass das resultierende Verhalten, welches durch die unterschiedlichen Ausprägungen der Verhaltensmodelle beschrieben wird, zueinander konsistent ist. So muss das logisch spezifische Verhaltensmodell (LB) unter Berücksichtigung zusätzlicher logisch spezifischer Architekturmerkmale das Verhalten des funktional spezifischen Verhaltensmodells (FB) innerhalb einer vorzugebenden Spanne zulässiger Abweichungen sowohl qualitativ als auch quantitativ erfüllen. Dasselbe gilt für das technisch spezifische Verhaltensmodell (TB), welches das logisch spezifische Verhaltensmodell (LB) adäquat zu konkretisieren bzw. präzisieren hat (siehe Abbildung 7.26).

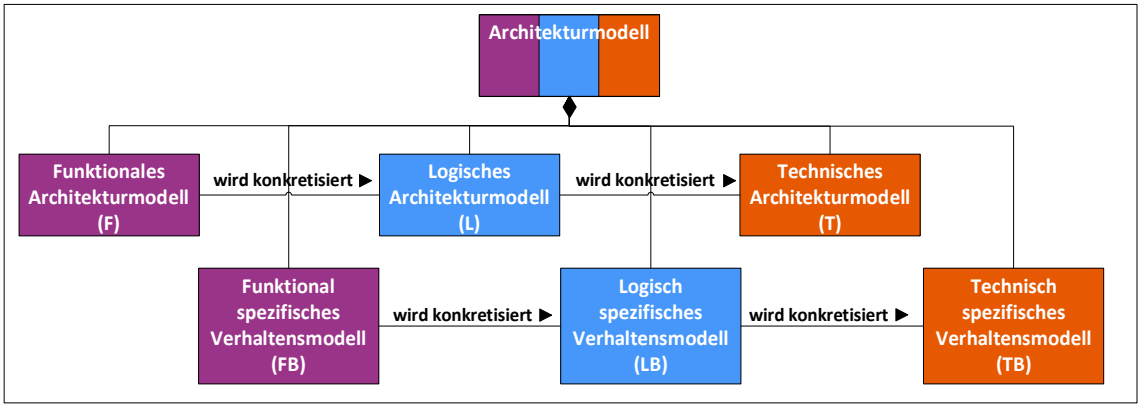


Abbildung 7.26: Dekomposition und über Assoziationen hergestellter Zusammenhang des Architekturmodells anhand der funktionalen (F), logischen (L) und technischen Architekturmodelle (T) sowie der funktional (FB), logisch (LB) und technisch spezifischen Verhaltensmodelle (TB).

Mit Hilfe der Kapselung im Sinne des Verbergens bzw. Aus- und Einblendens von im Bedarfsfall nicht benötigter oder sofern möglich von den Schnittstellen isoliert gehaltenen Informationen, müssen sowohl die funktionale Struktur (F) als auch die jeweiligen Schnittstellen des zu untersuchenden Verhaltensmodells (FB) mittels einer dynamischen Plug-and-Play-Verknüpfung logischer (LB) weiterhin noch realisierungsunabhängiger oder aber auch technisch spezifischer bzw. realisierungsabhängiger Verhaltensmodellvarianten (TB) für Laufzeitbetrachtungen nicht explizit verändert werden.

7.5 Fazit der Konzeption des agilen Betriebssicherheitslebenszyklusprozesses

Die Grundsätze des im Rahmen der vorliegenden Dissertation konzipierten Betriebssicherheitslebenszyklusprozesses leiten sich aus der Analyse der verschiedener regulatorischer Normungs- und Standardisierungsaktivitäten (vgl. Unterabschnitt 6.4.1), wesentlicher Industrie- und Forschungsprojekte (vgl. Unterabschnitt 6.4.2) als auch aus der Betrachtung einer umfassenden Auswahl veröffentlichter Arbeiten entsprechender Industrie- und Forschungseinrichtungen (vgl. Unterabschnitt 6.4.3) ab. Dabei ist die prinzipielle Struktur an das V-Modell sowie an die Top-Down-Prozessabschnitte der ISO 26262 und ISO 21448 angelehnt und um dazu kohärente übergeordnete Betriebssicherheitsentwicklungstätigkeiten vertikal erweitert. Hinzu kommt die Einbettung agiler iterativ-inkrementeller Vorgehensweisen sowie die prozessuale Anbindung des Automotive-PEP inkl. einer horizontalen Sicherheitszykluserweiterung bzw. Vertiefung im Hinblick auf die Phase des Betriebs, der Wartung und Außerbetriebnahme. Vor diesem Hintergrund wird der Gesamtprozess durch eine kontinuierliche Absicherung des iterativ-inkrementell zunehmenden Betriebssicherheitsreifegrads organisiert und vorangetrieben. Der klar strukturierte und modulare Aufbau ermöglicht in der Konsequenz ein durchgehend skalierbares Vorgehen.

Der allgemeine Entwicklungsablauf des modell- und simulationsbasierten Betriebssicherheitsentwicklungsansatzes bildet ein strukturiertes Gerüst und ermöglicht ein angemessenes Verständnis offener Kontextsysteme (z.B. hochautomatisiertes Ego-Fahrzeug und relevanter Teil der Umgebung im Sinne des Betriebsbereichs), der Wechselwirkungen und gegenseitigen Abhängigkeiten sowie potenzieller Unzulänglichkeiten (d.h. Annahmen und Einschränkungen, die vorübergehend oder dauerhaft ungültig sind). Die Annahmen werden im gesamten Entwicklungsprozess und innerhalb der jeweiligen Sichtweisen bezogenen Spezifikationen ermittelt und dokumentiert, um getroffene Entscheidungen zu erklären oder grundlegende Informationen festzuhalten, auf denen der Entwurf wiederum basiert. Daraus lassen sich wiederum notwendige Argumentations- sowie Evidenzgrundlagen und damit Validierungs- als auch Verifikationsaktivitäten ableiten. Das dadurch iterativ-inkrementell gewonnene Systemverständnis agiert hierbei als ein Grundpfeiler des ganzheitlichen Evidenz-, Argumentations- und Behauptungserstellungszyklus. Einen weiteren Beitrag hierzu liefert die Simulation analytisch dynamischer Verhaltensspezifikationen, wodurch ein profundes Verständnis sowohl vertikaler als auch horizontaler Abhängigkeiten gefördert wird.

Alles in allem führt das Multiple-SafeDevOps-V-Modell einen neuartigen Integrationsansatz ein, der klassische V-Modell-Strukturen erstmals mit agilen Reifegrad- und SafeDevOps-Zyklen verknüpft. Der Ansatz ermöglicht eine bisher nicht realisierte Synchronisation sicherheitsrelevanter Entwicklungs-, Integrations- und Testschritte mit den Freigaben des Automotive-PEP. Zudem berücksichtigt er kontinuierlich rückgeführte Evidenzen aus Simulationen und Felddatenpipelines und fügt diese systematisch in den Betriebssicherheitsnachweis ein. Dadurch entsteht ein skalierbarer, wiederholbarer und datengetriebener Betriebssicherheitslebenszyklus, der den bestehenden Stand der Wissenschaft und Technik erweitert.

Insgesamt bedeutet eine unzureichende Betriebssicherheitsargumentation nicht automatisch, dass das hochautomatisierte Kraftfahrzeug sich nachher im Feldbetrieb inakzeptabel verhalten wird. Sie deutet aber auf tiefgreifendere organisatorische und methodische Limitierungen in Bezug auf die jeweiligen Entwicklungsbeteiligten hin, den aktuellen Entwicklungsstand abrufen und angemessen mitteilen zu können. Analog dazu resultiert eine glaubwürdige Betriebssicherheitsargumentation auch nicht, sozusagen als Selbstverständlichkeit, in einem sich über den gesamten Betriebssicherheitslebenszyklus akzeptabel verhaltenden hochautomatisierten Kraftfahrzeug. Jedoch spricht eine nachvollziehbare Betriebssicherheitsargumentation für die Fähigkeit der Entwicklungsbeteiligten, deren Inhalt adäquat vermitteln zu können. Der im Rahmen dieser Dissertation entwickelte agile Betriebssicherheitslebenszyklusprozess bietet hierfür einen systematischen Weg, um die Erstellung eines argumentativ fundierten Betriebssicherheitsnachweises voranzutreiben. Dies erfolgt im Sinne eines modellbasierten, ganzheitlichen Ansatzes entlang der vier Säulen Prozess, modellbasierte Methode, Modellierungssprache und Modellierungswerkzeug.

8 Modell- und simulationsbasiertes Betriebssicherheitskonzept für die Längs- und Querführung eines hochautomatisierten Autobahnpiloten

„Alle Modelle sind falsch, aber manche sind nützlich."

Norbert Wiener

Für eine abschließende Evaluation wird im Verlaufe dieses Kapitels der agile Betriebssicherheitslebenszyklusprozess hinsichtlich der Erstellung eines modell- und simulationsbasierten Betriebssicherheitsnachweises konkretisiert und im Detail umgesetzt. Dies erfolgt mittels eines beispielhaften simulationsbasierten Anwendungsfalls im Hinblick auf die Längs- und Querführung eines hochautomatisierten (SAE-Level 4) Autobahnpiloten. Die Zielsetzung liegt darin unter expliziter Anwendung des agilen Betriebssicherheitslebenszyklusprozesses einen dem Problemfall „Freiheit von inakzeptablen fahrzeugregelungsbezogenen Risiken" zugeschnittenen Leitfaden darzulegen. Darunter fällt insbesondere die Herleitung einer verkehrsregelkonformen vertretbaren Fahrzeugverhaltensspezifikation. Unter Nichtberücksichtigung der RGA-MS 0 bezogenen Tätigkeiten stehen gemäß RGA-MS 1 die nachfolgenden virtuell zu erbringenden Liefergegenstände im Fokus (siehe Abbildung 8.1):

- **RGA-MS 1 – Anforderungsmanagement für Vergabeumfang:**
    - Vorläufige/frühzeitige virtuelle Betriebssicherheitsverifikation und -validierung
        - Betriebsbereichsfreigabe ODDR0.1
        - Item Freigabe IR0.1
        - Verfeinerte Betriebsbereichsfreigabe ODDR0.2

Vor diesem Hintergrund ergibt sich somit das Bestreben, die in den Entwurfs- und Integrationsphasen definierten Arbeitsprodukte bzw. Inkremente im Einklang mit den OpSa-ML1 Iterationen bzw. Zyklen des Multiple-SafeDevOps-V-Modells (vgl. Unterabschnitt 7.3.2) einerseits zu erstellen und andererseits die zur Erreichung der ersten Stufe des Betriebssicherheitsreifegrads gestellten Anforderungen zu erfüllen (siehe Tabelle B.2, Tabelle B.3 und Tabelle B.4). In dieser Hinsicht beinhaltet der zugeschnittene Entwicklungspfad als Schritt 1 den „Entwurfs- und Validierungszyklus gemäß der Betriebskonzeptphase" (vgl. Abschnitt 8.1 sowie Anhang C.1). Als Schritt 2 erfolgt der „Entwurfs- und Verifikationszyklus gemäß der Konzeptphase" (vgl. Abschnitt 8.2 sowie Anhang C.2) sowie als Schritt 3 der „Virtuelle Integrations- und Validierungszyklus im Rahmen des Bottom-Up-Übergangs von der Konzept- in die Betriebskonzeptphase" (vgl. Abschnitt 8.3 sowie Anhang C.3), wobei die L_1/L_2-Granularitätsebenen durchschritten werden (siehe Abbildung 8.1 und Abbildung 8.2).

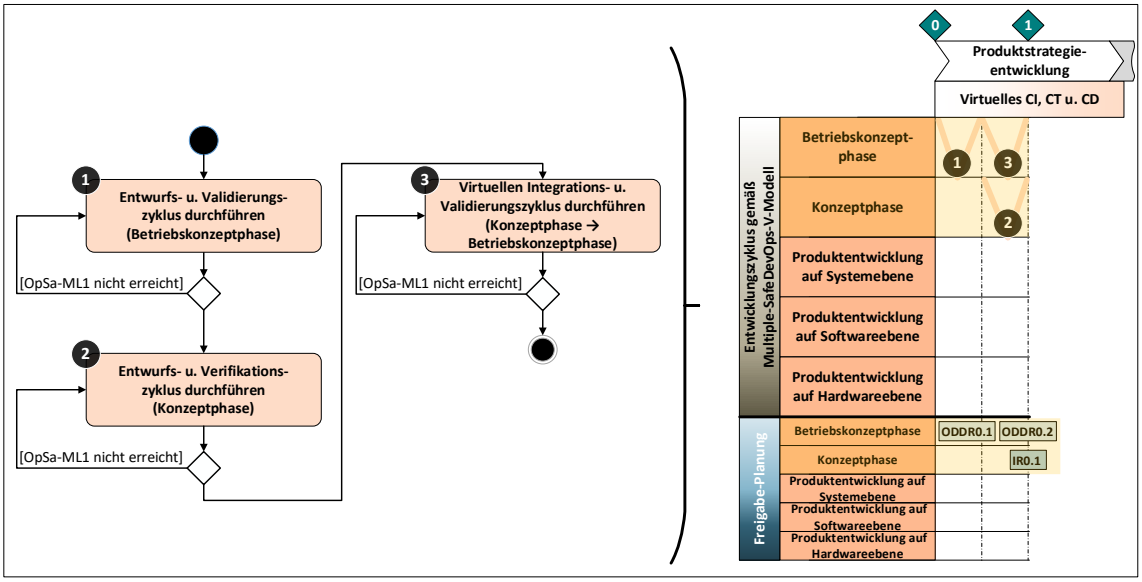


Abbildung 8.1: Ausschnitt der für das modell- und simulationsbasierte Betriebssicherheitskonzept relevanten vertikal verlaufenden Phasen des Betriebssicherheitslebenszyklusprozesses (gelber Bereich) und der horizontalverlaufenden Phasen des PEPs.

Insbesondere geht es um einen exemplarischen Top-Down- als auch Bottom-Up-Entwicklungspfad durch die Matrixelemente des modell- und simulationsbasierten Betriebssicherheitsentwicklungsansatzes, welcher wiederum aufzeigt, inwiefern über die Aktivitätsabschnitte der Sichtweisen („WIE“) zu den Zielsetzungen bzw. modell- und simulationsbasierten Liefergegenständen („WAS“) des agilen Betriebssicherheitslebenszyklusprozesses gelangt werden kann. Dabei werden die Aktivitätsabschnitte der Anforderungssichtweise sowie der funktionalen und logischen Sichtweise abgehandelt, wobei aus Gründen des Betrachtungsrahmens der vorliegenden Dissertation die technische Sichtweise keine Berücksichtigung findet (siehe Abbildung 8.2).

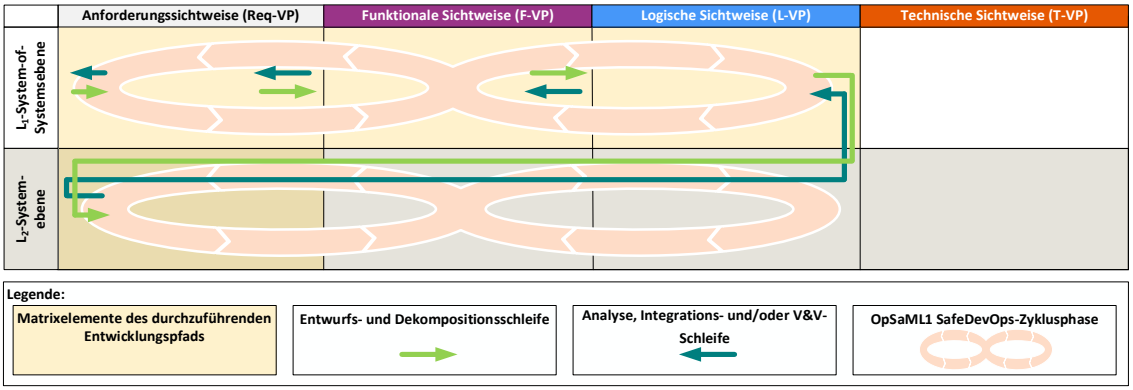


Abbildung 8.2: SPES-Matrix unter Hervorhebung der für das modell- und simulationsbasierte Betriebssicherheitskonzept relevanten Matrixelemente (gelber Bereich).

8.1 Entwurfs- und Validierungszyklus gemäß der Betriebskonzeptphase

Im weiteren Verlauf erfolgt die modell- und simulationsbasierte Umsetzung des Entwurfs- und Validierungszyklus gemäß der Betriebskonzeptphase einschließlich den Prozessabschnitten „Übergeordnete Interessenvertreterzielsetzung und Anwendungsfalldefinition“ (vgl. Unterabschnitt 8.1.1), „Identifikation und Analyse der Interessenvertreter“ (vgl. Unterabschnitt 8.1.2), „Betriebsbereichsdefinition und -analyse“ (vgl. Unterabschnitt 8.1.3), „Betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung“ (vgl. Unterabschnitt 8.1.4) sowie „Betriebssicherheitskonzept“ (vgl. Unterabschnitt 8.1.5). Im Fokus steht dabei die Anforderungssichtweise auf L_1-Granularitätsebene (siehe Abbildung 8.3). Des Weiteren sei darauf hingewiesen, dass die dabei generierten Betriebssicherheitsanforderungen, Annahmen, Entwurfsentscheidungen, Testfälle, Evidenzen etc. im Anhang C.1 dokumentiert werden.

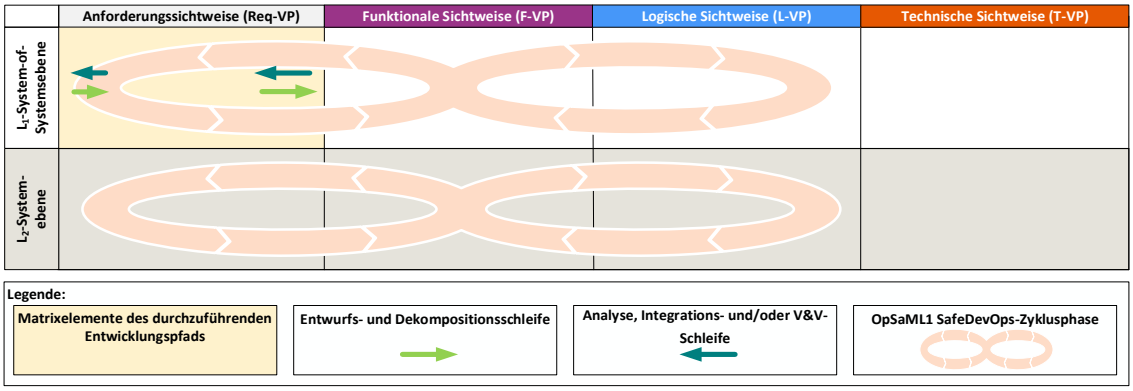


Abbildung 8.3: SPES-Matrix unter Hervorhebung der für das modell- und simulationsbasierte Betriebssicherheitskonzept relevanten Matrixelemente im Hinblick auf den Entwurfs- und Validierungszyklus gemäß der Betriebskonzeptphase (gelber Bereich).

8.1.1 Übergeordnete Interessenvertreterzielsetzung und Anwendungsfalldefinition

Die Anwendungsfalldefinition repräsentiert die Initiierung des gesamten Entwicklungsvorhabens und spiegelt im Sinne der Anforderungsentwicklung auf oberster Granularitätsebene den Ausgangspunkt für alle weiteren betriebssicherheitstechnischen Entwicklungsaktivitäten wider. Vor diesem Hintergrund stehen einerseits die Zielvorgaben 3-1.1 des Teil 3-1 „Übergeordnete Interessenvertreterzielsetzung und Anwendungsfalldefinition“ im Vordergrund (siehe Abbildung 8.4). Andererseits geht es im Zuge des ersten Iterationsdurchlaufs darum, die erforderliche Inhaltsstruktur des Inkrements bzw. Arbeitsprodukts WP-32 unter Bezugnahme der Erreichung des Betriebssicherheitsreifegrads OpSa-ML1 zu generieren. Den Ausgangspunkt für den modell- und simulationsbasierten Betriebssicherheitsnachweis des hochautomatisierten Autobahnpiloten, bilden Businessanalysen der wichtigsten Interessenvertreter (Betreiber, OEM, Zulieferer etc.) sowie Strategien im Hinblick auf ein Lebenszykluskonzept einschließlich vorläufiger Ideensammlungen. Diese werden unter Anwendung des ersten Aktivitätsabschnitts „L_1-A. Erfasse Spezifikationen“ innerhalb der Anforderungssichtweise auf L_1-Granularitäts- bzw. System-Of-Systems-Ebene in Richtung von initialen Interessenvertreterzielsetzungen konkretisiert (siehe Schritt 1 Abbildung 8.4).

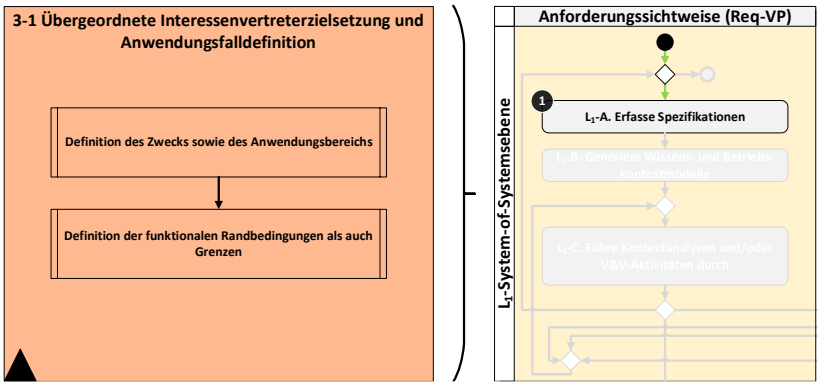


Abbildung 8.4: Durchzuführender Prozessabschnitt Teil 3-1 sowie zugehörige Aktivität innerhalb der L_1-Anforderungssichtweise.

Hieraus resultiert die übergeordnete Interessenvertreterzielsetzung bzw. -anforderung L1-SHReq. Insgesamt geht es hierbei darum, ein profitables Produkt im Sinne eines Autobahnpiloten für sicheres hochautomatisiertes Fahren innerhalb der definierten Systemgrenzen deutscher Autobahnen zu entwickeln und anschließend einzusetzen (siehe Tabelle 8.1). Anschließend werden die für den Anwendungsfall relevanten Akteure, Funktionsumfänge einschließlich des angestrebten Automatisierungsgrads, das jeweilige Wunschverhalten als auch die funktionalen Systemgrenzen einschließlich Annahmen, Einschränkungen und Randbedingungen beschrieben. An dieser Stelle wird im Zuge des Funktionsumfangs die Rolle der Anwender bzw. des „L_1-Fahrers/Passagiers_L“ als auch des zu automatisierenden Systems im Sinne des Autobahnpiloten für das „L_1-Ego-Kraftfahrzeug_L“ spezifiziert. Somit übernimmt dieses die vollständige Verantwortung der Durchführung der dynamischen Fahraufgabe[1], wobei der Akteur „L_1-Fahrer/Passagier_L“ gemäß der Randbedingung L1.1-BCOND nicht als Rückfallebene[2] in Frage kommt und sich währenddessen anderen Tätigkeiten widmen kann.

Tabelle 8.1: Übergeordnete Interessenvertreterzielsetzung in Bezug auf den Autobahnpiloten als auch Randbedingung im Hinblick auf den Ausschluss des „L_1-Fahrer/Passagiers_L“ als Rückfallebene.

<<Interessenvertreteranforderung>>
ID: L10000SHReq
L1-SHReq Autobahnpilot für die hochautomatisierte Beförderung von Personen auf deutschen Autobahnen
Es soll ein Autobahnpilot für den sicheren hochautomatisierten Betrieb des „L_1-Ego-Kraftfahrzeugs_L“ auf deutschen Autobahnen unter Einhaltung der Straßenverkehrsgesetzgebung, gültiger Normen und Standards sowie dem aktuellen Stand von Wissenschaft und Technik entwickelt, in Betrieb genommen und über einen festgelegten Zeitraum eingesetzt werden. Dabei soll das „L_1-Ego-Kraftfahrzeug_L“ die vollständige Verantwortung der hochautomatisierten Durchführung der dynamischen Fahraufgabe übernehmen.
<<Randbedingung>>
ID: L1.10000BCOND
L1.1-BCOND „L_1-Fahrer/Passagier_L“ stellt keine Rückfallebene dar
Während der hochautomatisierten Durchführung der dynamischen Fahraufgabe steht der „L_1-Fahrer/Passagier_L“ zu keinem Zeitpunkt als Rückfallebene zur Verfügung.

[1] Dynamische Fahraufgabe (vgl. Definition 2.3)

[2] Rückfallebene (vgl. Definition 2.8)

Dementsprechend wird der Automatisierungsgrad auf SAE-Level 4 gesetzt (siehe Tabelle C.1). Im Hinblick auf das Wunschverhalten werden die durchzuführenden Fahraufgaben und Manöver der hochautomatisierten Längs- und Querführung definiert. Seitens der Längsführung stehen die „Freifahrt“ unter Einhaltung der Geschwindigkeitsbegrenzung, das „Annähern“ als auch die „Abstandshaltung“ zum „L_1-Verkehrsteilnehmer_L“ im Fokus. Im Bereich der Querführung rückt das Wunschverhalten „Fahrstreifen Folgen“ unter Berücksichtigung der „L_1-FahrzeugexterneODDElemente_L“ in den Mittelpunkt. Was die funktionalen Systemgrenzen angeht, so wird die maximale Längsgeschwindigkeit des „L_1-Ego-Kraftfahrzeugs_L“ auf $36.11\ \frac{m}{s}\left(130\ \frac{km}{h}\right)$ eingeschränkt.

Darüber hinaus werden Spurwechsel- und/oder Ausweichmanöver ausgeschlossen, wobei der Frontsichtbereich auf den Ego-Fahrstreifen limitiert wird. Ferner wird der Betrieb auf Autobahnabschnitten innerhalb Deutschlands, auf ideale Straßenbedingungen als auch auf ideale Wetterbedingungen zur Tageszeit eingeschränkt. Zudem werden weder das mögliche Eintreten noch das Verlassen der Einsatzumgebung, sprich des Betriebsbereichs, noch die Interaktion mit dem Fahrer bzw. mit den Passagieren im Sinne des „L_1-Fahrers/Passagiers_L“ berücksichtigt.

Daraus wird wiederum der zentrale Anwendungsfall zur Erfüllung der betrachteten Interessenvertreterzielsetzung abgeleitet und modelliert. Hierbei wird zunächst der übergeordnete Anwendungsfall „L_1-TransportierePassagiereHochautomatisiertAufDerAutobahn_UC“ als elementarer Zweck des „L_1-Ego-Kraftfahrzeugs_L“ definiert und anschließend mittels der Enthält-Beziehung (engl. *Include*) des Anwendungsfalls bzw. Features L1.1-UC „L_1-FolgeFahrstreifenHochautomatisiertAufDerAutobahn_UC“ konkretisiert (siehe Abbildung 8.5). Weitere Attribute, wie z.B. Spurwechsel, Eintreten und Verlassen des Betriebsbereichs, Mensch-Maschine-Interaktion innerhalb des Fahrgastraums usw., können dem übergeordneten Anwendungsfall „L_1-Transportiere…_UC“ modular bzw. inkrementell mittels Enthält- und Erweitert-Beziehungen (engl. *Extend*) hinzugefügt werden. Dies ist allerdings aus Gründen des Umfangs nicht Bestandteil der vorliegenden Dissertation.

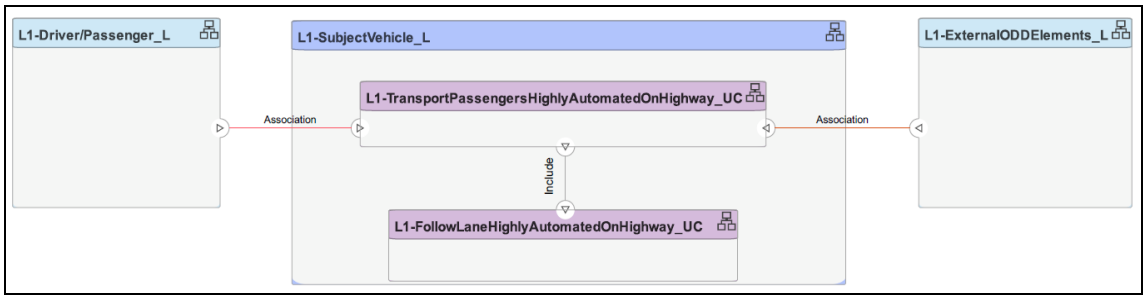


Abbildung 8.5: L_1-Anwendungsfalldiagramm, worin das „L_1-Ego-Kraftfahrzeug_L“ dem „L_1-Fahrer/Passagier_L“ die Dienstleistung „L_1-Transportiere…_UC“ zur Verfügung stellt.

8.1.2 Identifikation und Analyse der relevanten Interessenvertreter

Ausgehend von der Anwendungsfalldefinition erfolgt im Zuge von Teil 3-2 „Identifikation und Analyse der relevanten Interessenvertreter“ der Übergang in eine Kontextbetrachtung. Dies geschieht unter Anwendung der Aktivitätsabschnitts „L_1-B. Generiere Wissens- und Betriebskontextmodelle“ der Anforderungssichtweise auf L_1-Granularitätsebene (siehe Schritt 1 Abbildung 8.6), wobei die Zielvorgaben 3-2.1 des Arbeitsprodukt bzw. Inkrements WP-9 gemäß OpSa-ML1 erfüllt werden sollen. Hierbei wird vornehmlich

die funktionale Systemgrenze im Hinblick auf die Einschränkung des Betriebs auf Autobahnabschnitten innerhalb Deutschlands in den Mittelpunkt gerückt.

Infolgedessen werden die länderspezifischen produktbezogenen Gesetze, Richtlinien und Standards, sprich der jeweils geltende rechtliche Kontext und dessen Perspektive auf das Entwicklungsvorhaben betrachtet. Von besonderer Relevanz charakterisieren sich im Zuge der hier durchgeführten Identifikation der Interessenvertreter die deutsche StVO [47], der UN-Regelung Nr. 157 [309] für automatisierte Spurhaltesysteme (engl. *Automated Lane Keeping System {ALKS}*), der im Verlauf der vorliegenden Dissertation aufgesetzte Betriebssicherheitslebenszyklusprozess (vgl. Abschnitt 7.2), die Normen ISO 26262 [50], ISO 21448 [55], ISO 34502 [219] und ISO 34503 [91], als auch die Richtlinien für die Anlage von Autobahnen (RAA) [246]. Unter Bezugnahme der beabsichtigten Funktionalität einschließlich des Automatisierungsgrads SAE-Level 4 sowie der festgelegten Systemgrenzen und Einsatzumgebung im Sinne der hochautomatisierten Längs- und Querführung auf deutschen Autobahnabschnitten, werden die relevanten Interessenvertreter (deutsche StVO, UN-Regelung Nr. 157, etc.) des Entwicklungsvorhabens im Sinne der Einschränkung L1.1-CSTR festgelegt.

An dieser Stelle wird allerdings die Berücksichtigung unternehmensbezogener, organisatorischer und projektspezifischer Rahmenbedingungen im Hinblick auf den hier zu generierenden Betriebssicherheitsnachweis nicht im Detail aufgegriffen. Demzufolge fallen gemäß der Einschränkung L1.2-CSTR Interessenvertreter wie Hersteller-, Zulieferer-, und Betreiberorganisationen sowie ggf. weitere Institutionen nicht in den hier aufgespannten Betrachtungsrahmen. Auf Basis der vorangegangenen Schritte wird schließlich der Entwicklungskontext des zu entwerfenden und daraufhin zu betreibenden Autobahnpiloten abgeleitet und modelliert (siehe Abbildung 8.7).

Im Anschluss daran wird der abgeleitete Entwicklungskontext im Hinblick auf die gültigen Gesetze, behördlichen Vorgaben und Richtlinien, Normen und Standards sowie des aktuellen Stands von Wissenschaft und Technik gemäß „L_1-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch“ analysiert, um daraus die übergeordneten Interessenvertreteranforderungen des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“ gemäß „L_1-A Erfasse Spezifikationen“ abzuleiten (siehe Schritt 2 und 3 Abbildung 8.6).

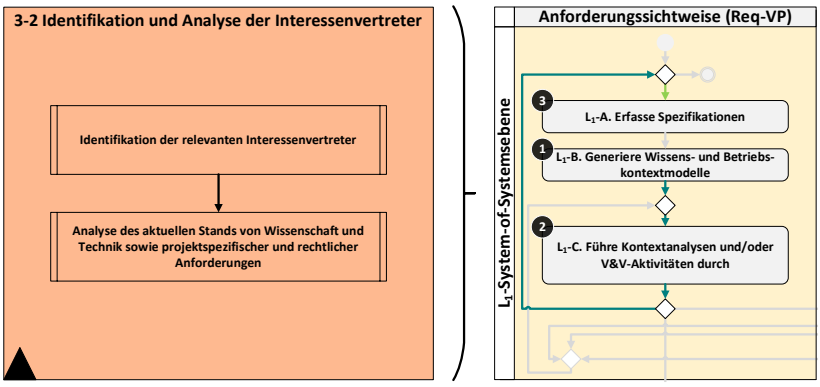


Abbildung 8.6: Durchzuführender Prozessabschnitt Teil 3-2 sowie zugehörige Aktivitäten innerhalb der L_1-Anforderungssichtweise.

Auf der einen Seite wird das Wissenskontextmodell sowie die darin enthaltenen Interessenvertreter einer Analyse in Bezug auf den Straßenverkehr als einen durch Rechtsvorschriften und -richtlinien geregelten Raum unterzogen (siehe Abbildung 8.7). Auf der anderen Seite wird die übergeordnete Interessenvertreterzielsetzung L1-SHReq im Hinblick auf die Einhaltung der Straßenverkehrsgesetzgebung, sowie gültiger Normen und Standards als auch dem aktuellen Stand von Wissenschaft und Technik herangezogen. Für das hochautomatisierte Kraftfahrzeuge gelten für eine gesetzeskonforme Fahrzeugverhaltensspezifikation genau jene Richtlinien, welche auch von den menschlichen Fahrern beim Führen eines Kraftfahrzeugs eingehalten werden müssen.

Demzufolge wird die Interessenvertreteranforderung L1-SHReq dahingehend ergänzt, die in der StVO als auch die in der UN-Regelung Nr. 157 enthaltenen Vorgaben und Richtlinien einzuhalten. Anschließend werden die in der StVO enthaltenen Dokumente insbesondere nach verhaltensrechtlichen Vorgaben durchsucht, um im Zuge der Entwicklung des Betriebssicherheitskonzepts (vgl. Unterabschnitt 8.1.5) ein Modell des beabsichtigten Sollverhaltens erstellen zu können. Im Hinblick auf den hier im Fokus stehenden Anwendungsfall L1.1-UC „L_1-FolgeFahrstreifen…_UC“ werden an erster Stelle die signifikanten Abschnitte von § 3 Geschwindigkeit [310], § 4 Abstand der StVO [311] sowie die jeweils in Betracht zu ziehende Absätze der UN-Regelung Nr. 157 [309] analysiert. Die jeweiligen Inhalte werden des Weiteren entlang der Verhaltensaspekte Geschwindigkeit, Abstand und Spurführung bzw. -haltung kategorisiert. Dabei werden die relevanten Paragrafen erfasst und in Interessenvertreteranforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ überführt (siehe Tabelle C.3, Tabelle C.4 und Tabelle C.5). Dasselbe gilt für die RAA [55], woraus weitere Vorschriften zur geometrischen Gestaltung als auch der Verkehrsführung abgeleitet werden (siehe Tabelle C.6).

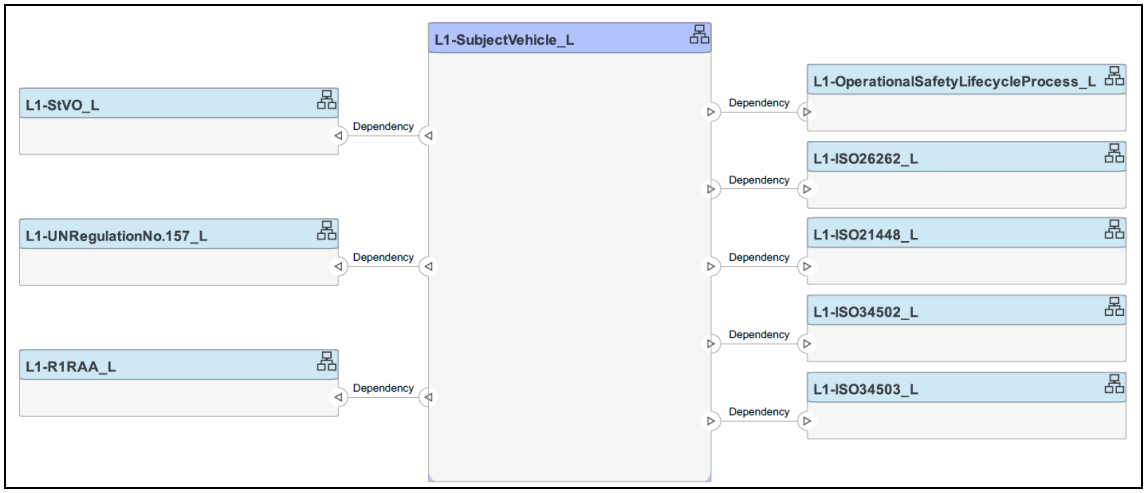


Abbildung 8.7: L_1-Kontextdiagramm, worin die entwicklungsbezogenen Abhängigkeiten zwischen dem „L_1-Ego-Kraftfahrzeug_L“ sowie den Elementen der Straßenverkehrsgesetzgebung, des Betriebssicherheitslebenszyklusprozesses sowie der Automotive-Sicherheitsstandards und -normen hervorgehoben werden.

8.1.3 Betriebsbereichsdefinition und -analyse

Ausgehend von der Anwendungsfalldefinition als auch der Wissenskontextanalyse erfolgt nun der Übergang in Teil 3-3 „Betriebsbereichsdefinition und -analyse“ (siehe Abbildung 8.8).

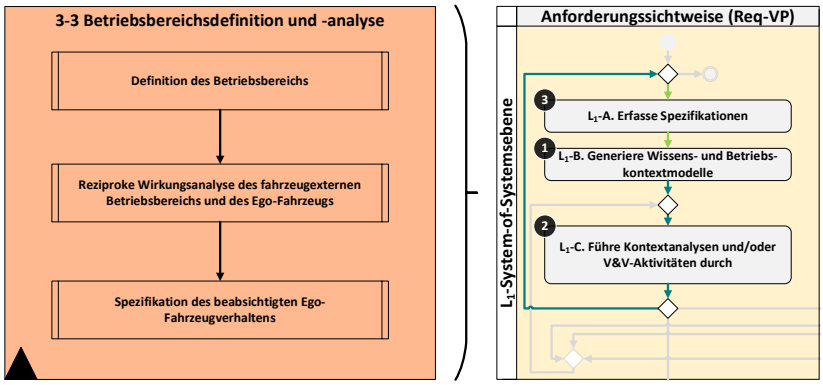


Abbildung 8.8: Durchzuführender Prozessabschnitt Teil 3-3 sowie zugehörige Aktivitäten innerhalb der L_1-Anforderungssichtweise.

Dies geht abermals anhand des zweiten Aktivitätsabschnitts „L_1-B. Generiere Wissens- und Betriebskontextmodelle“ vonstatten (siehe Schritt 1 Abbildung 8.8). Demzufolge wird angestrebt, mittels dem Arbeitsprodukt bzw. Inkrement WP-33 die Zielvorgaben 3-3.1 gemäß OpSa-ML1 zu erreichen. Dabei werden insbesondere die logischen Elemente bzw. Akteure „L_1-Ego-Kraftfahrzeug_L“, „L_1-Fahrer/Passagier_L“, „L_1-Verkehrsteilnehmer_L“, „L_1-FahrzeugexterneODDElemente_L“ in den Fokus gerückt. Auf Grundlage dessen werden die erfassten betrieblichen L_1-Kontextelemente sowie die innerhalb der Anwendungsfallartefakte abstrakt beschriebenen Interaktionspunkte für die Bereitstellung des Anwendungsfalls bzw. Features L1.1-UC „L_1-FolgeFahrstreifen…_UC“ konkretisiert. Hierbei erfolgt eine Erweiterung der logischen Kontextelemente, indem vornehmlich die „L_1-FahrzeugexternenODDElemente_L“ unter Anwendung der Betriebsbereichsontologie (vgl. Anhang B.3) anhand der Attribute „L_1-Zone_L“, „L_1-Fahrbahnbereich_L“, „L_1-Kreuzungen_L“, „L_1-Sonderstrukturen_L“ etc. detailliert wird.

Entlang der Dimensionen repräsentieren die dunkelgrau hervorgehobenen L_1-Attribute jeweils einen Bestandteil des definierten L_1-Betriebsbereichs. Im Gegensatz dazu sind die hellorangen L_1-Attribute aus der Definition ausgeschlossen und werden nicht näher betrachtet (siehe Tabelle 8.2). Infolgedessen wird eine Unterscheidung zwischen In-Scope und Out-of-Scope im Sinne der Spezifikation der Systemgrenzen sowie die Ableitung von primären Eigenschaften externer Schnittstellen und Randbedingungen vorgenommen. Somit wird hier einerseits die Entwurfsentscheidung L1.1-DECN getroffen, die logischen Kontextelemente „L_1-Zone_L“, „L_1-Fahrbahnbereich_L“, „L_1-Wetter_L“, „L_1-Fahrer/Passagier_L“, „L_1-Verkehrsteilnehmer_L“ sowie „L_1-Ego-Kraftfahrzeug_L“ als wesentliche Bestandteile des zu definierenden Betriebsbereichs (In-Scope) aufzunehmen. Andererseits werden die Kontextelemente „L_1-Kreuzungen_L“, „L_1-Sonderstrukturen_L“ usw. aus dem Betrachtungsrahmen ausgeschlossen (Out-of-Scope) (siehe Tabelle 8.2).

Diesbezüglich bezeichnet eine Dimension einen eindeutig abgegrenzten Kontext- oder Einflussfaktor, der als eigenständige Entscheidungsvariable im morphologischen Raum geführt wird. Die zugehörigen Alternativen repräsentieren die möglichen qualitativen Ausprägungen dieser Variable und können auch als feinere Unterdimensionen strukturiert werden, sofern sie logisch unterscheidbare Analyseaspekte derselben übergeordneten Dimension abbilden. Im Bereich der Attribute „L_1-Wetter_L“ sowie „L_1-Ausleuchtung_L“ werden ideale Witterungsbedingungen sowie Temperaturen über dem Gefrierpunkt bei Tageslicht als Annahme L1.1-ASMP dokumentiert. Hinzu kommen die Einschränkungen L1.3-CSTR und L1.4-CSTR, was den Ausschluss der Attribute „L_1-Kreuzungen_L“, „L_1-Sonderstrukturen_L“ usw. betrifft. Darunter fällt auch der Ausschluss der Betrachtung von Fußgängern, Wildtieren etc. innerhalb des Fahrbahnbereichs.

Tabelle 8.2: Zwicky-Box im Hinblick auf die Entwurfsentscheidung des definierten L_1-Betriebsbereichs.

<<Entwurfsentscheidung>>						
ID: L1.10000DECN						
L1.1-DECN L_1-Betriebsbereichsdefinition						
Dimension	Alternativen					
<<Szenerie>>	L_1-Zone_L	L_1-Fahrbahnbereich_L	L_1-Kreuzungen_L	L_1-Sonderstrukturen_L	L_1-BefestigteStraßenstrukturen_L	L_1-TemporäreStraßenstrukturen_L
<<Umgebungsbedingungen>>	L_1-Wetter_L	L_1-PartikelUnd-Feinstaub_L		L_1-Ausleuchtung_L	L_1-Konnektivität_L	
<<Dynamische Elemente>>	L_1-Ego-Kraftfahrzeug_L	L_1-Fahrer/Passagier_L		L_1-Verkehrsteilnehmer_L		

Außerdem sind spezielle Infrastrukturlösungen, wie z.B. der Zugriff auf V2X-Kommunikation, durch den Ausschluss des Elements „L_1-Konnektivität_L“ nicht Bestandteil des definierten Betriebsbereichs. Zudem wird im Hinblick auf Einschränkung L1.5-CSTR unter dem Kontextelement „L_1-Verkehrsteilnehmer_L“ insgesamt nur ein vorausfahrendes Kraftfahrzeug berücksichtigt. Darüber hinaus wird die Schnittstellenspezifikation gemäß der Mensch-Maschine-Interaktion sowie unter umgebungsbezogenen und fahrdynamischen Gesichtspunkten als Regelkreis spezifiziert. Unter Bezugnahme der vorangegangenen Aktivitäten wird der Betriebsbereich definiert und als logisches L_1-Betriebskontextdiagramm modelliert. Mit Hilfe der Modelle des logischen Betriebskontexts werden aus der Black-Box-Perspektive statisch strukturelle Wechselwirkungen sowie Schnittstellen des „L_1-Ego-Kraftfahrzeugs_L“ zu den damit in Interaktion stehenden L_1-Kontextelementen „L_1-Fahrbahnbereich_L, „L_1-Wetter_L“ etc. repräsentiert (siehe Abbildung 8.9).

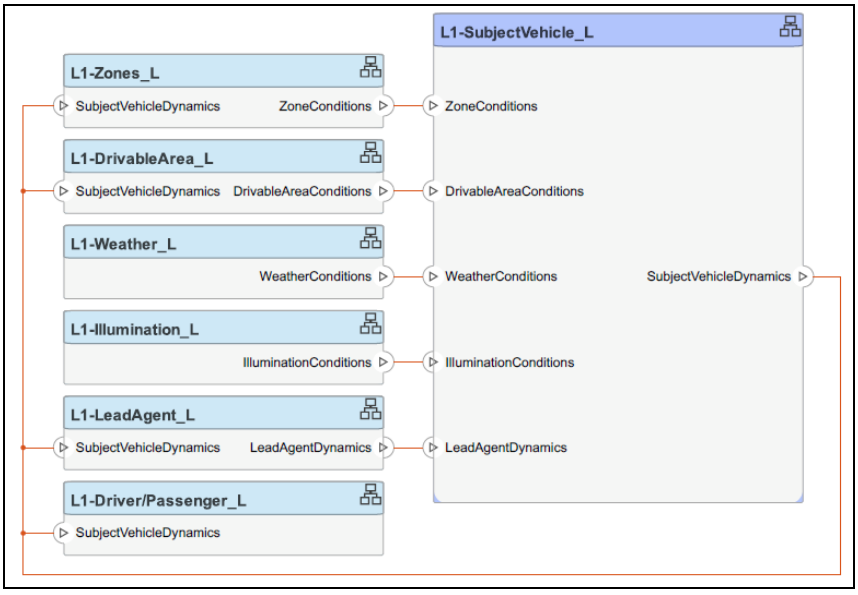


Abbildung 8.9: L_1-Betriebskontextdiagramm des definierten Betriebsbereichs, worin das „L_1-Ego-Kraftfahrzeug_L“ über rückgekoppelte Schleifen mit entsprechenden Attributen der „L_1-FahrzeugexternenODDElemente_L“ mittels Schnittstellen des Austauschs physikalischer Bedingungen (orange Konnektoren) verbunden ist.

Im weiteren Verlauf wird eine Betriebsbereichsanalyse unter dem Gesichtspunkt bzw. aus der Perspektive möglicher dynamischer Verhaltensmuster und Einflussgrößen der spezifizierten Betriebsbereichs- bzw. logischen L_1-Kontextelemente gemäß „L_1-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch“ vorgenommen (siehe Schritt 2 Abbildung 8.8). Insbesondere geht es darum, die dynamischen Interaktionen sowie die Verknüpfungen und Querbeziehungen zwischen dem hochautomatisierten „L_1-Ego-Kraftfahrzeug_L“ sowie den restlichen fahrzeugexternen Teil des Betriebsbereichs im Sinne statischer und dynamischer Objekte systematisch aufzuarbeiten. Genauer genommen handelt es sich um eine Betrachtung aus dem Blickwinkel des spezifischen Systembelangs im Hinblick auf das zu erwartende dynamische Verhalten. Darunter fallen im Speziellen die kinematischen Gesetze im Sinne der Bewegungsfreiheitsgrade (siehe Abbildung 8.10).

Andererseits wird der festgelegten Funktionsumfang sowie die Interessenvertreteranforderungen (siehe Tabelle C.3, Tabelle C.4 und Tabelle C.5) aus den anzuwendenden und einzuhaltenden Gesetzen bzw. Regularien herangezogen und in Bezug auf die möglichen dynamischen Verhaltensmuster analysiert. An dieser Stelle werden mit Blick auf „L_1-A Erfasse Spezifikationen“ die übergeordneten Wunschverhaltensweisen der Längsführungsmanöver „Freifahrt“, „Annähern“ und „Abstandshaltung“ als auch des Querführungsmanövers „Fahrstreifen Folgen“ konkretisiert (siehe Schritt 3 Abbildung 8.8). Hierbei wird mitunter die Einschränkung dahingehend vorgenommen, die Bewegungsfreiheitsgrade des „L_1-Ego-Kraftfahrzeugs_L“ als auch des „L_1-Verkehrsteilnehmers“ auf den dreidimensionalen Bereich zu begrenzen. Auf Grundlage dessen werden für die beiden Akteure jeweils ein fahrzeugfestes Koordinatensystem im Schwerpunkt gemäß der ISO 8855 sowie ein Koordinatensystem für den „L_1-Fahrbahnbereich_L“ als Bezugssystem eingeführt (siehe Abbildung 8.10).

Daraufhin wird das jeweilige Basisverhalten (Beschleunigen, Verzögern, Beibehaltung der Geschwindigkeit in Richtung der X-Achse, Lenken in Richtung der Y-Achse, Gieren um die Z-Achse als auch Stillstand wiederum im Hinblick auf die X_E-, Y_E- sowie Z_E-Achsen des Bezugssystems) zur Durchführung der im Fokus stehenden Fahrmanöver abgeleitet.

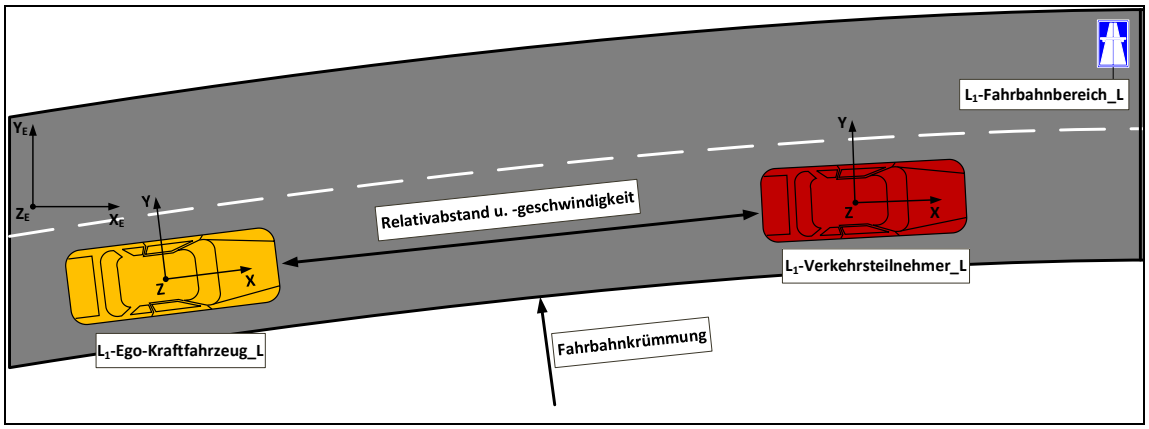


Abbildung 8.10: Betriebsbereichszentrierte Perspektive auf das Basisverhalten der Akteure „L_1-Ego-Kraftfahrzeug_L“ und „L_1-Verkehrsteilnehmer_L“ innerhalb des „L_1-Fahrbahnbereichs_L“ eines Autobahnabschnitts.

Insgesamt wird dabei das jeweils analytisch dynamische Verhalten gemäß Annahme L1.2-ASMP mittels der kinematischen Gesetzmäßigkeiten des Punktmassemodells

$$a_{X_E} = a_X \cos\psi - a_Y sin\psi - \dot{\psi}(v_X sin\psi - v_Y cos\psi)$$
$$a_{Y_E} = a_X sin\psi + a_Y cos\psi + \dot{\psi}(v_X cos\psi - v_Y sin\psi) \qquad 8.1$$

beschrieben (vgl. Gl. A.6 und Gl. A.7).

Außerdem wird der Betrachtungsumfang des längsdynamischen Grenzbereichs auf $a_{X,accel,max} = 2\ \frac{m}{s^2}$ bzw. $a_{X,decel,max} = -10\ \frac{m}{s^2}$ sowie des querdynamischen Grenzbereichs auf $a_{Y,max} = \pm 4\ \frac{m}{s^2}$ gemäß Einschränkung L1.6-CSTR limitiert. Dies gilt sowohl für das „L_1-Ego-Kraftfahrzeug_L“ als auch für das Element „L_1-Verkehrsteilnehmer_L“ und begründet darüber hinaus die zulässige bzw. physikalisch gesehen gerechtfertigte Einschränkung von deren Bewegungsfreiheitsgraden auf den dreidimensionalen Bereich [312]. Im Gegensatz zum „L_1-Ego-Kraftfahrzeug_L“ wird dem „L_1-Verkehrsteilnehmer_L“ das Durchführen von Fahrstreifenwechseln im Sinne des Einscherens (engl. *Cut-In*) in die Ego-Fahrspur sowie des Ausscherens (engl. *Cut-Out*) gestattet. Diese Verhaltensmerkmale liefern wiederum die notwendigen Aspekte, um die jeweils in Frage kommenden Basisszenarien zur Erfüllung des anfangs definierten Anwendungsfalls L1.1-UC „L_1-FolgeFahrstreifen…_UC“ abzuleiten (siehe Tabelle C.9, Tabelle C.10 und Tabelle C.11).

Unter Bezugnahme der vorangegangenen Schritte erfolgt einerseits die zustandsbasierte Modellierung des Basisverhaltens der Akteure „L_1-Ego-Kraftfahrzeug_L“ und „L_1-Verkehrsteilnehmer_L“. Hinsichtlich der Querführung wird dabei in Lenken bezüglich eines geradlinigen sowie eines gekrümmten Verlaufs des „L_1-Fahrbahnbereichs_L“ unterschieden (siehe Abbildung 8.11).

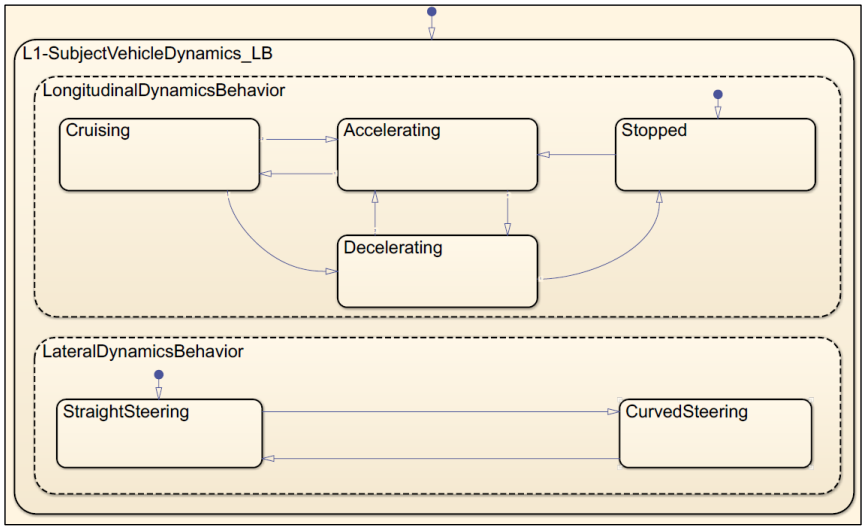


Abbildung 8.11: Zustandsautomat des Basisverhaltens des „L_1-Ego-Kraftfahrzeugs_L“ im Hinblick auf das parallel ablaufende dynamische Verhalten in Längs- und Querrichtung.

8.1.4 Betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung

Für Teil 3-4 „Betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung“ werden die im Verlauf der Systemverhaltens- und Betriebsbereichsbeschreibung abgeleiteten Situationen bzw. Basisszenarien herangezogen und gemäß „L_1-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch“ analytisch betrachtet (siehe Schritt 1 Abbildung 8.12). Genauer genommen werden vor dem Hintergrund der Zielvorgaben 3-4.1 potenzielle Gefährdungsereignisse und Risiken ermittelt, welche sich aus dem gefährdenden Verhalten des zu entwickelnden hochautomatisierten Autobahnpiloten respektive des „L_1-Ego-Kraftfahrzeugs_L“ ergeben können. Diese werden wiederum im Zuge von „L_1-A Erfasse Spezifikationen“ als OpSa-ML1 Arbeitsprodukte WP-34 und WP-10 dokumentiert (siehe Schritt 2 Abbildung 8.12).

In diesem Zusammenhang werden die Verhaltens- und Szenariomodelle unter dem Gesichtspunkt möglicher Gefährdungen und Gefährdungsereignisse betrachtet, wobei die systemische Sicherheitsanalysemethode STPA (vgl. Unterabschnitt 5.2.1) eingebunden wird. Dementsprechend geht es darum, gefährdende Verhaltensweisen und kritische Szenarien zu identifizieren. Hierbei werden mittels des ersten STPA-Schritts „Gegenstand der Analyse definieren“ sowie unter expliziter Berücksichtigung des logischen L_1-Betriebskontextmodells mögliche Verluste festgelegt. Im Anschluss daran werden im Hinblick auf den Anwendungsfall L1.1-UC „L_1-FolgeFahrstreifen…UC“ gefährdende Verhaltensweisen, welche insbesondere entlang der definierten Bewegungsfreiheitsgrade des „L_1-Ego-Kraftfahrzeugs_L“ auftreten können, abgeleitet. Hinzu kommt die Identifikation von Szenarien, die einerseits auslösende Bedingungen und andererseits Bedingungen umfassen, welche wiederum zu potenziellen Schäden führen können. Hierbei werden die identifizierten Verluste erfasst und dokumentiert (siehe Tabelle C.12).

Des Weiteren werden durch die Anwendung auf spezifische Betriebssituationen und/oder -szenarien die Gefährdungsereignisse im Hinblick auf die Betriebssicherheit ermittelt. Zunächst werden die Betriebssituationen anhand der Geschwindigkeit des „L_1-Ego-Kraftfahrzeugs_L“ als auch des „L_1-Verkehrsteilnehmers_L“ in fünf unterschiedlich große Äquivalenzklassen unterteilt. Diese Struktur erlaubt eine individuelle Zuordnung des ASIL, ohne dass die Einschätzung der Häufigkeit oder des Auftretens der Betriebssituationen unzulässig beeinträchtigt wird. Die Betriebssituationen werden überdies mittels der Attribute „L_1-Fahrbahnbereich_L“ und Verantwortung der Fahraufgabe charakterisiert.

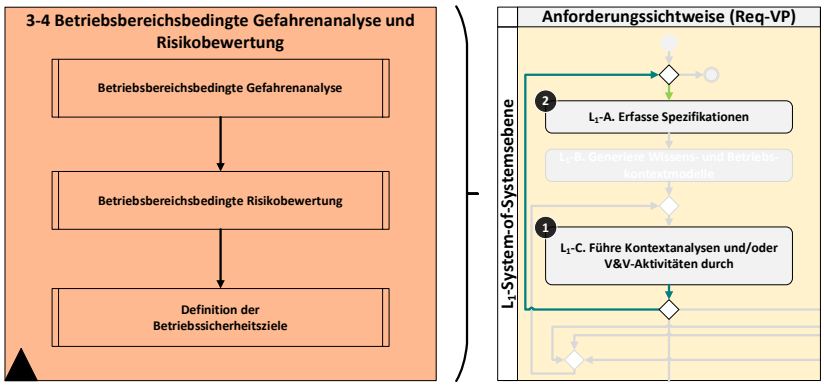


Abbildung 8.12: Durchzuführender Prozessabschnitt Teil 3-4 sowie zugehörige Aktivitäten innerhalb der L_1-Anforderungssichtweise.

Dadurch werden fünf spezifische Gefährdungsereignisse, entsprechend den jeweils zugehörigen gefährdenden Verhaltensweisen, innerhalb der definierten Geschwindigkeitsklassen berücksichtigt (siehe Tabelle C.13). Bei der Bewertung der Gefährdungsereignisse werden wiederum Annahmen getroffen. Da der menschliche Fahrer im Sinne des „L_1-Fahrers/Passagiers_L“ gemäß Randbedingung L1.1-BCOND nicht als Rückfallebene zur Verfügung steht, werden Situationen ohne fremde Beteiligung, z.B. Kollisionen mit der Randbebauung des „L_1-Fahrbahnbereichs_L“, als unkontrollierbar bzw. C3 eingestuft. Bei Kollisionen mit dem „L_1-Verkehrsteilnehmer_L“ wird die Kontrollierbarkeit abhängig vom Szenario und der Ego-Geschwindigkeit angesetzt. Bei höheren Geschwindigkeiten sinkt das Zeitfenster bis zu einer möglichen Kollision, so dass der Kontrollierbarkeitswert erhöht werden muss. Im Falle einer Frontkollision des „L_1-Ego-Kraftfahrzeugs_L“ mit dem „L_1-Verkehrsteilnehmer_L“ wird die Situation als schwer bzw. unkontrollierbar kategorisiert.

Auf deutschen Autobahnen wird der gesamte Geschwindigkeitsbereich von Stillstand bzw. Schrittgeschwindigkeit bei stockendem Verkehr bis zur maximalen Ego-Geschwindigkeit mit hoher Häufigkeit abgedeckt. Die Häufigkeit wird infolgedessen durchgängig mit E4 klassifiziert. Die Schwere der potenziellen Personenschäden wird nach [313] als auch unter Berücksichtigung einer statistischen Auswertung von Unfalldaten der Deutschen Studie zur vertieften Verkehrsunfalldatenerhebung GIDAS (German In-Depth Accident Study) aus dem Jahr 2019 für die darin enthaltenen Unfallkonfigurationen eingestuft. Darunter fallen Frontkollisionen, seitliche und schräge Kollisionen. Die Ergebnisse der Risikobewertung für die Gefährdungsereignisse werden dann nach Kollisionstyp und Geschwindigkeitsklasse gruppiert (siehe Tabelle C.13). Die ASILs der betrachteten Gefährdungsereignisse werden abschließend für jede gefährdende Verhaltensweise durch Auswahl des höchsten ASIL zusammengefasst (siehe Tabelle C.14).

Die Betriebssicherheitsziele resultieren aus der Invertierung der Gefährdungsereignisse im Sinne von deren Vermeidung gemäß „L_1-A Erfasse Spezifikationen“ (siehe Schritt 2 Abbildung 8.12). Für jedes Betriebssicherheitsziel wird zunächst der jeweils höchste ASIL aus den erfassten Geschwindigkeitsbereichen übernommen. Gefährdungsereignisse, welche seitliche Kollisionen mit Objekten am Straßenrand beschreiben, werden zusammengefasst, da die Wahrnehmung kleinerer Objekte anspruchsvoller ist und außerdem eine höhere ASIL-Einstufung gegeben ist. Ebenso werden Gefährdungsereignisse im Hinblick seitlicher Kollisionen mit dem „L_1-Verkehrsteilnehmer_L“ durch ein übergeordnetes Betriebssicherheitsziel abgedeckt (siehe Tabelle C.15).

Die Betriebssicherheitsziele lassen sich neben ihrer Gliederung nach Geschwindigkeitsbereichen bezüglich der Längsführung in zwei thematische Blöcke einteilen. Der erste Block beinhaltet die Einhaltung sicherer Abstände zu verschiedenen Objekten, insbesondere dem vorausfahrenden „L_1-Verkehrsteilnehmer_L“. Somit handelt es sich hierbei um gefährdende Verhaltensweisen, welche direkt vom „L_1-Ego-Kraftfahrzeug_L“ verursacht werden und auf den vorgesehenen Ego-Fahrstreifen beschränkt sind. Im zweiten Block wird der Fahrstreifen unbeabsichtigt verlassen, wobei zwischen einer Kollision mit dem „L_1-Verkehrsteilnehmer_L“ auf benachbarten Fahr- oder Standstreifen bzw. mit Objekten am Straßenrand unterschieden wird. Diesbezüglich ist der Frontsichtbereich des „L_1-Ego-Kraftfahrzeugs_L“ lediglich auf den Ego-Fahrstreifen im Sinne von Rechtfertigung L1.1-JSTF begrenzt. Darüber hinaus ist der definierte Betriebsbereich gemäß der Einschränkung L1.5-CSTR dahingehend spezifiziert, weitere Verkehrsteilnehmer hinter dem „L_1-Ego-Kraftfahrzeug“ nicht zu betrachten. Außerdem ist die Durchführung von Fahrstreifenwechseln, z.B. auf den Seitenstreifen, nicht Bestandteil des hier betrachteten Funktionsumfangs (siehe Tabelle C.1). Aufgrund dessen wird ein Stillstand auf dem aktuellen bzw. rechten Fahrstreifen als sicherer Zustand bzw. der Übergang dahin als Manöver minimalen Risikos gemäß Entwurfsentscheidung L1.2-DECN festgelegt.

8.1.5 Betriebssicherheitskonzept

Um die spezifizierten Betriebssicherheitsziele zu erfüllen, werden im Verlauf von Teil 3-5 „Betriebssicherheitskonzept“ Maßnahmen als OpSa-ML1 Inkrement bzw. Arbeitsprodukt WP-35 entwickelt. Im Kern geht es darum, unter Erfüllung der Zielvorgaben 3-5.1 inakzeptable Risiken in Richtung akzeptabler Risiken zu reduzieren. Dabei werden die Verhaltens- und Szenariomodelle sowohl unter dem Gesichtspunkt des beabsichtigten Basisverhaltens als auch der identifizierten Gefährdungsereignisse gemäß „L_1-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch“ dahingehend erfasst, eine gesetzeskonforme, proaktive, reaktive, aber auch möglichst unfallfreie Ego-Fahrzeugverhaltensspezifikation in Bezug auf „L_1-A Erfasse Spezifikationen“ abzuleiten (siehe Schritt 1 und 2 Abbildung 8.13).

In dieser Hinsicht wird SOCA (Scode for Open Context Analysis) als Kontextanalysemethode eingebunden (vgl. Anhang A.5) und in Bezug auf den Anwendungsfall L1.1-UC „L_1-FolgeFahrstreifenHochautomatisiertAufDerAutobahn_UC“ modifiziert. An erster Stelle erfolgt dabei das Hinzuziehen der logischen L_1-Betriebskontextmodelle und deren graphische Repräsentation mittels entsprechender Zonengraphen. Die Abstraktion der jeweiligen Situationen anhand von Zonen ist dabei der Schlüssel, um die Lücke zwischen der funktionalen Abstraktion (semantische Beschreibung) und der logischen Abstraktion (Parameterräume) zu schließen.

Des Weiteren wird die Ego-Fahrspur, sprich der räumliche „L_1-Fahrbahnbereich_L“ der Szenerie, den das „L_1-Ego-Kraftfahrzeug_L“ wiederum zu passieren beabsichtigt, als Fahrschlauch bzw. Fahrzone A_0 definiert. Diese Fahrzone erstreckt sich über den maximalen Frontsichtbereich des „L_1-Ego-Kraftfahrzeugs_L“, welcher seinerseits gemäß Rechtfertigung L1.1-JSTF auf den Ego-Fahrstreifen begrenzt ist. Darüber hinaus wird die Fahrzone mit der räumlichen Dynamik des „L_1-Ego-Kraftfahrzeugs_L“ verknüpft, wodurch sie sich mit jenem mitbewegt. Im Anschluss daran wird die Fahrzone A_0 in fünf Bereiche A_5 … A_1 unterschiedlicher Kritikalität separiert, wobei diese den Fahrschlauch repräsentieren (siehe Abbildung 8.14). Zusätzlich werden die Betriebssicherheitsziele in Bezug auf das präventive, regelkonforme und soweit wie praktikabel möglich unfallfreie Fahrverhalten im Sinne des Anwendungsfalls L1.1-UC „L_1-FolgeFahrstreifen…_UC“ und den darin definierten operativen Wunschverhaltensweisen „Freifahrt“, „Annähern“, „Abstandshaltung“ und „Fahrstreifen Folgen“ in Längs- und Querrichtung betrachtet.

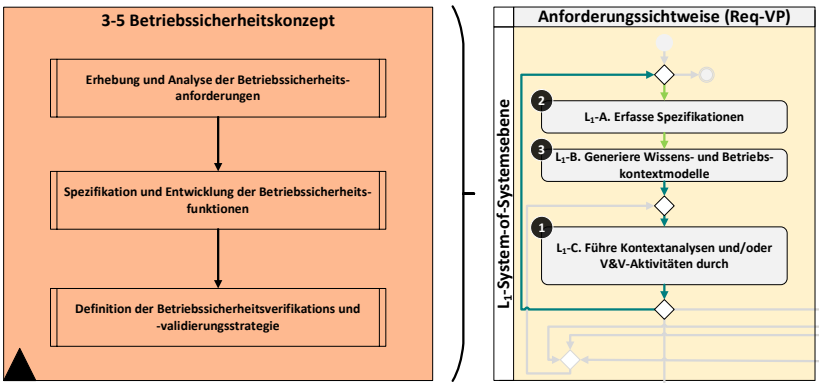


Abbildung 8.13: Durchzuführender Prozessabschnitt Teil 3-5 sowie zugehörige Aktivitäten innerhalb der L_1-Anforderungssichtweise.

Diese bilden die Grundlage für eine sichere Fahrzeugverhaltensspezifikation in Übereinstimmung mit den jeweils aus der StVO als auch den Verhaltensrichtlinien der UN-Regelung Nr. 157 erhobenen Betriebssicherheitsanforderungen (siehe Tabelle C.3, Tabelle C.4 und Tabelle C.5). Auf Basis des generierten Zonengraphen sowie der einzuhaltenden Verkehrsregeln der StVO respektive der Verhaltensrichtlinien der UN-Regelung Nr. 157 wird an dieser Stelle mittels einer Zwicky-Box ein Situations- und Entscheidungsraum für das „L_1-Ego-Kraftfahrzeug_L“ aufgespannt (siehe Tabelle 8.3).

An oberster Stelle wird der aktuelle Fahrmodus als Dimension erfasst. Diese kennzeichnet sich ihrerseits durch drei unterschiedliche Alternativen im Sinne der operativen Wunschverhaltensweisen „Freifahrt“, „Annähern“ und „Abstandshaltung“ in Längsrichtung. Die Wunschverhaltensweise „Fahrstreifen Folgen“ in Querrichtung äußert sich als übergeordneter Dauerzustand und wird deshalb nicht explizit aufgeführt. Als zweite Dimension wird die Ego-Längsgeschwindigkeit definiert, wobei diese sich durch drei unterschiedliche Alternativen charakterisiert. Hinzu kommen die Dimension der Relativgeschwindigkeit einschließlich vier Alternativen, die Dimension des Relativabstands im Hinblick auf die Fahrzone A_0 unter Berücksichtigung der fünf Bereiche bzw. Zonen A_5 … A_1 als Alternativen sowie die TTC (Time To Collision) einschließlich drei Alternativen (siehe Tabelle 8.3).

Das Resultat ist ein Situations- bzw. Entscheidungsraum mittels des kartesischen Produkts der Dimensionen bzw. deren Alternativen $P_K = D_1 \times \ldots \times D_n$, was zu $3 \cdot 3 \cdot 4 \cdot 6 \cdot 3 = 648$ möglichen Zuständen führt. In Abhängigkeit der Kombinatorik im Hinblick auf die Positionierung des „L_1-Verkehrsteilnehmers_L“ innerhalb der jeweiligen Zonen, der Relativgeschwindigkeit sowie der Ego-Längsgeschwindigkeit wird vom hochautomatisierten „L_1-Ego-Kraftfahrzeug_L“ eine adäquate Reaktion erwartet. Das Ganze muss wiederum unter Einhaltung der jeweils geltenden Verkehrsregeln, des Ego-Fahrzeugzustands sowie physikalischer Randbedingungen des „L_1-Fahrbahnbereichs_L“ vonstattengehen. Hierfür werden Basiszustände bzw. Verhaltensmodi für das „L_1-Ego-Kraftfahrzeug_L“ definiert. Dementsprechend wird das Basisverhalten entlang der Bewegungsfreiheitsgrade herangezogen und hinsichtlich des Zustands „Verzögerung“ (engl. *Decelerating*) mittels weiterer unterscheidbarer Zustände „Segeln“ (engl. *Coasting*), „Komfortables Abbremsen“ (engl. *Comfort Braking*), „Hartes Abbremsen“ (engl. *Hard Braking*) und „Notfallabbremsung“ (engl. *Emergency Braking*) verfeinert. Dadurch entstehen insgesamt acht disjunkte Verhaltensäquivalenzklassen. Diese werden wiederum dazu verwendet, um die jeweiligen Zonen A_5 … A_1 anhand von „A_5-EmergencyBrakingZone“, „A_4-HardBrakingZone“ etc. zu bezeichnen (siehe Tabelle C.17).

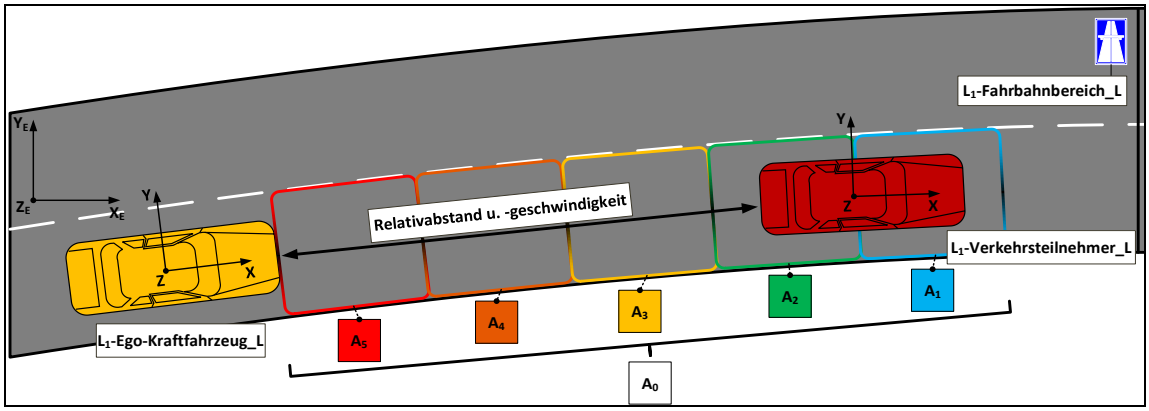


Abbildung 8.14: L_1-Betriebskontextmodell und dessen graphische Repräsentation mittels eines Zonengraphen.

Tabelle 8.3: Zwicky-Box in Bezug auf den Entscheidungsraum der Fahrzeugverhaltensspezifikation des hochautomatisierten L_1-Ego-Kraftfahrzeugs unter Hervorhebung (dunkelgrau) und Ausschluss (hellorange) der jeweiligen Alternativen gemäß L1.1-OpSaReq Verhaltensregel 1.

<<Entwurfsentscheidung>>						
ID: L1.30000DECN						
L1.3-DECN Entscheidungsraum der Fahrzeugverhaltensspezifikation des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“						
Dimension	Alternativen					
Ego-Kraftfahrzeug Modus	Abstandshaltung		Annähern		Freifahrt	
Fahrzone	A_5	A_4	A_3	A_2	A_1	A_0
Ego-Längsgeschwindigkeit $[\frac{m}{s}]$	$v_{sub} == 0$		$0 < v_{sub} < v_{sub,max}$		$v_{sub} = v_{sub,max}$	
Relativgeschwindigkeit $[\frac{m}{s}]$	$v_{rel} < 0$		$v_{rel} == 0$	$v_{rel} > 0$	Nichtzutreffend	
Time To Collision $[s]$	$TTC \leq TTC_{min}$		$TTC > TTC_{min}$		Nichtzutreffend	
Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>						
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>						
ID: L1.10000OpSaReq						
L1.1-OpSaReq Verhaltensregel 1 im Hinblick auf die Durchführung einer Notfallabbremsung (Modus 1)						
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A5$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = ($TTC \leq TTC_{min}$ ODER $TTC > TTC_{min}$)						
ASIL D						

Für die situationsbedingten Verhaltensweisen werden nun systematisch nachvollziehbare und rückverfolgbare „Wenn-dann-Regeln“ definiert (siehe Tabelle C.18, Tabelle C.19, Tabelle C.20, Tabelle C.21, Tabelle C.22, Tabelle C.23 und Tabelle C.24). Das Ganze erfolgt unter expliziter Einbindung der Längshomöstase der menschlichen Fahrzeugführung (vgl. Unterabschnitt 2.1.2). Der Kern dieser morphologischen Analyse besteht darin, den sich ergebenden kombinatorischen Situations- bzw. Entscheidungsraum systematisch in Äquivalenzklassen von Verhaltensweisen zu dekomponieren. Diese Äquivalenzklassen liefern in Kombination mit dem Zonengraphen einen Satz konsistenter, kontextabhängiger Verhaltensanforderungen bzw. -regeln auf L_1-System-Of-Systemsebene. Insbesondere geht es darum, wie das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ auf die jeweilige Situation („Wenn“) zu reagieren hat („dann“).

Die jeweiligen Fälle werden mit Hilfe der Denkweise eines Spiels zweier Akteure sozusagen verknüpft: „Wenn der „L_1-Verkehrsteilnehmer_L“ diese oder jene Handlungsweise durchführt (z.B. Einfädeln mit einer negativen Relativgeschwindigkeit in Zone A_4 sowie einer unterschrittenen TTC_{min}), dann muss das „L_1-Ego-Kraftfahrzeug_L“ seinerseits mit einer positiven Ego-Geschwindigkeit jenes tun (z.B. Notfallabbremsung), was wiederum die geforderte Betriebssicherheit gewährleistet" (siehe Tabelle 8.3). Eine gegebene Verkehrssituation wird aus der Perspektive des „L_1-Ego-Kraftfahrzeugs_L“ analysiert. Das Ganze basiert auf der Konfiguration der Szenerie, der dynamischen Elemente, dem Anfangszustand und der Absicht

des „L_1-Ego-Kraftfahrzeugs_L“ selbst. Die durchzuführenden Handlungen gründen wiederum auf den erhobenen Betriebssicherheitsanforderungen gemäß der StVO sowie der UN-Regelung Nr. 157 (siehe Tabelle C.3, Tabelle C.4 und Tabelle C.5). Generell ist die am wenigsten einschränkende Verhaltensmaßnahme im Sinne der Verzögerungsintensität zu ergreifen, welche ihrerseits noch in der Lage ist, den notwendigen Grad an Betriebssicherheit aufrecht zu erhalten.

Demnach wird bei Unterschreitung der minimal erforderlichen TTC unabhängig von der jeweiligen Fahrzone A_5 … A_1 ein Notfallbremsmanöver durchgeführt (siehe Tabelle C.18). Andererseits werden bei einer höheren TTC die jeweils weniger vehementen fahrzonenbasierten Verzögerungsmanöver ausgeführt. Alles in allem setzt dieses Vorgehen somit Annahmen und Einschränkungen über das Fahrverhalten des „L_1-Verkehrsteilnehmers_L“, den Zustand des „L_1-Ego-Kraftfahrzeugs_L“ sowie den „L_1-Fahrbahnbereich_L“ voraus, wobei unterschiedliche Annahmen zu unterschiedlichen Entscheidungen in derselben Situation führen können. Dabei kann ein sorgfältiges Gleichgewicht zwischen Vorsicht, Sicherheitserwägungen und natürlichem Fahrverhalten hergestellt werden. In dieser Hinsicht kann der Relativabstand auf der Grundlage von Annahmen über das vernünftigerweise vorhersehbare Verhalten des „L_1-Verkehrsteilnehmers_L“ angepasst werden, wobei nicht notwendigerweise die theoretischen Fähigkeiten des Worst-Case-Szenarios zu jeder Zeit berücksichtigt werden müssen. Ein solches Gleichgewicht ist für die Effizienz und Betriebssicherheit erforderlich, ohne den Verkehrsfluss unnötig einzuschränken (z.B. Fahrer, die sich unter allen Umständen an den ungünstigsten Abstandsregelungen orientieren).

Infolgedessen wird an dieser Stelle wiederum die Annahme L1.3-ASMP dahingehend getroffen, dass der „L_1-Verkehrsteilnehmer_L“ keine unzulässigen bzw. vernünftigerweise unvorhersehbar starken Bremsmanöver durchführt. Ist dies nicht der Fall, so kann eine Kollision ohne ein Notfallausweichmanöver auf eine benachbarte Fahrspur oder ggf. den Standstreifen unter Umständen nicht mehr verhindert werden. Zudem besteht die Einschränkung gemäß Rechtfertigung L1.1-JSTF dahingehend, dass der Frontsichtbereich des „L_1-Ego-Kraftfahrzeugs_L“ auf den Ego-Fahrstreifen begrenzt ist und dieses erst beim Einfädeln des „L_1-Verkehrsteilnehmers_L“ auf diesen reagieren kann. Weitere Einschränkungen und Annahmen betreffen den Ausschluss von Steigungen bzw. Gefälle des „L_1-Fahrbahnbereichs_L“ gemäß Einschränkung L1.3-CSTR, die Bekanntheit aller relevanten statischen Parameter der Szenerie, des Bewegungsmodells einschließlich einer perfekten Wahrnehmung des „L_1-Verkehrsteilnehmers_L“ sowie die Fehlerfreiheit des gesamten operativen Systemzustands des „L_1-Ego-Kraftfahrzeugs_L“ hinsichtlich der Annahme L1.4-ASMP.

Zu späteren Entwicklungszeitpunkten können diese idealisierten Annahmen gelockert werden, um weitere Bereiche des möglichen Ego-Kraftfahrzeugverhaltens abzudecken. Unter Berücksichtigung dieser Annahmen und Einschränkungen werden die jeweiligen Verhaltensregeln bzw. -anforderungen für das „L_1-Ego-Kraftfahrzeug_L“ abgeleitet. Hinzu kommt die Herleitung der Bedingungen der jeweiligen Zustandsübergänge mit Hilfe einer sogenannten Modusübergangsmatrix (engl. *Mode Transition Matrix*) (siehe Tabelle C.26 und Tabelle C.27).

Aufgrund der Dimension des Situationsraums mit insgesamt 648 möglichen Kombinationen können bereits Herausforderungen der vollständigen Spezifikationsabdeckung aller Zustände auftreten. Hierbei werden mögliche Kombinationen automatisiert durch die SCODE-ANALYZER Toolbox [314] als solche kenntlich gemacht. Damit können diese den jeweiligen Verhaltensregeln und Modi im weiteren Verlauf der Analyse durch die jeweiligen Experten zugewiesen werden, wobei formal existierende Kombinationen, die allerdings in der Realität nicht vorkommen können, als Nicht-System-Modi ausgeschlossen werden (siehe Tabelle C.28). Zwar kann damit die Problematik der Unendlichkeit des offenen Kontexts im Hinblick auf dessen vollständige Erfassung nicht gelöst werden (vgl. HF-1 und HF-2), jedoch ermöglicht

dieses Vorgehen eine nachweisbare mathematische Vollständigkeitsargumentation des aufgezogenen Situations- bzw. Entscheidungsraums.

Die Analyse ist vollständig, wenn der gesamte Entscheidungsraum durch die Äquivalenzklassen abgedeckt ist und diese konsistent sind, d.h. keine Überschneidungen aufweisen. Etwas formaler ausgedrückt, bedeutet Vollständigkeit, dass jede Kombination, die im Entscheidungsraum existiert, mindestens einer Äquivalenzklasse hinzugefügt wurde. Konsistenz bedeutet, dass jede Kombination aus dem Entscheidungsraum zu höchstens einer Äquivalenzklasse hinzugefügt wurde. Dadurch wird die Thematik der Vollständigkeit dahingehend verschoben, anhand des aufzuspannenden Entscheidungsraums den möglichst relevanten bzw. aussagekräftigen Anteil des tatsächlichen Situationsraums innerhalb eines realen Betriebsbereichs abzudecken. Folglich bietet SOCA eine relative Vollständigkeitsgarantie in dem Sinne, dass es die Vollständigkeit der abgeleiteten Äquivalenzklassen unter der Annahme garantiert, dass der identifizierte Entscheidungsraum vollständig ist.

Ein weiterer Vorteil dieses Ansatzes ist die Erweiterbarkeit des Analysegegenstands. Der SOCA-Formalisierungsansatz verwendet partielle Situationsmodelle, die sich ihrerseits zu einem Gesamtsituationsmodell zusammensetzen lassen. Diese Teilmodelle umfassen Bewegungsmodelle für das „L_1-Ego-Kraftfahrzeug_L“, Bewegungsmodelle für den „L_1-Verkehrsteilnehmer_L“, strukturelle Klassen anhand der Zonengraphen für die Szenerie sowie analysierte Äquivalenzklassen, die festlegen, welches Verhalten in einer spezifischen Situation erlaubt ist und welches nicht. So könnten die Zwicky-Boxen inkrementell und modular hinsichtlich weiterer Anwendungsfälle und damit Fahrstreifen, Verkehrsteilnehmer etc. als auch Ego-Manöver wie Spurwechsel, Ausweichmanöver usw. ergänzt und kombiniert werden.

Auf Grundlage der UN-Regelung Nr. 157 sowie den kinematischen Gesetzen im Hinblick auf die Punktmassendynamik werden nun die KPIs für quantifizierbare und damit validierbare Fahrverhaltensmuster der Einhaltung der oben definierten Verhaltensregeln gemäß „L_1-B Generiere Wissens- und Betriebskontextmodelle“ abgeleitet (siehe Schritt 3 Abbildung 8.13). Darunter fällt an erster Stelle die Festlegung der Gesamtfahrzeugreaktionszeit t_{react} auf Objekte und Ereignisse als nichtfunktionale Anforderung L1.19-OpSaReq (siehe Tabelle 8.4).

Tabelle 8.4: Gesamtfahrzeugreaktionszeit auf Objekte und Ereignisse.

Übergeordneter Anforderungstyp: <<Nichtfunktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.190000OpSaReq
L1.19-OpSaReq Gesamtfahrzeugreaktionszeit auf Objekte und Ereignisse innerhalb des definierten Betriebsbereichs
Die Gesamtreaktionszeit des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“ im Sinne der Objekt- und Ereigniserkennung als auch die Ausführung der Reaktion darauf (engl. Object and Event Detection Reaction {OEDR}) soll $0.8\ s$ $(800\ ms)$ *nicht überschreiten.*
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D

Diese orientiert sich an der menschlichen Wahrnehmungs- und Handlungsreaktionszeit von ca. $600\ ms$ zuzüglich der Übertragungszeiten der Aktuatoren von ca. $200\ ms$ (vgl. Unterabschnitt 2.1.2). Darüber hinaus werden Abstands- und Geschwindigkeitskorridore gemäß den Fahrzonen A_5 … A_1 deduziert. Zunächst wird der mathematische Zusammenhang der Relativgeschwindigkeit

$$v_{rel} = v_{lead} - v_{sub} \tag{8.2}$$

herangezogen, wobei sich diese zunächst aus der Differenz der Geschwindigkeit des „L_1-Verkehrsteilnehmers_L“ und der Ego-Geschwindigkeit des „L_1-Ego-Kraftfahrzeugs_L“ ergibt.

Die

$$TTC = \frac{d_{rel}}{v_{rel}} \tag{8.3}$$

wird gemäß der UN-Regelung Nr. 157 [309] berechnet.

Auf Basis der Relativgeschwindigkeit v_{rel} wird dann eine Fallunterscheidung für die Berechnung der jeweiligen Fahrzonen A_5 … A_1 vorgenommen. Ist die Relativgeschwindigkeit v_{rel} größer als $-1\frac{m}{s}$, so berechnet sich die Distanz der Zonen A_n in Abhängigkeit der Geschwindigkeit v_{lead} des „L_1-Verkehrsteilnehmers_L“ sowie einer zonenabhängigen Zeitkonstante t_n, welche aus der UN-Regelung Nr. 157 übernommen (siehe Tabelle C.29) und über die Zonen skaliert wird (siehe Tabelle C.17).

Ist die Relativgeschwindigkeit v_{rel} kleiner als $-1\frac{m}{s}$, so berechnet sich die Distanz der Zonen A_n in Abhängigkeit der Ego-Reaktionszeit t_{react} gemäß Betriebssicherheitsanforderung L1.19-OpSaReq und der Ego-Geschwindigkeit v_{sub}, sowie der Relativgeschwindigkeit v_{rel} und einer zonenabhängigen Maximalverzögerung $a_{X,decel,n}$ (siehe Tabelle C.17), als auch eines minimalen Sollabstands $d^*_{rel,min}$ im Falle der Abbremsung in den Stillstand:

$$\begin{gathered} if\ (v_{rel} > -1\tfrac{m}{s}) \\ A_n = t_n \cdot v_{lead} \\ else\ if\ (v_{rel} < -1\tfrac{m}{s}) \\ A_n = v_{sub} \cdot t_{react} + \frac{v_{rel}^2}{2 \cdot a_{X,decel,n}} + d^*_{rel,min} \end{gathered} \tag{8.4}$$

Zusätzlich wird die Beschleunigung $a_{X,accel}$ sowie die zonenabhängige Maximalverzögerung in Längsrichtung $a_{X,decel,n}$ im Hinblick auf die kombinierte Längs- und Querführung gemäß Annahme L1.5-ASMP limitiert. Dies erfolgt unter Berücksichtigung der absoluten Maxima der Beschleunigungs- bzw. Verzögerungsgrenzwerte $a_{X,accel,decel,max}$ gemäß L1.6-CSTR sowie der Gesetzmäßigkeiten der jeweils maximal zu erreichenden Reifenlängs- bzw. Reifenquerkraft

$$\begin{aligned} F_{XT,max} &= \sqrt{(\mu^2 \cdot F_{ZT}^2) - F_{YT}^2} \\ F_{YT,max} &= \sqrt{(\mu^2 \cdot F_{ZT}^2) - F_{XT}^2} \end{aligned} \tag{8.5}$$

in Abhängigkeit der Radaufstandskraft F_{ZT} als auch des vorliegenden Reibkoeffizienten μ (vgl. Gl. A.24).

Das Ganze ist notwendig, um ein ausreichendes Kraftschlusspotenzial

$$\left|a_{X,accel,decel,n}\right| \leq \sqrt{\frac{\left(\mu^2 \cdot m^2 \cdot {a_{X,accel,decel,max}}^2\right) - \left(m^2 \cdot a_{Y,nec}^2\right)}{m^2}} \qquad 8.6$$

$$\left|a_{Y,nec}\right| = v_X^2 \cdot \kappa^*$$

in Querrichtung gewährleisten zu können. Hierbei repräsentiert $a_{Y,nec}$ die benötigte Querbeschleunigung und

$$\dot{\psi}_{nec} = v_X \cdot \kappa^* \qquad 8.7$$

die notwendige Gier bzw. Kurswinkelrate, um das „L_1-Ego-Kraftfahrzeug_L“ bei einer vorliegenden Längsgeschwindigkeit v_X innerhalb des gekrümmten Sollbahnverlaufs κ^* halten zu können.

Für die Beschreibung der Ego-Kraftfahrzeugdynamik wird auf den physikalischen Zusammenhang der Punktemassemodelle inkl. der Bahnfolge im ortsfesten Koordinatensystem zurückgegriffen (vgl. Anhang A.4). Hierfür werden die oben hergeleiteten Sollgrößen $a_{X,decel,n}$ und $\dot{\psi}_{nec}$ direkt eingesetzt. Hinzu kommen der Beschleunigungswunsch $a_{X,accel}$ in Längsrichtung, sowie die Wind- und Reibungswiderstandskräfte F_{WX} und F_{RX}.

Für die Bewegung in X_E-Koordinaten ergibt sich durch Einsetzen von Gl. 8.6 und Gl. 8.7 in Gl. 8.1

$$a_{X_E} = \underbrace{\left(a_{X,accel} + a_{X,decel,n} - \frac{1}{m}\left(F_{WX} + F_{RX}\right)\right)}_{a_X} \cos\psi \qquad 8.8$$

$$- \underbrace{a_{Y,nec}}_{a_Y} sin\psi \underbrace{-\dot{\psi}_{nec}}_{\dot{\psi}} \left(v_X sin\psi - v_Y cos\psi\right)$$

als Zusammenhang. Die Querdynamik in globalen Y_E-Koordinaten wird durch Einsetzen von Gl. 8.6 und Gl. 8.7 in Gl. 8.1

$$a_{Y_E} = \underbrace{\left(a_{X,accel} + a_{X,decel,n} - \frac{1}{m}\left(F_{WX} + F_{RX}\right)\right)}_{a_X} sin\psi + \underbrace{a_{Y,nec}}_{a_Y} cos\psi \qquad 8.9$$

$$+ \underbrace{\dot{\psi}_{nec}}_{\dot{\psi}} \left(v_X cos\psi - v_Y sin\psi\right)$$

erfasst. Für die Drehung um die Z_E-Achse gilt durch Einsetzen von Gl. 8.7

$$\dot{\psi} = \dot{\psi}_{nec} \qquad 8.10$$

als Abbildung der Kurswinkelrate. Die jeweiligen Geschwindigkeiten v_X und v_Y sowie der Kurs- bzw. Gierwinkel ψ ergeben sich durch Integration der Beschleunigungen $a_{X,accel}$ bzw. $a_{X,decel,n}$ sowie $a_{Y,nec}$ und $\dot{\psi}_{nec}$.

Um die Querführung innerhalb der Ego-Fahrspur bewerten zu können, erfolgt die Erfassung der Querabweichung mittels

$$\dot{s}_{Ye} = v_X \cdot sin\psi_e \tag{8.11}$$

und die Abbildung der Kurswinkelabweichung

$$\dot{\psi}_e = \dot{\psi} - v_X \frac{cos\psi_e}{1 - s_Y \kappa^*} \kappa^* \tag{8.12}$$

gemäß der Krümmung κ^* der Sollbahn.

Unter Bezugnahme der vorangegangenen Schritte erfolgt die Ergänzung der zustandsbasierten Modellierung des Basisverhaltens des „L_1-Ego-Kraftfahrzeugs_L“. Dieses wird einerseits um die zusätzlichen Zustände „Segeln“ (engl. *Coasting*), „Komfortables Abbremsen“ (engl. *Comfort Braking*), „Hartes Abbremsen“ (engl. *Hard Braking*) und „Notfallabbremsung“ (engl. *Emergency Braking*) erweitert. Andererseits werden die Transitionen bzw. Zustandsübergänge einschließlich der jeweiligen Verhaltensregeln (siehe Tabelle C.27) im Sinne von Bedingungen und Events mittels der im Zuge der SOCA-Methode generierten Modusübergangsmatrix (siehe Tabelle C.26) spezifiziert (siehe Abbildung 8.15).

Auf Grundlage der spezifizierten Verhaltensmuster und Einflussgrößen des „L_1-Ego-Kraftfahrzeugs_L“ werden dann dessen notwendige Fähigkeiten zur Umsetzung des Wunschverhaltens abgeleitet. Im Hinblick darauf werden einerseits den betrachteten Verhaltensweisen „Freifahrt“ unter Einhaltung der Geschwindigkeitsbegrenzung, „Annähern“ an den „L_1-Verkehrsteilnehmer_L“, „Abstandshaltung“ zum „L_1-Verkehrsteilnehmer_L“ sowie „Fahrstreifen Folgen“ die Black-Box-Funktion bzw. Betriebssicherheitsfunktion „L_1-FahreHochautomatisiert_F“ zugeordnet. Andererseits werden die abgeleiteten Anforderungen aus der StVO sowie der UN-Regelung Nr. 157 (siehe Tabelle C.3, Tabelle C.4 und Tabelle C.5) sowie die spezifizierten Betriebssicherheitsziele (siehe Tabelle C.15) erfasst.

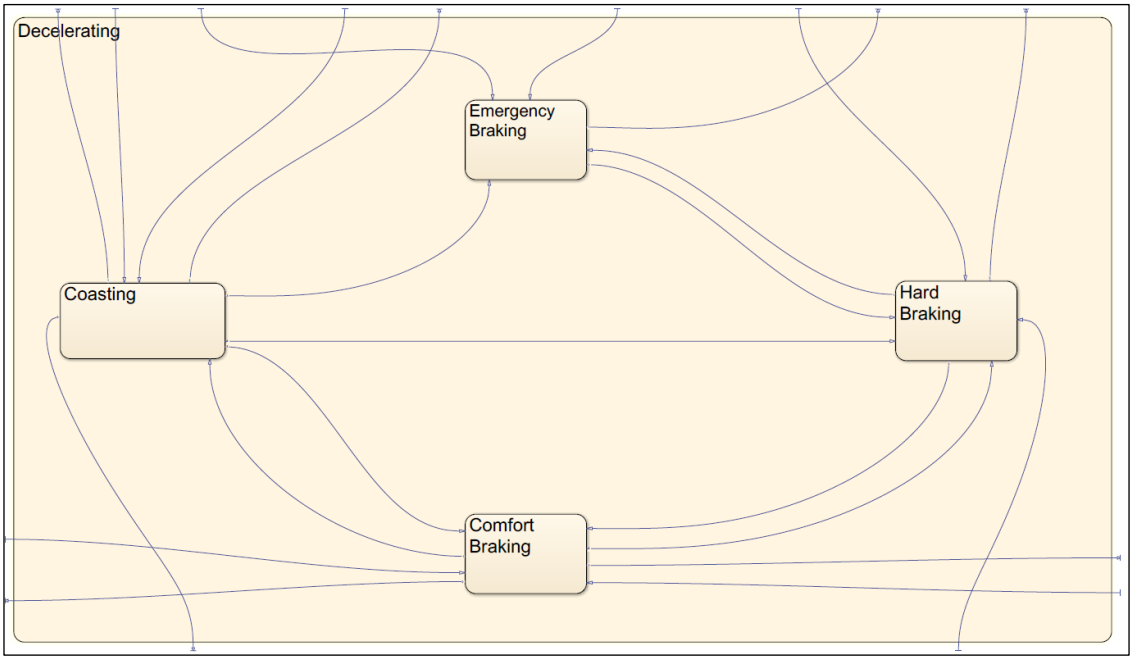


Abbildung 8.15: Erweiterung des Zustandsautomaten (siehe Abbildung 8.11) des Basisverhaltens des „L_1-Ego-Kraftfahrzeugs_L“ im Hinblick auf den übergeordneten Zustand „Verzögerung“.

Für die Planung, Umsetzung und Überwachung einer gesetzeskonformen, proaktiven, reaktiven, aber auch unfallfreien (so weit wie praktikabel möglich) Fahrzeugverhaltensspezifikation werden gemäß den L_1-Anforderungen (siehe Tabelle C.18, Tabelle C.19, Tabelle C.20, Tabelle C.21, Tabelle C.22, Tabelle C.23 und Tabelle C.24) die jeweils benötigten L_1-Fähigkeiten (siehe Tabelle C.30) definiert. Ferner beziehen sich die Fahrzeugfähigkeiten darauf, die jeweiligen L_1-Betriebssicherheitsziele (siehe Tabelle C.15) zu erfüllen bzw. zu konkretisieren, wodurch wiederum die ASIL-Klassifikationen weitervererbt bzw. übernommen werden. Zum Abschluss wird unter Berücksichtigung der vorangegangenen Aktivitäten die Betriebssicherheitsfunktion „L_1-FahreHochautomatisiert_F“ als funktionales Black-Box-Modell gemäß „L_1-B Generiere Wissens- und Betriebskontextmodelle“ repräsentiert (siehe Schritt 3 Abbildung 8.13). Diese Black-Box-Funktion beschreibt den für den vorliegenden Anwendungsfall Hauptzweck des „L_1-Ego-Kraftfahrzeugs_L“, welcher innerhalb des definierten Betriebsbereichs erfüllt werden soll. Dabei werden die aus dem logischen L_1-Betriebskontextmodell abgeleiteten Systemgrenzen der Black-Box-Funktion „L_1-FahreHochautomatisiert_F“ als syntaktische Schnittstellen definiert, welche ihrerseits über Ein- und Ausgänge physikalische Bedingungen des Fahrbahnbereichs, Witterungsverhältnisse, die Dynamik des vorausfahrenden „L_1-Verkehrsteilnehmers_L“ etc. unter Berücksichtigung des funktionalen Zusammenhangs austauschen. Hinzu kommt die funktionale Black-Box-Beschreibung „L_1-StelleBetriebsbereichsbedingungenBereit_F“ im Hinblick auf den „L_1-Fahrer/Passagier_L“, den „L_1-Fahrbahnbereich_L“, der idealen Umgebungsbedingungen als auch den vorausfahrenden „L_1-Verkehrsteilnehmer_L“ des definierten Betriebsbereichs. Die jeweiligen Funktionen abstrahieren die Verhaltensmodelle der Betriebsbereichsdefinition, wobei diese in Übereinstimmung mit dem logischen L_1-Betriebskontextmodell (siehe Abbildung 8.9) als geschlossener Regelkreis angeordnet werden (siehe Abbildung 8.16).

Anschließend wird der generierte Situationsraum einschließlich der definierten Äquivalenzklassen des jeweils beabsichtigten Verhaltens im Hinblick auf die Ableitung von Szenarien und Testfällen unter erneuter Durchführung von „L_1-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch“ betrachtet (siehe Schritt 1 Abbildung 8.13). Die Zielsetzung liegt darin, eine zunächst simulationsbasierte Verifikations- und Validierungsstrategie einschließlich der Validierungsziele, Erfüllungskriterien und Metriken gemäß „L_1-A Erfasse Spezifikationen“ zu definieren (siehe Schritt 2 Abbildung 8.13). Die Randbedingungen des im Fokus stehenden Anwendungsfalls L1.1-UC als auch der definierte Betriebsbereich kennzeichnen sich als wesentliche Einflussgrößen des Ego-Kraftfahrzeugverhaltens in Längs- und Querrichtung (siehe Tabelle 8.2).

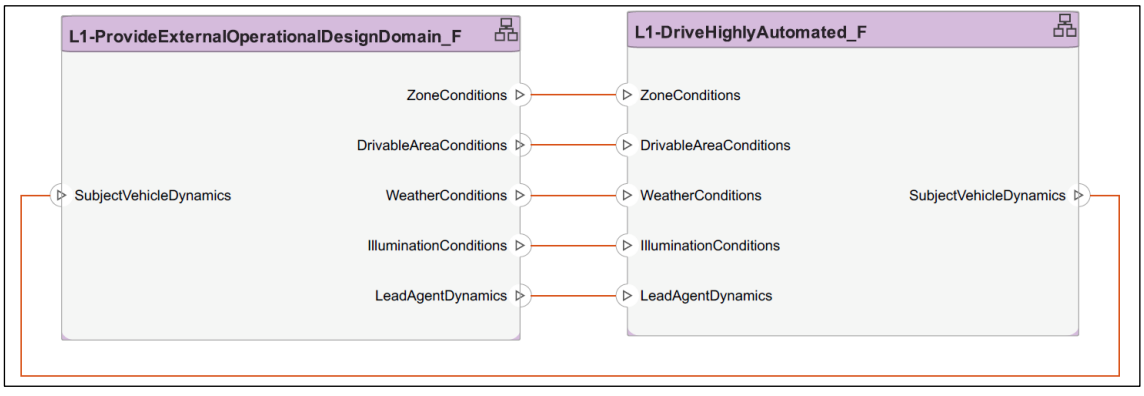


Abbildung 8.16: L_1-Black-Box-Modell, worin die Funktion „L_1-FahreHochautomatisiert_F“ die Schnittstellen des „L_1-Ego-Kraftfahrzeugs_L“ übernimmt und mit der Black-Box-Funktion „L_1-StelleFahrzeugexterne…F“ im Sinne eines geschlossenen Regelkreises interagiert.

Hierbei werden die im Zuge der vorangegangenen Schritte betrachteten Betriebssituationen durch eine zeitliche Abfolge von aufeinanderfolgenden Szenen in Richtung von funktionalen Szenarien bzw. Testfällen ausgeweitet (siehe Tabelle C.31, Tabelle C.32, Tabelle C.33 und Tabelle C.34). Dabei werden Kriterien für die Auswahl verwendet, um z.B. die identifizierten Lücken zwischen funktionalen Betriebssituationen und Verhaltensänderungen zu berücksichtigen. Infolgedessen charakterisieren sich die erfassten Betriebssituationen, die spezifizierten Betriebssicherheitsziele sowie die Anforderungen an die durchzuführende Fahrzeugverhaltensüberprüfung der UN-Regelung Nr. 157 als Grundlage für die Generierung von szenariobasierten Testfällen. Die jeweiligen Sequenzen werden mit unterschiedlichen Modi („Geschwindigkeitsbeibehaltung", „Verzögerung", „Beschleunigung" etc.) und prognostizierten Trajektorien des „L_1-Verkehrsteilnehmers_L" sowie verschiedenen Bereichen der Positionierung innerhalb der dynamischen Fahrzonen zu einem funktionalen Szenario verknüpft.

Logische respektive konkrete Szenarien sind dann die jeweils parametrisierten Instanzen davon. Weiterhin wird dem jeweiligen Szenario ein zu erwartendes korrektes Verhalten des „L_1-Ego-Kraftfahrzeugs_L" aus den Zonengraphen bzw. den SOCA-Modellen zugeordnet. Des Weiteren repräsentieren die jeweiligen Betriebsbereichsmerkmale „L_1-Fahrbahnbereich_L", „L_1-Wetter_L", „L_1-Ausleuchtung_L" und „L_1-Verkehrsteilnehmer_L" spezifische Eingangsgrößen bzw. funktionale Einflussparameter. Die Auswahl und Analyse der Einflussgrößen bildet eine weitere Säule für die Generierung der konkreten szenariobasierten Testfälle mittels einer systematischen Testfallableitung gemäß dem Ansatz von Schuldt [84]. Dabei stellen die Betriebsbereichseinflussgrößen und das zu untersuchende „L_1-Ego-Kraftfahrzeug_L" die Szenenelemente innerhalb der Szenarien dar. Unter Berücksichtigung der UN-Regelung Nr. 157 [309] und der RAA [246] erfolgt dann die Ableitung und Abgrenzung von Äquivalenzklassen anhand von Diskretisierungsstufen.

Die Äquivalenzklassenbildung kategorisiert die wertkontinuierlichen Wirkparameter in diskrete Größen, welche wiederum eine systematische Prüfung des Ego-Kraftfahrzeugverhaltens in Längs- und Querrichtung begünstigen. Die Diskretisierungsstufen der Parameteruntermengen ermöglichen ihrerseits die systematische Spezifikation von kombinatorischen Testfällen einschließlich $\binom{n}{t_c}$-Testabdeckung. Dieser Ansatz ermöglicht es dann, spezifische Abfolgen von Bedingungen zu generieren, die zum systematischen Testen im Hinblick auf die Betriebssicherheitsziele (siehe Tabelle C.15) sowie der acht Verhaltensäquivalenzklassen des „L_1-Ego-Kraftfahrzeugs_L" führen (siehe Tabelle C.28).

8.1.6 Vorläufige Betriebssicherheitsvalidierung

Der Abschluss der Betriebskonzeptphase bezieht sich auf die nachvollziehbare und rückverfolgbare Argumentation des Betriebssicherheitskonzepts im Hinblick auf Teil 3-6 „Betriebssicherheitsvalidierung" sowie den darin verankerten Zielvorgaben 3-6.1. Dies wird durch frühzeitige simulationsbasierte Verifikations- und Validierungsaktivitäten gemäß „L_1-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch" begleitet. Diese sollen durch zu generierende OpSa-ML1 Arbeitsprodukte WP-11 und WP-76 bestätigen, dass das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L" die gesetzlichen Anforderungen sowie die Betriebssicherheitsziele erfüllt (siehe Schritt 1 Abbildung 8.17). Hierunter fällt zu diesem frühen Entwicklungszeitpunkt vornehmlich die verhaltensbasierte Überprüfung der Betriebssicherheitsfunktionen und Anwendungsfälle des Betriebskonzepts einschließlich deren relevanter Einschränkungen und Grenzen im Hinblick auf Konformität mit den spezifizierten Betriebssicherheitszielen.

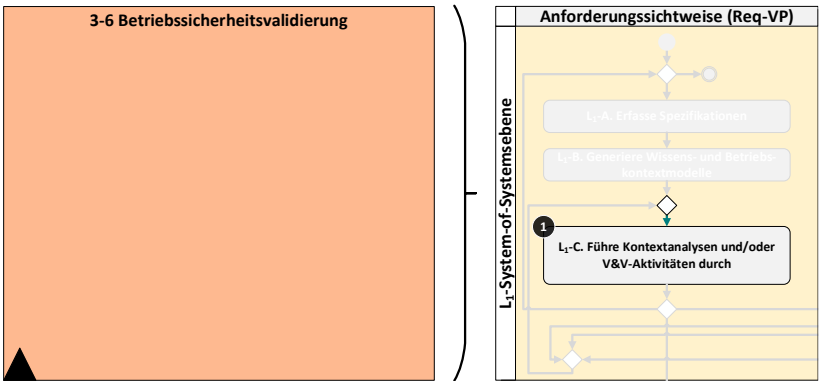


Abbildung 8.17: Durchzuführender Prozessabschnitt Teil 3-6 sowie zugehörige Aktivität innerhalb der L_1-Anforderungssichtweise.

Dafür werden zum einen die L_1-Verhaltens- und Szenariomodelle (siehe Abbildung 8.11 und Abbildung 8.15) und zum anderen die verhaltensbezogenen Betriebssicherheitsziele (siehe Tabelle C.15) sowie die spezifizierten Testfälle (siehe Tabelle C.31, Tabelle C.32, Tabelle C.33 und Tabelle C.34) herangezogen und ausgewertet. Zur Durchführung der frühzeitigen Validierungsaktivitäten wird die Methode der äquivalenzklassenbasierten Simulation im Hinblick auf die zu erwartenden Verhaltensweisen (siehe Tabelle C.18, Tabelle C.19, Tabelle C.20, Tabelle C.21, Tabelle C.22, Tabelle C.23 und Tabelle C.24) des „L_1-Ego-Kraftfahrzeugs_L“ sowie des definierten Betriebsbereichs eingesetzt. Dabei handelt es sich insbesondere um die Interaktion des „L_1-Ego-Kraftfahrzeugs_L“ mit dem „L_1-Verkehrsteilnehmer_L“, was die jeweiligen Wunschverhaltensweisen „Freifahrt“ unter Einhaltung der Geschwindigkeitsbegrenzung, „Annähern“ sowie „Abstandshaltung“ zum „L_1-Verkehrsteilnehmer_L“ angeht.

Für die jeweiligen Testfälle wird eine Sichtweite $d_{sight} = 150\,m$, eine maximale Gesamtreaktionszeit $t_{react} = 0.8\,s$ sowie eine maximal stellbare Verzögerung $a_{dec,max} = -10\,\frac{m}{s^2}$ des „L_1-Ego-Kraftfahrzeugs_L“ angenommen. Der Parameterraum der Testfälle wird durch den initialen Relativabstand $d_{rel} \in \{2;\ 150\}\,m$ die initiale Ego-Geschwindigkeit $\boldsymbol{v}_{sub} = [11.11 \quad 19.44 \quad 27.78 \quad 36.11]\,\frac{m}{s}$ sowie die initiale Relativgeschwindigkeit $v_{rel} \in \{-v_{sub};\ 36.11 - v_{sub}\}\frac{m}{s}$ des vorausfahrenden „L_1-Verkehrsteilnehmers_L“ beschrieben. Das Ganze erfolgt bei konstanter Kurvenfahrt im Zuge des maximal möglichen Krümmungsradius auf Autobahnen $R_P = 720\,m$ bzw. $\kappa^* = \frac{1}{720\,m}$ (siehe Tabelle C.6).

Die Simulationsläufe gestalten sich im Zuge äquivalenzklassenbasierten Simulation durch eine schrittweise Abtastung innerhalb der spezifizierten Parameterräume, wobei direkt zu Simulationsbeginn der „Cut-In“ bzw. das „Einscheren“ des vorausfahrenden „L_1-Verkehrsteilnehmers_L“ in die Ego-Fahrspur vollzogen wird. Hierbei wird ein exemplarisch extrahierter Testschritt repräsentiert (siehe Abbildung 8.18), wobei der vorausfahrende „L_1-Verkehrsteilnehmer_L“ mit einer Relativgeschwindigkeit von $v_{rel} = -17\,\frac{m}{s}\left(60\,\frac{km}{h}\right)$ zum Zeitpunkt $t = 0\,s$ in die Fahrzone A_5 einschert. Innerhalb der maximal zulässigen Reaktionszeit $t_{react} = 0.8\,s$ initiiert das „L_1-Ego-Kraftfahrzeug_L“ aufgrund der Unterschreitung der TTC_{min} von $2.0\,s$ das erforderliche Notfallbremsmanöver mit $a_{X,decel} = -7\,\frac{m}{s^2}$, durchschreitet die jeweils definierten Modi „Segeln“, „Notfallabbremsung“, „Beschleunigung“ und „Geschwindigkeitsbeibehaltung“ bis schließlich die fahrzonenbasierte Abstandszielzone A_1 mit einer Relativgeschwindigkeit von $v_{rel} = 0\,\frac{m}{s}$ erreicht und eingehalten wird (siehe Abbildung 8.18).

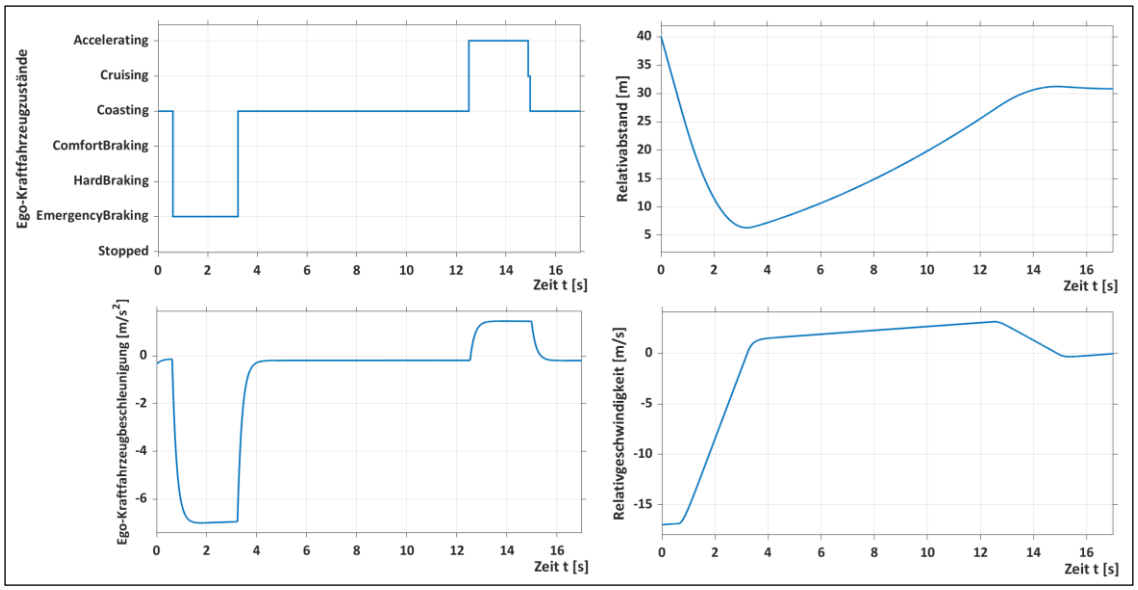


Abbildung 8.18: Zeitlicher Verlauf der Ego-Fahrzeugzustände in Längsrichtung gemäß des Zustandsdiagramms (siehe Abbildung 8.11 und Abbildung 8.15) bezüglich eines exemplarisch extrahierten Testschritts des „Cut-In-Testfalls“ L1.4-TC.

Des Weiteren erweisen sich die fahrdynamischen Betrachtungen im Hinblick auf die kombinierten Längs- und Querführung im Zuge eines gekrümmt verlaufenden „L_1-Fahrbahnbereichs_L“ als zweckdienlich (vgl. Gl. 8.6). Dadurch kann das „L_1-Ego-Kraftfahrzeug_L“ auch unter dem Einfluss starker Notbremsmanöver in Längsrichtung der gekrümmten Sollbahn im querdynamischen Gleichgewichtszustand folgen (siehe Abbildung 8.19). Analog dazu wird der gesamte Parameterraum abgetastet und in Form von Konturdiagrammen mit den Achsen initialer Relativabstand und initiale Relativgeschwindigkeit dargestellt. Für jede anfängliche Ego-Geschwindigkeit wird ein eigenes Diagramm dargestellt (siehe Abbildung 8.20).

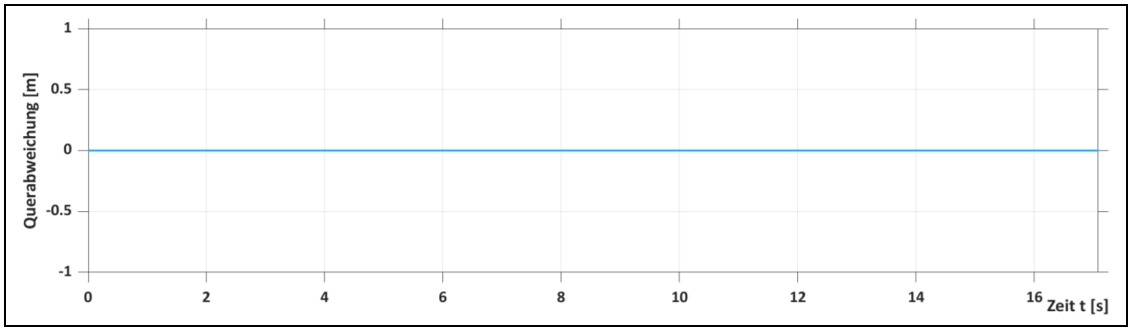


Abbildung 8.19: Querabweichung im Zuge eines exemplarisch extrahierten Testschritts des „Cut-In-Testfalls“ L1.4-TC.

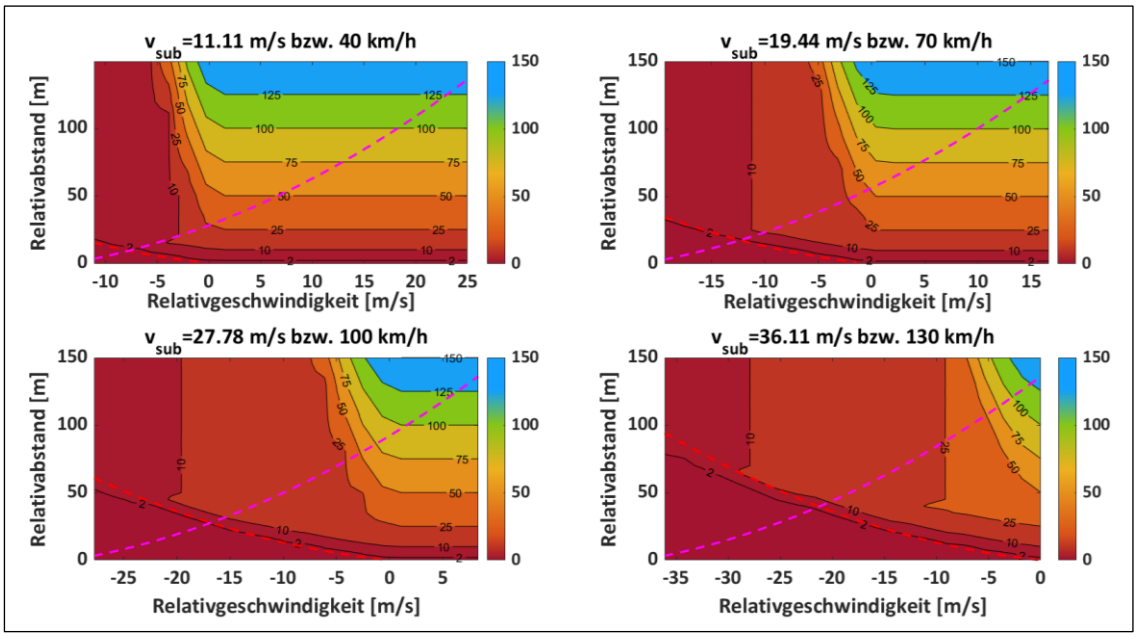


Abbildung 8.20: Minimaler Relativabstand im Hinblick auf die Durchführung der Testfälle L1.2-TC, L1.3-TC und L1.4-TC bei konstanter Kurvenfahrt auf L_1-Granularitätsebene.

Zusätzlich enthält jedes Diagramm eine schraffierte, rot eingefärbte Kurve, welche den physikalisch bzw. minimal erforderlichen Relativabstand für einen kollisionsfreien Verlauf darstellt, wobei dieser gemäß

$$d_{rel,phys,min} = \frac{1}{2}\frac{v_{rel}^2}{a_{rel}} - v_{rel} \cdot t_{react} \qquad 8.13$$

berechnet wird. Magenta schraffiert ist der Sollabstand, wenn das „L_1-Ego-Kraftfahrzeug_L“ sich an die Geschwindigkeit des „L_1-Verkehrsteilnehmers_L“ anpasst (siehe Abbildung 8.20). Insgesamt weist die Längsführung eine adäquate Übereinstimmung im Sinne der praktikabel realisierbaren Kollisionsvermeidung unter Berücksichtigung der physikalischen Grenzen des „L_1-Ego-Kraftfahrzeugs_L“ als auch mit den aus der StVO als auch der UN-Regelung Nr. 157 abgeleiteten Interessenvertreteranforderungen (siehe Tabelle C.3, Tabelle C.4 und Tabelle C.5) bzw. daraus deduzierten Verhaltensregeln auf (siehe Tabelle C.18, Tabelle C.19, Tabelle C.20, Tabelle C.21, Tabelle C.22, Tabelle C.23 und Tabelle C.24). Für geringe Geschwindigkeiten des vorausfahrenden „L_1-Verkehrsteilnehmers_L“ wird aufgrund der sich daran anpassenden Ego-Geschwindigkeit stets ein niedriger Relativabstand erzielt, so dass Isolinien des Relativabstands im Diagramm entstehen (siehe Abbildung 8.20). Mit zunehmender Geschwindigkeit des vorausfahrenden „L_1-Verkehrsteilnehmers_L“ wächst auch der minimale Relativabstand. Für Relativgeschwindigkeiten größer null geht der minimale Relativabstand zügig in den initialen Abstand über (siehe Abbildung 8.20). Der eingeschränkte Sichtbereich wird anhand der maximalen Verzögerung während der Szenarien deutlich. Ab einer Ego-Geschwindigkeit von $v_{sub} = 36.11\ \frac{m}{s}\ \left(130\ \frac{km}{h}\right)$ ist bei einer maximalen Sichtweite von $d_{sight} = 150\ m$ überwiegend eine Notfallabbremsung mit $a_{X,decel} \leq -5\ \frac{m}{s^2}$ nötig (siehe Abbildung 8.21). Das hier aufgezeigte Vorgehen der simulationsbasierten Testfalldurchführung müsste für die restlichen noch verbliebenen Testschritte des Geradeausfalls einschließlich der Betrachtung eines beschleunigenden oder verzögernden vorausfahrenden „L_1-Verkehrsteilnehmers_L“ durchgeführt werden. Aus Gründen des Umfangs wird dies im Zuge der vorliegenden Dissertation jedoch nicht weiter umgesetzt.

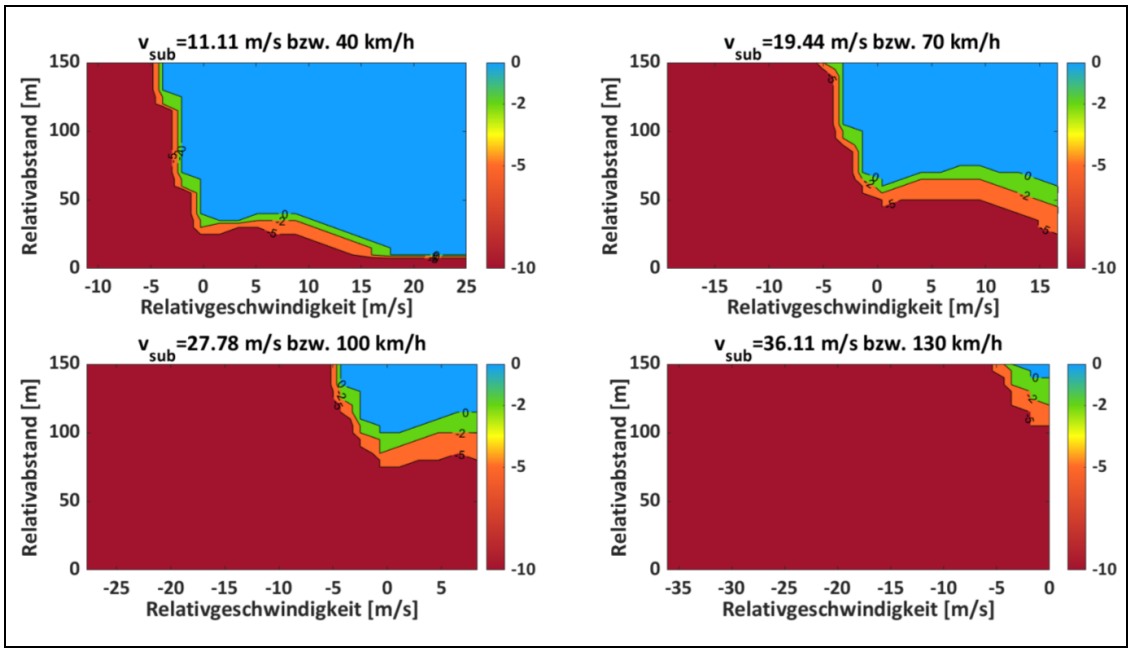


Abbildung 8.21: Maximale Ego-Verzögerung im Hinblick auf die Durchführung der Testfälle L1.2-TC, L1.3-TC und L1.4-TC bei konstanter Kurvenfahrt auf L_1-Granularitätsebene.

Es sei darauf hingewiesen, dass zu diesem frühen Entwicklungszeitpunkt die simulationsbasierte Validierung der Spurhaltung im Kontext der Querführung auf konstante Kurvenfahrten beschränkt ist. Einflüsse wie Sollsprünge der Krümmung, Auslenkungen aus der statischen Ruhelage, Störgrößen oder ähnliche Effekte innerhalb der Ego-Fahrspur können derzeit noch nicht angemessen bewertet werden. Dynamische Querführungsmanöver, die über das statische Gleichgewicht hinausgehen, müssen daher zu einem späteren Entwicklungszeitpunkt getestet werden. Dafür sind umfassendere dynamische Modelle erforderlich, die regelungstechnische Algorithmen integrativ in die Fahrzeugarchitektur einbinden. Dies schließt die Bereiche Umgebungswahrnehmung, Planung, Regelung und Aktuatorik ein, von L_3-Subsystemen über L_4-Komponenten bis hin zu L_5-Einheiten. Im Verlauf der durchgeführten simulationsbasierten Validierungsaktivitäten wurden insgesamt keine inakzeptablen Diskrepanzen bzw. Verletzungen der Betriebssicherheitsziele festgestellt. Dadurch kann das Betriebsbereichsfreigabeartefakt L1-ODDR0.1 der erfolgreichen frühzeitigen Verifikations- und Validierungsaktivitäten generiert werden.

Tabelle 8.5: OpSa-ML1 Betriebsbereichsfreigabe ODDR0.1.

<<Freigabe>>
ID: L10000ODDR0.1
L1-ODDR0.1 OpSa-ML1 Betriebsbereichsfreigabe
Die Testfälle L1.2-TC, L1.3-TC und L1.4-TC wurden unter Berücksichtigung der physikalischen Gesetzmäßigkeiten eines Punktemassemodells für die konstante Kurvenfahrt bestanden. Dadurch untermauern diese die Betriebssicherheitsargumentation sowie die OpSa-ML1 Betriebsbereichsfreigabe der Fahrzeugverhaltensspezifikation des „L_1-Ego-Kraftfahrzeugs_L“ im Hinblick auf die Interaktion mit dem „L_1-Verkehrsteilnehmer_L“. Eine analytisch dynamische Validierung der Spurhaltung im Sinne der Querführung außerhalb des statischen Gleichgewichtszustands konnte allerdings nicht durchgeführt werden. Hierfür sind umfassendere dynamische Modelle erforderlich, die regelungstechnische Algorithmen integrativ in die Fahrzeugarchitektur einbinden.

8.2 Entwurfs- und Verifikationszyklus gemäß der Konzeptphase

Im Folgenden wird der modell- und simulationsbasierte Entwurfs- und Verifikationszyklus gemäß der Konzeptphase dargelegt, wobei der Schwerpunkt auf der „Item Definition bzw. Spezifikation und Design gemäß der Konzeptphase“ (vgl. Unterabschnitt 8.2.1) sowie auf der „Vorläufigen Verifikation der Item Definition respektive der Spezifikation und des Designs gemäß der Konzeptphase“ (vgl. Unterabschnitt 8.2.2) liegt. Hinsichtlich des Entwurfs und der Integration stehen insbesondere die L_1/L_2-Granularitätsebenen einschließlich der Anforderungssichtweise, der funktionalen Sichtweise sowie der logischen Sichtweise im Fokus (siehe Abbildung 8.22).

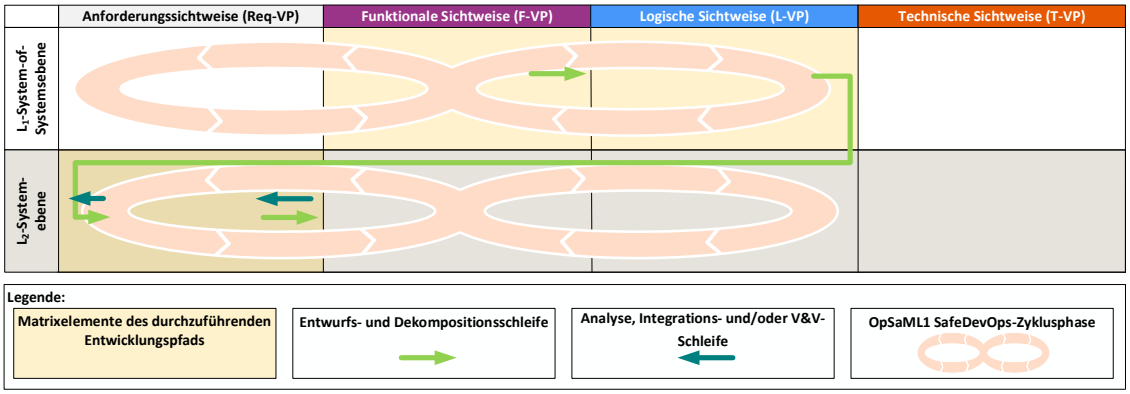


Abbildung 8.22: SPES-Matrix unter Hervorhebung der für das modell- und simulationsbasierte Betriebssicherheitskonzept relevanten Matrixelemente im Hinblick auf den Entwurfs- und Verifikationszyklus gemäß der Konzeptphase (gelber Bereich).

8.2.1 Item Definition respektive Spezifikation und Design gemäß der Konzeptphase

Auf Basis der Betriebskonzeptphase erfolgt mit dem weiteren Voranschreiten der Entwicklungstätigkeiten der Übergangsbereich in die Konzeptphase inkl. Teil 4-5 „Item Definition“ gemäß ISO 26262 bzw. Teil 5 „Spezifikation und Design“ gemäß ISO 21448. Die beiden Teile können miteinander verknüpft werden, da die Definition des Items[3] (ISO 26262) mit der Spezifikation der beabsichtigten Funktionalität auf Fahrzeugebene (ISO 21448) dieselben Inhalte umfassen (siehe Abbildung B.2). Im Zuge dessen erfolgt die Beschreibung der beabsichtigten Funktionalität sowie die Darstellung von Interdependenzen der Funktion zu anderen Fahrzeugfunktionen und -systemen inkl. den jeweils relevanten Umweltbedingungen. Zudem müssen das Verhalten des Items sowie sämtliche anzunehmende Betriebszustände und -szenarien evaluiert werden. Dieser Aspekt wird wiederum durch Teil 3-7 „Granularitätsebenenabhängige Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs“ und der darin formulierten Zielvorgaben 3-7.1 adressiert (siehe Abbildung 8.23).

[3] Bei einem Item handelt es sich um ein System oder eine Kombination von Systemen, auf welchem eine Funktion oder ein Teil einer Funktion auf Fahrzeugebene implementiert ist [50].

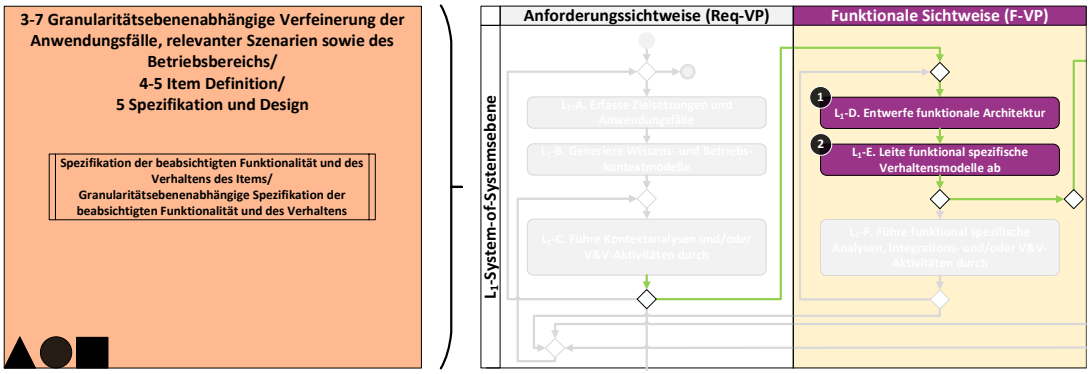


Abbildung 8.23: Durchzuführende Prozessabschnitte der Teile 3-7, 4-5 und 5 sowie zugehörige Aktivitäten innerhalb der L_1-Funktionale Sichtweise.

Die detaillierten Zielvorgaben in Bezug auf Teil 4-5 „Item Definition“ sowie Teil 5 „Spezifikation und Design“ können der ISO 26262 [50] bzw. der ISO 21448 [55] entnommen werden. Insgesamt wird in Anbetracht der hier im Fokus stehenden Prozessabschnitte wiederum die Zielsetzung verfolgt, die dafür relevanten Arbeitsprodukte bzw. Inkremente WP-36 und WP-37 unter Erfüllung des OpSa-ML1 zu generieren. Im Hinblick darauf erfolgt der Übergang in die funktionale Sichtweise auf L_1-Granularitätsebene gemäß den durchzuführenden Aktivitäten „L_1-D. Entwerfe funktionale Architektur“ sowie „L_1-E. Leite funktional spezifische Verhaltensmodelle ab“ (siehe Schritt 1 und Schritt 2 Abbildung 8.23).

In Anbetracht dessen wird die Black-Box-Funktion „L_1-FahreHochautomatisiert_F“ aus der Anforderungssichtweise in den Mittelpunkt gerückt (siehe Abbildung 8.16) und in die White-Box-Funktionen „L_2-RegleAutomatisierteFahraufgabe_F“, „L_2-StelleNotwendigeLeistungsUndEnergieformenBereit_F“, „L_2-Befördere PassagiereUndRealisiereFahrzeugbewegung_F“ dekomponiert (siehe Abbildung 8.24).

Im weiteren Entwicklungsverlauf wird dann ein funktional spezifisches Verhaltensmodell im Hinblick auf die sequenzielle Interaktion anhand entsprechender Timing Budgets der jeweiligen L_2-White-Box-Funktionen abgeleitet und definiert. Auf Grundlage dessen wird dann die sequenzielle Interaktion der White-Box-Funktionen „L_2-RegleAutomatisierte…F“, „L_2-StelleNotwendige…F“ sowie „L_2-BefördерePassagiere…F“ beschrieben. Dabei werden diese entlang von sogenannten Lebenslinien (engl. *Lifeline*) angeordnet, wobei die jeweiligen Schnittstellen des Lenk-, Verzögerungs- und Beschleunigungsbefehls etc. bezüglich der Interaktion zwischen den L_2-White-Box-Funktionen übernommen werden. Hinzu kommt eine Verteilung der Timing-Budgets im Sinne von Kommunikations- und Ausführungszeiten gemäß der zu erreichenden Fahrzeugreaktionszeit $t_{react} = 0.8\ s\ (800\ ms)$ (siehe Abbildung 8.25).

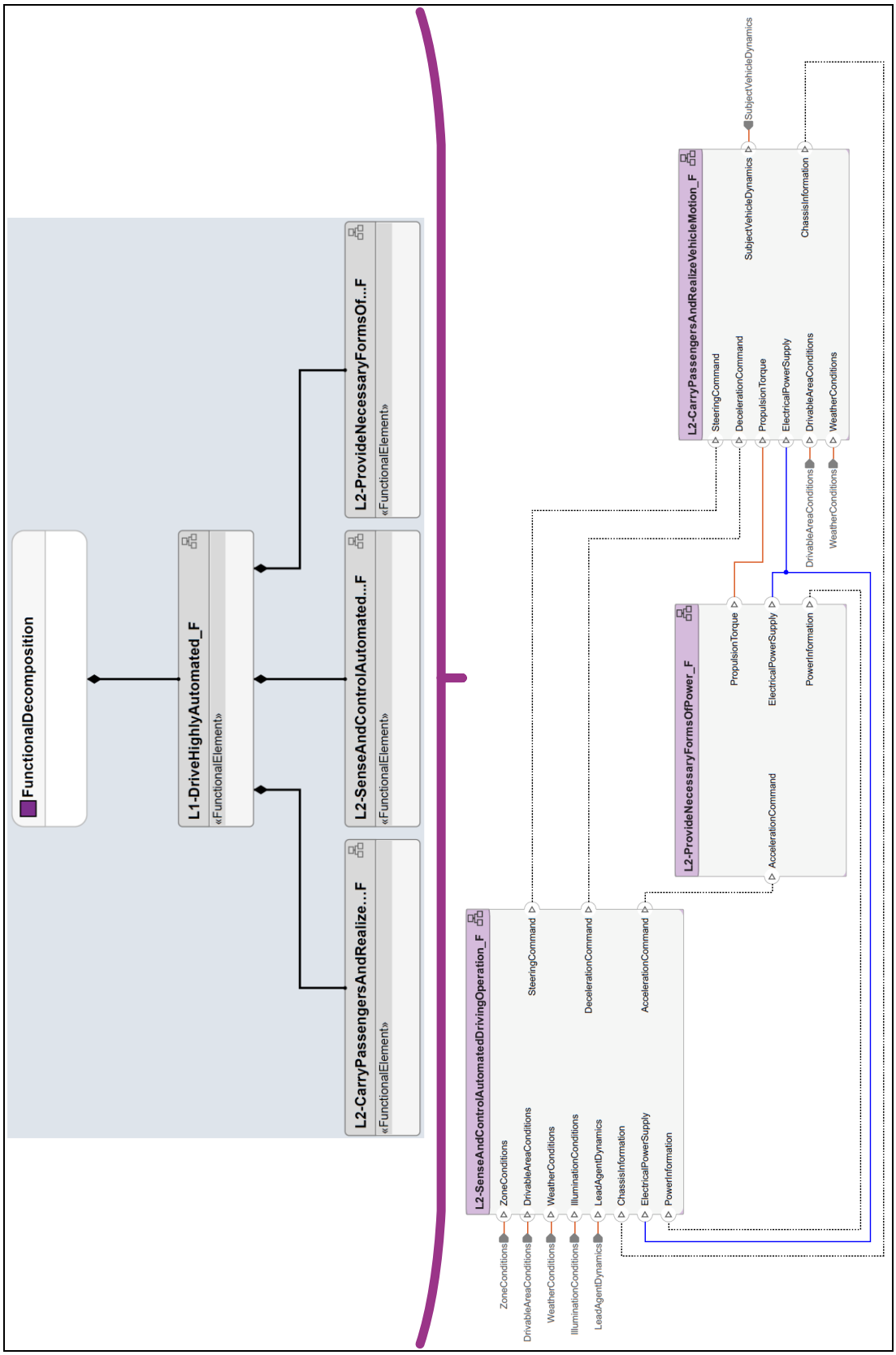


Abbildung 8.24: Dekomposition der Black-Box-Funktion „L_1-FahreHochautomatisiert_F“ in die White-Box-Funktionen „L_2-RegleAutomatisierte…F“, „L_2-StelleNotwendige…F“ sowie „L_2-BefördereMitPassagiere…F“.

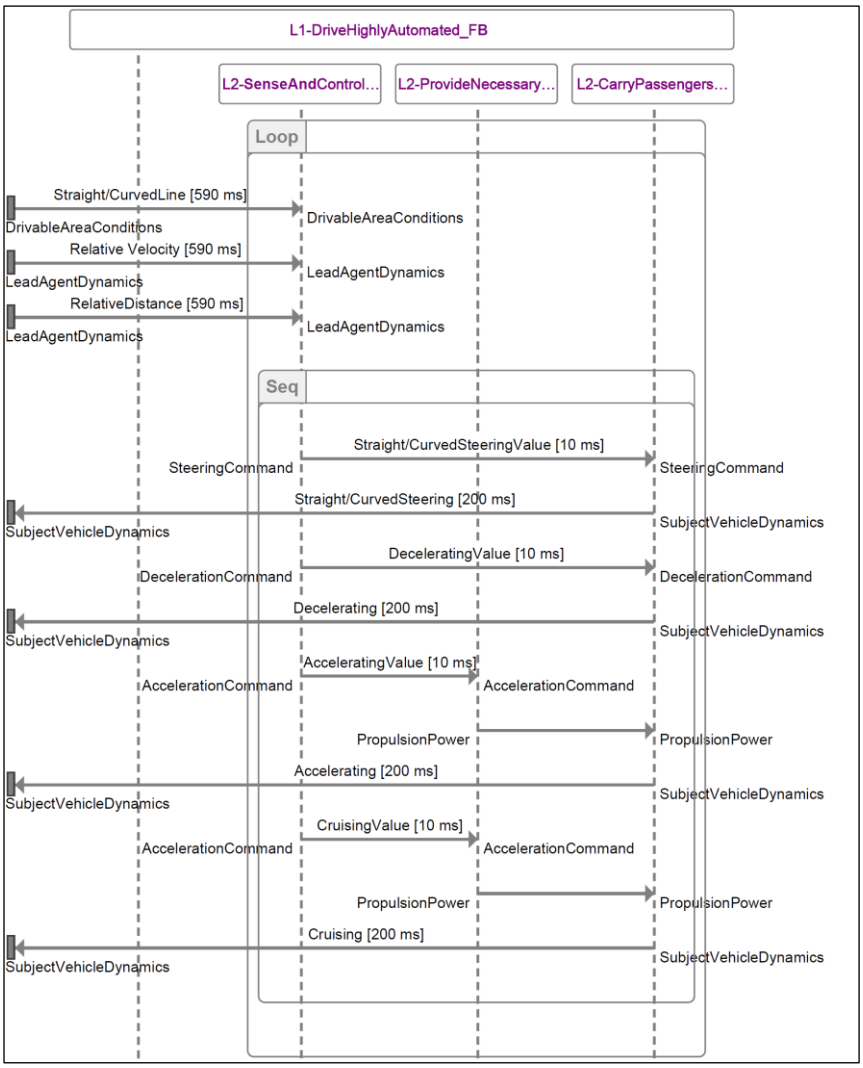


Abbildung 8.25: Sequenzdiagramm als funktional spezifisches Verhaltensmodell auf L_1-Granularitätsebene zur Darstellung der Abfolge der zeitlich bezogenen Interaktionen zwischen den L_2-White-Box-Funktionen.

Im Anschluss daran erfolgt die Fortsetzung der Entwicklungsaktivitäten wiederum direkt innerhalb der logischen Sichtweise auf der L_1-Granularitätsebene. Die Beschreibung der logischen Architektur erfolgt im Hinblick auf die Aktivität „L_1-G. Entwerfe logische Architektur“ sowie die Darstellung von Interdependenzen des Items zu anderen Fahrzeugsystemen als auch den jeweils relevanten Umweltbedingungen. Zudem müssen das Verhalten des Items sowie sämtliche anzunehmende Betriebszustände und -szenarien mittels der Aktivität „L_1-H. Leite logisch spezifische Verhaltensmodelle ab“ evaluiert werden (siehe Schritt 1 und Schritt 2 Abbildung 8.26).

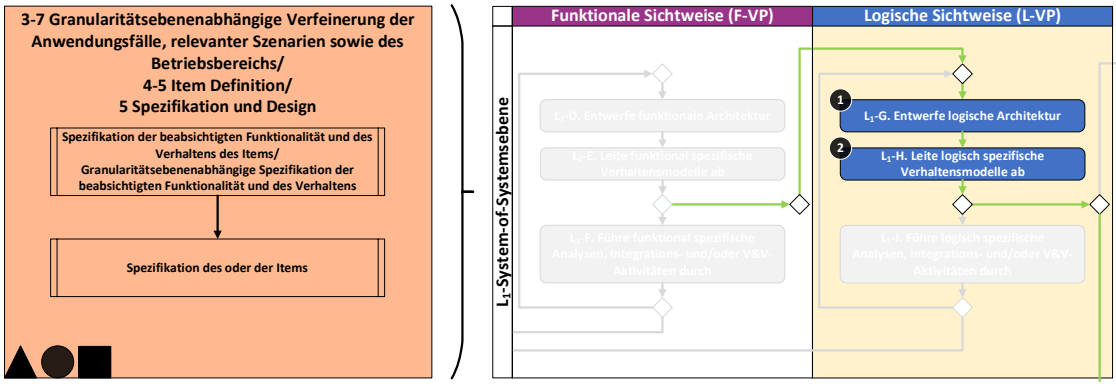


Abbildung 8.26: Durchzuführende Prozessabschnitte der Teile 3-7, 4-5 und 5 sowie zugehörige Aktivitäten innerhalb der L_1-Logische Sichtweise.

Hierfür werden einerseits das funktionale L_2-White-Box-Modell (siehe Abbildung 8.24) und andererseits das logische L_1-Betriebskontextmodell (siehe Abbildung 8.14) im Hinblick auf mögliche Elemente, was die Umsetzung der L_2-White-Box-Funktionen betrifft, betrachtet. Darauf basierend werden bezüglich der Umsetzung der White-Box-Funktionen „L_2-RegleAutomatisierte…F“, „L_2-StelleNotwendige…F“ sowie „L_2-BefördereP assagiere…F“ insgesamt drei logische L_2-Systeme definiert (siehe Abbildung 8.27). Dementsprechend wird die White-Box-Funktion „L_2-RegleAutomatisierte…F“ dem System „L_2-Fahrzeugführung_L“ zugewiesen, wobei dieses die jeweiligen Schnittstellen übernimmt. Analog dazu wird die White-Box-Funktion „L_2-StelleNotwendige…F“ dem logischen Element „L_2-EnergieUndAntrieb_L“ und die Funktion „L_2-BefördereP assagiere…F“ wiederum dem „L_2-Chassis_L“ zugeteilt (siehe Abbildung 8.27). Diese werden als logische L_2-Regelkreisarchitektur innerhalb des „L_1-Ego-Kraftfahrzeugs_L“ angeordnet und repräsentieren dabei das Item gemäß ISO 26262 (siehe Abbildung 8.28).

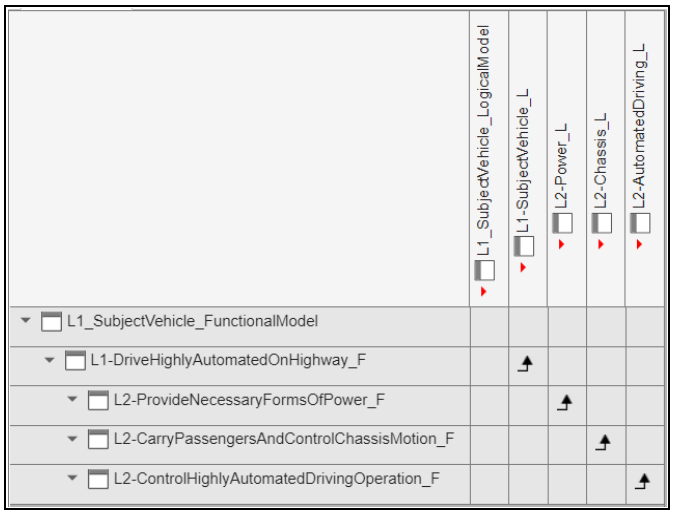


Abbildung 8.27: Allokationsmatrix der White-Box-Funktionselemente sowie der logischen Architekturelemente des „L_1-Ego-Kraftfahrzeugs_L“.

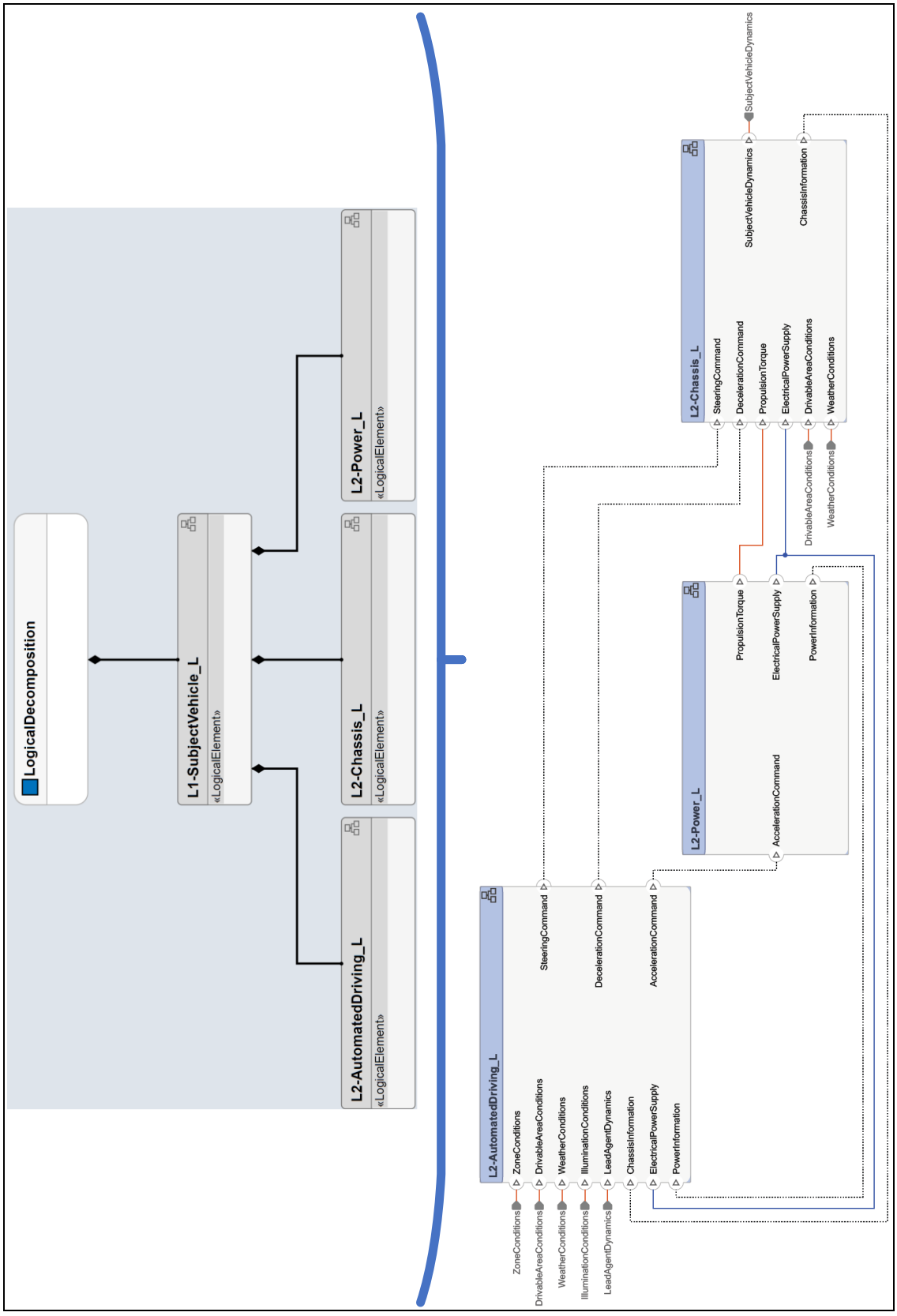


Abbildung 8.28: Dekomposition des logischen Elements „L_1-Ego-Kraftfahrzeug_L“ in die Elemente „L_2-Fahrzeugführung_L“, „L_2-EnergieUndAntrieb_L“ sowie „L_2-Chassis_L“.

Darüber hinaus erfolgt hier eine granularitätsebenenabhängige Verfeinerung des definierten Betriebsbereichs. Somit wird mit Blick auf die fahrzeugexternen Betriebsbereichsattribute der „L_1-Fahrbahnbereich_L“ in die Elemente „L_2-Fahrbahntyp_L“, „L_2-Fahrbahngeometrie_L“, „L_2-Fahrbahnspezifikation_L“ sowie „L_2-Fahrbahnoberfläche_L“ dekomponiert. Dies gilt auch für die „L_1-Zone_L“, worunter das Attribut „L_2-Regionen/Staaten_L“ fällt. Gleichermaßen wird das Element „L_1-Wetter_L“ mittels des Attributs „L_2-Wind_L“ konkretisiert. Analog dazu wird das Kontextelement „L_1-Ausleuchtung_L“ in die untergeordneten Attribute „L_2-Bewölkung_L“ und „L_2-NatürlicheAusleuchtung_L“ zerlegt. Entlang der Dimensionen spiegeln die dunkelgrau hervorgehobenen L_2-Attribute jeweils einen Bestandteil des definierten L_2-Betriebsbereichs, wohingegen die hellorangen L_2-Attribute aus der Definition ausgeschlossen bzw. nicht näher betrachtet werden (siehe Tabelle 8.6).

Auf Basis der logischen L_2-Architektur geht es anschließend darum (siehe Abbildung 8.28), entsprechende Verhaltensweisen der jeweiligen Elemente abzuleiten. Zusätzlich wird das funktional spezifische Modell im Sinne des Sequenzdiagramms herangezogen (siehe Abbildung 8.25), um die darin beschriebenen Interaktionen in Richtung von analytisch dynamischen zu konkretisieren. Vor diesem Hintergrund wird die funktionale Topologie der White-Box-Funktionen „L_2-RegleAutomatisierte…F“, „L_2-StelleNotwendige…F“ und „L_2-BefördereP assagiere…F“ verwendet, wobei deren parametrische Ausprägungen im Hinblick auf die in Frage kommenden logischen Elemente „L_2-Fahrzeugführung_L“, „L_2-EnergieUndAntrieb_L“ als auch „L_2-Chassis_L“ festgelegt und das logisch spezifische Verhalten über mathematisch-physikalische Gesetzmäßigkeiten repräsentiert wird. Dabei resultiert dies gemäß der funktionalen Architektur der übergeordneten Verhaltensrepräsentation „L_1-FahreHochautomatisiert_LB“ in den logisch spezifischen Verhaltensbestandteilen „L_2-RegleAutomatisierte…LB“, „L_2-StelleNotwendige…LB“ sowie „L_2-BefördereP assagiere…LB“ (siehe Abbildung 8.29).

Tabelle 8.6: Zwicky-Box im Hinblick auf die Entwurfsentscheidung des definierten L_2-Betriebsbereichs.

<table>
<tr><th colspan="7"><<Entwurfsentscheidung>></th></tr>
<tr><td colspan="7">ID: L2.10000DECN</td></tr>
<tr><td colspan="7">L2.1-DECN L_2-Betriebsbereichsdefinition</td></tr>
<tr><td>Dimension</td><td colspan="6">Alternativen</td></tr>
<tr><td>L_1-Zone</td><td>L_2-Geofencing Zone_L</td><td>L_2-Feste-Zone_L</td><td>L_2-Dyna-mischeZone_L</td><td>L_2-Interferenz-zone_L</td><td colspan="2">L_2-Regionen/ Staaten_L</td></tr>
<tr><td>L_1-Fahrbahn-bereich</td><td>L_2-Fahr-bahntyp_L</td><td>L_2-Fahr-bahngeo-metrie_L</td><td>L_2-Fahr-bahnspezi-fikation_L</td><td>L_2-Fahr-bahnbe-schilde-rung_L</td><td>L_2-Fahr-bahnrand-bebau-ung_L</td><td>L_2-Fahr-bahnober-fläche_L</td></tr>
<tr><td>L_1-Wetter</td><td colspan="2">L_2-Wind_L</td><td colspan="2">L_2-Regen_L</td><td colspan="2">L_2-Schneefall_L</td></tr>
<tr><td>L_1-Ausleuch-tung</td><td colspan="2">L_2-Tag_L</td><td>L_2-Nacht_L</td><td>L_2-Bewölkung_L</td><td colspan="2">L_2-KünstlicheAus-leuchtung_L</td></tr>
</table>

Auf Grundlage der vorangegangen Entwicklungsschritte wird an dieser Stelle die zustandsbasierte Verhaltensspezifikation (siehe Abbildung 8.11 und Abbildung 8.15) zur Generierung der Beschleunigungs- sowie Verzögerungsbefehle $a_{X,accel,req}$ bzw. $a_{X,decel,req}$ sowie die Bereitstellung der Antriebs- und Verzögerungsmomente $M_D = m \cdot a_{X,accel,req} \cdot r_{dyn}$ bzw. $M_B = m \cdot a_{X,decel,req} \cdot r_{dyn}$ mittels entsprechender Übertragungsfunktionen

$$G_{M_D}(s) = \frac{K_{M_D}}{T_{M_D}s + 1} e^{-sT_{t,a_{X,accel,req}}} \qquad 8.14$$

$$G_{M_B}(s) = \frac{K_{M_B}}{T_{M_B}s + 1} e^{-sT_{t,a_{X,decel,req}}}$$

für die Längsdynamik erfasst.

Die räumliche Kinematik in Längsrichtung gemäß den X-Koordinaten ergibt sich anhand

$$a_X = \frac{1}{m}\left(\frac{1}{r_{dyn}}(i_{tot}\eta_{tot}M_D + M_B) - F_{WX} - F_{RX}\right) \qquad 8.15$$

im Sinne der Dynamik des „L_2-Chassis_L“ unter Berücksichtigung der Luft- und Rollwiderstandskräfte F_{WX} bzw. F_{RX} (vgl. Gl. A.19 und A.20). Zudem stellen i_{tot} das Gesamtübersetzungsverhältnis des Antriebsstrangs und η_{tot} entsprechend den Gesamtwirkungsgrad dar, wobei r_{dyn} den dynamischen Halbmesser abbildet.

Im Zusammenhang mit der Querführung werden der Querbeschleunigungs- und Gierratenbefehl im Kontext des Lenkbefehls beschrieben und deren Umsetzung anhand der Übertragungsfunktionen

$$G_{a_{Y,req,\psi,req}}(s) = \frac{K_{a_{Y,req,\psi,req}}}{T_{a_{Y,req,\psi,req}}s + 1} e^{-sT_{t,a_{Y,req,\psi,req}}} \qquad 8.16$$

abgebildet. Die räumliche Kinematik in Querrichtung gemäß den Y-Koordinaten wird durch

$$G_{a_Y}(s) = \frac{K_{a_Y}}{T_{a_Y}s + 1} \qquad 8.17$$

$$a_Y = G_{a_Y}(s) \cdot G_{a_{Y,req}}(s)$$

dargestellt. Analog dazu wird die Erfassung der Drehung um die Z-Koordinaten

$$G_{\dot{\psi}}(s) = \frac{K_{\dot{\psi}}}{T_{\dot{\psi}}s + 1} \qquad 8.18$$

$$\dot{\psi} = G_{\dot{\psi}}(s) \cdot G_{\dot{\psi}_{req}}(s)$$

im Sinne der Gierrate vorgenommen.

Abschließend erfolgt hierbei die Zuteilung der Timing-Budgets und/oder Ausführungszeiten gemäß dem innerhalb der funktionalen Sichtweise definierten Sequenzdiagramms (siehe Abbildung 8.25). Hinzu kommt die Berücksichtigung der Kommunikationslatenz zwischen den jeweiligen L_2-Systemen, wobei dies mittels der Totzeiten $T_{t,L_{2,com}}$ abgebildet wird (siehe Abbildung 8.29).

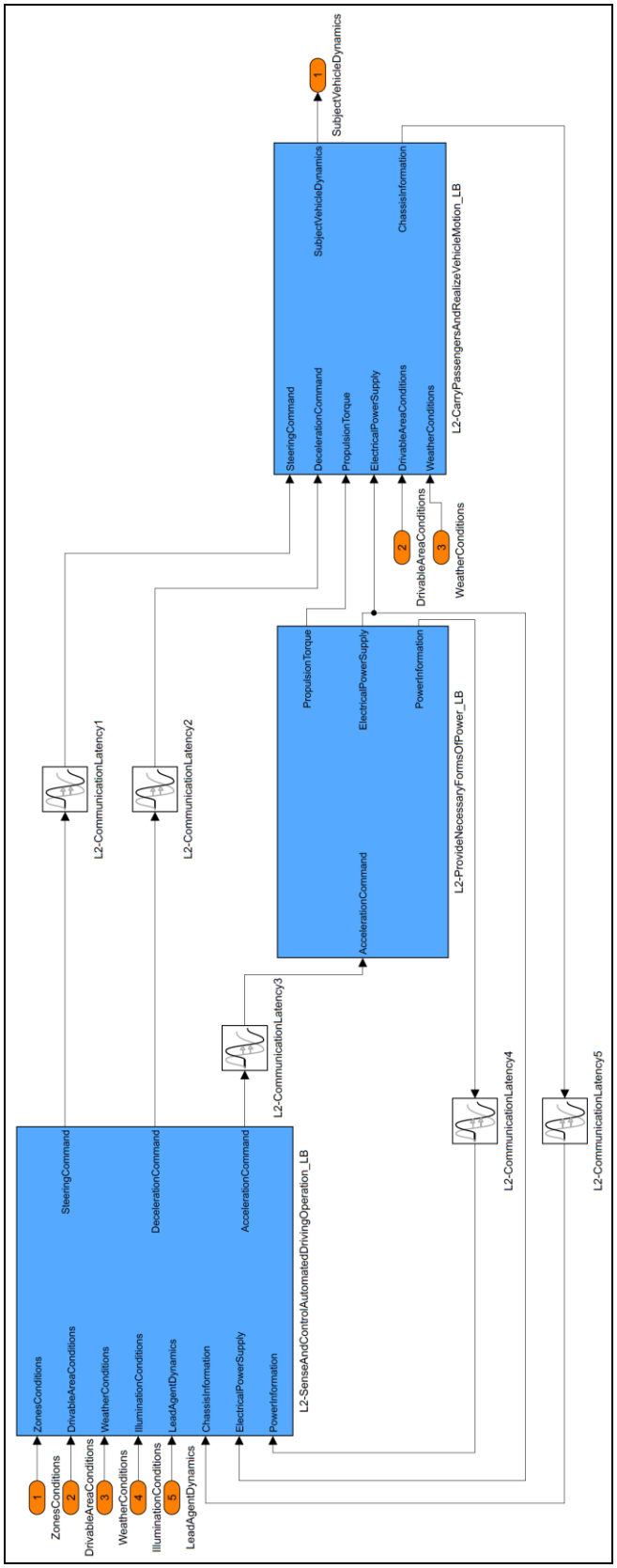


Abbildung 8.29: Ableitung des logisch spezifischen Verhaltensmodells auf L_1-Granularitätsebene.

Die oben beschriebenen Aktivitätsschritte bilden den Abschluss der Tätigkeiten auf der L_1-Granularitätsebene. Die technische Sichtweise wird zu diesem frühen Entwicklungszeitpunkt noch nicht berücksichtigt, wodurch im weiteren Verlauf der Top-Down-Übergang in die Anforderungssichtweise gemäß der L_2-Granularitätsebene vollzogen wird. In diesem Zusammenhang werden die jeweiligen L_2-Systeme einschließlich der fahrzeugexternen L_2-Betriebsbereichselemente erfasst (siehe Abbildung 8.28 bzw. Tabelle 8.6). Auf Grundlage dessen werden funktionale, nicht-funktionale sowie regulatorische und gesetzliche Anforderungen hinsichtlich des Items selbst, den Elementen des Items sowie den Interaktionen des Items mit dessen Umgebungskontext gemäß „L_2-A. Erfasse Spezifikationen“ dokumentiert. Unter diese Betrachtung fallen auch die Anforderungen des Umgebungskontexts an das Item als auch umgekehrt im Sinne von „L_2-B. Generiere Wissens- und Betriebskontextmodelle“ (siehe Schritt 1 und 2 Abbildung 8.30).

Da die innerhalb der funktionalen Sichtweise beschriebene funktionale Architektur auf L_1-Granularitätsebene in die Anforderungssichtweise der L_2-Granularitätsebene überführt wird, werden die L_2-White-Box-Funktionen nicht mehr als White-Box, sondern als L_2-Black-Box-Modelle erfasst. Außerdem werden die logischen L_2-Systeme im Hinblick auf die jeweils zu übernehmenden Verantwortlichkeiten bewertet. An dieser Stelle werden die für die Planung, Umsetzung und Überwachung einer gesetzeskonformen, proaktiven, reaktiven, aber auch möglichst unfallfreien Fahrzeugverhaltensspezifikation jeweils benötigten L_2-Fähigkeiten konkretisiert. Diesbezüglich werden die Betriebssicherheitsanforderungen der L_1-Granularitätsebene (siehe Tabelle C.30) zerlegt und den logischen Systemen „L_2-Fahrzeugführung_L“ (siehe Tabelle C.35), „L_2-EnergieUndAntrieb_L“ (siehe Tabelle C.36) sowie „L_2-Chassis_L“ (siehe Tabelle C.37) zugewiesen.

Daraufhin werden einerseits das logisch spezifische L_2-Verhaltensmodell einschließlich der getroffenen Entwurfsentscheidungen sowie andererseits die funktionalen und nichtfunktionalen Betriebssicherheitsanforderungen, Betriebssicherheitsziele etc. im Hinblick auf die jeweiligen L_2-Systemverhaltensweisen reflektiert. Auf Grundlage dessen werden die funktionalen und nichtfunktionalen Betriebssicherheitsanforderungen, was die L_2-Granularitätsebene betrifft, gemäß den logisch spezifischen L_2-Verhaltensbeschreibungen erhoben und dokumentiert. Hierbei werden insbesondere die Anforderungen einzuhaltender Ausführungs- und Kommunikationszeiten spezifiziert (siehe Tabelle C.38). Anschließend erfolgt der nahtlose Übergang in die weitere Testfallspezifikation gemäß Teil 9 „Definition der Verifikations- und Validierungsstrategie“ der ISO 21448. Diese muss die Bewertung potenziell gefährlicher Szenarien sowie eine ausreichende Abdeckung des relevanten Szenarienraums umfassen.

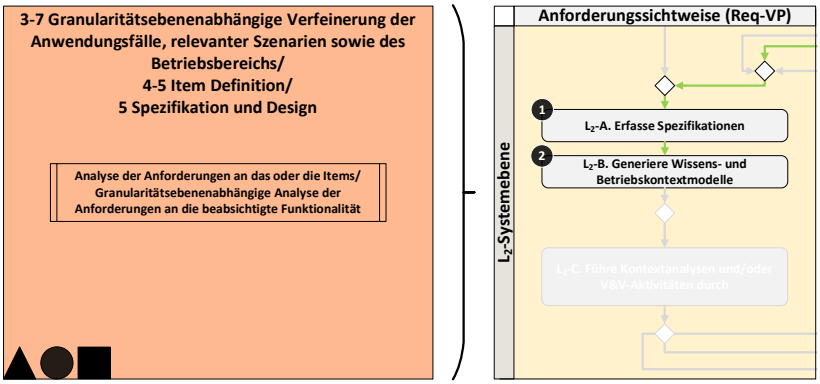


Abbildung 8.30: Durchzuführende Prozessabschnitte der Teile 3-7, 4-5 und 5 sowie zugehörige Aktivitäten im Zuge des Top-Down-Übergangs in die L_2-Anforderungssichtweise.

Erforderliche Nachweise, wie Analyseergebnisse, Testberichte und spezifische Untersuchungen, sind ebenfalls einzubeziehen. Darüber hinaus sind klare Verfahren zur Generierung dieser Nachweise festzulegen. Zudem muss die Eignung der ausgewählten Methoden und Ziele für die Verifikation und Validierung nachvollziehbar begründet werden. Die detaillierten Zielvorgaben hierzu sind in der ISO 21448 [55] zu finden. Im Fokus steht somit die OpSa-ML1 Generierung des Arbeitsprodukts WP-26 der SotiF-bezogenen Verifikations- und Validierungsstrategie gemäß „L_2-A. Erfasse Spezifikationen“ (siehe Schritt 1 Abbildung 8.31).

Hierbei werden wiederum Black-Box- bzw. Leistungsfähigkeitstests spezifiziert (siehe Tabelle C.39, Tabelle C.40 und Tabelle C.41). Diese dienen der Überprüfung der jeweiligen L_2-Systeme im Hinblick auf die Erfüllung der nicht-funktionalen Betriebssicherheitsanforderungen (siehe Tabelle C.38) bzw. der Einhaltung der maximalen Timing-Budgets der daraus aggregierten Fahrzeugreaktionszeit $t_{react} = 0.8\ s\ (800\ ms)$ gemäß der Betriebssicherheitsanforderung L1.19-OpSaReq.

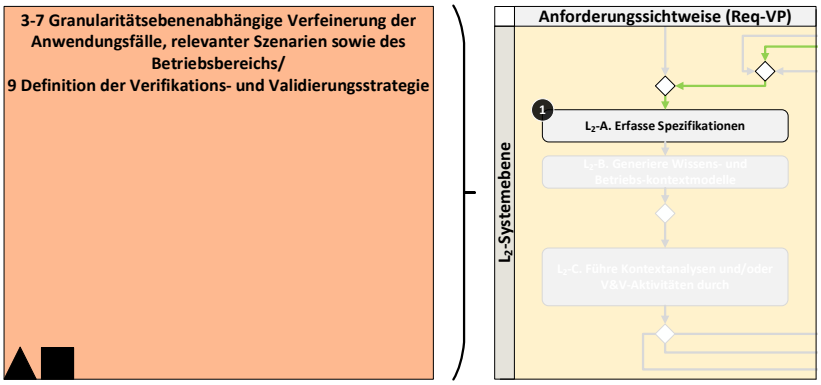


Abbildung 8.31: Durchzuführende Prozessabschnitte der Teile 3-7, und 9 sowie zugehörige Aktivitäten im Zuge des Top-Down-Übergangs in die L_2-Anforderungssichtweise.

8.2.2 Vorläufige Verifikation der Item Definition respektive der Spezifikation und des Designs gemäß der Konzeptphase

Auf Basis der SotiF-bezogenen Verifikations- und Validierungsstrategie wird nun die vorläufige Verifikation der Item Definition bzw. der Spezifikation und des Designs gemäß der Konzeptphase im Sinne von Teil 10 „Granularitätsebenenabhängige Bewertung bekannter Szenarien“ gemäß ISO 21448 inkl. Teil 3-7 „Granularitätsebenenabhängige Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs“ vorangetrieben. Dabei steht wiederum die Aktivität „L_2-C. Führe Kontextanalysen und/oder V&V-Aktivitäten durch“ im Vordergrund (siehe Schritt 1 Abbildung 8.32). Vor diesem Hintergrund werden die Zielvorgaben dahingehend verfolgt, ob das Item bzw. die beabsichtigte Systemfunktionalität sich wie spezifiziert verhalten. Weitere Einzelheiten hierzu sind in der ISO 21448 [55] zu finden. Insgesamt wird wiederum angestrebt, die OpSa-ML1 Generierung der Arbeitsprodukte bzw. Inkremente WP-82 und WP-37 der granularitätsebenenabhängigen Bewertung bekannter Szenarien unter Berücksichtigung der granularitätsebenenabhängigen Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs zu realisieren.

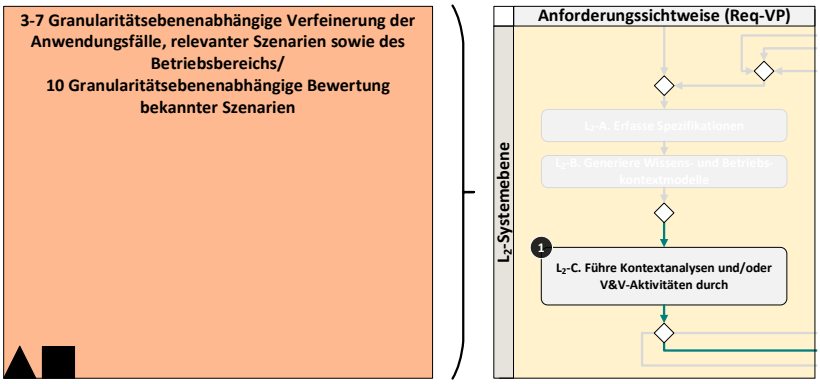


Abbildung 8.32: Durchzuführende Prozessabschnitte der Teile 3-7 und 10 sowie zugehörige Aktivität innerhalb der L_2-Anforderungssichtweise.

Zur Durchführung der frühzeitigen Verifikationsaktivitäten wird die Methode des regelungstechnischen Black-Box- bzw. Leistungsfähigkeitstests (vgl. Anhang A.5) im Hinblick auf das zu erwartende Übertragungsverhalten einschließlich der Reaktionszeiten der Systeme „L_2-Fahrzeugführung_L“, „L_2-EnergieUndAntrieb_L“ sowie „L_2-Chassis_L“ eingesetzt. Insgesamt liegt die Zielsetzung darin, im Zuge einer simulationsbasierten Überprüfung die Erfüllung bzw. Verifikation der nichtfunktionalen Betriebssicherheitsanforderungen in Bezug auf das dynamische Übertragungsverhalten zu gewährleisten. Dabei werden die jeweiligen Verhaltensmodelle mit einem Sollsprung am Eingang angeregt und deren analytisch dynamisches Verhalten ausgewertet. In Bezug auf das System „L_2-Fahrzeugführung_L“ wird die Zeitkonstante der Übertragungsfunktion, einschließlich einer Kommunikationslatenz von $0.01\ s$ $(10\ ms)$, berücksichtigt. Nach einer Zeit von $0.6\ s$ $(600\ ms)$ wird der Sollwert des Beschleunigungsbefehls (oben) bzw. des Verzögerungsbefehls (unten) erreicht (T_t-Verhalten gemäß Gl. A.4). Dadurch wird die Betriebssicherheitsanforderung L2.19-OpSaReq erfüllt (siehe Abbildung 8.33).

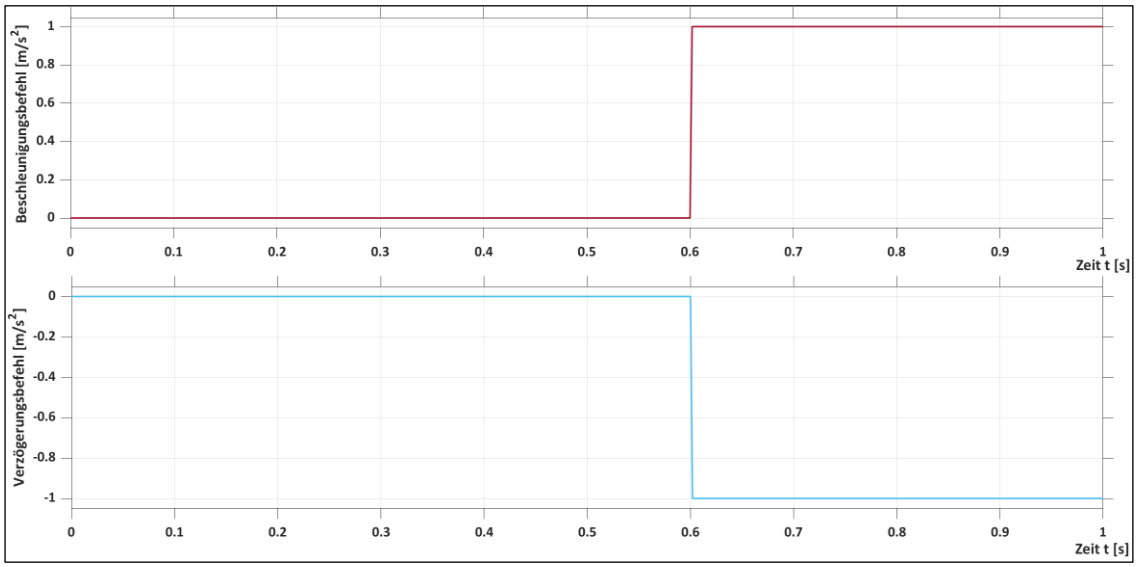


Abbildung 8.33: Analytisch dynamisches Verhalten des Systems „L_2-Fahrzeugführung_L“ im Hinblick auf „L_2-RegleAutomatisierte…LB“ gemäß dem Testfall L2.1-TC.

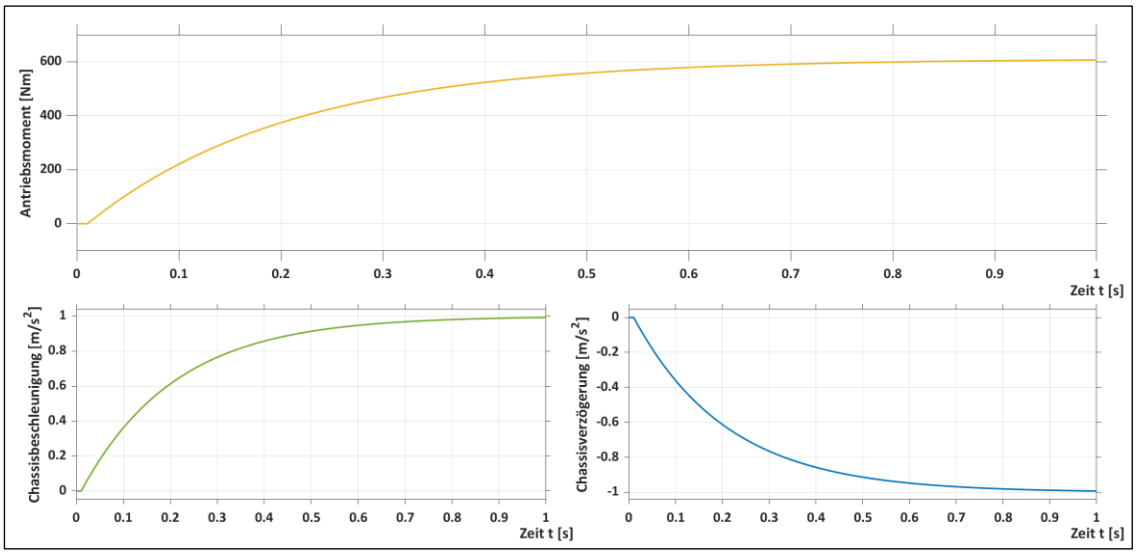


Abbildung 8.34: Analytisch dynamisches Verhalten der Systeme „L_2-EnergieUndAntrieb_L“ im Hinblick auf „L_2-StelleNotwendige…LB“ (oben) sowie „L_2-Chassis_L“ bezüglich „L_2-BefördereP assagiere…LB“ (unten) gemäß den Testfällen L2.2-TC und L2.3-TC.

Was die Systeme „L_2-EnergieUndAntrieb_L“ und „L_2-Chassis_L angeht, so werden die Zeitkonstanten der Übertragungsfunktionen einschließlich der Kommunikationslatenz von $0.01\ s\ (10\ ms)$ nach $0.2\ s\ (200\ ms)$ jeweils ca. $63\ \%$ des Sollwerts erreicht (PT_1T_t-Verhalten gemäß Gl. A.5), wodurch die Betriebssicherheitsanforderungen L2.20-OpSaReq und L2.21-OpSaReq erfüllt werden (siehe Abbildung 8.34).

Im Verlauf der durchgeführten simulationsbasierten Verifikationsaktivitäten werden keine Diskrepanzen zwischen dem erwarteten und dem tatsächlichen Verhalten der Systemreaktion als auch der Übertragungszeiten festgestellt (siehe Abbildung 8.33 und Abbildung 8.34). Dadurch wird das Item Freigabeartefakt L2-IR0.1 der frühzeitigen Verifikation generiert.

Tabelle 8.7: OpSa-ML1 Item Freigabe IR0.1.

<<Freigabe>>
ID: L20000IR0.1
L2-IR0.1 OpSa-ML1 Item Freigabe
Die Testfälle L2.1-TC, L2.2-TC und L2.3-TC wurden mittels regelungstechnischen Black-Box- bzw. Leistungsfähigkeitstests im Sinne einer eingangsseitigen Sollsprunganregung erfolgreich bestanden. Dadurch untermauern diese die analytisch dynamische Verifikation der Betriebssicherheitsanforderungen im Hinblick auf die Gesamtausführungszeiten und Kommunikationslatenz und somit die OpSa-ML1 Item Freigabe der Systeme „L_2-Fahrzeugführung_L“, „L_2-EnergieUndAntrieb_L“ und „L_2-Chassis_L“.

8.3 Virtueller Integrations- und Validierungszyklus gemäß des Bottom-Up-Übergangs der Konzept- in die Betriebskonzeptphase

Die oben beschriebenen Entwicklungsaktivitäten führen zum Abschluss der modellbasierten Systemspezifikation bzw. Item Definition. Um die darin generierten Anforderungen, Begründungen, Entwurfsentscheidungen und Entwurfsartefakte frühzeitig auf deren verhaltensbezogene Korrektheit im Gesamtkontext des L_1-Betriebsbereichs überprüfen zu können, erfolgt nachfolgend die direkte Überleitung in den virtuellen Integrations- und Validierungszyklus gemäß des Bottom-Up-Übergangs der Konzept- in die Betriebskonzeptphase (siehe Abbildung 8.35).

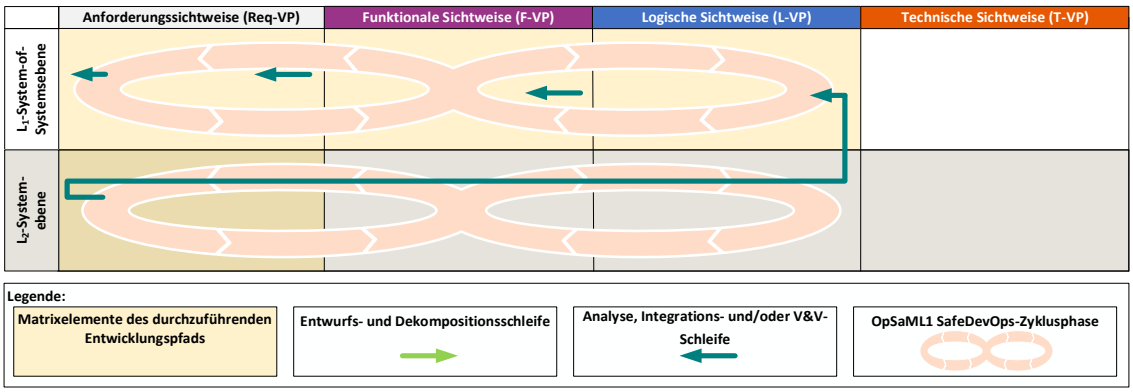


Abbildung 8.35: SPES-Matrix unter Hervorhebung der für das modell- und simulationsbasierte Betriebssicherheitskonzept relevanten Matrixelemente im Hinblick auf den virtuellen Integrations- und Validierungszyklus gemäß des Bottom-Up-Übergangs der Konzept- in die Betriebskonzeptphase (gelber Bereich).

Der dadurch eingeleitete Vorgang bezieht sich abermals auf die nachvollziehbare und rückverfolgbare Argumentation des Betriebssicherheitskonzepts im Hinblick auf Teil 3-6 „Betriebssicherheitsvalidierung“ sowie den darin verankerten Zielvorgaben 3-6.1. Dies wird durch frühzeitige simulationsbasierte Verifikations- und Validierungsaktivitäten gemäß „L_1-I. Führe logisch spezifische Analysen, Integrations- und/oder V&V-Aktivitäten durch“ sowie „L_1-C Führe Kontextanalysen und/oder V&V-Aktivitäten durch“ begleitet (siehe Schritt 1 und 2 Abbildung 8.36). Diese sollen durch zu generierende OpSa-ML1 Inkremente WP-11 und WP-76 bestätigen, dass das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ die gesetzlichen Anforderungen sowie die Betriebssicherheitsziele im Zuge der virtuellen Integration des Items im Sinne der logischen Systeme „L_2-Fahrzeugführung_L“, „L_2-EnergieUndAntrieb_L“, sowie „L_2-Chassis_L“ nach wie vor erfüllt. Hierbei werden zum einen die übergeordneten L_1-Interessenvertreteranforderungen herangezogen, woraus zum anderen die jeweiligen Testfälle L1.2-TC, L1.3-TC und L1.4-TC auf L_1-System-Of-Systemsebene hervorgehen. Anschließend geht es insbesondere darum, deren logisch spezifisches Gesamtverhalten in Bezug auf die jeweiligen Anforderungen und Betriebssicherheitsziele (siehe Tabelle C.15) der darüberliegenden L_1-Granularitätsebene innerhalb der Anforderungssichtweise virtuell zu validieren. Im weiteren Verlauf wird zur Durchführung der frühzeitigen Validierungsaktivitäten abermals die Methode der äquivalenzklassenbasierten Simulation im Hinblick auf die zu erwartenden Verhaltensweisen (siehe Tabelle C.18, Tabelle C.19, Tabelle C.20, Tabelle C.21, Tabelle C.22, Tabelle C.23 und Tabelle C.24) des „L_1-Ego-Kraftfahrzeugs_L“ als auch des definierten Betriebsbereichs eingesetzt (vgl. Unterabschnitt 8.1.6).

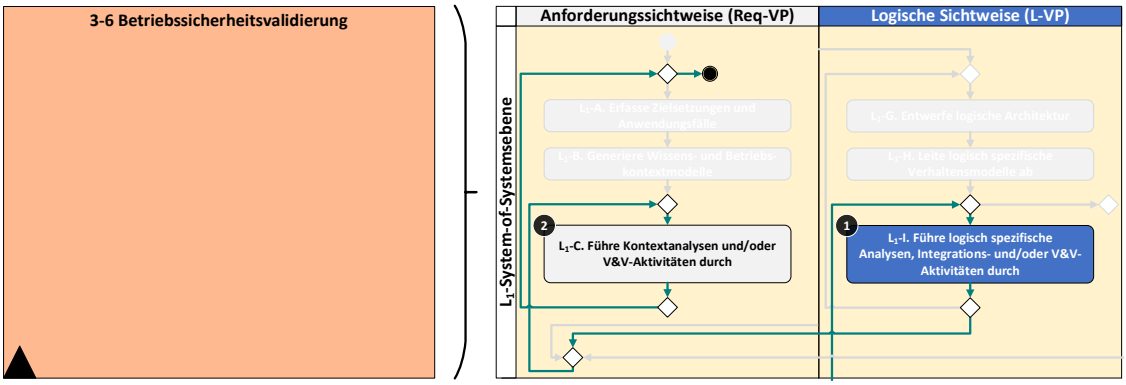


Abbildung 8.36: Durchzuführender Prozessabschnitt Teil 3-6 sowie zugehörige Aktivitäten im Zuge des Bottom-Up-Übergangs in die L_1-Logische Sichtweise respektive L_1-Anforderungssichtweise.

Von zentraler Bedeutung ist allerdings der dabei durchzuführende systematische Vergleich zwischen dem erwarteten und interpretierten Verhalten mit dem spezifischeren integrierten Gesamtverhalten auf L_1-Betriebsbereichs- bzw. L_1-System-Of-Systemebene. Neben der horizontalen Interaktion werden durch diese Herangehensweise auch die vertikale, ebenenübergreifende Abhängigkeiten systematisch berücksichtigt, wodurch die Entwurfsentscheidungen bezogen auf die jeweilige L_1/L_2-Granularitätsebene validiert werden können. Darunter fallen an dieser Stelle vornehmlich die jeweiligen Reaktionszeiten der Systeme „L_2-Fahrzeugführung_L“, “L_2-EnergieUndAntrieb_L“ sowie „L_2-Chassis_L“ einschließlich der Berücksichtigung der Kommunikationslatenz untereinander.

Vor diesem Hintergrund werden die im Verlauf der Item Definition entwickelten Verhaltensmodelle in Bezug auf „L_2-Fahrzeugführung_L“, „L_2-EnergieUndAntrieb_L“ sowie „L_2-Chassis_L“ in die Gesamtfahrzeugdynamik des „L_1-Ego-Kraftfahrzeug_L“ eingebettet. An dieser Stelle wird die ursprünglich im Betriebssicherheitskonzept beschriebene Fahrzeugdynamik (vgl. Gl. 8.8, 8.9 und 8.10), anhand der Plug-and-Play Modellein- und Modellausblendung dahingehend modifiziert (vgl. Unterabschnitt 7.4.2), um nun unter Berücksichtigung des Item- bzw. Systemverhaltens die Gesamtfahrzeugdynamik detaillierter und aussagekräftiger zu repräsentieren (siehe Abbildung C.3).

Für die Bewegung in X_E-Koordinaten ergibt sich durch Einsetzen von Gl. 8.15, Gl. 8.17 und Gl. 8.18 in die ursprüngliche Gl. 8.8

$$a_{X_E} = \underbrace{\left(\frac{1}{m}\left(\frac{1}{r_{dyn}}(i_{tot}\eta_{tot}M_D + M_B) - F_{WX} - F_{RX}\right)\right)}_{a_x}\cos\psi - \underbrace{G_{a_Y}(s)G_{a_{Y,req}}(s)}_{a_y}\,sin\psi - \underbrace{G_{\psi}(s)G_{\psi_{req}}(s)}_{\dot{\psi}}\,(v_X sin\psi - v_Y cos\psi) \tag{8.19}$$

als Zusammenhang. Die Querdynamik in globalen Y_E-Koordinaten wird durch Einfügen von Gl. 8.15, Gl. 8.17 und Gl. 8.18 in Gl. 8.9

$$a_{Y_E} = \underbrace{\left(\frac{1}{m}\left(\frac{1}{r_{dyn}}(i_{tot}\eta_{tot}M_D + M_B) - F_{WX} - F_{RX}\right)\right)}_{a_x} sin\psi \tag{8.20}$$

$$+\underbrace{G_{a_Y}(s)G_{a_{Y,req}}(s)}_{a_y} cos\psi + \underbrace{G_{\psi}(s)G_{\psi_{req}}(s)}_{\dot{\psi}} (v_X cos\psi - v_Y sin\psi)$$

beschrieben. Für die Drehung um die Z_E-Achse gilt durch Einsetzen von Gl. 8.18 in Gl. 8.10

$$\dot{\psi} = G_{\psi}(s)G_{\psi_{req}}(s) \qquad 8.21$$

als Abbildung der Kurswinkelrate.

Die jeweiligen Geschwindigkeiten v_X und v_Y sowie der Kurs- bzw. Gierwinkel ψ ergeben sich durch Integration der Beschleunigungen a_X sowie a_Y und $\dot{\psi}$. Der Zusammenhang im Hinblick auf die Quer- und Kurswinkelabweichung gemäß Gl. 8.11 und Gl. 8.12 bleibt an dieser Stelle unverändert. Abbildung 8.37 visualisiert hierbei einen exemplarisch extrahierten Testschritt.

Hierbei wird das spezifischere integrierte Gesamtverhalten dem Verhalten gemäß der vorläufigen Betriebssicherheitsverifikation und -validierung (vgl. Unterabschnitt 8.1.6) gegenübergestellt (siehe Abbildung 8.37). Zudem erweisen sich die fahrdynamischen Betrachtungen im Hinblick auf die kombinierten Längs- und Querführung im Zuge eines gekrümmt verlaufenden „L_1-Fahrbahnbereichs_L“ weiterhin als zweckdienlich, wodurch das „L_1-Ego-Kraftfahrzeug_L“ auch unter dem Einfluss starker Notbremsmanöver in Längsrichtung der gekrümmten Sollbahn im querdynamischen Gleichgewichtszustand folgen kann (siehe Abbildung 8.38). Im Anschluss wird wiederum der definierte Parameterbereich der Testfälle L1.2-TC, L1.3-TC und L1.4-TC simulativ abgetastet und in Form von Konturdiagrammen mit den Achsen initialer Relativabstand und initiale Relativgeschwindigkeit dargestellt wird. Die jeweiligen Verläufe kennzeichnen sich hinsichtlich Relativabstand und Relativgeschwindigkeit durch eine angemessene Übereinstimmung im Vergleich zum reinen L_1-Simulationsmodell (siehe Abbildung C.1 im Vergleich zu Abbildung 8.20). Auch in Bezug auf Relativabstand, Relativgeschwindigkeit sowie Ego-Kraftfahrzeugbeschleunigung erweisen sich die jeweiligen Verläufe im Vergleich zum reinen L_1-Simulationsmodell als adäquat (siehe Abbildung C.2 im Vergleich zu Abbildung 8.21).

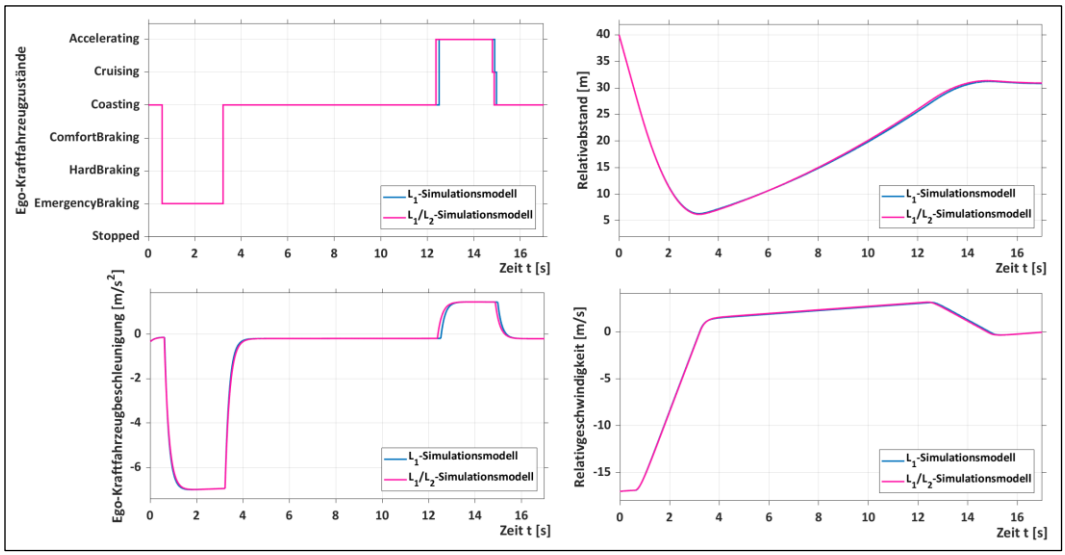


Abbildung 8.37: Vergleich des rein auf L_1-Granularitätsebene definierten L_1-Simulationsmodells mit dem L_1/L_2-Simulationsmodell bezüglich eines exemplarisch extrahierten Testschritts des „Cut-In-Testfalls“ L1.4-TC.

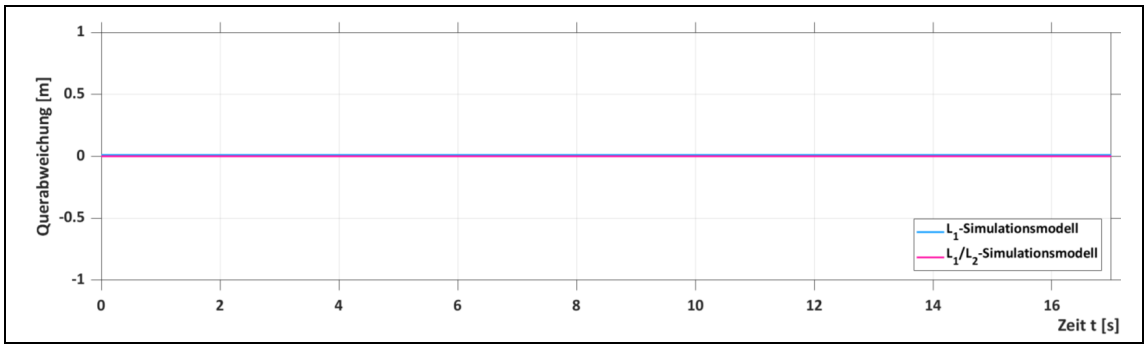


Abbildung 8.38: Vergleich des rein auf L_1-Granularitätsebene definierten L_1-Simulationsmodells mit dem L_1/L_2-Simulationsmodell hinsichtlich Querabweichung gemäß eines exemplarisch extrahierten Testschritts des „Cut-In-Testfalls" L1.4-TC.

Im Verlauf der durchgeführten simulationsbasierten Verifikations- und Validierungsaktivitäten werden insgesamt keine Diskrepanzen zwischen dem erwarteten und tatsächlichen simulationsbasierten Verhalten detektiert. Infolgedessen kann das Betriebsbereichsfreigabeartefakt L1-ODDR0.2 der erfolgreichen frühzeitigen Validierungsaktivitäten generiert werden. Genauer genommen handelt es sich hierbei um die Validität der Modellierungsannahmen und Entwurfsentscheidungen auf den L_1/L_2-Granularitätsebenen, was die Systemreaktionszeiten unter Berücksichtigung der latenzbehafteten Interaktion der L_2-Systemelemente angeht.

Es sei an dieser Stelle erneut darauf hingewiesen, dass zu diesem frühen Entwicklungszeitpunkt eine simulationsbasierte Validierung der Spurhaltung im Sinne der Querführung weiterhin ausschließlich für konstante Kurvenfahrten durchgeführt werden kann. Insbesondere können Einflüsse wie Sollsprünge der Krümmung, Auslenkungen aus der statischen Ruhelage, Störgrößen oder ähnliche Effekte innerhalb der Ego-Fahrspur noch nicht adäquat bewertet werden. Daher müssen Testfälle, die dynamische Querführungsmanöver außerhalb des statischen Gleichgewichtszustands berücksichtigen, zu einem späteren Entwicklungszeitpunkt auf L_3/L_4-Granularitätsebene durchgeführt werden. Hierfür werden umfassendere dynamische Modelle benötigt, welche regelungstechnische Algorithmen in die Fahrzeugarchitektur einbeziehen. Dies umfasst die Bereiche Umgebungswahrnehmung, Planung, Regelung und Aktuatorik im Hinblick auf L_3-Subsysteme, L_4-Komponenten bis hin zu L_5-Einheiten.

Tabelle 8.8: OpSa-ML1 Betriebsbereichsfreigabe ODDR0.2 unter Berücksichtigung der virtuellen Item- bzw. Systemintegration.

<<Freigabe>>
ID: L10000ODDR0.2
L1-ODDR0.2 OpSa-ML1 Betriebsbereichsfreigabe unter Berücksichtigung der virtuellen Item-bzw. Systemintegration
Die Testfälle L1.2-TC, L1.3-TC und L1.4-TC wurden unter Berücksichtigung der physikalischen Gesetzmäßigkeiten eines Punktemassemodells für die konstante Kurvenfahrt und unter Berücksichtigung der analytisch dynamischen Gesamtausführungszeiten und Kommunikationslatenz der virtuell integrierten L_2-Systeme bestanden. Dadurch untermauern diese die Betriebssicherheitsargumentation sowie die OpSa-ML1 Betriebsbereichsfreigabe der Fahrzeugverhaltensspezifikation des „L_1-Ego-Kraftfahrzeugs_L" im Hinblick auf die Interaktion mit dem „L_1-Verkehrsteilnehmer_L" auch unter dem Einfluss des L_2-Systemverhaltens. Eine analytisch dynamische Validierung der Spurhaltung im Sinne der Querführung außerhalb des statischen Gleichgewichtszustands konnte weiterhin nicht durchgeführt werden. Hierfür werden umfassendere dynamische Modelle benötigt, welche regelungstechnische Algorithmen in die Fahrzeugarchitektur einbeziehen.

8.4 Fazit des modell- und simulationsbasierten Betriebssicherheitskonzepts

Im Verlauf dieses Kapitels wurde der agile Betriebssicherheitslebenszyklusprozess im Hinblick auf ein modellbasiertes und simulativ ausführbares Betriebssicherheitskonzept für die Längs- und Querführung eines hochautomatisierten SAE-Level-4-Autobahnpiloten umgesetzt. Das gestaltete Betriebssicherheitskonzept umfasst die L_1-System-Of-Systemsebene bis einschließlich des Übergangs in die L_2-Systemebene und berücksichtigt eine der vier wesentlichen Sicherheitsthemen des hochautomatisierten Fahrens. Hierunter handelt es sich um die Spezifikation einer regelkonformen Fahrzeugverhaltensspezifikation. Auf Grundlage eines hierfür definierten hierarchisch strukturierten Betriebsbereichs wurde eine StVO-konforme Fahrverhaltensspezifikation des Autobahnpiloten systematisch auf Basis der menschlichen Längshomöstase hergeleitet (vgl. Unterabschnitt 8.1.5) und anhand architekturell integrierter simulativ ausführbarer Verhaltensmodelle sowie unter Berücksichtigung von Kurvenfahrten evaluiert (vgl. Unterabschnitt 8.1.6).

Insgesamt wurde ein speziell auf den Problemfall abgestimmter Entwicklungsablauf sowie ein Leitfaden vorgestellt, der sowohl top-down als auch bottom-up durch die verschiedenen Granularitätsebenen und Sichtweisen des SPES-Modellierungsrahmenwerks führt. Dieser Ansatz ermöglicht eine strukturierte und durchgängige Betrachtung der Betriebssicherheit, indem alle relevanten Modellierungsebenen integriert betrachtet werden. Entlang der SafeDevOps-Zyklen des Multiple-SafeDevOps-V-Modells erfolgten eine iterative Generierung und virtuelle OpSa-ML1 Freigabe der jeweils erforderlichen betriebssicherheitsbezogenen Arbeitsprodukte bzw. Inkremente. Diese iterativ-inkrementelle Vorgehensweise gewährleistet eine kontinuierliche Integration und Bereitstellung sowie die Verifikation und Validierung der Betriebssicherheitsanforderungen. Dabei wird eine enge Verzahnung zwischen Entwicklung und Entwurf einerseits und dem virtuellen Betrieb gemäß szenariobasiertem Testen bis hin zu Realfahrten andererseits sichergestellt. Die dabei entwickelte iterativ-inkrementelle Betriebssicherheitsnachweisführungskette ist modular aufgebaut und ermöglicht eine schrittweise Erweiterung sowie Anpassung an unterschiedliche Systemanforderungen und Betriebskontexte. Dadurch kann diese nahtlos auf den gesamten Betriebssicherheitslebenszyklusprozess ausgeweitet bzw. skaliert werden. Dies stellt sicher, dass der Nachweis der Betriebssicherheit auch bei zunehmenden Systemumfängen konsistent gehalten werden kann.

9 Schlussfolgerung und Ausblick

Zum Abschluss dieser Dissertation wird nachfolgend ein Resümee über die vorgestellten Ansätze, Methoden und Ergebnisse gezogen als auch der wissenschaftliche Beitrag hervorgehoben. Im Ausblick werden Themen dargelegt, welche im Rahmen der vorliegenden Arbeit nicht oder nur unvollständig behandelt wurden und Anknüpfungspunkte für zukünftige Forschungsarbeiten repräsentieren.

9.1 Zusammenfassung und wissenschaftlicher Beitrag

Im Rahmen dieser Dissertation wurde ein agiler Systementwicklungsansatz für den modellbasierten Betriebssicherheitsnachweis hochautomatisierter Fahrzeuge entlang von drei Konzeptionsphasen gestaltet. Hierfür wurde im Verlauf der ersten Konzeptionsphase ein Betriebssicherheitslebenszyklusprozess für die Hochautomatisierung von Kraftfahrzeugen aufgesetzt (vgl. Abschnitt 7.2). Dieser basiert auf den Prozessphasen und -abschnitten des ISO 26262 bzw. ISO 21448 V-Modells und bietet eine vertikale Erweiterung und Vertiefung, um eine Top-Down-Ableitung des Zusammenspiels der System-Of-Systems (Ego-Kraftfahrzeug, andere Verkehrsteilnehmer, V2X-Kommunikationssysteme etc.) innerhalb der gesamten Mobilitätsinfrastruktur und ihres Betriebsbereichs beginnend auf System-Of-Systemsebene sicherzustellen (vgl. AF-1 und AF-3).

Dabei handelt es sich um die ganzheitliche betriebsbereichszentrierte Perspektive auf die jeweiligen Sicherheitsthemen (vgl. AF-4), was insbesondere die Beherrschung inakzeptabler Risiken hervorgerufen durch Fehlfunktionen in den an der Ausführung der Funktion beteiligten E/E-Systemen (vgl. HF-6), Unzulänglichkeiten der beabsichtigten Funktionalität selbst (vgl. HF-3), eine unzureichende regelkonforme und ethisch vertretbare Fahrzeugverhaltensspezifikation (vgl. HF-9) sowie vorhersehbaren, vorsätzlichen oder versehentlichen Fehlgebrauch als auch Defizite der Mensch-Maschine-Interaktion angeht (vgl. HF-5). Dies resultiert in einem gesamtheitlichen Betriebssicherheitsentwicklungsansatz für die Hochautomatisierung der Fahraufgabe, welcher für die Aufrechterhaltung eines prozessualen Gesamtüberblicks die verschiedenen Sicherheitsthemen konsistent zusammenführt und miteinander verknüpft.

Zudem gründet der Betriebssicherheitslebenszyklusprozess auf einer strukturierten Nachweisführungskette Evidenz, Argument und Behauptung, welche granularitätsebenenübergreifend die Erstellung eines nachvollziehbaren sowie rückverfolgbaren Betriebssicherheitsnachweises einschließlich der hierarchischen Top-down- und Bottom-up-Anforderungsentwicklung unterstützt (vgl. AF-2). Im Zuge der zweiten Konzeptionsphase wurde der Entwicklungsablauf des Betriebssicherheitslebenszyklus horizontal mit dem Automotive-PEP sowie im Sinne eines Multiple-SafeDevOps-V-Modells entlang von Reifegradabsicherungsmeilensteinen synchronisiert (vgl. Abschnitt 7.3).

Das Multiple-SafeDevOps-V-Modells ermöglicht hierbei die konsistente Zusammenführung des klassischen V-Modells der Automotive-Sicherheitsentwicklung und agiler Entwicklungsansätze (vgl. AF-18). Darüber hinaus wird eine zielgerichtete Vorgehensweise vorgestellt, die aufzeigt, wie und anhand welcher Struktur die einzelnen Sprints bzw. Iterationen entlang des Betriebssicherheitslebenszyklusprozesses geplant und koordiniert werden sollten. Dies führt zu einem klar definierten Rahmenwerk mit dedizierten Qualitätskriterien, welche innerhalb der jeweiligen Sprints oder Zyklen des Multiple-SafeDev-Ops-V-Mo-

dells erreicht werden müssen. Zudem wurde eine methodische Verknüpfung der Iterationen und Inkremente entwickelt, so dass diese aufeinander abgestimmt und mit dem Ablauf des Automotive-PEPs harmonisiert werden können (vgl. AF-19).

Diese Konstellation ermöglicht die prozessorientierte Einbindung der Serienphase bzw. des Feldbetriebs, wobei ein iterativer, kontinuierlicher Entwicklungs-, Integrations-, Test- und Bereitstellungszyklus konzipiert werden konnte (vgl. HF-13). Dieser besteht wiederum aus in die Entwurfsphasen systematisch zurückgeführten Feedbackpipelines aufgezeichneter Daten, um dann gemäß der kontinuierlichen Integration, des kontinuierlichen Testens sowie der kontinuierlichen Bereitstellung von inkrementellen Updates, Anpassungen, Erweiterungen und Verbesserungen ins Feld ausgerollt zu werden.

Im Verlauf der dritten Konzeptionsphase erfolgte die methodische Anbindung des agilen Betriebssicherheitslebensprozesses an die modellbasierte Systementwicklung gemäß dem SPES-Modellierungsrahmenwerk (vgl. Abschnitt 7.4). Dieses führt schrittweise durch die Prozessphasen, -abschnitte und -schritte des Betriebssicherheitslebenszyklusprozesses. Der gestaltete Entwicklungsablauf bildet eine strukturierte Systematik für den Umgang mit dem fragmentarischen, iterativ verfeinerten Wissen über den betrieblichen System-Of-Systems-Entwurf, den System- und Subsystementwurf (einschließlich von Entwurfsalternativen), die Implementierung der Komponenten und Einheiten sowie der erforderlichen Verifikations- und Validierungsargumentation über alle Granularitätsebenen hinweg (vgl. AF-13). Dies ermöglicht ein erweitertes Verständnis sogenannter offener Kontextsysteme (z.B. hochautomatisiertes Ego-Kraftfahrzeug und relevanter Teil der Umgebung im Sinne des Betriebsbereichs), der Wechselwirkungen und gegenseitigen Abhängigkeiten sowie potenzieller Unzulänglichkeiten (d.h. Annahmen, Hypothesen, Einschränkungen, die vorübergehend oder dauerhaft ungültig sind vgl. HF-12).

Ein weiteres Werkzeug des im Rahmen dieser Dissertation weiterentwickelten SPES-Modellierungsrahmenwerks ist die nahtlose Einbindung von Simulationen analytisch dynamischer Verhaltensspezifikationen, einschließlich des szenariobasierten Testens (vgl. HF-4). Zwar lässt sich eine vollständige Simulation offener Kontextsysteme nicht verwirklichen, jedoch kann ein signifikanter Anteil für die Analyse von Szenarien und daher Evidenzen zur Untermauerung des ausgearbeiteten robusten Entwurfs, der definierten Metriken und Akzeptanzkriterien, der Wiederherstellungs- und Degradationsstrategien etc. frühzeitig im Entwurfsprozess zur Verfügung gestellt werden. Mit anderen Worten, verstärkt und bekräftigt die Simulation diejenigen Argumente, welche im Pfeiler des Systemverständnisses gebildet wurden. Insgesamt charakterisiert sich das an dieser Stelle auf Basis der SPES-Matrix konzipierte Modellierungsrahmenwerk als ein möglicher Schritt in Richtung einer von Umeda [315] als „ideale Funktionsmodellierung“ designierten Herangehensweise: *„Die ideale Funktionsmodellierung sollte daher Funktionen und physikalische Strukturen nahtlos über Verhaltensweisen abbilden und den schrittweisen Beschreibungsprozess von Funktionen und physikalischen Strukturen parallel zur Beibehaltung der Abbildung über Verhaltensweisen und in einer bidirektionalen Weise unterstützen, d.h. vom Abstrakten zum Konkreten im Entwurf und vom Elementaren zum Ganzen in der Interpretation wie z.B. der Fehlerdiagnose.“* Dieser Kerngedanke wird über die gesamte Vorgehensweise verfolgt.

Abschließend wurde der modell- und simulationsbasierte Betriebssicherheitsentwicklungsansatz bezüglich der Längs- und Querführung eines hochautomatisierten Level 4 Autobahnpiloten umgesetzt (vgl. Kapitel 1). Im Zuge dessen wurde ein exemplarisch darauf zugeschnittener Entwicklungsablauf dargelegt, welcher sowohl top-down als auch bottom-Up rekurrierend über die jeweiligen Granularitätsebenen und Sichtweisen des SPES-Modellierungsrahmenwerks hinweg führt. In diesem Kontext wurde die modellbasierte Beschreibung der Gesamtarchitektur des hochautomatisierten Autobahnpiloten innerhalb seines Betriebsbereichs durch die präzise Abfolge von Aktivitäten im Sinne des „WIE“ veranschaulicht. Dabei

wurde aufgezeigt, in welcher Weise die erforderlichen Anforderungen für die Konzeption eines simulationsbasierten Betriebssicherheitskonzepts systematisch und hierarchisch strukturiert abgearbeitet werden können, um diesen als Hauptliefergegenstand im Sinne des „WAS" zu generieren. In dieser Hinsicht wurden Kontextanalysemethoden wie SOCA (vgl. Anhang A.8) sowie modellbasierte Analyse- und Testmethoden inkl. des szenariobasierten Testens (vgl. Abschnitt 4.7 und 4.8) systematisch in das Modellierungsrahmenwerk eingearbeitet und nahtlos umgesetzt.

Das dabei konzipierte Betriebssicherheitskonzept erstreckt sich angefangen von der L_1-System-Of-Systemsebene bis hin zum Übergang in die L_2-Systemebene und berücksichtigt exemplarisch eine der vier zentralen Sicherheitsthemen des hochautomatisierten Fahrens, worunter zunächst die Beherrschung inakzeptabler fahrzeugregelungsbezogener Risiken hervorgerufen durch Unzulänglichkeiten der Herleitung einer verkehrsregelkonformen Fahrzeugverhaltensspezifikation. Im Hinblick darauf wurde auf Grundlage des übergeordneten Anwendungsfalls „L_1-FolgeFahrstreifen…UC“ als auch eines hierfür definierten Betriebsbereichs eine StVO-konforme Fahrverhaltensspezifikation des Autobahnpiloten systematisch hergeleitet und simulativ bewertet. Insgesamt ging es darum, eine funktionale und logische Architekturrepräsentation eines hochautomatisierten Kraftfahrzeugs eingebettet in dessen Betriebsbereich unter Anwendung des SPES-Rahmenwerks modell- und simulationsbasiert zu entwickeln. Im Einklang dazu wurde wiederum dessen analytisch dynamisches Verhalten auf einem Autobahnabschnitt in einer virtuellen Simulationsumgebung unter Anwendung von Methoden des szenariobasierten Testens validiert (vgl. Unterabschnitt 8.1.5, 8.1.6 und Abschnitt 8.3).

Zusammenfassend stellen die nachfolgenden Abhandlungen den wissenschaftlichen Beitrag der vorliegenden Dissertation nochmals kompakt dar:

- Der aus der ISO 26262 bzw. ISO 21448 abgeleitete und um Themen der Kraftfahrzeug- und Verkehrsumgebung als auch des Feldbetriebs sowohl vertikal als auch horizontal erweiterte Betriebssicherheitslebenszyklusprozess stellt aufgrund der ganzheitlichen Sicherheitsbetrachtung eine Neuerung im Hinblick auf die Prozesssäule dar. Dadurch werden die unterschiedlichen Sicherheitsthemen in Bezug auf die Hochautomatisierung der Fahraufgabe konsistent und kohärent miteinander in Einklang gebracht und strukturell entlang der Nachweisführungskette Evidenz, Argument und Behauptung zusammengeführt.

- Das Multiple-SafeDevOps-V-Modell bietet einen strukturierten Ansatz, der die Stärken des klassischen V-Modells mit den Stärken agiler Entwicklungsansätzen vereint. Dadurch wird ein agiler Betriebssicherheitsentwicklungsprozess geschaffen, der eine kontinuierliche Bewertung und Bereitstellung sicherheitskritischer, softwarebasierter Systeme ermöglicht. Im Sinne des „Teile-und-Herrsche“-Prinzips fördert das dabei geschaffene Vorgehensmodell die Entwicklung, das Testen und die Bereitstellung entlang eines stufenweise bzw. iterativ ansteigenden Betriebssicherheitsreifegrads von inkrementellen Teilfunktionalitäten.

- Der agile Betriebssicherheitslebenszyklusprozess bringt die zeitlich und organisatorisch verteilten Entwicklungsphasen inkl. Musterstände, Fahrfreigaben etc. des PEPs sowie die Sicherheitsentwicklungsaktivitäten gemäß Multiple-SafeDevOps-V-Modell im Sinne eines ganzheitlichen Projekt- und Betriebssicherheitsplans miteinander in Einklang. Des Weiteren wird eine zusätzliche Fokussierung und systematische Einbindung der Serienphase bzw. des Feldbetriebs bereitgestellt.

- Der modell- und simulationsbasierte Betriebssicherheitsentwicklungsansatz repräsentiert ein ganzheitliches Vorgehensmodell, welches die Generierung eines modellbasierten Betriebssicherheitsnachweises entlang der Säulen Prozess, modellbasierte Methode, Modellierungssprache und Modellierungswerkzeug ermöglicht. Insbesondere wird dadurch der Weg für eine simulativ ausführbare Spezifikation, Analyse und Absicherung des Verhaltens eines hochautomatisierten Kraftfahrzeugs in dessen Betriebsbereich geebnet.

- Der modell- und simulationsbasierte Betriebssicherheitsentwicklungsansatz schließt im Sinne der Methodensäule die Lücke zwischen der modellbasierten Systementwicklung, der Simulationsentwicklung sowie der Automotive-Sicherheitsentwicklung. In dieser Hinsicht kann dieses je nach Anwendungs- und Problemfall flexibel auf einen projekt- und/oder organisationsspezifischen Entwicklungsablauf zugeschnitten werden. Ferner gestattet der modell- und simulationsbasierte Betriebssicherheitsentwicklungsansatz eine nahtlose Integration und eine anwenderspezifische Erweiterung in Bezug auf Methoden der Sicherheitsanalyse, der Kontextanalyse, des szenariobasierten Testens sowie ggf. neu aufkommender Methoden, z.B. aus dem VVM-Projektkontext (vgl. Abschnitt 4.8), für die Verifikation und Validierung der Betriebssicherheit des hochautomatisierten Fahrens.

- Hinzu kommt mittels des modell- und simulationsbasierten Betriebssicherheitsentwicklungsansatzes die Einbettung der modellbasierten Systementwicklung innerhalb des Betriebssicherheitslebenszyklusprozesses für das hochautomatisierte Fahren. Des Weiteren erfolgt eine konsequente Berücksichtigung dessen, was die Thematik einer systematischen Verifikation und Validierung von Annahmen, Hypothesen und Einschränkungen über den gesamten Modellierungsvorgang angeht. Dabei wird ein systematisches Verständnis und eine Bewusstseinsschaffung im Hinblick auf Entscheidungsfindungen ermöglicht.

- Darüber hinaus beinhaltet der modell- und simulationsbasierte Betriebssicherheitsentwicklungsansatz eine eindeutige Differenzierung zwischen Problemanalyse und Lösungsfindung (Problemraum vs. Lösungsraum) und stellt darauf basierend anwender- und rollenspezifische Sichtweisen in Bezug auf die zu generierenden Systemmodelle bereit. Zudem wird eine strukturierte und hierarchische Systemarchitekturbetrachtung und -dekomposition ausgehend von System-Of-Systems in Systeme, Subsysteme, Komponenten sowie Einheiten im Sinne der Kapselung als auch Modularisierung anhand von Granularitätsebenen über die anwender- und rollenspezifischen Sichten hinweg integriert.

- Außerdem wird mit Hilfe des modell- und simulationsbasierten Betriebssicherheitsentwicklungsansatzes eine iterativ-inkrementelle und somit ein konsistentes Entwickeln entsprechender Systemmodelle verwirklicht. Im Speziellen geht es hierbei um die kohärente Synthese als auch Analyse funktionaler, logischer und technischer Architekturen sowie eine darauf konsistent abgebildete Verhaltensmodellierung. Dies ermöglicht wiederum eine integrierte disziplinübergreifende Verhaltensspezifikation und frühzeitige Simulation, welche zu späteren Entwicklungsphasen durch disziplinspezifische realisierungsabhängige Simulationen über die Granularitätsebenen mit höherem Detaillierungsgrad sowie die anwender- und rollenspezifischen Sichtweisen hinweg nahtlos vervollständigt werden kann.

9.2 Bewertung des wissenschaftlichen Beitrags

Die im Rahmen dieser Dissertation formulierten Forschungsfragen (vgl. Abschnitt 1.2) lassen sich vor dem Hintergrund der in Abschnitt 9.1 dargestellten Ergebnisse beantworten. Des Weiteren erfolgt eine systematische Bewertung des entwickelten wissenschaftlichen Beitrags der Dissertation anhand der in Abschnitt 1.2 festgelegten Kriterien sowie eine methodische Einordnung der zur Ausgestaltung des Prozesses erforderlichen Modellierungs-, Analyse- und Verifizierungsverfahren.

9.2.1 Beantwortung der Forschungsfragen

- **FF 1: Wie lässt sich ein Lebenszyklusprozess entwickeln, der die Automotive-Sicherheitsnormen ISO 26262 und ISO 21448 erweitert, um die Betriebssicherheit hochautomatisierter Fahrfunktionen sicherzustellen?**

  Die eingeführte vertikale Sicherheitslebenszykluserweiterung im Sinne der Betriebskonzeptphase (vgl. Abschnitt 7.2) adressiert die Lücken zwischen existierenden Sicherheitsnormen und den Anforderungen offener sowie hochvariabler Betriebsbereiche hochautomatisierter Fahrfunktionen. Sie schafft somit die prozessuale Grundlage, diese Aspekte normativ abzubilden und in zukünftigen Standardisierungsaktivitäten berücksichtigen zu können. Diese vertikale Erweiterung stellt damit einen wissenschaftlichen Beitrag zur Weiterentwicklung sicherheitsbezogener Normlandschaften dar.

- **FF 2: Wie kann dieser betriebssicherheitsbezogene Lebenszyklusprozess ausgestaltet werden, um eine agile und industrielle Umsetzung zu ermöglichen?**

  Die horizontale Sicherheitslebenszykluserweiterung (vgl. Abschnitt 7.3) bekräftigt, dass eine agile und industrielle Umsetzung durch die Einführung eines strukturierten, über alle Entwicklungsphasen hinweg ausrollbaren Betriebssicherheitsentwicklungsansatzes vorangetrieben werden kann. Dieser Ansatz koppelt die sicherheitsrelevanten Entwicklungs-, Integrations-, Verifikations- und Bereitstellungsaktivitäten in Form eines Multiple-SafeDevOps-V-Modells und ermöglicht damit eine operationalisierte Verbindung zwischen dem normativen Sicherheitslebenszyklus und den Abläufen des Automotive-PEP. Dadurch wird eine durchgängig agile und kontinuierlich operative Umsetzung des Betriebssicherheitslebenszyklusprozesses innerhalb industrieller Projekte realisierbar. Folglich beantwortet die horizontale Erweiterung die Frage, wie der normativ erweiterte Sicherheitslebenszyklus (FF 1) in die industrielle Realität überführt werden kann.

- **FF 3: Wie kann dieser agile Betriebssicherheitslebenszyklusprozess im Rahmen eines modellbasierten Systementwicklungsrahmenwerks methodisch und praktisch umgesetzt werden?**

  Durch die Verknüpfung von Architektur- und Verhaltensmodellen entlang funktionaler, logischer und technischer Sichten entsteht ein konsistenter modellbasierter Betriebssicherheitsentwicklungsansatz (vgl. Abschnitt 7.4), welcher anhand des Fallbeispiels des hochautomatisierten Autobahnpiloten von Kapitel 8 als industriell umsetzbar und praktikabel dargelegt wird. Zusammengefasst repräsentiert die modellbasierte Umsetzung das Bindeglied, welches die normativ beschriebene vertikale Erweiterung (FF 1) und die industriell benötigte horizontale Erweiterung (FF 2) in einen praktisch anwendbaren, formalisierten Entwicklungs- und Nachweisprozess überführt.

9.2.2 Evaluierung des wissenschaftlichen Lösungsansatzes anhand definierter Kriterien

Die tabellarische Evaluierung der erarbeiteten Lösungsansätze der vorliegenden Dissertation umfasst die Skala „sehr niedrig“, „niedrig“, „mittel“, „hoch“ und „sehr hoch“ hinsichtlich der in Abschnitt 1.2 als wissenschaftlicher Bewertungsrahmen spezifizierten Kriterien (siehe Tabelle 9.1).

Tabelle 9.1: Bewertung der Dissertationsergebnisse entlang definierter Kriterien.

Kriterium	Bewertung	Begründung / Bezug zur vorliegenden Dissertation
Skalierbarkeit	Hoch	Die Skalierbarkeit des Ansatzes ist als hoch einzustufen. Durch das Multiple-SafeDevOps-V-Modell wurde ein Rahmen geschaffen, welcher modular und konsistent über die System-of-Systems-, System-, Subsystem-, Komponenten- und Einheitenebene angewendet werden kann. Die iterativ-inkrementelle Reifegradsteigerung (OpSa-ML1 bis ML4) unterstützt den Einsatz des Prozesses sowohl in frühen Konzeptphasen als auch in fortgeschrittenen Integrations- und Validierungsphasen bis einschließlich der Phase des Betriebs.
Kompatibilität	Sehr hoch	Der Betriebssicherheitslebenszyklusprozess repräsentiert eine normkonforme und stufenweise Erweiterung zur ISO 26262 und ISO 21448. Darüber hinaus werden etablierte Praktiken des Automotive-PEPs berücksichtigt und agile Vorgehensmodelle ohne strukturbedingte Konflikte oder Widersprüchlichkeiten integriert. Zudem bestätigt die methodische und praktische Umsetzung mittels eines modellbasierten Systementwicklungsrahmenwerks die Anschlussfähigkeit an industrielle Entwicklungslandschaften.
Kohärenz der Nachweisführung	Hoch	Die Nachweisführung weist eine hohe Kohärenz auf. Das Ganze lässt sich auf die logische Verknüpfung von Evidenzen, Argumenten und Behauptungen zurückführen, welche durchgängig von der Phase des Betriebskonzepts bis hin zur simulationsbasierten Validierung vorangetrieben wird. Dadurch entsteht ein systematisch zusammenhängendes Nachweisführungskonstrukt für betriebssicherheitsrelevante Artefakte.
Modellbasierte Integrationstiefe	Sehr hoch	Die Integrationstiefe ist sehr hoch. Die Einbettung in die SPES-Matrix als modellbasiertes Systementwicklungsrahmenwerk sowie die Kopplung von SafeDevOps-Zyklen über funktionale, logische und technische Sichtweisen ermöglicht eine durchgängige Rückverfolgbarkeit und Wiederverwendbarkeit der betriebssicherheitsbezogenen Liefergegenstände.
Praktische Anwendbarkeit	Mittel	Die praktische Anwendbarkeit kann als mittel bewertet werden. Die Fallstudie im Hinblick auf den hochautomatisierten Autobahnpiloten legt dar, dass der ganzheitliche Betriebssicherheitsansatz reale Sicherheitsfragestellungen adressieren kann und frühzeitige Validierungen ermöglicht. Andererseits ergeben sich Einschränkungen in der Szenarienvielfalt, der industriellen Implementierung und Bereitstellung von Fahrzeugführungssystemen als auch der Einbindung von realen Felddaten, wodurch eine vollständige praxisnahe Industriereife noch nicht erreicht ist.

Umgang mit Unsicherheiten	Mittel	Der Umgang mit Unsicherheiten ist als mittel einzustufen. Epistemische und aleatorische Unsicherheiten werden in der Betriebskonzeptphase adressiert. Offen bleiben quantitative Risikoakzeptanzkriterien sowie die Behandlung umfangreicher Kontextunsicherheiten anhand spezifischer Modellierungs- und Verifikationsmethoden. Diese Aspekte stellen Ansatzpunkte zukünftiger Forschung dar.

Insgesamt können durch den im Verlauf der vorliegenden Dissertation entwickelten Prozessansatz die zentralen Kriterien an einen ganzheitlichen Betriebssicherheitslebenszyklus für hochautomatisierte Fahrfunktionen erfüllt werden. Besonders hervorzuheben sind die hohe Kompatibilität zu bestehenden Normen und Standards der Automotive-Produkt- und Sicherheitsentwicklung, die starke modellbasierte Integration sowie die hohe Skalierbarkeit. Darüber hinaus bildet die im Rahmen dieser Dissertation ausgearbeitete Betriebskonzeptphase in Kombination mit dem SIFAD-Rahmenwerk [276] die prozessual-methodische Grundlage für das zukünftige szenariobasierte und datengetriebene Sicherheitsrahmenwerk der BMW Group zur systematischen Spezifikation, Analyse und kontinuierlichen Bewertung automatisierter Fahrfunktionen. Gleichzeitig veranschaulicht die Evaluation, dass insbesondere im Umgang mit vielschichtigen Unsicherheiten des offenen Betriebskontexts sowie in der Integration innerhalb von Normungs- und Standardisierungsgremien als auch der praktischen industriellen Umsetzung weiteres Forschungs- und Entwicklungspotenzial besteht (vgl. Abschnitt 9.3).

9.2.3 Methodische Anforderungen zur Bewältigung des offenen betrieblichen Kontexts

Obwohl die konkrete Ausgestaltung einzelner Modellierungs- und Verifizierungsmethoden nicht Gegenstand dieser Dissertation ist, lassen sich aus dem entwickelten Betriebssicherheitslebenszyklusprozess spezifische Anforderungen im Hinblick auf deren notwendige Eigenschaften ableiten, um die Herausforderungen des offenen betrieblichen Kontexts automatisierter Fahrfunktionen zu bewältigen:

- **Fähigkeit zur Abbildung offener, hochvariabler Kontexte:** Methoden müssen Szenarien, Umgebungszustände und Interaktionen mit Verkehrsteilnehmern als unvollständige, probabilistische und dynamische Modelle erfassen können. Darunter fällt die formale Abbildung von Szenarien, Umgebungszuständen und Interaktionsmustern zwischen Verkehrsteilnehmern unter Bedingungen hoher Kontextvariabilität.

- **Explizite Unsicherheitsmodellierung:** Sowohl epistemische Unsicherheiten, sprich strukturelle Wissenslücken innerhalb der System- und Umweltbeschreibung, als auch aleatorische Unsicherheiten im Sinne stochastischer Variabilität müssen formalisiert und im Betriebssicherheitsnachweis quantifizierbar sein. Relevante Ansätze umfassen Bayes‘sche Risikoakkumulation über Szenarioräume, statistische Unfall- und Ereignisratenmodellierung, probabilistische Unsicherheitspropagation sowie quantitative Metriken wie die Positive Risk Balance.

- **Szenarioraumexploration und -priorisierung:** Zudem müssen Methoden systematische Mechanismen zur Exploration und Priorisierung des relevanten Szenarienraums bereitstellen, um insbesondere sicherheitskritische Randfälle identifizieren und bewerten zu können.

- **Architekturebenenübergreifende Konsistenz:** Die eingesetzten Methoden müssen sowohl auf funktionaler als auch auf logischer und technischer Ebene adaptierbar sein und eine durchgängige Rückverfolgbarkeit der sicherheitskritischen Artefakte sicherstellen.

- **Integrierbarkeit in simulations- und datengetriebene Toolchains:** Eine weitere Schlüsselanforderung besteht in der Integrationsfähigkeit in simulations- und datengetriebene Entwicklungs- und Absicherungsinfrastrukturen. MiL-, SiL-, HiL- und ViL-Umgebungen erfordern Methoden, die Anschlussfähigkeit an automatisierte Toolchains, Datenplattformen und validierungsgetriebene Analysepipelines besitzen. Hierzu gehören skalierbare Pipelines für Datenaufzeichnung (engl. *Data-Logging*), vor- und nachgelagerte Datenaufbereitung sowie -analyse (engl. *Pre- and Post-Processing*), Annotation und Szenariogenerierung sowie Simulation und Test.

Vor diesem Hintergrund ist die in der Phase des Betriebssicherheitskonzepts (vgl. Unterabschnitt 8.1.5) eingesetzte SOCA-Methode (vgl. Anhang A.8) ein vielversprechender Baustein für die Modellierung offener Kontexte in frühen Entwicklungsphasen. Ihr Beitrag liegt insbesondere in der stabilen qualitativen Abstraktion von Verkehrssituationen mittels Zonengraphen sowie in der systematischen Zerlegung hochdimensionaler Entscheidungsräume über die morphologische Analyse anhand von Zwicky-Boxen. Allerdings ist SOCA vornehmlich qualitativ ausgerichtet und adressiert weder quantitative Unsicherheiten noch stochastische Verkehrsdynamiken. Aus diesem Grund eignet sich SOCA verstärkt als Methode zur frühzeitigen Betriebsbereichsdefinition und -analyse sowie zur Strukturierung von Szenarien, muss jedoch durch daten- und simulationsgetriebene Verfahren ergänzt werden, um eine adäquate Abdeckung realer offener Kontexte voranzutreiben.

Was KI-basierte Wahrnehmungs-, Prädiktions- und Entscheidungsfunktionen angeht, so ergeben sich zusätzliche Herausforderungen. Diesbezüglich müssen die jeweiligen Methoden eine datengetriebene Modellvalidierung mit Unsicherheitsquantifizierung ermöglichen, um Fehlverhalten und Verdeckungen in vielschichtigen Umgebungsbedingungen nachvollziehbar bewerten zu können. Darüber hinaus müssen Modelle zur Nachvollziehbarkeit und Erklärbarkeit von getroffenen Entscheidungen sowie sogenannte Surrogatmodelle zur betriebssicherheitsgerichteten Argumentation bereitgestellt werden. Hinzu kommt der Bedarf an Testverfahren bezüglich adversariale oder perturbationsbasierte Störungen sowie Mechanismen zur Anpassung an veränderte Datenverteilungen im Feldbetrieb. Die vertikale und horizontale Erweiterung im Hinblick auf den Betriebssicherheitslebenszyklusprozess bietet hierfür einen strukturellen Ordnungsrahmen, verdeutlicht jedoch zugleich den Bedarf an der Weiterentwicklung entsprechender Ansätze und Methoden hinsichtlich Datenvalidierung und Modellformalisierung unter Berücksichtigung der ISO 8800 [264].

9.3 Anknüpfungspunkte für zukünftige Forschungsarbeiten

Basierend auf den im Verlauf dieser Arbeit gewonnenen Erkenntnissen werden nachfolgend wissenschaftliche Fragestellungen für eine sukzessive Weiterführung der Forschungsarbeiten dargestellt.

9.3.1 Vertiefung des Betriebssicherheitslebenszyklusprozesses im Hinblick auf Mobilitätsdienste und Platooning im Personen- und Güterverkehr

Der im Rahmen der vorliegenden Dissertation aufgesetzte Betriebssicherheitslebenszyklusprozess berücksichtigt unterstützende Infrastruktursysteme bis hin zu intelligenten Verkehrsleitsystemen mit zugehörigen Mobilitätsdiensten. An dieser Stelle ergeben sich allerdings weitere Potenziale, insbesondere was die Generierung eines Betriebssicherheitskonzepts bzw. eines Betriebssicherheitsmanagementsystems angeht. Dabei handelt es sich um Mobilitätsdienste und Platooningkonzepte im Personen- und Güterverkehr, wie z.B. das ITIV-Kooperationsprojekt TEMPUS [316]. In Anbetracht dessen besteht der Bedarf, die hier bereits beschriebenen Tätigkeiten gemäß Teil 3-5 „Betriebssicherheitskonzept“ prozessual zu vertiefen. Hierunter fällt mitunter die eindeutig definierte Verteilung der Verantwortlichkeiten der Betriebssicherheit, beispielsweise im Hinblick auf eine hochautomatisierte Fahrzeugflotte eines Mobilitätsdienstleisters oder eines Logistikbetreibers.

Dabei umfassen die Betriebssicherheitsverantwortlichkeiten Aufgaben, Funktionen und Aspekte im Zusammenhang mit Inspektionen, Disposition, Wartung und Reparatur, fahrzeugspezifischer Nutzung im Rahmen des bestimmungsgemäßen Gebrauchs innerhalb des dafür vorgesehenen Betriebsbereichs, Überwachung von Fahrzeugzustand und Status im Betrieb, Reaktion auf Vorfälle, Unfalluntersuchung und -berichterstattung, Remotebedienung, Personal, Schulung, Aufzeichnungsführung und weitere damit verbundene Tätigkeiten. In dieser Hinsicht muss im Zuge eines ganzheitlichen Betriebssicherheitskonzepts dargelegt werden, inwiefern diese Funktionen und Tätigkeiten zwischen Flottenbetreiber, Betreiber eines Betriebsbereichs, Wartungspersonal, Fahrzeughersteller, Kunden, Anwender usw. adäquat zugeordnet und im Einklang mit der jeweils geltenden Straßenverkehrsgesetzgebung abgesprochen werden. Die korrekte und konsistente Einhaltung von Richtlinien, Verfahren und Strategien zur Erfüllung der relevanten Betriebssicherheitsverantwortlichkeiten im Zusammenhang mit hochautomatisierten Fahrzeugflotten wird entscheidend dafür sein, neu entstehende Risikoklassen, welche im Zuge von hochautomatisierten Flottenoperationen wie Platooning, Remotebedienung, V2X-Kommunikation, Mensch-Maschine-Interaktion mit Robotaxis etc. entstehen können, systematisch zu identifizieren und angemessen zu reduzieren.

9.3.2 Systematische Ableitung von quantitativen Risikoakzeptanzkriterien

Ein weiteres anzugehendes Forschungsfeld ergibt sich im Bereich der Definition und Berücksichtigung von quantitativen Risikoakzeptanzkriterien sowie Validierungszielen als auch deren Integration insbesondere in Teil 3-4 „Betriebsbereichsbedingte Gefahrenanalyse und Risikobewertung“ des hier konzipierten Betriebssicherheitslebenszyklusprozesses. Hierbei ist eine systematische Argumentation der Abwesenheit eines inakzeptablen Risikos unter Festlegung von Risikoakzeptanzkriterien, z.B. die maximal zulässige Anzahl von Unfällen pro Stunde, sowie quantitative und messbare Kriterien für die Akzeptanz von Restrisiken zu definieren und eine schlüssige Rechtfertigung für die gewählten Risikoakzeptanzkriterien einschließlich deren Testabdeckung durch quantitative Validierungsziele zu formulieren. Explizite Risikoakzeptanzkriterien können hierbei beispielsweise aus einer Kombination von Schadensfolgen und ihren jeweiligen Häufigkeitsgrenzen bestehen. Die dabei jeweils gewählte Kombinatorik hat unter Bezugnahme von behördlichen und industriellen Regularien, geltende Rechtsvorschriften, Unfallstatistiken, Verkehrsanalysen und -daten als auch dem aktuellen Stand von Wissenschaft und Technik zu erfolgen. Hierbei müssen Maßstäbe im Hinblick auf die Wirksamkeit festgelegt werden, welche z.B. auf einem Vergleich mit einer geforderten Mindestreduzierung der jährlich auftretenden Kollisionen einschließlich der Berücksichtigung von deren Schwere basieren.

Diese können mit Daten aus Studien, nationalen Statistiken, lokalen Datenbanken (z.B. Polizeimeldungen) und Versicherungsdatenbaken kombiniert werden, um quantitativ das Risikoakzeptanzkriterium zu deduzieren. Die zu begründende Gesamtargumentation des tolerierbaren Risikos kann dann beispielsweise auf dem Ansatz einer positiven Risikobilanz respektive Benchmark (z.B. Restrisiko geringer als Unfallrisiko durch menschliche Fahrer im Zuge des herkömmlichen Straßenverkehrs) gemäß dem SIFAD-Ansatz von Werling et al. [276] beruhen (vgl. Unterabschnitt 6.4.3). Weitere Lösungsansätze im Sinne eines Risikomanagementrahmenwerks können beispielsweise den VVM-Veröffentlichungen Putze et al. [317] entnommen werden. Im Zuge der Definition von Sicherheitsschwellen und Kritikalitätsmetriken und deren quantitative Risikoklassifizierung böte sich darüber hinaus auch die Möglichkeit, die im Verlauf der vorliegenden Dissertation generierten Fahrzonen (vgl. Unterabschnitt 8.1.5) heranzuziehen. Je nach Fahrzone bzw. Aufenthaltsbereich könnte eine Risikoklassifizierung vorgenommen werden, welche während des Betriebs überwacht und aufgezeichnet wird.

9.3.3 Integration weiterer Methoden für den Entwurf als auch die Verifikation und Validierung des hochautomatisierten Fahrens

Im Verlauf des generierten modell- und simulationsbasierten Betriebssicherheitskonzepts für einen hochautomatisierten Autobahnpiloten wurden bereits Methoden der Betriebskontextanalyse (SOCA vgl. Unterabschnitt 8.1.5), des szenariobasierten Testens (vgl. Unterabschnitt 8.1.6) durchgeführt und nahtlos in das SPES-Modellierungsrahmenwerk integriert werden. Aber auch hier ergeben sich aufgrund der Allgemeingültigkeit und Generalisierbarkeit des Modellierungsrahmenwerks Potenziale, weitere Methoden auf Basis der abgeleiteten Anforderungen aus dem Betriebssicherheitslebenszyklusprozess (vgl. Unterabschnitt 9.2.3) im Hinblick auf den Entwurf als auch die Verifikation und Validierung des hochautomatisierten Fahrens einzubetten. Vor diesem Hintergrund ergibt sich die Option, Methoden des Contract-Based Designs gemäß den ITIV-Forschungsarbeiten von Guissouma et al. [318] einzubinden. Dadurch könnte das Treffen von Annahmen und Vornehmen von Einschränkungen formalisiert und demnach mittels automatisierten Konsistenzprüfungen (engl. *Consistency Checks*) analysiert werden.

Für die in der Industrie verbreiteten Simulations- und Szenarioumgebungen existieren bereits standardisierte Mechanismen und Schnittstellen. In diesem Zusammenhang stellen ASAM OpenODD, OpenScenario, OpenDRIVE etc. [307] verbreitete Standardformate für die einheitliche Beschreibung von Betriebsbereichs- als auch Szenario-Informationen dar und treiben einen allgemeingültigen Informationsaustausch zwischen den Modellentwicklungsumgebungen voran. Hinzu kommen Ansätze aus dem PEGASUS- und VVM-Projektumfeld sowie den ITIV- bzw. FZI-Forschungsarbeiten (vgl. Unterabschnitte 4.8.1 und 4.8.2) als auch Methoden des maschinellen Lernens im Sinne der iterativen, rekursiven und inkrementellen Konzeption neuronaler Netze. Jene sind insbesondere in Bezug auf die betriebssicherheitsbezogene Entwicklung von Wahrnehmungsalgorithmen für die Verarbeitung von Kamera-, Lidar- und Radardaten etc. von Relevanz. Ein zusätzlicher Fokus kann an dieser Stelle auf die Chancen und Möglichkeiten verschiedener Datenanalyse- und -explorationsverfahren gelegt werden, um in aufgezeichneten Datensätzen enthaltene und womöglich bisher unbekannte Abhängigkeiten des analytisch dynamischen Verhaltens zu detektieren. Diese können wiederum als Grundlage für die Definition von ergänzenden Bewertungsmetriken und für die Auswahl spezifischer Testszenarien herangezogen werden. Dies gilt auch für die weitere Integration von Ansätzen aus der Stochastik, wie z.B. Markov-Ketten, Bayes‘sche Netze, Monte-Carlo-Simulationen, Elemente der Chaos-Theorie, Big-Data-Analysen als auch experimentelle Designmethoden hinsichtlich der Beherrschung der offenen Kontextthematik der realen Welt (vgl. Abschnitt 4.8). Hierzu zählt auch

die im Rahmen der vorliegenden Dissertation entwickelte und publizierte Arbeit „Formal Safety and Robustness Verification of Nonlinear Vehicle Systems Under Uncertainty Using Sum-of-Squares Optimization“ [319], da sie die Formalisierung und systematische Behandlung von Unsicherheiten im Kontext der Betriebssicherheitsanalyse unterstützt und somit einen weiteren methodischen Baustein für den modellbasierten Nachweisprozess bereitstellt.

9.3.4 Einbettung in Normungs- und Standardisierungsarbeiten sowie industrielle Umsetzung

Die in dieser Dissertation entwickelte Betriebskonzeptphase bietet Potenzial für die Weiterentwicklung und Einbettung in die Normungs- und Standardisierungsgremien der ISO 5083 [261]. Dieser Sachverhalt gilt insbesondere hinsichtlich der prozessualen Strukturierung der Interessenvertreteranalyse, der Betriebsbereichsdefinition, der szenariobasierten Risikoidentifizierung und -bewertung sowie des Betriebssicherheitskonzepts. Im Hinblick darauf könnten die entwickelten Prozessbausteine die notwendige Nachvollziehbarkeit, Prozessfähigkeit und Konsistenz der Sicherheitsnachweisführung über den gesamten Entwicklungs- und Betriebszyklus hinweg stärken und einen nahtlosen Übergang in die etablierten Sicherheitsstandards ISO 26262 und ISO 21448 ermöglichen.

Ausgehend von der Referenzarchitektur hochautomatisierter Kraftfahrzeuge (vgl. Unterabschnitt 2.2.1) ergibt sich insbesondere auf Führungsebene innerhalb der Planung und Regelung das Potenzial, die hier spezifizierte Fahrverhaltensspezifikation in Richtung von hochautomatisierten Spurwechselmanövern einschließlich der Betrachtung einer 360 ° Umgebungswahrnehmung und Objekterkennung als auch von mehreren Fahrstreifen sowie Nutzung von Kartendaten eines Autobahnabschnitts sukzessive zu erweitern. An der Stelle ergibt sich wiederum Handlungsbedarf bezüglich der Betriebssicherheitsargumentation der auf maschinellem Lernen basierenden Lokalisierungs- und Wahrnehmungsalgorithmen sowie den Lokalisierungs- und Umgebungssensoren unter optionaler Hinzunahme von V2X-Kommunikationsschnittstellen. Hinzu kommt die Beherrschung von temporären Straßenstrukturen wie Baustellen als auch von Wetterverhältnissen in Bezug auf Regen, Nebel und ggf. Schneefall. Weiterer Forschungs- und Entwicklungsbedarf eröffnet sich im Hinblick auf die Mensch-Maschine-Interaktion, was beispielsweise das Be- und Abfahren im Sinne des Eintretens und Verlassens des definierten Betriebsbereichs Autobahnabschnitt angeht.

Weiterer Handlungsbedarf ergibt sich in der Vertiefung der hier vorgestellten Aktivitätsschritte, was die Hardware- und Softwareentwicklung der konzipierten Längs- und Querregelalgorithmen auf Einheitenebene unter Bezugnahme der technischen Sichtweise angeht. Des Weiteren besteht die Notwendigkeit, das auf die Produktstrategiephase bezogene virtuelle Betriebssicherheitskonzept über die jeweiligen Automotive-PEP Phasen der Fahrzeugentwicklung, des Produktions- und Verkaufsstart bis hin zum Betrieb, der Wartung sowie der Außerbetriebnahme sukzessive zu erweitern und insbesondere zu vertiefen (siehe Abbildung 8.1 bzw. Abbildung 7.20). Darunter fällt eine auf den jeweils aktuellen Betriebssicherheitsreifegrad basierende Entwicklung der A-, B-, C-, D-Muster bis hin zur Serie sowie deren Verifikation und Validierung im Sinne von SiL-, HiL-, ViL-Testläufen als auch Realfahrten, um u.a. auch die hier eingesetzten Fahrdynamikmodelle (vgl. Anhang A.4) datengetrieben zu validieren und ggf. anzupassen.

Literaturverzeichnis

[1] T. u. I. Rat für Forschung, "Informationsgesellschaft. Chancen, Innovationen und Herausforderungen," Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, Bonn, 1995.

[2] A. Bühl, Die virtuelle Gesellschaft des 21. Jahrhunderts, Wiesbaden: VS Verlag für Sozialwissenschaften, 2000.

[3] Klaus Schwab, "https://www.handelsblatt.com," Handelsblatt GmbH, 20 January 2016. [Online]. Available: https://www.handelsblatt.com/politik/international/davos-2016/davos-2016-die-vierte-industrielle-revolution/12836622.html. [Accessed 5 June 2020].

[4] R. Deckert, Digitalisierung und Industrie 4.0: Technologischer Wandel und individuelle Weiterentwicklung, Wiesbaden: Springer Fachmedien Wiesbaden, 2019.

[5] WirtschaftsWoche Online, "WirtschaftsWoche Online," Handelsblatt GmbH, 1 Oktober 2020. [Online]. Available: https://www.wiwo.de/technologie/digitale-welt/ranking-zur-wettbewerbsfaehigkeit-deutschland-faellt-im-digitalen-wettbewerb-weiter-zurueck/26235682.html. [Accessed 24 Dezember 2020].

[6] United Nations Economic Commission for Europe, "https://unece.org," [Online]. Available: https://unece.org/member-states-and-member-states-representatives. [Accessed 25 Dezember 2020].

[7] F. Pfeil, "Megatrends und die dritte Revolution der Automobilindustrie," 2018.

[8] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles,* SAE International J3016, 2021.

[9] J. Ebberg, "https://www.bosch-presse.de," Robert Bosch GmbH, 6 March 2018. [Online]. Available: https://www.bosch-presse.de/pressportal/de/de/bosch-auswertung-fahrerassistenzsysteme-sind-weiter-stark-auf-dem-vormarsch-148032.html. [Accessed 5 June 2020].

[10] *Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates,* Amtsblatt der Europäischen Union L 325/1, 2019.

[11] Seunghyuk Choi and Fredrik Hansson and Hans-Werner Kaas and John Newman, *Capturing the advanced driver assistance systems opportunity,* McKinsey & Company, 2016.

[12] K. Bengler, K. Dietmayer, B. Farber, M. Maurer, C. Stiller and H. Winner, "Three Decades of Driver Assistance Systems: Review and Future Perspectives," *IEEE Intelligent Transportation Systems Magazine,* vol. 6, p. 6–22, 10 2014.

[13] Lisanne Bainbridge, "Ironies of automation," *Automatica,* vol. 19, p. 775–779, 11 1983.

[14] Thomas B. Sheridan, "Humans and automation: System design and research issues," *Wiley series in system engineering and management: HFES issues in human factors and ergonomics series,* vol. 3, 2002.

[15] S. M. Casner, E. L. Hutchins and D. Norman, "The challenges of partially automated driving," *Communications of the ACM,* vol. 59, p. 70–77, 4 2016.

[16] D. A. Norman, "The Human Side of Automation," in *Road Vehicle Automation 2*, G. Meyer and S. Beiker, Eds., Cham, Springer International Publishing, 2015, p. 73–79.

[17] Christopher Poulin and Neville A Stanton and David Cebon and Wolfgang Epple, *Response to: Autonomous vehicles,* 2015.

[18] N. Strand, J. Nilsson, I. C. M. Karlsson and L. Nilsson, "Semi-automated versus highly automated driving in critical situations caused by automation failures," *Transportation Research Part F: Traffic Psychology and Behaviour,* vol. 27, p. 218–228, 11 2014.

[19] J. Nilsson, N. Strand, P. Falcone and J. Vinter, "Driver performance in the presence of adaptive cruise control related failures: Implications for safety analysis and fault tolerance," in *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, 2013.

[20] Johnna Crider, "https://cleantechnica.com," CleanTechnica, 23 April 2020. [Online]. Available: https://cleantechnica.com/2020/04/23/waymo-our-autopilot-was-very-advanced/. [Accessed 5 June 2020].

[21] *Rechtssicher Fahren mit automatisierten Fahrzeugen,* Verbraucherzentrale Bundesverband e.V., 2017.

[22] H. Winner, "Introducing autonomous driving: an overview of safety challenges and market introduction strategies," *at - Automatisierungstechnik,* vol. 66, p. 100–106, 2 2018.

[23] T. Frese, N. Gerber, D. Hatebur, I. Côté and M. Heisel, "Functional Safety Processes and Advanced Driver Assistance Systems: Evolution or Revolution?," in *Mobilität und digitale Transformation*, H. Proff and T. M. Fojcik, Eds., Wiesbaden, Springer Fachmedien Wiesbaden, 2018, p. 199–216.

[24] Hyperdrive, "https://www.bloomberg.com," Bloomberg L.P., 15 May 2020. [Online]. Available: https://www.bloomberg.com/features/2020-self-driving-car-race/. [Accessed 5 June 2020].

[25] Patrick Setzer, "https://www.manager-magazin.de," manager magazin, 7 November 2019. [Online]. Available: https://www.manager-magazin.de/lifestyle/artikel/waymo-one-autonome-taxis-von-google-haengen-deutsche-hersteller-ab-a-1295413.html. [Accessed 5 June 2020].

[26] *Fahrplan zu einem einheitlichen europäischen Verkehrsraum – Hin zu einem wettbewerbsorientierten und ressourcenschonenden Verkehrssystem,* Europäische Kommission, 2011.

[27] Thomas Winkle, "Sicherheitspotenzial automatisierter Fahrzeuge: Erkenntnisse aus der Unfallforschung," in *Autonomes Fahren*, Berlin, Heidelberg: Springer-Verlag GmbH Berlin Heidelberg, 2015, p. 351–376.

[28] M. Bertoncello and D. Wee, "Ten ways autonomous driving could redefine the automotive world," McKinsey & Company, 2015.

[29] Wissenschaftlicher Beirat beim Bundesminister für Verkehr und digitale Infrastruktur, "Automatisiertes Fahren im Straßenverkehr," *Zeitschrift für Straßenverkehrstechnik,* 2017 April 2017.

[30] Barbara Lenz and Eva Fraedrich, "Neue Mobilitätskonzepte und autonomes Fahren: Potenziale der Veränderung," in *Autonomes Fahren*, Berlin, Heidelberg: Springer-Verlag GmbH Berlin Heidelberg, 2015, p. 175–195.

[31] Nicole Lücke, "https://www.vdi.de," VDI Verein Deutscher Ingenieure e.V, 7 May 2019. [Online]. Available: https://www.vdi.de/themen/autonomes-fahren/status-quo-des-autonomen-fahrens. [Accessed 5 June 2020].

[32] Deloitte, "Urbane Mobilität und autonomes Fahren im Jahr 2035," Deloitte, 2019.

[33] Kelsey Piper, "https://www.vox.com," Vox Media, LLC, 28 February 2020. [Online]. Available: https://www.vox.com/future-perfect/2020/2/14/21063487/self-driving-cars-autonomous-vehicles-waymo-cruise-uber. [Accessed 5 June 2020].

[34] Kersten Heineke and Philipp Kampshoff and Armen Mkrtchyan and Emily Shao, *Self-driving car technology: When will the robots hit the road?,* McKinsey & Company, 2017.

[35] S. Grundhoff and R. Schwinnen, "https://www.blick.ch," Blick.ch, 17 May 2020. [Online]. Available: https://www.blick.ch/auto/news_n_trends/selbstfahrende-autos-nicht-vor-2030-schiffbruch-fuers-autonome-fahren-id15891598.html. [Accessed 5 June 2020].

[36] B. W. Boehm, "Verifying and Validating Software Requirements and Design Specifications," in *IEEE Software vol.1, no. 1*, 1984.

[37] R. Hussain and S. Zeadally, "Autonomous Cars: Research Results, Issues, and Future Challenges," *IEEE Communications Surveys & Tutorials,* vol. 21, p. 1275–1313, 2019.

[38] "Continental-Mobilitätsstudie 2024," Continental AG, 2024. [Online]. Available: https://www.continental.com/de/presse/initiativen-umfragen/continental-mobilitaetsstudien/mobilitaetsstudie-2024/. [Accessed 14 5 2025].

[39] "bitkom," Bitkom e.V., 4 12 2024. [Online]. Available: https://www.bitkom.org/Presse/Presseinformation/Vorteile-Autonomer-Fahrzeuge. [Accessed 14 5 2025].

[40] Shai Shalev-Shwartz and Shaked Shammah and Amnon Shashua, "On a Formal Model of Safe and Scalable Self-driving Cars," 2017.

[41] B. Tefft, AAA Foundation for Traffic Safety, Januar 2018. [Online]. Available: https://aaafoundation.org/american-driving-survey-2015-2016/#:~:text=On%20average%2C%20drivers%20reported%20making,2.62%20trillion%20miles%20in%202016.. [Accessed 24 Dezember 2020].

[42] *Safety First for Automated Driving,* Aptiv Services US, LLC; AUDI AG; Bayrische Motoren Werke AG; Beijing Baidu Netcom Science Technology Co., Ltd; Continental Teves AG & Co oHG; Daimler AG; FCA US LLC; HERE Global B.V.; Infineon Technologies AG; Intel; Volkswagen AG., 2019.

[43] "https://www.handelsblatt.com," Handelsblatt GmbH, 7 May 2018. [Online]. Available: https://www.handelsblatt.com/unternehmen/industrie/autonomes-fahren-softwarefehler-fuehrte-wohl-zu-toedlichem-uber-unfall/21254056.html?ticket=ST-745618-ImOIbD2gprutTAYDZ4FG-ap1. [Accessed 5 June 2020].

[44] Gregor Hebermehl, "https://www.auto-motor-und-sport.de," Motor Presse Stuttgart GmbH & Co.KG, 3 January 2020. [Online]. Available: https://www.auto-motor-und-sport.de/elektroauto/tesla-autopilot-unfall-honda-civic/. [Accessed 5 June 2020].

[45] M. Haun, Handbuch Robotik, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[46] P. Koopman and M. Wagner, "Autonomous Vehicle Safety: An Interdisciplinary Challenge," *IEEE Intelligent Transportation Systems Magazine,* vol. 9, p. 90–96, 2017.

[47] stvo.de - Das Portal zur Staßenverkehrsordnung (StVO), "Das Portal zur Staßenverkehrsordnung (StVO)," FORUM VERLAG HERKERT GMBH, [Online]. Available: https://www.stvo.de/strassenverkehrsordnung/89-1-grundregeln. [Accessed 24 Dezember 2020].

[48] T. Gindele, S. Brechtel and R. Dillmann, "Learning Driver Behavior Models from Traffic Observations for Decision Making and Planning," *IEEE Intelligent Transportation Systems Magazine,* vol. 7, p. 69–79, 2015.

[49] P. Koopman and M. Wagner, "Challenges in Autonomous Vehicle Testing and Validation," *SAE International Journal of Transportation Safety,* vol. 4, p. 15–24, 4 2016.

[50] *Road vehicles - Functional safety - Part 1-12,* ISO 26262-1-12:2018, 2018.

[51] *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1 bis 7,* IEC 61508:2011, 2011.

[52] V. Gebhardt, G. M. Rieger, J. Mottok and C. Gießelbach, Funktionale Sicherheit nach ISO 26262 : Ein Praxisleitfaden zur Umsetzung, Heidelberg: dpunkt.verlag, 2013.

[53] E. Sax, Automatisiertes Testen Eingebetteter Systeme in der Automobilindustrie, Carl Hanser Verlag GmbH & Co. KG, 2008.

[54] E. Westkämper, "Produkt Life Cycle Management als Beitrag für ein nachhaltiges Wirtschaften," in *EXPO 2000 - Global Dialogue "Science and Technology - Thinking the Future"*, 2000.

[55] *Road vehicles - Safety of the intended functionality,* ISO 21448:2022, 2022.

[56] S. Eichler, C. Schroth and J. Eberspächer, "Car-to-car communication," 2006.

[57] O. Burkacky, J. Deichmann, G. Doll and C. Knochenhauer, "Rethinking car software and electronics architecture," *McKinsey & Company,* 2018.

[58] Tristan Shale-Hester, "Driverless cars will require one billion lines of code, says JLR," 4 2019. [Online]. Available: https://www.autoexpress.co.uk/car-news/106617/driverless-cars-will-require-one-billion-lines-of-code-says-jlr. [Accessed 5 Juni 2020].

[59] J. Schäuffele and T. Zurawka, Automotive Software Engineering, 7. Auflage ed., Wiesbaden: Springer Vieweg, 2024.

[60] K. Reif, Ed., Grundlagen Fahrzeug- und Motorentechnik, Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

[61] S. Kraus, "Fahrverhaltensanalyse zur Parametrierung situationsadaptiver Fahrzeugführungssysteme," 2012.

[62] Markus Maurer, "Flexible Automatisierung von Straßenfahrzeugen mit Rechnersehen," München, 2000.

[63] T. Müller, "Fahrerassistenz auf dem Weg zur automatisierten Fahrzeugführung," *ATZ-Automobiltechnische Zeitschrift,* p. 58–64, 2007.

[64] Bettina Abendroth and Ralph Bruder, "Die Leistungsfähigkeit des Menschen für die Fahrzeugführung," in *Handbuch Fahrerassistenzsysteme*, Third edition ed., Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 3–15.

[65] Georg Geiser, "Mensch-Maschine-Kommunikation im Kraftfahrzeug," *ATZ-Automobiltechnische Zeitschrift,* p. 77–84, 1985.

[66] Heiner Bubb, "Einführung," in *Automobilergonomie*, Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 1–25.

[67] "Straßenverkehrsordnung § 23 Sonstige Pflichten von Fahrzeugführenden," 6 2021. [Online]. Available: https://www.stvo.de/strassenverkehrsordnung/106-23-sonstige-pflichten-von-fahrzeugfuehrenden. [Accessed 10 Juni 2021].

[68] Andreas Christian Reschka, "Fertigkeiten- und Fähigkeitengraphen als Grundlage des sicheren Betriebs von automatisierten Fahrzeugen im öffentlichen Straßenverkehr in städtischer Umgebung," 2017.

[69] Thomas Jürgensohn, "Hybride Fahrermodelle," Berlin, 1997.

[70] Manfred Plöchl and Johannes Edelmann, "Driver models in automobile dynamics application," *Vehicle System Dynamics,* p. 699–741, 6 2007.

[71] Ilit Oppenheim and David Shinar and Oliver Carsten and Yvonne Barnard and Frank Lai and Frédéric Vanderhaegen and Philippe Polet and Simon Enjalbert and Marianne Pichon and Haakan Hasewinkel and Margareta Lützhöft and Albert Kircher and Lena Kecklund, "Critical review of models and parameters for Driver models in different surface transport systems and in different safety critical situations," *ITERATE Consortium,* 2010.

[72] Jens Rasmussen, "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models," *IEEE Transactions on Systems, Man and Cybernetics,* vol. Bd. 13, p. 257–266, 1983.

[73] Edmund Donges, "Aspekte der aktiven Sicherheit bei der Führung von Personenkraftwagen," *Automob-Ind,* 1982.

[74] D. G. Myers, Psychologie, Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[75] D. A. Tobinski, Kognitive Psychologie, Berlin, Heidelberg: Springer Berlin Heidelberg, 2017.

[76] Edmund Donges, "Fahrerverhaltensmodelle," in *Handbuch Fahrerassistenzsysteme*, Third edition ed., Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 17–26.

[77] Hermann Winner, "Grundlagen von Frontkollisionsschutzsystemen," in *Handbuch Fahrerassistenzsysteme*, Third edition ed., Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 893–912.

[78] Stefan Kupschick, "Modellierung menschähnlichen Fahrerverhaltens," Berlin, 2021.

[79] K. Steinbuch, Automat und Mensch - Kybernetische Tatsachen und Hypothesen, Springer Berlin Heidelberg, 1965.

[80] *DIN V 19233 Prozessautomatisierung,* DIN Deutsches Institut für Normung e. V., 1998.

[81] Markus Maurer, "Entwurf und Test von Fahrerassistenzsystemen," in *Handbuch Fahrerassistenzsysteme*, First edition ed., Wiesbaden, Vieweg +Teubner, 2009, p. 43–54.

[82] Heiner Bubb, "Das Regelkreisparadigma der Ergonomie," in *Automobilergonomie*, Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 27–65.

[83] S. Ulbrich, A. Reschka, J. Rieken, S. Ernst, G. Bagschik, F. Dierkes, M. Nolte and M. Maurer, "Towards a functional system architecture for automated vehicles," *arXiv preprint arXiv:1703.08557,* 2017.

[84] Fabian Schuldt, "Ein Beitrag für den methodischen Test von automatisierten Fahrfunktionen mit Hilfe von virtuellen Umgebungen," 2017.

[85] Tom M. Gasser, "Rechtsfolgen zunehmender Fahrzeugautomatisierung," Bergisch Gladbach, 2012.

[86] "Automatisierung - Von Fahrerassistenzsystemen zum automatisierten Fahren," Berlin, 2015.

[87] Krzysztof Czarnecki, *Operational Design Domain for Automated Driving Systems Taxonomy of Basic Terms,* University of Waterloo, 2018.

[88] Krzysztof Czarnecki, *Operational World Model Ontology for Automated Driving Systems Part 1: Road Structure,* University of Waterloo, 2018.

[89] Krzysztof Czarnecki, *Operational World Model Ontology for Automated Driving Systems Part 2: Road Users, Animals, Other Obstacles, and Environmental Conditions,* University of Waterloo, 2018.

[90] *Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification,* PAS 1883:2020, 2020.

[91] *Road Vehicles - Test scenarios for automated driving systems - Specification for operational design domain,* ISO 34503:2023, 2023.

[92] E. Thorn, S. C. Kimmel, M. Chaka, B. A. Hamilton and others, "A framework for automated driving system testable cases and scenarios," 2018.

[93] Philip Koopman and Frank Fratrik, "How Many Operational Design Domains, Objects, and Events?," in *SafeAI@ AAAI*, 2019.

[94] Iain Whiteside, *Ontologies and ODDs at Five,* 2020.

[95] M. Gyllenhammar, R. Johansson, F. Warg, D. Chen, H.-M. Heyn, M. Sanfridson, J. Söderberg, A. Thorsén and S. Ursing, "Towards an operational design domain that supports the safety argumentation of an automated driving system," in *10th European Congress on Embedded Real Time Systems (ERTS 2020)*, 2020.

[96] Ingo Wolf, "Wechselwirkung Mensch und autonomer Agent," in *Autonomes Fahren*, Berlin, Heidelberg: Springer-Verlag GmbH Berlin Heidelberg, 2015, p. 103–125.

[97] Heiner Bubb and Klaus Bengler and Jurek Breuninger and Christian Gold and Magnus Helmbrecht, "Systemergonomie des Fahrzeugs," in *Automobilergonomie*, Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 259–344.

[98] P. Madhavan and D.A. Wiegmann, "Similarities and differences between human-human and human-automation trust: An integrative review," *Theoretical Issues in Ergonomics Science,* vol. 8, p. 277–301, 2007.

[99] U. Winkelhake, Die digitale Transformation der Automobilindustrie, Berlin, Heidelberg: Springer Berlin Heidelberg, 2017.

[100] J. Schäuffele and T. Zurawka, Automotive Software Engineering, Wiesbaden: Springer Fachmedien Wiesbaden, 2016.

[101] M. Eigner and R. Stelzer, Product Lifecycle Management: ein Leitfaden für Product Development und Life Cycle Management, 2., neu bearb. Aufl ed., Dordrecht: Springer, 2013.

[102] Andrea Denger and Klaus Zamazal, "Product Lifecycle Challenges for Powertrain Systems in the Automotive Industry," in *Systems Engineering for Automotive Powertrain Development*, Cham, Switzerland: Springer Nature Switzerland AG, 2021, p. 105–122.

[103] T. Streichert and M. Traub, Elektrik/Elektronik-Architekturen im Kraftfahrzeug, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[104] *Reifegradabsicherung für Neuteile: Methoden, Messkriterien, Dokumentationen,* Verband der Automobilindustrie e.V. (VDA), 2022.

[105] R.Wenger, "Elektronischer Vergabeprozess bei direkten Gütern," St.Gallen, 2006.

[106] H. Wildemann, Advanced Purchasing - Leitfaden zur Einbindung der Beschaffungsmärkte in den Produktentstehungsprozess, München: TCW-Verlag, 2005.

[107] Ingo Renner, "Methodische Unterstützung funktionsorientierter Baukastenentwicklung am Beispiel Automobil," München, 2007.

[108] N. Adler, Modellbasierte Entwicklung funktional sicherer Hardware nach ISO 26262, Karlsruhe: KIT Scientific Publishing, 2015.

[109] *Systems and software engineering - Vocabulary,* ISO/IEC/IEEE 24765:2015.

[110] Frank Eugen Wißler, "Ein Verfahren zur Bewertung technischer Risiken in derPhase der Entwicklung komplexer Serienprodukte," Stuttgart, 2006.

[111] Stefan Schmerler, Softwaretest in der Praxis: Grundlagen, Methoden und Technologien, Berlin: epubli, 2020.

[112] P. Kranabitl, M. Bajzek, M. Atzwanger, D. Schenk and H. Hick, "Automotive Powertrain Development Process," in *Systems Engineering for Automotive Powertrain Development*, H. Hick, K. Küpper and H. Sorger, Eds., Cham, Springer International Publishing, 2021, p. 383–402.

[113] F. Wolf, Fahrzeuginformatik: Eine Einführung in die Software- und Elektronikentwicklung aus der Praxis der Automobilindustrie, Wiesbaden: Springer Fachmedien Wiesbaden, 2018.

[114] *ISO/IEC/IEEE Standard for Systems and Software Engineering - Software Life Cycle Processes,* ISO/IEC/IEEE 12207:2008(E), 2008.

[115] "Duden," Cornelsen Verlag GmbH, 2024, [Online]. Available: https://www.duden.de/rechtschreibung/Methode. [Accessed 18 Dezember 2024].

[116] W. W. Royce, "Managing the Development of Large Software Systems," in *Proceedings IEEE WESCON*, Los Angeles, 1970.

[117] B. W. Boehm, "A spiral model of software development and enhancement," *Computer 21.5,* pp. 61-72, 1988.

[118] Reinhard Höhn and Stephan Höppner, Das V-Modell XT, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[119] W. Dröschel and M. Wiemers, Das V-Modell 97, De Gruyter, 2015.

[120] "CMMI for Development, Version 1.3," Carnegie Mellon University, 2010.

[121] *Automotive SPICE Process Assessment / Reference Model Version 3.1,* VDA QMC Working Group 13 / Automotive SIG, 2017.

[122] *Systems and software engineering - Vocabulary,* ISO/IEC/IEEE 24765:2017, 2017.

[123] K. Reif, Automobilelektronik: Eine Einführung für Ingenieure, Wiesbaden: Vieweg+ Teubner, 2009.

[124] C. Haubelt and J. Teich, Digitale Hardware/Software-Systeme: Spezifikation und Verifikation, Heidelberg Dordrecht London New York: Springer-Verlag Berlin Heidelberg, 2010.

[125] Andreas Spillner and Tilo Linz, Basiswissen Softwaretest, Sixth edition ed., dpunkt.verlag, 2019.

[126] *Software and systems engineering - Software testing - Part 1: Concepts and definitions,* ISO/IEC/IEEE 29119-1, 2013.

[127] M. Hillenbrand, Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen, Karlsruhe: KIT Scientific Publishing, 2012.

[128] K. Reif, Automobilelektronik: Eine Einführung für Ingenieure, Wiesbaden: Springer Fachmedien Wiesbaden, 2014.

[129] Kent Beck, "Manifest für Agile Softwareentwicklung," 2001. [Online]. Available: https://agilemanifesto.org/iso/de/manifesto.html. [Accessed 25 September 2021].

[130] M. Eigner, "Überblick Disziplin-spezifische und -übergreifende Vorgehensmodelle," in *Modellbasierte virtuelle Produktentwicklung*, M. Eigner, D. Roubanov and R. Zafirov, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, p. 15–52.

[131] J. Sutherland and K. Schwaber, "SCRUM GUIDES," [Online]. Available: https://scrumguides.org/. [Accessed 18 Dezember 2024].

[132] "Scrum.org," [Online]. Available: https://www.scrum.org/learning-series/what-is-scrum/. [Accessed 18 Dezember 2024].

[133] J. Fritz, C. Zingel, J. Kokko, G. Lenardon and B. Brier, "Systems Engineering Methods and Tools," in *Systems Engineering for Automotive Powertrain Development*, H. Hick, K. Küpper and H. Sorger, Eds., Cham, Springer International Publishing, 2021, p. 271–302.

[134] Stephan Hakuli and Markus Krug, "Virtuelle Integration," in *Handbuch Fahrerassistenzsysteme*, Third edition ed., Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 125–138.

[135] H. Palm, J. Holzmann, R. Klein, S.-A. Schneider and D. Gerling, "A novel approach on virtual systems prototyping based on a validated, hierarchical, modular library," *Embedded World, Nuremberg, Germany,* 2013.

[136] "Digital Playbook," [Online]. Available: https://aiotplaybook.org/index.php/AIoT_101. [Accessed 18 Dezember 2024].

[137] "Agile V-Model," [Online]. Available: https://aiotplaybook.org/index.php?title=Agile_V-Model#Applying_the_Agile_V-Model_to_ACME:Vac. [Accessed 18 Dezember 2024].

[138] J. Mittelstraß, Ed., Enzyklopädie Philosophie und Wissenschaftstheorie Band 4: Sp-Z, Stuttgart: J.B. Metzler, 1996.

[139] Mirko Meboldt, "Mentale und formale Modellbildung in der Produktentstehung – als Beitrag zum integrierten Produktentstehungs-Modell (iPeM)," Karlsruhe, 2008.

[140] Eckehard Schnieder, Prozessinformatik. Automatisierung mit Rechensystemen. Einführung mit Petrinetzen., Second edition ed., Braunschweig: Vieweg, 1993.

[141] E. Schnieder, Methoden der Automatisierung, Wiesbaden: Vieweg+Teubner Verlag, 1999.

[142] *Systems and software engineering - System of systems (SoS) considerations in life cycle stages of a system,* ISO/IEC/IEEE 21839:2019, 2019.

[143] E. Schnieder and L. Schnieder, Verkehrssicherheit, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[144] J. S. Gero and U. Kannengiesser, "The Function-Behaviour-Structure Ontology of Design," in *An Anthology of Theories and Models of Design*, A. Chakrabarti and L. T. M. Blessing, Eds., London, Springer London, 2014, p. 263–283.

[145] Lars Schnieder, "Formalisierte Terminologien technischer Systeme und ihrer Zuverlässigkeit," Braunschweig, 2009.

[146] *Leittechnik; Regelungstechnik und Steuerungstechnik; Allgemeine Grundbegriffe,* DIN 19226-1, 1994.

[147] Arthur D. Hall, A Methodology for Systems Engineering, Van Nostrand, 1968.

[148] Stephen J. Kapurch, NASA Systems Engineering Handbook, DIANE Publishing, 2010.

[149] "Guide to the Systems Engineering Body of Knowledge (SEBoK)," 5 2021. [Online]. Available: https://www.sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK). [Accessed 25 September 2021].

[150] Peter Walker, Chambers science and technology dictionary, Cambridge University Press, 1988.

[151] J. Weber, Automotive Development Processes, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[152] F. Hüning, Embedded Systems für IoT, Berlin, Heidelberg: Springer Berlin Heidelberg, 2019.

[153] Bernd Schürmann, Eingebettete Systeme. AG Entwurfsmethodik eingebetteter Systeme der Universität Kaiserslautern, 2001.

[154] P. Scholz, Softwareentwicklung eingebetteter Systeme: Grundlagen, Modellierung, Qualitätssicherung, Berlin: Springer, 2005.

[155] K. Reif and R. B. GmbH, Eds., Bosch Autoelektrik und Autoelektronik: Bordnetze, Sensoren und elektronische Systeme ; mit 43 Tabellen, 6., überarb. und erw. Aufl ed., Wiesbaden: Vieweg + Teubner, 2011.

[156] Philipp Obergfell, "Entwurfsmethodik für hybride Software- und Systemarchitektur," Karlsruhe, 2021.

[157] Frank Thomas Piller and Daniela Waringer, Modularisierung in der Automobilindustrie : neue Formen und Prinzipien ; modular sourcing, Plattformkonzept und Fertigungssegmentierung als Mittel des Komplexitätsmanagements, Aachen: Shaker Verlag, 1999.

[158] Bosch Automotive Electrics and Automotive Electronics: Systems and Components, Networking and Hybrid Drive, Wiesbaden: Springer Fachmedien Wiesbaden, 2014.

[159] ISO/IEC/IEEE 42010:2011, *Systems and software engineering — Architecture description,* ISO/IEC/IEEE, 2011.

[160] O. Vogel, Ed., Software-Architektur: Grundlagen - Konzepte - Praxis, 2. Aufl ed., Heidelberg: Spektrum Akad. Verl, 2009.

[161] M. Broy, M. Gleirscher, P. Kluge, W. Krenzer, S. Merenda and D. Wild, "Automotive architecture framework: Towards a holistic and standardised system architecture description," 2009.

[162] M. Bajzek, J. Fritz, H. Hick, M. Maletz, C. Faustmann and G. Stieglbauer, "Model Based Systems Engineering Concepts," in *Systems Engineering for Automotive Powertrain Development*, H. Hick, K. Küpper and H. Sorger, Eds., Cham, Springer International Publishing, 2021, p. 195–234.

[163] Herbert Stachowiak, Allgemeine Modelltheorie, Wien, New: Springer-Verlag, 1973.

[164] M. Törngren, D. Chen, D. Malvius and J. Axelsson, "Model-Based Development of Automotive Embedded Systems," in *Automotive Embedded Systems Handbook*, Taylor & Francis Inc, 2008.

[165] "INCOSE Systems Engineering Vision 2020," San Diego, CA, USA, 2007.

[166] U. Dahmen and J. Rossmann, "Experimentable Digital Twins for a Modeling and Simulation-based Engineering Approach," 2018.

[167] D. D. Walden, G. J. Roedler, K. Forsberg, R. D. Hamelin, T. M. Shortell and I. C. on Systems Engineering, Eds., INCOSE Systems engineering handbook: a guide for system life cycle processes and activities, 4th edition ed., Hoboken, New: Wiley, 2015.

[168] Lenny Delligatti, SysML Distilled: A Brief Guide to the Systems Modeling Language, Addison-Wesley Professional, 2013.

[169] Jörn Neuhausen, "Methodik zur Gestaltung modularer Produktionssysteme für Unternehmen der Serienprodukt ion," Aachen, 2002.

[170] J. A. Estefan, "Survey of model-based systems engineering (MBSE) methodologies," *Incose MBSE Focus Group,* 2007.

[171] R. Zafirov, "Modellbildung und Spezifikation," in *Modellbasierte virtuelle Produktentwicklung*, M. Eigner, D. Roubanov and R. Zafirov, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, p. 77–96.

[172] T. Huth and T. Vietor, "Systems Engineering in der Produktentwicklung: Verständnis, Theorie und Praxis aus ingenieurswissenschaftlicher Sicht," *Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO),* vol. 51, p. 125–130, 3 2020.

[173] A. Albers and G. Moeser, "Modellbasierte Prinzip-und Gestaltvariation," in *14. Gemeinsames Kolloquium Konstruktionstechnik 2016. Traditio et Innovatio–Entwicklung und Konstruktion, am 6. und 7. Oktober 2016 in Rostock: Tagungsband*, 2016.

[174] *Systems and Software engineering - Methods and tools for model-based systems and software engineering,* ISO/ IEC/IEEE 24641:2023, 2023.

[175] The MathWorks, Inc., "Simulink," The MathWorks, Inc., [Online]. Available: https://de.mathworks.com/products/simulink.html?s_tid=hp_ff_p_simulink. [Accessed 18 August 2023].

[176] The MathWorks, Inc., "Stateflow," The MathWorks, Inc., [Online]. Available: https://de.mathworks.com/products/stateflow.html. [Accessed 18 August 2023].

[177] The MathWorks, Inc., "System Composer," The MathWorks, Inc., [Online]. Available: https://de.mathworks.com/products/system-composer.html. [Accessed 18 August 2023].

[178] T. Gilz, "Requirements Engineering und Requirements Management," in *Modellbasierte virtuelle Produktentwicklung*, M. Eigner, D. Roubanov and R. Zafirov, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, p. 53–75.

[179] *Simulation von Logistik-, Materialfluss- und Produktionssystemen - Grundlagen,* VDI 3633 Blatt 1, 2014.

[180] R. Isermann and M. Münchhof, Identification of Dynamic Systems: An Introduction with Applications, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[181] The Modelica Association, *Modelica® - A Unified Object-Oriented Language for Systems Modeling Language Specification Version 3.4.*

[182] The MathWorks, Inc., "Simscape," The MathWorks, Inc., [Online]. Available: https://de.mathworks.com/products/simscape.html. [Accessed 18 August 2023].

[183] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems*, 2008.

[184] *OMG Meta Object Facility (MOF) Core Specification Version 2.5.1,* Object Management Group, 2019.

[185] V. Gruhn, D. Pieper and C. Röttgers, MDA: effektives Software-Engineering mit UML 2 und Eclipse, Berlin: Springer, 2006.

[186] M. Nebel, Formale Grundlagen der Programmierung, Wiesbaden: Vieweg+Teubner Verlag, 2012.

[187] *OMG Unified Modeling Language Version 2.5.1,* Object Management Group, 2017.

[188] *Information technology - Open Distributed Processing - Unified Modeling Language (UML) Version 1.4.2,* ISO/IEC 19501, 2005.

[189] *OMG Systems Modeling Language Version 1.6,* Object Management Group, 2019.

[190] S. Friedenthal, A. Moore and R. Steiner, A practical guide to SysML: the systems modeling language, Third edition ed., Amsterdam ; Boston: Elsevier, MK, Morgan Kaufmann is an imprint of Elsevier, 2015.

[191] Julian Broy, "Modellbasierte Entwicklung und Optimierung flexibler zeitgesteuerter Architekturen im Fahrzeugserienbereich," Karlsruhe, 2010.

[192] K. Pohl, H. Hönninger, R. Achatz and M. Broy, Eds., Model-Based Engineering of Embedded Systems, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[193] K. Pohl, M. Broy, H. Daembkes and H. Hönninger, Eds., Advanced Model-Based Engineering of Embedded Systems, Cham: Springer International Publishing, 2016.

[194] S. Otten, J. Bach, C. Wohlfahrt, C. King, J. Lier, H. Schmid, S. Schmerler and E. Sax, "Automated Assessment and Evaluation of Digital Test Drives," in *Advanced Microsystems for Automotive Applications 2017*, C. Zachäus, B. Müller and G. Meyer, Eds., Cham, Springer International Publishing, 2018, p. 189–199.

[195] Christoph Roth, "Parallele und kooperative Simulation für eingebettete Multiprozessorsysteme," Karlsruhe, 2015.

[196] J.-F. Raskin, "An introduction to hybrid automata," in *Handbook of networked and embedded control systems*, Springer, 2005, p. 491–517.

[197] *IEEE Standard VHDL Analog and Mixed-Signal Extensions,* IEEE Std 1076.1-2017, 2017.

[198] *IEEE Standard for Standard SystemC® Analog/Mixed-Signal Extensions Language Reference Manual,* IEEE Std 1666.1-2016, 2016.

[199] H. Bucher, "Integrierte modell- und simulationsbasierte Entwicklung zur dynamischen Bewertung automobiler Elektrik/Elektronik-Architekturen," Karlsruhe, 2020.

[200] P. G. Larsen, J. Fitzgerald, J. Woodcock, P. Fritzson, J. Brauer, C. Kleijn, T. Lecomte, M. Pfeil, O. Green, S. Basagiannis and others, "Integrated tool chain for model-based design of Cyber-Physical Systems: The INTO-CPS project," in *2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, 2016.

[201] A. Pfouga, J. Stjepandic, T. Wekerle and C. Blume, "Smart Systems Engineering (SmartSE) - uniformed approach for exchange of functional and behavior models for simulation using Functional Mockup Interface (FMI)," 2018.

[202] H. Holzmann, "Anwendungsorientierte Übersicht kommerzieller Fahrzeug-Simulations-Systeme," in *Fahrdynamik-Regelung*, Springer, 2006, p. 93–116.

[203] Johannes Bach, "Methoden und Ansätze für die Entwicklung und den Test prädiktiver Fahrzeugregelungsfunktionen," Karlsruhe, 2018.

[204] R. Isermann, J. Schaffnit and S. Sinsel, "Hardware-in-the-loop simulation for the design and testing of engine-control systems," *Control Engineering Practice,* vol. 7, p. 643–653, 1999.

[205] T. Bock, "Bewertung von Fahrerassistenzsystemen mittels der Vehicle in the Loop-Simulation," in *Handbuch Fahrerassistenzsysteme*, H. Winner, S. Hakuli and G. Wolf, Eds., Wiesbaden, Vieweg+Teubner Verlag, 2012, p. 76–83.

[206] R. Pfeffer and T. Leichsenring, "Continuous Development of Highly Automated Driving Functions with Vehicle-in-the-Loop Using the Example of Euro NCAP Scenarios," in *Simulation and Testing for Vehicle Technology*, C. Gühmann, J. Riese and K. von Rüden, Eds., Cham, Springer International Publishing, 2016, p. 33–42.

[207] *Intelligent transport systems - Adaptive cruise control systems - Performance requirements and test procedures,* ISO 15622:2018, 2018.

[208] W. Wachenfeld and H. Winner, "Die Freigabe des autonomen Fahrens," in *Autonomes Fahren*, M. Maurer, J. C. Gerdes, B. Lenz and H. Winner, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, p. 439–464.

[209] N. Kalra and S. M. Paddock, "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?," *Transportation Research Part A: Policy and Practice,* vol. 94, p. 182–193, 12 2016.

[210] C. Neurohr, L. Westhofen, T. Henning, T. de Graaff, E. Möhlmann and E. Böde, "Fundamental considerations around scenario-based testing for automated driving," in *2020 IEEE intelligent vehicles symposium (IV)*, 2020.

[211] Raphael Pfeffer, "Szenariobasierte simulationsgestützte funktionale Absicherung hochautomatisierter Fahrfunktionen durch Nutzung von Realdaten," Karlsruhe, 2020.

[212] "Tesla Autonomy Day," Tesla, [Online]. Available: https://www.youtube.com/watch?v=Ucp0TTmvqOE. [Accessed 18 Dezember 2024].

[213] Adrian Ebner, "Referenzszenarien als Grundlage für die Entwicklung und Bewertung von Systemen der Aktiven Sicherheit," Berlin, 2014.

[214] S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt and M. Maurer, "Definition der begriffe szene, situation und szenario für das automatisierte fahren," in *10. Workshop Fahrerassistenzsysteme FAS*, 2015.

[215] M. Steimle, G. Bagschik, T. Menzel, J. T. Wendler and M. Maurer, "Ein Beitrag zur Terminologie für den szenarienbasierten Testansatz automatisierter Fahrfunktionen," *AAET-Automatisiertes und vernetztes Fahren. Hrsg. von ITS Niedersachsen,* 2018.

[216] S. Geyer, M. Baltzer, B. Franz, S. Hakuli, M. Kauer, M. Kienle, S. Meier, T. Weißgerber, K. Bengler, R. Bruder, F. Flemisch and H. Winner, "Concept and development of a unified ontology for generating test and use-case catalogues for assisted and automated vehicle guidance," *IET Intelligent Transport Systems,* vol. 8, p. 183–189, 5 2014.

[217] Heiner Bubb and Mark Vollrath and Klaus Reinprecht and Erhard Mayer and Moritz Körber, "Der Mensch als Fahrer," in *Automobilergonomie*, Wiesbaden, Springer Fachmedien Wiesbaden, 2015, p. 67–162.

[218] Jörg Henning Schneider, "Modellierung und Erkennung von Fahrsituationen und Fahrmanövern für sicherheitsrelevante Fahrerassistenzsysteme," Chemnitz, 2009.

[219] *Road vehicles - Test scenarios for automated driving systems - Scenario based safety evaluation framework,* ISO 34502:2022, 2022.

[220] "Forschungsprojekt PEGASUS: AUTOMATISIERTES FAHREN EFFEKTIV ABSICHERN.," PEGASUS, [Online]. Available: https://www.pegasusprojekt.de. [Accessed 17 August 2023].

[221] "PEGASUS Method - An Overview," PEGASUS, 2019. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS-Gesamtmethode.pdf. [Accessed 17 August 2023].

[222] "Forschungsprojekt V&V-Methoden (VVM)," [Online]. Available: https://www.vvm-projekt.de/. [Accessed 18 August 2023].

[223] R. Pfeffer, K. Bredow and E. Sax, "Trade-off analysis using synthetic training data for neural networks in the automotive development process," in *IEEE Intelligent Transportation Systems Conference (ITSC)*, Auckland, NZ, 2019.

[224] R. Pfeffer, J. He and E. Sax, "Development and Implementation of a Concept for the Meta Description of Highway Driving Scenarios with Focus on Interactions of Road Users," in *6th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2020)*, Prague, Czech Republic, 2020.

[225] C. King, "Bewertung von Fahrerassistenzsystemen im Umfeld des szenariobasierten Testens," Karlsruhe, 2023.

[226] C. King, L. Ries, C. Kober, C. Wohlfahrt and E. Sax, "Automated Function Assessment in Driving Scenarios," in *IEEE Conference on Software Testing, Validation and Verification (ICST)*, Xi'an, China, 2019.

[227] C. King, T. Braun, C. Braess, J. Langner and E. Sax, "Capturing the Variety of Urban Logical Scenarios from Bird-view Trajectories," in *7th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2021)*, 2021.

[228] F. M. Reisgys, "Glaubwürdigkeit und Einsatz des szenariobasierten X-in-the-Loop-Tests für Fahrerassistenzsysteme," Karlsruhe, 2023.

[229] F. Reisgys, J. Plaum, A. Schwarzhaupt and E. Sax, "Scenario-based X-in-the-Loop Test for Development of Driving Automation," in *Workshop Fahrerassistenzsysteme und automatisiertes Fahren*, 2022.

[230] F. Reisgys, C. Steinhauser, A. Schwarzhaupt and E. Sax, "How Uncertainty Affects Test Results for Driving Automation," in *IEEE International Automated Vehicle Validation Conference (IAVVC)*, Austin, TX, USA, 2023.

[231] B. Schütt, "Exploration and Cluster-Based Analysis of Simulated Logical Scenarios for Testing Automated Driving Systems," Karlsruhe, 2024.

[232] B. Schütt, S. Otten and E. Sax, "Clustering-based Criticality Analysis for Testing of Automated Driving Systems," in *IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*, Bilbao, Spain, 2023.

[233] B. Schütt, M. Zhang, C. Steinhauser and E. Sax, "Evolutionary Behavior Tree Generation for Dynamic Scenario Creation in Testing of Automated Driving Systems," in *7th International Conference on System Reliability and Safety (ICSRS)*, Bologna, Italy , 2023.

[234] B. Schütt, M. Zipfl, J. M. Zöllner and E. Sax, "Inverse Universal Traffic Quality - a Criticality Metric for Crowded Urban Traffic Scenes," in *IEEE Intelligent Vehicles Symposium (IV)*, Anchorage, AK, USA, 2023.

[235] B. Schütt, T. Braun, S. Otten and E. Sax, "SceML: a graphical modeling framework for scenario-based testing of autonomous vehicles," 2020.

[236] J. Bernhard, "Adaptive scenario selection for simulative testing of perception functions in automated driving," Karlsruhe, 2024.

[237] J. Bernhard, M. Schutera and E. Sax, "Optimizing test-set diversity: Trajectory clustering for scenario-based testing of automated driving systems," in *IEEE International Intelligent Transportation Systems Conference (ITSC)*, Indianapolis, IN, USA, 2021.

[238] J. Bernhard, T. Schulik, M. Schutera and E. Sax, "Adaptive test case selection for DNN-based perception functions," in *IEEE International Symposium on Systems Engineering (ISSE)*, Vienna, Austria, 2021.

[239] L. Ries, "Fahrsequenz-Clustering zur datenbasierten Szenarienanalyse für die Validierung urbaner automatisierter Fahrfunktionen," Karlsruhe, 2024.

[240] L. Ries, J. Langner, S. Otten, J. Bach and E. Sax, "A Driving Scenario Representation for Scalable Real-Data Analytics with Neural Networks," in *IEEE Intelligent Vehicles Symposium (IV)*, Paris, France, 2019.

[241] L. Ries, M. Stumpf, J. Bach and E. Sax, "Semantic Comparison of Driving Sequences by Adaptation of Word Embeddings," in *IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, Rhodes, Greece, 2020.

[242] L. Ries, P. Rigoll, T. Braun, T. Schulik, J. Daube and E. Sax, "Trajectory-Based Clustering of Real-World Urban Driving Sequences with Multiple Traffic Objects," in *IEEE International Intelligent Transportation Systems Conference (ITSC)*, Indianapolis, IN, USA, 2021.

[243] Peter Hentschel and Peter König and Peter Dauer, Straßenverkehrsrecht : Straßenverkehrsgesetz, Straßenverkehrs-Ordnung, Fahrerlaubnis-Verordnung, Fahrzeug-Zulassungsverordnung, Straßenverkehrs-Zulassungs-Ordnung, Bußgeldkatalog, Gesetzesmaterialien, Verwaltungsvorschriften und einschlägige Bestimmungen des StGB und der StPO., vol. 40, München: Beck, 2009.

[244] *19. Convention on Road Traffic,* United Nations Conference on Road Traffic, 1968.

[245] *"Straßenverkehrsgesetz (StVG) in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), das zuletzt durch Artikel 1 des Gesetzes vom 12. Juli 2021 (BGBl. I S. 3108) geändert worden ist.".*

[246] *Guidelines for the Design of Motorways,* Forschungsgesellschaft für Straßen- und Verkehrswesen e.V., 2011.

[247] *"Produktsicherheitsgesetz vom 27. Juli 2021 (BGBl. I S. 3146, 3147), das durch Artikel 2 des Gesetzes vom 27. Juli 2021 (BGBl. I S. 3146) geändert worden ist",* 2021.

[248] *"Produkthaftungsgesetz vom 15. Dezember 1989 (BGBl. I S. 2198), das zuletzt durch Artikel 5 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2421) geändert worden ist",* 1989.

[249] E. Dubrova, Fault-Tolerant Design, New, York: Springer New York, 2013.

[250] *Qualitätsmanagementsysteme – Grundlagen und Begriffe,* DIN EN ISO 9000:2015, 2015.

[251] *Terminologie der Zuverlässigkeit,* VDI 4001 Blatt 2, 2006.

[252] *Safety aspects — Guidelines for their inclusion in standards,* ISO/IEC GUIDE 51:2014(E), 2014.

[253] *Medical devices - Application of risk management to medical devices,* ISO 14971:2019, 2019.

[254] Ole Hans, "Beitrag zur Risikobetrachtung auf Bundesautobahnen unter besonderer Berücksichtigung des automobilen Bereiches," Wuppertal, 2020.

[255] *Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung,* ISO 12100:2010, 2011.

[256] B. Bertsche, P. Göhner, U. Jensen, W. Schinköthe and H.-J. Wunderlich, Zuverlässigkeit mechatronischer Systeme, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[257] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing,* vol. 1, p. 11–33, 2004.

[258] N. Leveson, "A new accident model for engineering safer systems," *Safety Science,* vol. 42, p. 237–270, 4 2004.

[259] *Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation,* ISO/TR 4804:2020, 2020.

[260] Helmut Schittenhelm, "VVM safeguarding automation –how to ensure a safe operation of an automated drivingsystem by a methodological approach?," 2022.

[261] *Road vehicles - Safety for automated driving systems - Design, verification and validation,* ISO/TS 5083:2025, 2025.

[262] *Road vehicles - Test scenarios for automated driving systems - Scenario categorization,* ISO 34504:2024, 2024.

[263] *Road vehicles - Test scenarios for automated driving systems - Scenario evaluation and test case generation,* ISO/DIS 34505:2024, 2024.

[264] *Road Vehicles - Safety and artificial intelligence,* ISO/PAS 8800:2024, 2024.

[265] *UL 4600 Standard for Safety for Evaluation of Autonomous Products,* ANSI/UL 4600-2023, 2023.

[266] Donald Firesmith and Peter Capell and Joseph P. Elm and Michael Gagliardi and Tim Morrow and Linda Roush and Lui Sha, *QUASAR: A Method for the QUality Assessment of Software-Intensive System ARchitectures,* Carnegie Mellon University, 2006.

[267] *Intelligent transport systems - Motorway chauffeur systems (MCS),* ISO/TS 23792:2023, 2023.

[268] *Road vehicles - Cybersecurity engineering,* ISO/SAE 21434:2021, 2021.

[269] M. Scholtes, L. Westhofen, L. R. Turner, K. Lotto, M. Schuldes, H. Weber, N. Wagener, C. Neurohr, M. Bollmann, F. Körtke and others, "6-Layer Model for a Structured Description and Categorization of Urban Traffic and Environment," *arXiv preprint arXiv:2012.06319,* 2020.

[270] F. Favaro, L. Fraade-Blanar, S. Schnelle, T. Victor, M. Peña, J. Engstrom, J. Scanlon, K. Kusano and D. Smith, "Building a Credible Case for Safety: Waymo's Approach for the Determination of Absence of Unreasonable Risk," *arXiv preprint arXiv:2306.01917,* 2023.

[271] S. Burton, J. A. McDermid, P. Garnett and R. Weaver, "Safety, Complexity, and Automated Driving: Holistic Perspectives on Safety Assurance," *Computer,* vol. Volume 54, no. Issue 8, pp. 22-32, 2021.

[272] S. Burton, J. A. McDermid, P. Garnett and R. Weaver, "Safer Complex Systems: An Initial Framework," 2021.

[273] S. Burton and J. A. McDermid, "Closing the gaps: Complexity and uncertainty in the safety assurance and regulation of automated driving," 2023.

[274] Hans-Leo Ross, Funktionale Sicherheit im Automobil - Die Herausforderung für Elektromobilität und automatisiertes Fahren, München: Carl Hanser Verlag, 2019.

[275] H.-L. Ross, Safety for Future Transport and Mobility, Cham: Springer International Publishing, 2021.

[276] M. Werling, R. Faller, W. Betz and D. Straub, "Safety integrity framework for automated driving," in *arXiv preprint arXiv:2503.20544*, 2025.

[277] Krzysztof Czarnecki, *On-Road Safety of Automated Driving System (ADS) Taxonomy and Safety Analysis Methods,* University of Waterloo, 2018.

[278] Krzysztof Czarnecki, *Automated Driving System (ADS) High-Level Quality Requirements Analysis Driving Behavior Safety,* University of Waterloo, 2018.

[279] A. Abdulkhaleq, D. Lammering, S. Wagner, J. Röder, N. Balbierer, L. Ramsauer, T. Raste and H. Boehmert, "A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles," *Procedia Engineering,* vol. 179, p. 41–51, 2017.

[280] Nancy G. Leveson and John P. Thomas, STPA Handbook, NANCY LEVESON AND JOHN THOMAS, 2018.

[281] N. Grabbe, A. Kellnberger, B. Aydin and K. Bengler, "Safety of automated driving: The need for a systems approach and application of the Functional Resonance Analysis Method," *Safety Science,* vol. 126, p. 104665, 6 2020.

[282] E. Hollnagel, FRAM, the functional resonance analysis method: modelling complex socio-technical systems, Farnham, Surrey, UK England ; Burlington, VT: Ashgate, 2012.

[283] K. Post and C. K. Davey, "Integrating SOTIF and Agile Systems Engineering," 2019.

[284] A. Ahlbrecht and O. Bertram, "Evaluating System Architecture Safety in Early Phases of Development with MBSE and STPA," 2021.

[285] M.-A. Meyer, S. Silberg, C. Granrath, C. Kugler, L. Wachtmeister, B. Rumpe, S. Christiaens and J. Andert, "Scenario- and Model-Based Systems Engineering Procedure for the SOTIF-Compliant Design of Automated Driving Functions," 2022.

[286] N. Jäckel, A. Karaduman, R. A. University, J. Andert, C. Granrath, B. Rumpe and L. Wachtmeister, "Feature-Driven Specification of VTOL Air-Taxis with the Use of the Model-Based System Engineering (MBSE) Methodology CUBE," 2021.

[287] C. Sippl, F. Bock, C. Lauer, A. Heinz, T. Neumayer and R. German, "Scenario-based systems engineering: An approach towards automated driving function development," in *2019 IEEE International Systems Conference (SysCon)*, 2019.

[288] J. Dawson and D. Garikapati, "Extending ISO26262 to an Operationally Complex System," 2021.

[289] X. Yang, M. Li, Y. Liu, C. Sun, M. Wu and S. Zhou, "Development of ISO 26262 and ISO 21448 Concept Design Process Integration: ISO 26262 and ISO/PAS 21448 Design Process Integration," 2022.

[290] W. Kröger, "How safe should automated vehicles be? - A survey and proposal for discussion," *Next Research,* vol. Volume 2, no. Issue 2, 2025.

[291] M. A. Mehlhorn, A. Richter and Y. A. Shardt, "Ruling the Operational Boundaries: A Survey on Operational Design Domains of Autonomous Driving Systems," *IFAC-PapersOnLine,* vol. Volume 56, no. Issue 2, pp. 2202-2213, 2023.

[292] H. Wang, W. Shao, C. Sun, K. Yang and D. C. J. Li, "A Survey on an Emerging Safety Challenge for Autonomous Vehicles: Safety of the Intended Functionality," *Engineering,* vol. Volume 33, pp. 17-34, 2024.

[293] C. Correa-Jullian, M. Ramos, A. Mosleh and J. Ma, "Operational safety hazard identification methodology for automated driving systems fleets," *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability,* vol. Volume 239, no. Issue 2, pp. 310-343, 2024.

[294] A. Aniculaesei, I. Aslam, D. Bamal, F. Helsch, A. Vorwald, M. Zhang and A. Rausch, "Connected Dependability Cage Approach for Safe Automated Driving," in *arXiv preprint arXiv:2307.06258*, 2023.

[295] C. A. J. Hanselaar, E. Silvas, A. Terechko and W. P. M. H. Heemels, "The Safety Shell: An Architecture to Handle Functional Insufficiencies in Automated Driving," in *arXiv preprint arXiv:2311.08413*, 2023.

[296] M. Stoffel, "On-Demand Triple Modular Redundancy for Autonomous Vehicles," Karlsruhe, 2025.

[297] M. Stoffel and E. Sax, "Distributed Voters for Automotive Applications," in *IEEE Intelligent Vehicles Symposium (IV)*, Anchorage, AK, USA, 2023.

[298] M. Stoffel, M. Schindewolf and E. Sax, "On-Demand Triple Modular Redundancy for Automotive Applications," in *IEEE International Systems Conference (SysCon)*, Montreal, QC, Canada, 2024.

[299] Z. Jiang, W. Pan, J. Liu, Y. Han, Z. Pan and H. Li, "Enhancing Autonomous Vehicle Safety Based on Operational Design Domain Definition, Monitoring, and Functional Degradation: A Case Study on Lane Keeping System," in *IEEE Transactions on Intelligent Vehicles*, 2024.

[300] P. Weissensteiner, G. Stettinger, S. Khastgir and D. Watzenig, "Operational Design Domain-Driven Coverage for the Safety Argumentation of Automated Vehicles," in *IEEE Access (Volume: 11)*, 2023.

[301] R. Kallweit, U. Gropengießer, J. Männel and R. Singh, "Safe and Robust Function Development for Urban Autonomous Driving Based on Agile Methodology and DevOps," in *Automatisiertes Fahren 2020*, 2021.

[302] T. Myklebust, T. Stålhane and G. K. Hanssen, "Agile Safety Case and DevOps for the Automotive Industry," in *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 2020.

[303] P. Munk and M. Schweizer, "DevOps and Safety? SafeOps! Towards Ensuring Safety in Feature-Driven Development with Frequent Releases," in *Computer Safety, Reliability, and Security. SAFECOMP 2022 Workshops*, 2022.

[304] M. Zeller, "Towards Continuous Safety Assessment in Context of DevOps," in *Computer Safety, Reliability, and Security. SAFECOMP 2021 Workshops*, 2021.

[305] J. Erz, S. Burton and E. Sax, "Extending the Automotive Safety Life Cycle Towards Operational Safety of Automated Driving," in *IEEE International Automated Vehicle Validation Conference (IAVVC)*, Baden-Baden, Deutschland, 2025.

[306] J. Erz, B. Schutt, T. Braun, H. Guissouma and E. Sax, "Towards an Ontology That Reconciles the Operational Design Domain, Scenario-based Testing, and Automated Vehicle Architectures," in *IEEE International Systems Conference (SysCon)*, Montreal, QC, Kanada , 2022.

[307] "ASAM OpenSCENARIO," ASAM e. V., [Online]. Available: https://www.asam.net/standards/detail/openscenario/. [Accessed 18 August 2023].

[308] *Straßenfahrzeuge - Fahrzeugdynamik und Fahrverhalten - Begriffe,* ISO 8855:2013, 2013.

[309] *UN-Regelung Nr. 157,* UN-Regelung Nr. 157, 2021.

[310] "Straßenverkehrs-Ordnung (StVO) § 3 Geschwindigkeit," [Online]. Available: https://www.gesetze-im-internet.de/stvo_2013/__3.html. [Accessed 9 Juni 2024].

[311] "Straßenverkehrs-Ordnung (StVO) § 4 Abstand," [Online]. Available: https://www.gesetze-im-internet.de/stvo_2013/__4.html. [Accessed 9 Juni 2024].

[312] R. Isermann, Automotive Control - Modeling and Control of Vehicles, Darmstadt: Springer-Verlag GmbH Germany, 2022.

[313] J. Krampe and M. Junge, "Injury Severity for Hazard & Risk Analyses:Calculation of ISO 26262 S-parameter Values from Real-World Crash Data," *Accident Analysis & Prevention,* vol. 138, no. 105321, 2020.

[314] "SCODE Workbench: Regelungssysteme modellieren, analysieren, verifizieren und implementieren," ETAS GmbH, [Online]. Available: https://www.etas.com/de/anwendungen/applications_functional_safety_iso_26262.php#heading-96a48ea3-eb11-456f-94f2-06f182a0d332. [Accessed 10 Juni 2024].

[315] Y. Umeda, "Function Modeling," in *CIRP Encyclopedia of Production Engineering*, T. I. A. for Produ, L. Laperrière and G. Reinhart, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, p. 1–9.

[316] "TEMPUS-Testfeld München – Pilotversuch Urbaner automatisierter Straßenverkehr," [Online]. Available: https://www.itiv.kit.edu/294_8019.php. [Accessed 10 Juni 2024].

[317] L. Putze, L. Westhofen, T. Koopmann, E. Böde and C. Neurohr, "On Quantification for SOTIF Validation of Automated Driving Systems," *arXiv preprint arXiv:2304.10170,* 2023.

[318] H. Guissouma, S. Leiner and E. Sax, "Towards Design and Verification of Evolving Cyber Physical Systems Using Contract-Based Methodology," in *5th IEEE International Symposium on Systems Engineering*, 2020.

[319] J. Erz, S. Burton and E. Sax, "Formal Safety and Robustness Verification of Nonlinear Vehicle Systems Under Uncertainty Using Sum-of-Squares Optimization," in *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Wien, Österreich, 2025.

[320] *Model Architecture and Interfaces Recommended Practice for Ground Vehicle System and Subsystem Dynamical Simulation,* SAE International J3049, 2015.

[321] J. Lunze, Regelungstechnik 1, Berlin, Heidelberg: Springer Berlin Heidelberg, 2016.

[322] M. Mitschke and H. Wallentowitz, Dynamik der Kraftfahrzeuge, Wiesbaden: Springer Fachmedien Wiesbaden, 2014.

[323] F. Tränkle, Modellbasierte Entwicklung Mechatronischer Systeme, Heilbronn: Walter de Gruyter GmbH, Berlin/Boston, 2021.

[324] H. B. Pacejka, Tire Characteristics and Vehicle Handling and Stability, Elsevier, 2012.

[325] M. Butz, C. Heinzemann, M. Herrmann, J. Oehlerking, M. Rittel, N. Schalm and D. Ziegenbein, "SOCA: Domain Analysis for Highly Automated Driving Systems," in *IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, Rhodes, Greece, 2020.

[326] F. Zwicky, "A Way of Thinking: Discovery, Invention, Research, through the Morphological Approach," *Science,* vol. 163, p. 1316–1317, 1969.

Eigene wissenschaftliche Beiträge

J. Erz, B. Schutt, T. Braun, H. Guissouma and E. Sax, "Towards an Ontology That Reconciles the Operational Design Domain, Scenario-based Testing, and Automated Vehicle Architectures," in *IEEE International Systems Conference (SysCon)*, Montreal, QC, Kanada, 2022.

H.-L. Ross, J. Erz, "Sensor Principles for Digital Sound Twin" *in Organic and Inorganic Materials Based Sensors (eds S. Das, S. Thomas and P.P. Das)*, 2023. https://doi.org/10.1002/9783527834266.ch47

J. Erz, S. Burton, and E. Sax, "Extending the Automotive Safety Life Cycle Towards Operational Safety of Automated Driving," in *IEEE International Automated Vehicle Validation Conference (IAVVC)*, Baden-Baden, Deutschland, 2025.

J. Erz, S. Burton, and E. Sax, "Formal Safety and Robustness Verification of Nonlinear Vehicle Systems Under Uncertainty Using Sum-of-Squares Optimization," in *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Wien, Österreich, 2025.

Betreute Abschlussarbeiten

Ole Hans, "Beitrag zur Risikobetrachtung auf Bundesautobahnen unter besonderer Berücksichtigung des automobilen Bereiches," Wuppertal, 2020.

A. Reisgys, "Modellbasierter Regelungsentwurf für einen Highway Pilot sowie dessen Sicherheitsanalyse und Validierung in einer Gesamtfahrzeugsimulation," Karlsruhe, 2022.

P. Bertsch, "Entwurf und Validierung eines modellbasierten Sicherheitskonzepts für die Longitudinalführung eines hochautomatisierten Highway Pilot," Heilbronn, 2022.

A Anhang Grundlagen und Methoden

A.1 Erläuterungen zur Farbsemantik und Systems Modeling Language (SysML) Verbindungstypen

Nachfolgend wird die im Zuge der vorliegenden Dissertation gewählte Farbsemantik der Abbildungen dargelegt:

- Zum einen repräsentiert ein dunkler werdender Farbverlauf die Zunahme der Granularität, vom Groben ins Feine. Dabei erfolgt dies entweder über den Hintergrundfarbton (siehe Abbildung 7.13) oder aber den Farbton des jeweiligen Elements selbst (siehe Abbildung 4.1).

- Zum anderen wird die Zunahme des Reifegrads durch einen dunkler werdenden Farbverlauf visualisiert (siehe Abbildung 7.10 und Abbildung 7.20)

- Der Aspekt eines technischen Systems wird in hellblau hervorgehoben. Hinzu kommt die farbliche Unterscheidung der Systemattribute Funktion (lila), Verhalten und Zustand (grün) und Struktur (blau) (siehe Abbildung 4.2). Diese Farbsemantik wird darüber hinaus auf die Thematik der Fahrzeugsystemarchitekturen und Modellierungsrahmenwerke übertragen, wobei die technische Architektur in orange und der Anforderungsaspekt in grau hervorgehoben wird (siehe Abbildung 4.4 und Abbildung 4.11). Des Weiteren werden fahrzeugexterne Betriebsbereichsattribute in hellblau dargestellt, wohingegen fahrzeuginterne Systeme, Subsysteme, Komponenten und Einheiten in einem kräftigeren Blau abgegrenzt werden (siehe Abbildung 2.3 und Abbildung 2.5). Es sei anzumerken, dass diesbezüglich das Systemattribut der Struktur bzw. der logischen Architektur maßgebend ist.

- Das Ego-Kraftfahrzeug wird durchgehend in gelber Farbe dargestellt, wobei der menschliche Fahrer in einem hellen Hautton abgebildet wird (siehe Abbildung 1.1 und Abbildung 6.1).

- Im Rahmen der Vorgehensmodelle und Prozessreferenzen wird die allgemeine Systementwicklung in hellgrün visualisiert (siehe Abbildung 3.4). Aspekte der funktionalen Sicherheit (FuSa) werden in hellem Lila, Elemente der Sicherheit der beabsichtigten Funktionalität (SotiF) in hellem Gelb und Elemente der übergreifenden Betriebssicherheit werden in hellem Orange dargestellt. Hinzu kommt die Hervorhebung der Nachweisführungskette Evidenz → Argument → Behauptung in dunklem Beige (siehe Abbildung 7.1).

Im Kontext der SysML Klassendiagramme werden insgesamt drei Verbindungstypen eingesetzt (siehe Abbildung A.1):

- Komposition (engl. *Composition*): Die Komposition beschreibt eine sogenannte Ganzes-Teil-Beziehung, bei der ein Teil ohne das übergeordnete Ganze nicht unabhängig existieren kann (z.B. ein Motor als Bestandteil eines Autos) [189].

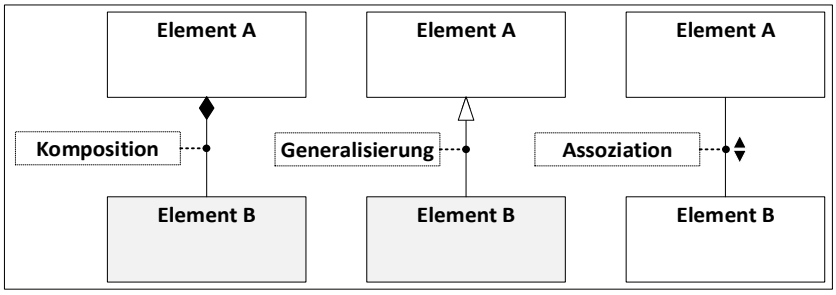


Abbildung A.1: Verbindungstypen der SysML Klassendiagramme.

- Generalisierung/Vererbung (engl. *Generalization*): Die Generalisierung modelliert eine Vererbungsbeziehung, bei der eine spezialisierte Klasse alle Eigenschaften und Beziehungen ihrer übergeordneten, allgemeineren Klasse erbt [189].
- Assoziation (engl. *Association*): Die Assoziation stellt eine lose Beziehung zwischen zwei Klassen dar, die miteinander interagieren (Schwerpunkt der Richtung über Pfeilspitzen dargestellt siehe Abbildung A.1) oder in einem bestimmten Zusammenhang stehen, ohne dass eine strukturelle Abhängigkeit besteht [189].

A.2 Strukturierung und Schnittstellenbeschreibung von Fahrzeugsystemarchitekturen

Im Zuge der Entwicklung funktionaler, logischer und technischer Architekturen (vgl. Abschnitt 4.2) ergibt sich mitunter die Fragestellung anhand welcher Kriterien bzw. anhand von welchem Strukturierungsmuster die Funktionen sowie das jeweilige Verhalten und die dazu adäquaten logischen und ggf. technischen Architekturbausteine abgeleitet werden können. In der SAE J3049 [320] wird dargelegt, dass jedes logische System-Of-Systems, System, Subsystem, Komponente oder Einheit intern über vier unterscheidbare elementare Funktions- und/oder Verhaltensbausteine verfügen kann. Darunter fallen Regler-, Stellglieder- bzw. Aktuatoren, Regelstrecken- und Sensorfunktionen bzw. -verhalten. Diese Funktionsstruktur überträgt sich zudem auf die interne logische Partitionierung eines System-Of-Systems, Systems, Subsystems, einer Komponente oder einer Einheit, wodurch diese in Regler-, Aktuatoren-, Regelstrecken- und Sensorelemente (engl. *Controller, Actuator, Process, Sensor {CAPS}*) unterteilt werden. Den logisch und/oder technischen Elementen sind die jeweiligen Regler-, Aktuatoren-, Regelstrecken- und Sensorfunktionen bzw. -verhalten (Farbübergang lila-grün) zugeteilt. Diese sind wiederum über Schnittstellen zur Energieübertragung (blaue Konnektoren), zum Austausch physikalischer Bedingungen (orange Konnektoren), der Kommunikation und Nachrichtenübertragung (schwarz gepunktete Konnektoren) als auch ggf. Schnittstellen der Mensch-Maschine-Interaktion (rosa Konnektoren) verknüpft (siehe Abbildung A.2).

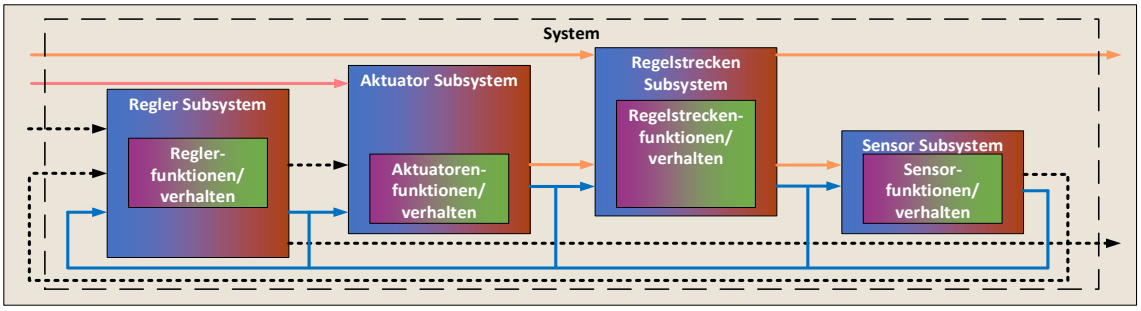


Abbildung A.2: Logische und/oder technische Partitionierung (dargestellt durch Farbübergang blau-braun) eines Systems in CAPS-Subsysteme.

Als zusätzlicher Baustein wird ein Schnittstellenkonzept für eine konsistente standardisierte Betrachtung der Interaktionspunkte bzw. Schnittstellen der jeweiligen funktionalen, logischen und technischen Architekturen benötigt. Vor diesem Hintergrund werden vier allgemeine Arten von Schnittstellen gemäß der SAE 3049 [320] hergeleitet und im Detail erläutert:

- **Schnittstelle zur Energieübertragung (engl. *Energy Transport Interface*):** Der Zweck der Energieübertragungsschnittstellen besteht darin, den Betrieb der miteinander verbundenen Funktionen sowie logischer und technischer Elemente im Hinblick auf die Energie als sogenannte konservierbare Menge (engl. *Conservable Quantity*) im Sinne der Energieerhaltung zu beschreiben und hervorzuheben, welche zwischen diesen ausgetauscht wird. Im Allgemeinen hängen die Schnittstellen der Energieübertragung von den verwendeten Modellierungsannahmen ab, insbesondere in Bezug auf die zu berücksichtigenden oder zu vernachlässigenden physikalischen Phänomene. Darunter fallen Aspekte wie Energien, welche im Zuge translatorischer und rotatorischer Mechanik erhalten bzw. übertragen werden. Des Weiteren beziehen sich diese Schnittstellen auf den Austausch elektrischer, magnetischer, thermischer, thermodynamischer, hydraulischer, pneumatischer Energien im Zuge der jeweiligen Stoff- und Materialflüsse bzw. Volumenströme. Diese Aufzählung erhebt keinen Anspruch auf Vollständigkeit, d.h. es kann je nach den Modellierungsannäherungen und den verwendeten, analysierten und modellierten Energietypen noch weitere Arten von Energie geben. Allerdings werden Energien als reine Träger von Informationen, beispielsweise aus dem Bereich der Akustik und Strahlung im Sinne der signalbasierten Interaktion, nicht unter Schnittstellen der Energieübertragung aufgefasst, insofern ausschließlich die Informationsübertragung im Fokus steht. Diese werden dann als Schnittstellen der Kommunikation und Nachrichtenübertragung betrachtet.

- **Schnittstelle zum Austausch physikalischer Bedingungen, Eigenschaften und Größen (engl. *Physical Condition Interface*):** Die Schnittstellen für den Austausch von physikalischen Bedingungen stellen Größen zur Verfügung, welche sich auf Bedingungen außerhalb der Energieübertragung und -erhaltung von Funktionen, logischen und technischen Elementen beziehen. Hierunter fallen statische und dynamische Bewegungsgrößen wie Positionen, Geschwindigkeiten, Beschleunigungen, Ruck etc. sowie Kräfte und Drehmomente. Des Weiteren sind diese Schnittstellen für die Interaktion mit analogen und kontinuierlichen elektromagnetischen Strahlungswellen/Signalen angedacht, wie z.B. das Leuchten von Fahrtrichtungsanzeigern, Verkehrsampeln, analogen Funkwellen, analogen Schallwellen usw. Dabei handelt es sich mitunter um atmosphärische Bedingungen sowie geometrische Strukturen und Oberflächen der Straße oder der Umge-

bung, die beispielsweise über eine Umgebungsperzeption wahrgenommen werden. Es sei an dieser Stelle darauf hingewiesen, dass der Transport von Energie und Impulsen über diese elektromagnetischen Wellen nicht Gegenstand dieser Betrachtung ist.

- **Schnittstelle der Kommunikation und Nachrichtenübertragung (engl. *Controller and/or Data Interface*):** Die Schnittstellen der Steuerung und Regelung zielen darauf ab, den Austausch von Informationen, Daten oder Signalen zwischen Funktionen, logischen und technischen Elementen zu ermöglichen. Genauer gesagt werden diese Schnittstellen für die Kommunikation und Nachrichtenübertragung von Signalen zwischen Steuergeräten (z.B. Statusabfragen, Befehle, Sensormesswerte, berechnete Variablen usw.), von Signalen zwischen Steuergeräten und Sensoren sowie Aktuatoren (z.B. Aktuatorstellbefehle, Sensorsignale usw.) sowie von Informationen, beispielsweise über den topologischen und geometrischen Zustand des Verkehrs, der Straßen, des Geländes, als auch der jeweils vorherrschenden Umgebungsbedingungen benötigt. Diese Schnittstellen werden somit für die Interaktion mit digitalen bzw. diskreten numerischen Signalen herangezogen. Insgesamt handelt es sich demzufolge vornehmlich um protokollbasierte Schnittstellen für den Austausch interpretierter und digitalisierter Signale und Botschaften. Innerhalb der technischen Architektur werden diese Schnittstellen anhand der jeweiligen CAN-, LIN-, FlexRay-, MOST- oder Ethernet-Kommunikationsnetzwerke detailliert bzw. spezifiziert.

- **Schnittstellen der Mensch-Maschine-Interaktion (engl. *Human-Machine-Interaction Interfaces*):** Darüber hinaus werden Schnittstellen der Mensch-Maschine-Interaktion zur Steuerung, Regelung und Überwachung von Funktionen, logischen und technischen Elementen bzw. Systemen benötigt. Diese Schnittstellen beinhalten Pedale, Hebel, Knöpfe, Schalter, Lenkräder, Touchscreens usw., worauf über physikalische Mechanismen (ohne Übertragungsmedien wie Smartphone, Autoschlüssel, diese gehören wiederum zu den Schnittstellen der Steuerung und Regelung) im Sinne des Einsatzes von Händen oder Füßen eingewirkt wird. Hinzu kommen akustische Sprachbefehle sowie visuelle Gestensteuerungen. Ferner werden darunter auch Anzeigen, Displays, Leuchten, akustische Warnsignale, Vibratoren usw. erfasst, welche durch den menschlichen Anwender physisch mit dessen Sinnesorganen (Sehen, Hören, Gleichgewicht, Fühlen usw.) wahrgenommen werden.

A.3 Klassifikation von analytischen Verhaltensbeschreibungen

Im Hinblick auf die Klassifikation von Modellen im Kontext der modellbasierten Systementwicklung (vgl. Abschnitt 4.4) lassen sich Simulations- bzw. analytische Verhaltensmodelle anhand unterschiedlicher Kriterien nochmals spezifischer charakterisieren [321]:

- **Statisch vs. dynamisch:** Bei analytisch statischen Simulationsmodellen erfolgt keine Abspeicherung des Verlaufs einer eingangsseitigen Stimulierung und die Abbildung der Eingangsgrößen erfolgt mittels algebraischer Gleichungen. Dahingegen wird bei analytisch dynamischen Simulationsmodellen der zeitliche Verlauf einer am Modell bzw. Systemeingang wirkenden Anregung abgespeichert und es findet ein Einschwingvorgang in Bezug auf den jeweiligen Stimulus statt (siehe Abbildung A.3).

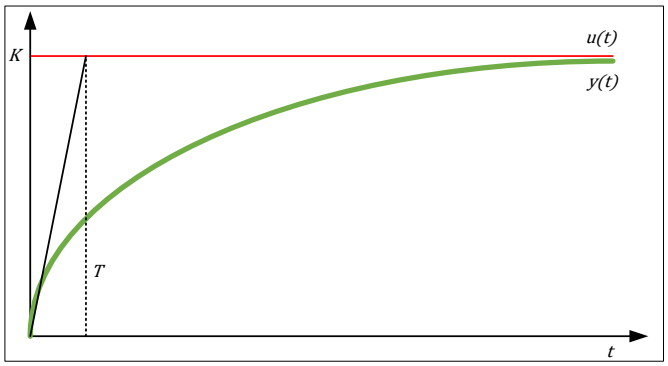


Abbildung A.3: Analytisch dynamischer bzw. zeitlicher Verlauf der Ausgangsgröße $y(t)$ eines PT_1-Glieds nach einer eingangsseitigen Sprunganregung $u(t)$. Hierbei bezeichnet K den Verstärkungsfaktor und T die Zeitkonstante.

Dieser dynamische Zusammenhang lässt sich in Form der ODE

$$\dot{y}(t) = \frac{1}{T}\left(K \cdot u(t) - y(t)\right) \tag{A.1}$$

für das Verzögerungsglied erster Ordnung (PT_1-Glied) darstellen.

Mittels der Laplace-Transformation ergibt sich wiederum

$$G_{PT_1}(s) = \frac{K}{Ts + 1} \tag{A.2}$$

als Übertragungsfunktion im Frequenz- bzw. Bildbereich.

Das Totzeit- bzw. T_t-Glied wird mittels der ODE

$$y(t) = u(t - T_t) \tag{A.3}$$

dargestellt und verschiebt das Eingangssignal auf der Zeitachse um T_t nach rechts. Für die Übertragungsfunktion ergibt sich wiederum

$$G_{T_t}(s) = e^{-sT_t} \tag{A.4}$$

als Ausdruck.

Das PT_1T_t-Glied

$$G_{PT_1T_t}(s) = \frac{K}{Ts + 1} e^{-sT_t} \tag{A.5}$$

entsteht wiederum durch das hintereinander Schalten eines PT_1- und eines T_t-Glieds.

- **Zeitkontinuierlich vs. zeitdiskret:** Bei zeitkontinuierlichen Simulationsmodellen werden die Signalverläufe zu einem jeden beliebigen Zeitpunkt aufgezeichnet. Dadurch eignet diese Modellart insbesondere für die Modellierung und Simulation dynamischer physikalischer Prozesse bzw. Systeme deren Abbildung auch anhand von ODEs erfolgt. Im Gegensatz dazu liegen bei zeitdis-

kreten Simulationsmodellen die Signalwerte nur zu bestimmten Zeitpunkten vor. Das Grundprinzip dieser Modelle basiert auf einer zeitdiskreten Sequenz an Interaktionen bzw. Ereignissen (engl. *Events*), welche einen Einfluss auf den Zustand eines Systems oder Prozesses nehmen.

- **Wertekontinuierlich vs. wertediskret:** Bei wertekontinuierlichen Simulationsmodellen existieren keine Beschränkungen, was den Wertebereich zur Abbildung einer Funktion über Zustandsvariablen angeht, wodurch beispielsweise physikalische Prozesse oder Effekte einem exakten Wert zugeordnet werden können. Dahingegen ist der Wertebereich wertediskreter Modelle auf einen endlichen quantisierten Bereich limitiert. Darauf bezugnehmend spiegelt eine Werteänderung ein entsprechendes Ereignis wider.

- **Zeitinvariant vs. zeitvariant:** Zeitinvariante Simulationsmodelle weisen unabhängig vom Zeitpunkt der Anregung bei identischen Eingangssignalen stets dasselbe Verhalten auf. Im Gegensatz dazu handelt es sich um zeitvariante Modelle, wenn sich Parameter bzw. Koeffizienten in Relation zur Zeit verändern.

- **Kausal vs. akausal:** Das Verhalten kausaler Simulationsmodelle hängt exklusiv vom zeitlichen Verlauf der gegebenen Eingangsgrößen ab. Folglich können diese ausschließlich zukünftige Werte und damit keine Zustandsgrößen zu einem in der Vergangenheit liegenden Zeitpunkt beeinflussen. Akausale Modelle hingegen beruhen auf bestimmten physikalischen Einschränkungen, exemplarisch seien hier die Kirchhoff'schen Gesetze bei elektrischen Schaltungen genannt, und können nicht anhand von Eingangs- und Zustandsgrößen, sprich unter Anwendung von ODEs abgebildet werden.

- **Linear vs. nichtlinear:** Die Systemgleichungen linearer Simulationsmodelle erfüllen sowohl das Verstärkungs- als auch das Superpositionsprinzip arbiträrer Eingangsanregungen zu sämtlichen Zeitpunkten. Im Gegensatz dazu handelt es sich um nichtlineare Modelle, wenn Potenz-, Multiplikations- als auch Divisionsoperationen der Eingangsstimuli oder Zustandsgrößen vorliegen. Die ODEs nichtlinearer Systeme können nicht explizit gelöst werden und müssen mit numerischen Verfahren angenähert werden.

A.4 Analytisch dynamische Verhaltensbeschreibungen der Fahrzeugdynamik und Aktuatorik

Hinsichtlich der analytisch dynamischen Verhaltensbeschreibung der Fahrdynamik kennzeichnet sich die Fahrphysik als maßgebend, wobei diese in Längs-, Quer- und Vertikaldynamik unterteilt wird (siehe Abbildung A.4).

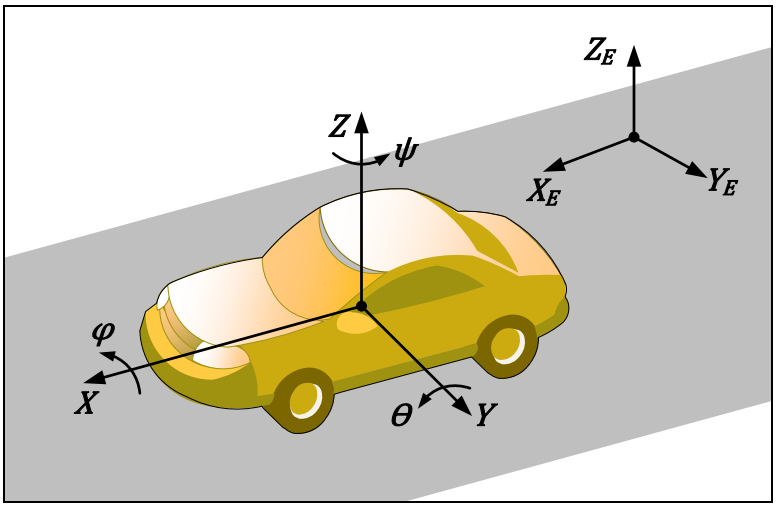


Abbildung A.4: Horizontiertes und ortsfestes Koordinatensystem gemäß ISO 8855 [308].

Die dabei vorliegenden Bewegungsfreiheitsgrade werden gemäß der ISO 8855 [308] vorgegeben, wobei die Achsen und Rotationswinkel im horizontierten X, Y, Z-Koordinatensystem wie folgt definiert sind:

- X: Fahrzeuglängsachse
- Y: Fahrzeugquerachse
- Z: Fahrzeugvertikalachse
- φ: Fahrzeugwankwinkel
- θ: Fahrzeugnickwinkel
- ψ: Fahrzeuggierwinkel

Die Analyse der Vertikaldynamik ist insbesondere dann relevant, wenn Schwingungen aufgrund von Straßeneinwirkungen untersucht werden sollen [322]. Im Kontext von Simulationen für die Fahrzeugautomatisierung spielt dies jedoch eine untergeordnete Rolle. In Bezug auf die Längs- und Querdynamik stellt das Beschleunigungsmodell einer Punktmasse eine grundlegende Methode zur Beschreibung von Geschwindigkeits- und Positionsänderungen im ortsfesten X_E, Y_E, Z_E-Koordinatensystem dar. In diesem Kontext werden die Beschleunigungen in den X_E- und Y_E-Koordinaten unter Einbeziehung des Kurs- bzw. Fahrzeuggierwinkels ψ um die Z_E-Achse betrachtet (siehe Abbildung A.5).

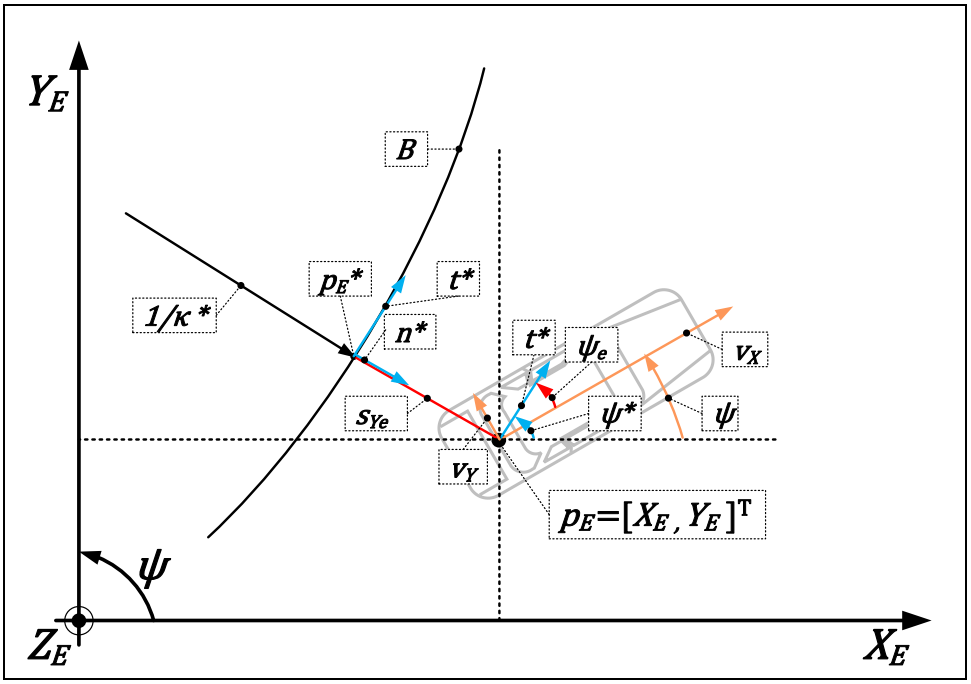


Abbildung A.5: Fahrzeugbewegungs- und Fahrbahngrößen zur Bestimmung der Quer- und Kurswinkelabweichung gemäß [323].

Die Beschleunigung in X_E-Richtung wird durch

$$a_{X_E} = a_X \cos\psi - a_Y sin\psi - \dot{\psi}(v_X sin\psi - v_Y cos\psi) \quad \text{A.6}$$

beschrieben.

Die Beschleunigung in Y_E-Richtung wird wiederum durch

$$a_{Y_E} = a_X sin\psi + a_Y cos\psi + \dot{\psi}(v_X cos\psi - v_Y sin\psi) \quad \text{A.7}$$

abgebildet.

Infolgedessen kann die Fahrzeugbewegung durch eine rein translatorische Bewegung des Fahrzeughinterachsmittelpunkts entlang der Fahrzeuglängsachse in Kombination mit einer Rotationsbewegung um diesen Punkt repräsentiert werden. Diesbezüglich ist der zum Fahrzeugbezugspunkt bzw. Fahrzeughinterachsmittelpunkts $\boldsymbol{p}_E$ am nächsten liegende Punkt auf der Sollbahn der Referenzpunkt $\boldsymbol{p}_E^*$, um aus einem Vergleich der aktuellen Fahrzeugposition zu diesem Referenzpunkt auf der Sollbahn die Quer- und Kurswinkelabweichung zu berechnen. Hierfür werden drei einzelne skalare Regelabweichungen betrachtet. Darunter fallen der tangentiale Abstand s_{Xe} des Fahrzeugbezugspunkts $\boldsymbol{p}_E$ zum nächsten Punkt $\boldsymbol{p}_E^*$ auf der Sollbahnkurve, der orthogonale Abstand s_{Ye} des Fahrzeugbezugspunkts $\boldsymbol{p}_E$ zum nächsten Punkt $\boldsymbol{p}_E^*$ auf der Sollbahnkurve als auch die Kurswinkelabweichung ψ_e des Kurswinkels ψ zum Richtungswinkel ψ^*der Sollbahnkurve am nächstgelegen Referenzpunkt $\boldsymbol{p}_E^*$. Die Bogenlänge $s*$ am Referenzpunkt $\boldsymbol{p}_E^*$ resultiert aus der orthogonalen Projektion des Fahrzeughinterachsmittelpunkts $\boldsymbol{p}_E$ auf die Sollbahn B. Die Sollbahn wird wiederum durch den Referenzkurswinkel ψ^* und ihre bogenlängenabhängige Krümmung $\kappa^*(s^*)$ beschrieben (siehe Abbildung A.5).

Der hierfür notwendige Normalvektor

$$\boldsymbol{n}^*(\boldsymbol{p}_E^*) = \begin{bmatrix} -sin\psi^* \\ cos\psi^* \end{bmatrix} \tag{A.8}$$

wird zunächst aus dem Richtungswinkel θ^* der Sollbahnkurve determiniert, wobei der Tangentialvektor gemäß

$$\boldsymbol{t}^*(\boldsymbol{p}_E^*) = \begin{bmatrix} cos\psi^* \\ sin\psi^* \end{bmatrix} \tag{A.9}$$

angegeben wird.

Hierbei verschwindet der tangentiale Abstand bzw. die tangentiale Abweichung

$$s_{Xe} = \underbrace{[\boldsymbol{p}_E - \boldsymbol{p}_E^*]}_{\boldsymbol{s}_e^T}{}^T \boldsymbol{t}^*(\boldsymbol{p}_E^*) = 0 \tag{A.10}$$

zur Sollbahnkurve, da sich der nächstgelegene Referenzpunkt $\boldsymbol{p}_E^*$ auf der Sollbahn aus einer orthogonalen Projektion des Fahrzeugschwerpunkts $\boldsymbol{p}_E$ auf die Sollbahnkurve B ergibt. Darüber hinaus wird durch eine Projektion des Differenzvektors $\boldsymbol{s}_e^T$ auf die Normale zur Sollbahnkurve anschließend der orthogonale Abstand

$$s_{Ye} = \underbrace{[\boldsymbol{p}_E - \boldsymbol{p}_E^*]}_{\boldsymbol{s}_e^T}{}^T \boldsymbol{n}^*(\boldsymbol{p}_E^*) \tag{A.11}$$

des Fahrzeughinterachsmittelpunkts $\boldsymbol{p}_E$ des „L_1-Ego-Kraftfahrzeugs_L“ zum Referenzpunkt $\boldsymbol{p}_E^*$ ermittelt.

Insgesamt ergibt sich

$$\dot{s}_Y = v_X \cdot sin\psi_e \tag{A.12}$$

als Dynamik der Querabweichung.

Die Dynamik der Bogenlänge wird mittels

$$\dot{s}^* = v_X \frac{cos\psi_e}{1 - s_Y \cdot \kappa^*(s^*)} \tag{A.13}$$

abgebildet.

Die Kurswinkelabweichung

$$\psi_e = \psi - \psi^*(\boldsymbol{p}_E^*) \tag{A.14}$$

resultiert ihrerseits aus der Differenz des tatsächlichen Kurs- bzw. Gierwinkels ψ des „L_1-Ego-Kraftfahrzeugs_L“ zum Richtungs- bzw. Referenzkurswinkel ψ^*der Sollbahnkurve.

Aus den vorangegangenen Betrachtungen kann nun die Dynamik der Kurswinkelabweichung mittels

$$\dot{\psi}_e = \dot{\psi} - \kappa^*(s^*) \cdot \dot{s}^* = \dot{\psi} - \dot{\psi}^* = \dot{\psi} - v_X \frac{cos\psi_e}{1 - s_Y \cdot \kappa^*(s^*)} \kappa^*(s^*) \tag{A.15}$$

beschrieben werden.

Für eine detailliertere Beschreibung der Fahrdynamik kann das dynamische nichtlineare Einspurmodell herangezogen werden (siehe Abbildung A.6).

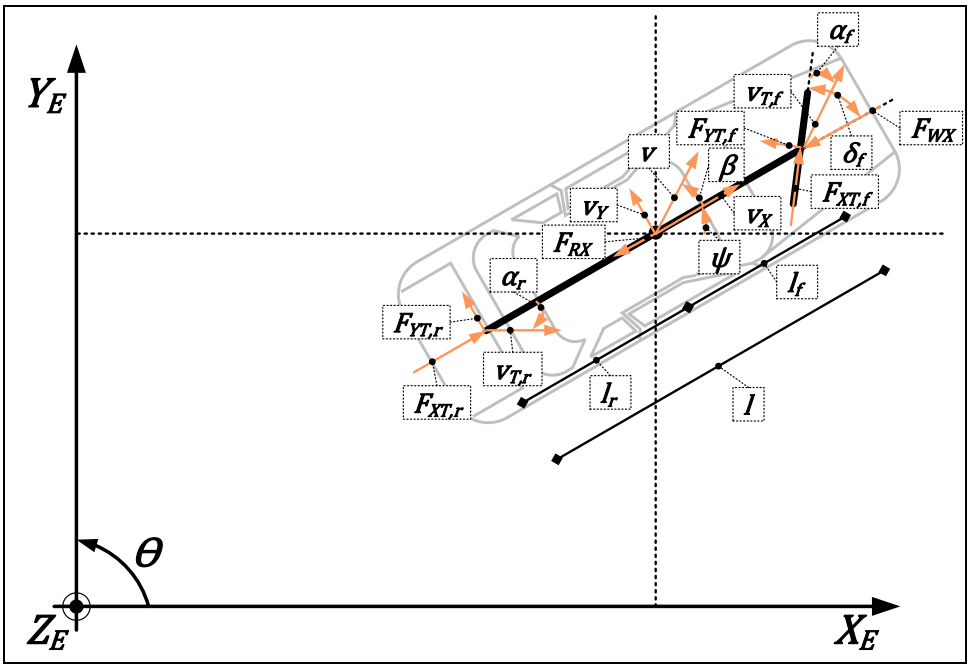


Abbildung A.6: Durch Reifenkräfte hervorgerufene Bewegungsgrößen des dynamischen Einspurmodells gemäß [322].

Dieses berücksichtigt sowohl die Reifenlängs- als auch die Reifenquerkräfte sowie die rotatorische Massenträgheit [322]. Dabei wird der Referenzpunkt entlang der Längsachse im Schwerpunkt des Fahrzeugs platziert (siehe Abbildung A.6). Insgesamt zeichnet sich das dynamische Einspurmodell durch folgende Eigenschaften und Modellannahmen aus:

- Die Lenkung erfolgt ausschließlich durch die Vorderachse, der Fahrzeugkörper ist starr und es erfolgt keine Berücksichtigung von Nick- und Wankbewegungen und damit variierenden Radlasten.
- Das Gesamtfahrzeug wird als starrer Körper erfasst, wodurch unter Vernachlässigung der Nick- und Wankdynamik die Möglichkeit besteht, die Hinterräder und Vorderräder zu jeweils einem einzelnen virtuellen Rad auf der Fahrzeuglängsachse zusammenzufassen.
- Die Räder werden als Punkte im Raum betrachtet, ihre Positionen sind starr zum Fahrzeugkörper, wobei die Querbewegung der Räder mit einem Schräglauf versehen ist. Dadurch ist es möglich, die Fahrzeugquerdynamik bis zu Querbeschleunigungen von $\pm 4\ \frac{m}{s^2}$ realitätsnah abzubilden.

Mit Hilfe des Drallsatzes lässt sich für die Gierwinkelbeschleunigung $\ddot{\psi}$ der Zusammenhang

$$\ddot{\psi} = \frac{1}{J_Z}\left(F_{XT,f} l_f \cdot sin\delta_f + F_{YT,f} l_f \cdot cos\delta_f - F_{YT,r} l_r\right) \qquad \text{A.16}$$

ableiten.

Hierbei repräsentiert J_z das Massenträgheitsmoment um die Gier- bzw. Z-Achse im Schwerpunkt. Des Weiteren können die Längs- und Querbeschleunigungen entsprechend

$$a_X = \frac{1}{m}\left(F_{XT,f} \cdot cos\delta_f + F_{XT,r} - F_{YT,f} \cdot sin\delta_f + mv_Y\dot{\psi} - F_{WX} - F_{RX}\right) \quad \text{A.17}$$

$$a_Y = \frac{1}{m}\left(F_{XT,f} \cdot sin\delta_f + F_{YT,f} \cdot cos\delta_f + F_{YT,r} - mv_X\dot{\psi}\right)$$

beschrieben werden.

Unter Bezugnahme trigonometrischen Relationen der Längs- und Quergeschwindigkeit kann wiederum der Schwimmwinkel

$$\beta = \text{atan}\left(\frac{v_Y}{v_X}\right) \quad \text{A.18}$$

berechnet werden.

Die auf die Längsdynamik als Störgröße wirkende Rollwiderstandskraft

$$F_{RX} = F_z c_R \quad \text{A.19}$$

wird mittels der Vertikalkraft F_z als auch dem Rollwiderstandsbeiwert c_R abgebildet.

Darüber hinaus wird die Luftwiderstandskraft

$$F_{WX} = c_{WX} A_f \frac{\rho}{2} v_X^2 \quad \text{A.20}$$

im Fahrzeugschwerpunkt erfasst.

Die Berechnung der Reifenlängskräfte

$$F_{XT,f,r} = \frac{M_{M,f,r} - M_{BS,f,r}}{r_{dyn}} \quad \text{A.21}$$

erfolgt jeweils über das anliegende Antriebsmoment $M_{M,f,r}$ und Bremsmoment $M_{BS,f,r}$ der Vorder- und Hinterachse sowie der Hebelarmwirkung des dynamischen Rollradius r_{dyn}.

Um die Reifenquerkräfte F_{YT} zu bestimmen, müssen einerseits die Schräglaufwinkel

$$\alpha_f = \delta_f - \text{atan}\left(\frac{v_Y + l_f\dot{\psi}}{v_X}\right) \quad \text{A.22}$$

$$\alpha_r = -\text{atan}\left(\frac{v_Y - l_f\dot{\psi}}{v_X}\right)$$

ermittelt werden. Andererseits wird die semiempirische Magic Formula von Pacejka [324]

$$F_{YT,f,r} = D_{Y,\alpha}\sin\left[C_{Y,\alpha}\arctan(B_{Y,\alpha}\alpha_{f,r} - E_{Y,\alpha}\left(B_{Y,\alpha}\alpha_{f,r} - \text{atan}\left(B_{Y,\alpha}\alpha_{f,r}\right)\right)\right] \quad \text{A.23}$$

herangezogen.

Um den Sachverhalt kombinierter Reifenlängs- und querkräfte zu vereinfachen, kann die jeweils maximal zu erreichende Reifenlängs- bzw. -querkraft

$$F_{XT,f,r,max} = \sqrt{\left(\mu^2 \cdot F_{ZT,f,r}^2\right) - F_{YT,f,r}^2} \quad \text{A.24}$$

$$F_{YT,f,r,max} = \sqrt{\left(\mu^2 \cdot F_{ZT,f,r}^2\right) - F_{XT,f,r}^2}$$

in Abhängigkeit der Radaufstandskraft F_{ZT} als auch des vorliegenden Reibkoeffizienten μ im Sinne des Kamm'schen Kreises [322] beschrieben werden.

Moderne Kraftfahrzeug sind heutzutage mit elektromechanischen Servolenkungen (engl. *Electric Power Steering {EPS}*) ausgestattet. Es gibt zwei Haupttypen von Schnittstellen zur EPS: die Lenkwinkel- und die Momentenschnittstelle. Die Lenkwinkelschnittstelle wird vor allem dann herangezogen, wenn der EPS direkt ein Lenkwinkelbefehl vorgegeben werden soll. Die untergeordnete Lenkwinkelregelung und die Lenkung selbst stehen nicht im Fokus dieser Arbeit. Demnach wird ein vereinfachtes analytisch dynamisches Regelkreisverhalten mittels der Übertragungsfunktion

$$G_{\delta_f}(s) = \frac{K_{\delta_f}}{T_{\delta_f} s + 1} e^{-sT_{t,\delta_f}} \qquad \text{A.25}$$

im Sinne der PT_1T_t-Dynamik (vgl. Gl. A.5) mit dem Verstärkungsfaktor K_{δ_f}, der Zeitkonstante T_{δ_f} als auch der Totzeit T_{t,δ_f} für die Umsetzung eines Lenkwinkelbefehls herangezogen.

Im Hinblick auf den Antrieb im Sinne einer permanent erregten Synchronmaschine erfolgt die Umsetzung des Beschleunigungsbefehls ebenfalls im Zuge eines vereinfachten analytisch dynamischen Regelkreisverhaltens mittels der PT_1T_t-Übertragungsfunktion (vgl. Gl. A.5)

$$G_{M_M}(s) = \frac{K_{M_M}}{T_{M_M} s+1} e^{-sT_{t,M_M}}, \qquad \text{A.26}$$

wobei der Verstärkungsfaktor K_{M_M}, die Zeitkonstante T_{M_M} als auch die Totzeit T_{t,M_M} die Umsetzung des Antriebsmoments M_M charakterisieren.

Was das geschlossene Regelkreisverhaltens des Bremssubsystems angeht, so erfolgt die Realisierung des Verzögerungsbefehls wiederum anhand eines analytisch dynamischen PT_1T_t-Übertragungsverhaltens (vgl. Gl. A.5)

$$G_{M_{BS}}(s) = \frac{K_{M_{BS}}}{T_{M_{BS}} s+1} e^{-sT_{t,M_{BS}}}, \qquad \text{A.27}$$

wobei der Verstärkungsfaktor $K_{M_{BS}}$, die Zeitkonstante $T_{M_{BS}}$ als auch die Totzeit $T_{t,M_{BS}}$ die Umsetzung des Bremsmoments M_{BS} charakterisieren.

A.5 Beschreibung der Teile 1 - 7 der ISO 26262

Nachfolgend werden die für die Dissertation relevanten Teile der ISO 26262 näher erläutert:

- **Teil 1 - „Vokabular“:** Teil 1 der ISO 26262 umfasst das Glossar und beinhaltet die relevanten Begriffe, deren Definitionen und Abkürzungen.
- **Teil 2 - „Management von funktionaler Sicherheit“:** Teil 2 der ISO 26262 formuliert die Anforderungen an das Management von funktionaler Sicherheit. Diese Anforderungen können auf der einen Seite projektunabhängige und auf der anderen Seite projektspezifische Aspekte umfassen.

Für die jeweiligen Phasen des Sicherheitslebenszyklus werden die Sicherheitskultur, das Kompetenz- und Qualitätsmanagement als auch Regeln und Prozesse in Abhängigkeit zur Organisationsstruktur aufgesetzt. Des Weiteren werden Rollen und Verantwortlichkeiten definiert sowie die Planung, Überwachung und Koordinierung der Sicherheitsaktivitäten als auch deren projektspezifische Anpassung bzw. Tailoring vollzogen. Ferner werden die Sicherheitsargumentation bzw. der Sicherheitsnachweis (engl. *Safety Case*) sowie das Audit und Assessment der funktionalen Sicherheit etabliert [50].

- **Teil 3 - „Konzeptphase“:** In Teil 3 der ISO 26262 werden die Anforderungen der Konzeptphase aufgeführt. Die Konzeptphase selbst wird durch die „Item Definition“ initiiert (siehe Abbildung A.7). Bei einem Item handelt es sich um ein System oder eine Kombination von Systemen, auf welchem eine Funktion oder ein Teil einer Funktion auf Fahrzeugebene implementiert ist. Hierfür werden als Input eine grobe Systembeschreibung als auch eine vorläufige Systemarchitektur benötigt. Dementsprechend steht Teil 3 der ISO 26262 in engem Bezug zur Systemanforderungsanalyse (SE1) als auch zum Systementwurf (SE2) des V-Modells (siehe Abbildung 5.2). Im Zuge der Item Definition werden funktionale, nichtfunktionale sowie regulatorische und gesetzliche Anforderungen des Items selbst, den Elementen des Items sowie den Interaktionen des Items mit dessen Umgebungskontext analysiert und dokumentiert. Zudem müssen das Verhalten des Items sowie sämtliche anzunehmende Betriebszustände und -szenarien evaluiert werden. Unter diese Betrachtung fallen auch die Anforderungen des Umgebungskontexts an das Item als auch umgekehrt [50].

  Im Anschluss an die Item Definition erfolgt die Gefahrenanalyse und Risikobewertung (engl. *Hazard and Risk Analysis {HARA}*) (siehe Abbildung A.7). Hierbei sollen zum einen die Gefährdungsereignisse, welche durch Fehlfunktionen des Items hervorgerufen werden können, identifiziert und klassifiziert werden. Darauf basierend werden Sicherheitsziele (engl. *Safety Goal*) mit den Automotive-Sicherheitsintegritätslevel (engl. *Automotive Safety Integrity Level {ASIL}*) zur Prävention oder Minderung von Gefährdungsereignissen spezifiziert, um ein inakzeptables Risiko zu vermeiden. Der ASIL stellt folglich die notwendigen Anforderungen und Sicherheitsmaßnahmen, welche spezifiziert werden müssen, um ein inakzeptables Risiko des zu entwickelten Systems oder der zu entwickelnden Komponente zu vermeiden, anhand von vier Ebenen dar. Dabei ist ASIL A die niedrigste Sicherheitsebene und ASIL D die höchste [50]. Die ASIL-Einstufungen der ISO 26262 stehen allerdings nicht in direktem Bezug zu den SIL-Einstufungen der IEC 61508 [51]. So gibt es in der ISO 26262 keinen SIL 4 da angenommen wird, dass katastrophale Auswirkungen mit vielen Toten nicht durch Fehlfunktionen eines Fahrzeugsystems verursacht werden können.

  Ein Gefährdungsereignis entsteht aus der Kombination gefährdenden Verhaltens (z.B. ungewollte Fahrzeugbeschleunigung) und einer Betriebssituation bzw. eines Szenarios (z.B. Heranfahren an einen Zebrastreifen oder eine Ampel, Kurvenfahrt, Geradeausfahrt, Fahren bei Regen usw.). Dabei werden mögliche funktionale Fehler (z.B. Verlust der Bremsunterstützung oder fehlinterpretierter Beschleunigungswunsch), ohne auf deren Ursache einzugehen, identifiziert. Anschließend wird analysiert, wie sich solche Fehlfunktionen auf Fahrzeugebene auswirken und wie stark der Einfluss auf die Kraftfahrzeug- und Verkehrsumgebung (Fahrer, Passagiere, Fußgänger andere Verkehrsteilnehmer etc.) ist. Diese hervorgerufenen Auswirkungen werden anhand der jeweils möglichen Betriebssituationen bzw. des Szenarios untersucht.

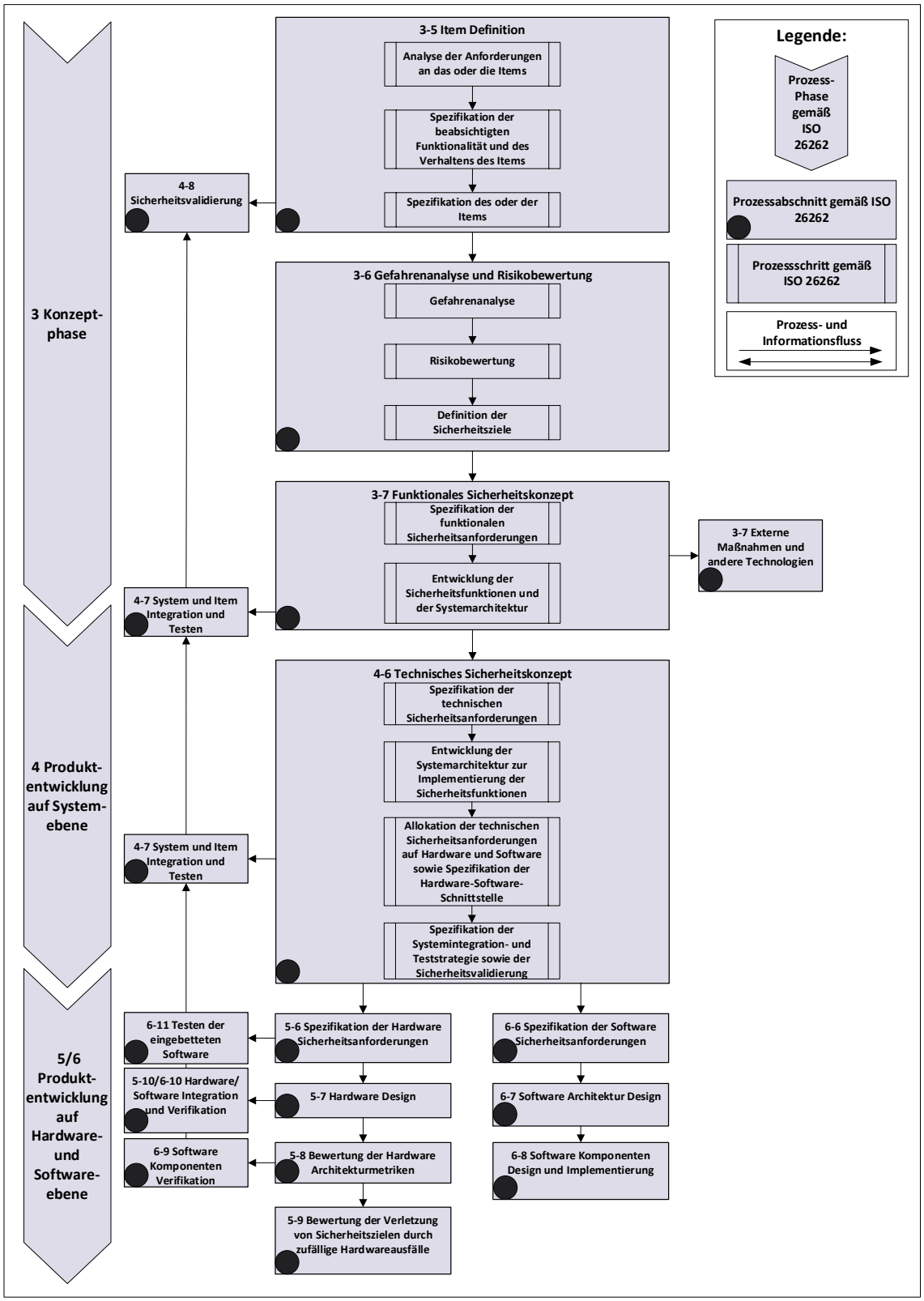


Abbildung A.7: Systementwicklungsbezogenen Prozessphasen, -abschnitte und -schritte gemäß ISO 26262.

Die Klassifizierung der Gefährdungsereignisse erfolgt anhand der Schwere (engl. *Severity*) eines möglichen Schadens, der Häufigkeit (engl. *Exposure*) der Betriebssituation bzw. des Szenarios sowie der Beherrschbarkeit (engl. *Controllability*) der jeweils innerhalb eines Gefährdungsereignisses beteiligten Akteure (siehe Tabelle 5.1). Unter Bezugnahme von statistischen Daten, Unfallanalysen sowie Erfahrungswerten basierend auf Expertenwissen erfolgt die ASIL-Klassifizierung der jeweiligen Gefährdungsereignisse. Nach der Festlegung der ASIL-Klassen werden im Anschluss die Sicherheitsziele als Anforderungen auf oberster Ebene definiert. Diese beschreiben Zielvorgaben zur Vermeidung oder Verminderung von Risiken, welche durch Gefährdungsereignisse hervorgerufen werden, sollen jedoch keine Auskunft darüber geben, wie die technische Realisierung zu gestalten ist [50].

Als letzter Prozessschritt der Konzeptphase erfolgt die Entwicklung des funktionalen Sicherheitskonzepts (engl. *Functional Safety Concept {FSC}*) (siehe Abbildung A.7). Um die im vorherigen Prozessschritt definierten Sicherheitsziele zu erfüllen, müssen im Zuge der Erstellung des funktionalen Sicherheitskonzepts Sicherheitsmaßnahmen und -mechanismen entwickelt werden. Auf Grundlage der Sicherheitsziele werden funktionale Sicherheitsanforderungen (engl. *Functional Safety Requirement {FSR}*) abgeleitet und an die Systemarchitektur oder an externe Maßnahmen allokiert. Im Rahmen dessen wird das funktionale oder degradierte Item Verhalten in Übereinstimmung mit den Sicherheitszielen spezifiziert. Dabei werden Beschränkungen hinsichtlich geeigneter sowie rechtzeitiger Erkennung und Beherrschung von relevanten Fehlern festgelegt. Ferner werden Maßnahmen auf Ebene des Items konzipiert, um die erforderliche Fehlertoleranz zu erreichen oder die Auswirkungen relevanter Fehler durch das Item selbst, den menschlichen Fahrer oder externe Maßnahmen angemessen zu mindern. Dies umfasst Strategien zur Fehlererkennung und -vermeidung, Überführung in einen sicheren Zustand, Mechanismen der Fehlertoleranz, Warnung des menschlichen Fahrers sowie die Arbitrierung von Regelsignalen. Darüber hinaus werden Kriterien für die Sicherheitsvalidierung festgelegt [50].

- **Teil 4 - „Produktentwicklung auf Systemebene“:** Teil 4 der ISO 26262 umfasst zunächst Anforderungen sowie Aktivitäten und Methoden auf Systemebene vor der Aufteilung in Hardware- und Softwarekomponenten als auch die durchzuführende Systemintegration (siehe Abbildung A.7). Dementsprechend weisen die Phasen des Systementwurfs (SE2), der Hardware- und Software Anforderungsanalyse (SE3) auf dem linken Schenkel als auch die Systemintegration (SE 8) und Überleitung in die Nutzung (SE 9) auf dem rechten Schenkel des V-Modells Wechselwirkungen mit Teil 4 der ISO 26262 auf (siehe Abbildung 5.2). Im Zuge dessen werden aus den realisierungsunabhängigen funktionalen Sicherheitsanforderungen sowie dem funktionalen Sicherheitskonzept realisierungsabhängige technische Sicherheitsanforderungen (engl. *Technical Safety Requirement {TSR}*) deduziert. Die technischen Sicherheitsanforderungen legen die technische Umsetzung der Anforderungen an die funktionale Sicherheit, unter Berücksichtigung der Item Definition als auch der Systemarchitektur, auf der jeweiligen Hierarchieebene fest. Daraufhin werden die technischen Sicherheitsanforderungen den Hardware- und Softwarekomponenten zugewiesen.

  Im Anschluss daran erfolgen das Systemdesign und die Entwicklung des technischen Sicherheitskonzepts (engl. *Technical Safety Concept {TSC}*) (siehe Abbildung A.7). Hierbei müssen quantitative Vorgaben für Fehlertoleranzintervalle und Diagnoseabdeckung auf der Ebene der Elemente

in Abhängigkeit des ASILs konzipiert werden, um Fehlerursachen durch zufällige Hardwareeffekte bewältigen zu können. Zur Sicherheitsanalyse des Systemdesigns und Vermeidung systematischer Fehler werden unterschiedliche Sicherheitsanalysemethoden eingesetzt.

Ferner werden die Schnittstellen zwischen Hardware und Software (engl. *Hardware-Software Interface {HSI}*) festgelegt (siehe Abbildung A.7), welche wiederum im Zuge der Produktentwicklung auf Hardware- und Softwareebene (Teil 5 und 6) im Detail spezifiziert werden. Im Anschluss daran werden die Spezifikationen der Anforderungen für Produktion, Betrieb, Wartung und Außerbetriebnahme definiert. Daraufhin wird das Systemdesign auf Vollständigkeit und Konformität mit dem technischen Sicherheitskonzept verifiziert und auf Teil 5 und 6 der ISO 26262 ausgeweitet. Weiter muss das Item im Zuge der Systemintegration und des Testens auf Erfüllung sämtlicher Sicherheitsanforderungen überprüft werden. Dies geschieht anhand von drei Phasen. Die erste Phase integriert die Hardware und Software, welche im Zuge der zweiten Phase zu einem Item zusammengefügt werden. Im Verlauf der dritten Phase wird das Item mit weiteren Systemen und dem Gesamtfahrzeug vereint. Ferner wird das funktionale Sicherheitskonzept in Bezug auf dessen Übereinstimmung und Konformität mit den definierten Sicherheitszielen und -anforderungen verifiziert. Dies kann durch Tests, Erprobung an Prototypen sowie Simulationen geschehen (vgl. Anhang A.7). Danach erfolgen die Sicherheitsvalidierung und im Anschluss die Erteilung der Freigabe zur Produktion [50].

- **Teil 5 - „Produktentwicklung auf Hardwareebene":** In diesem Teil der ISO 26262 werden die Anforderungen der Sicherheitsaktivitäten in den einzelnen Teilphasen der Hardwareentwicklung über die Detaillierung der Hardware- und Softwareschnittstellen bis hin zur Hardwareintegration und -verifizierung beschrieben (siehe Abbildung A.7). Folglich stehen die Phasen der Hardware Anforderungsanalyse (SE3) sowie der Grobentwurf (SE4), der Feinentwurf (SE5), die Implementierung (SE6) als auch die Integration von Hardware (SE7) des V-Modells und Teil 5 der ISO 26262 unter wechselseitigem Einfluss (siehe Abbildung 5.2). Die Aktivitäten in Teil 5 umfassen die Hardware Implementierung des Sicherheitskonzepts, die Analyse möglicher Hardwarefehler und deren Auswirkungen sowie die Koordinierung der Softwareentwicklung. Basierend auf den technischen Sicherheitsanforderungen sowie dem technischen Sicherheitskonzept wird mit der Erhebung der Sicherheitsanforderungen der jeweiligen Hardwarekomponenten begonnen. Daraufhin erfolgt unter Berücksichtigung des Systemdesigns die Spezifikation des Hardwaredesigns sowie die Implementierung und Integration, welche im Anschluss gegen die Sicherheitsanforderungen an die Hardware verifiziert werden muss. Außerdem müssen zum einen die Wiederverwendung etablierter Hardwarekomponenten und zum anderen nichtfunktionale Fehlerursachen während des Designs der Hardwarearchitektur betrachtet werden. Weiter muss unter Einbeziehung von Hardwarearchitektur-Metriken nachgewiesen werden, dass der Entwurf der Hardwarearchitektur des Items sicherheitsrelevante zufällige Hardwareausfälle zu einem gewissen Grad erkennen und beherrschen kann. Dabei müssen Ausfallraten der sicherheitsrelevanten Hardwarekomponenten bestimmt werden. Weiter muss der Nachweis erbracht werden, dass die Wahrscheinlichkeit einer Verletzung der Sicherheitsziele durch zufällige Hardwareausfälle angemessen gering ist. Bei der Determinierung der Ausfallraten kann auf anerkannte Dokumente, Statistiken und Expertenmeinungen zurückgegriffen werden [50].

- **Teil 6 - „Produktentwicklung auf Softwareebene":** Parallel zu Teil 5 werden in Teil 6 der ISO 26262 die Anforderungen der Sicherheitsaktivitäten in den einzelnen Teilphasen der Software-

entwicklung über die Detaillierung der Hardware- und Softwareschnittstellen bis hin zur Softwareintegration und -verifizierung beschrieben (siehe Abbildung A.7). Infolgedessen sind die Phasen der Software Anforderungsanalyse (SE3) als auch des Grobentwurfs (SE4), des Feinentwurfs (SE5), der Implementierung (SE6) sowie der Integration von Software (SE7) des V-Modells und Teil 5 der ISO 26262 eng miteinander verknüpft (siehe Abbildung 5.2). Im Zuge dessen erfolgt die weitere Detaillierung der Sicherheitsanforderungen an die Software, welche aus den technischen Sicherheitsanforderungen sowie dem technischen Sicherheitskonzept und dem Design der Systemarchitektur abgeleitet wurden. Darüber hinaus werden die für die Implementierung erforderlichen sicherheitsrelevanten Funktionalitäten und Eigenschaften der Software definiert. Im Anschluss an die Spezifikation der Sicherheitsanforderungen an die Software, findet die Entwicklung der Softwarearchitektur statt. Das Design der Softwarearchitektur repräsentiert die jeweiligen Elemente und deren Wechselwirkungen anhand einer hierarchischen Struktur. Statische Aspekte, wie Schnittstellen zwischen den Softwarekomponenten, sowie dynamische Aspekte, wie Prozessabläufe und Zeitverhalten, werden dabei beschrieben und festgehalten. Die Sicherheitsanforderungen an die Software sind den Softwarekomponenten bis hin zu den einzelnen Softwarekomponenten hierarchisch zuzuordnen. Abschließend finden die Integration und Verifizierung der Software bezüglich deren korrekter Funktionsweise und Konformität gegen die sicherheitstechnischen Anforderungen statt [50].

Teil 7 - „Produktion, Betrieb, Wartung und Außerbetriebnahme": Teil 7 der ISO 26262 hat zum einen das Ziel, einen Produktionsprozess für sicherheitsrelevante Elemente oder Items zu entwickeln und diesen aufrecht zu erhalten. Zum anderen sollen die erforderlichen Informationen in Bezug auf Betrieb, Service (Wartung und Reparatur) und Außerbetriebnahme für Benutzer, die mit den sicherheitsrelevanten Items oder Elementen interagieren, entwickelt werden. Demzufolge bezieht sich Teil 7 auf die Phase der Überleitung in die Nutzung (SE 9) des V-Modells (siehe Abbildung 5.2). Durch die formulierten Anforderungen und beschriebenen Aktivitäten in Teil 7 soll sichergestellt werden, dass die funktionale Sicherheit während des gesamten Lebenszyklus des Fahrzeugs erreicht wird. Dabei sollen die hierfür erhobenen Anforderungen gewährleisten, dass sicherheitsrelevante Besonderheiten in die Produktionsplanung und -steuerung unter Berücksichtigung der Produktionsbeteiligten wie OEM und Zulieferer miteinbezogen werden. Des Weiteren enthält Teil 7 der ISO 26262 Anforderungen in Bezug auf die Entwicklung von Serviceinformationen und Benutzerinformationen (einschließlich des Benutzerhandbuchs), die Planung, Durchführung und Überwachung von Wartungsarbeiten, Reparaturanweisungen, Anweisungen zur Außerbetriebnahme sowie Vorgaben und Informationen für Rettungsdienste [50].

A.6 Beschreibung der Teile 5 - 13 der ISO 21448

Die für die Dissertation signifikanten Teile 5 - 13 der ISO 21448 werden im Folgenden näher beschrieben:

- **Teil 5 - „Spezifikation und Design":** Auf Ebene der „Konzeptphase" der ISO 26262 repräsentiert Teil 5 der ISO 21448 den Ausgangspunkt und das Grundgerüst der Entwicklung von automatisierten Fahrfunktionen (siehe Abbildung 5.5). Hierbei erfolgt die Beschreibung der Zielsetzung des Entwicklungsvorhabens im Sinne der beabsichtigten Funktion sowie die Darstellung von Interdependenzen der Funktion zu anderen Fahrzeugfunktionen und -systemen, relevanten Umweltbedingungen als auch Interaktionen zwischen System und menschlichem Fahrer (siehe Abbildung A.8) [55].

- **Teil 6 - „Identifizierung und Bewertung von Gefährdungen“:** Teil 6 formuliert Anforderungen der systematischen Identifizierung und Bewertung von Gefährdungen, die durch funktionale Unzulänglichkeiten oder zu erwartendem (Miss-) Gebrauch hervorgerufen werden können (siehe Abbildung A.8). Das Vorgehen gründet in erster Linie auf dem Wissen über die Funktion und ihre möglichen Abweichungen von der gegebenen Spezifikation. Dies kann durch Anwendung der in ISO 26262 vorgeschlagenen Methoden der „Gefahrenanalyse und Risikobewertung“ unter expliziter Berücksichtigung der Leistungsbeschränkungen der beabsichtigten Funktion durchgeführt werden. Infolgedessen können dieselben Kriterien zur ASIL-Klassifizierung der Gefährdungsereignisse herangezogen werden. Zudem werden erste Validierungsziele definiert, welche die geltenden staatlichen und industriellen Vorschriften sowie das aktuelle Niveau der funktionalen Performanz, das zur Gewährleistung der Sicherheit erforderlich ist, berücksichtigen [55].

- **Teil 7 - „Identifizierung und Bewertung potenzieller Funktionsdefizite und möglicher auslösender Bedingungen“:** Teil 7 bezieht sich ebenfalls auf die „Gefahrenanalyse und Risikobewertung“ im Zuge der „Konzeptphase“ der ISO 26262 hat aber die Zielsetzung, sogenannte auslösende Ereignisse[1] (engl. *Triggering Events*), die ein nicht beabsichtigtes Systemverhalten bzw. Systemschwächen offenlegen und Gefährdungen zur Folge haben können, ausfindig zu machen (siehe Abbildung 5.5). Insbesondere geht es darum, Unzulänglichkeiten der Leistungsfähigkeit der Sensoren, Algorithmen und Aktuatoren zu analysieren und zu identifizieren (siehe Abbildung A.8) [55].

- **Teil 8 - „Funktionale Modifikationen zur Berücksichtigung von SOTIF-bezogenen Risiken“:** Teil 8 der ISO 21448 kann mit der Ebene der „Konzeptphase“ (Funktionales Sicherheitskonzept) als auch der „Produktentwicklung auf System-, Hardware- und Softwareebene“ (Technisches Sicherheitskonzept einschließlich Hardware- und Software) der ISO 26262 in Relation gesetzt werden (siehe Abbildung 5.5). Dieser Teil beschreibt Anforderungen der Umsetzung von Maßnahmen zur Optimierung der Systemspezifikation (Leistungsfähigkeit und Robustheit der Sensorik, Algorithmen und Aktuatorik) als auch dem Entwurf von funktionalen Einschränkungen und Limitierungen der automatisierten Fahrfunktionen, um SOTIF-bezogene Risiken ausreichend zu minimieren (siehe Abbildung A.8) [55].

- **Teil 9 - „Definition der Verifikations- und Validierungsstrategie“:** Teil 9 der ISO 21448 kann auf die „Konzeptphase sowie auf die „Produktentwicklung auf System-, Hardware- und Softwareebene“ der ISO 26262 bezogen werden. Dieser umfasst die Definition einer Verifikations- und Validierungsstrategie als auch eines strukturierten Verfahrens einschließlich entsprechender Methoden zur Erbringung der erforderlichen Nachweise der Sicherheit der beabsichtigten Funktion durch Analyseergebnisse, Testberichte und weitere spezifische Untersuchungen (siehe Abbildung A.8) [55].

[1] Auslösende Ereignisse implizieren zum einen Wetter- und Umgebungsbedingungen wie z.B. Regen, Nebel, Schnee und Straßenbeschaffenheit. Zum anderen sind darunter auch unerwartetes Verhalten anderer Verkehrsteilnehmer, mechanische Störungen und Schwingungen, akustische Störungen und Schwingungen als auch Effekte der elektromagnetischen Verträglichkeit (EMV) aufzufassen [55].

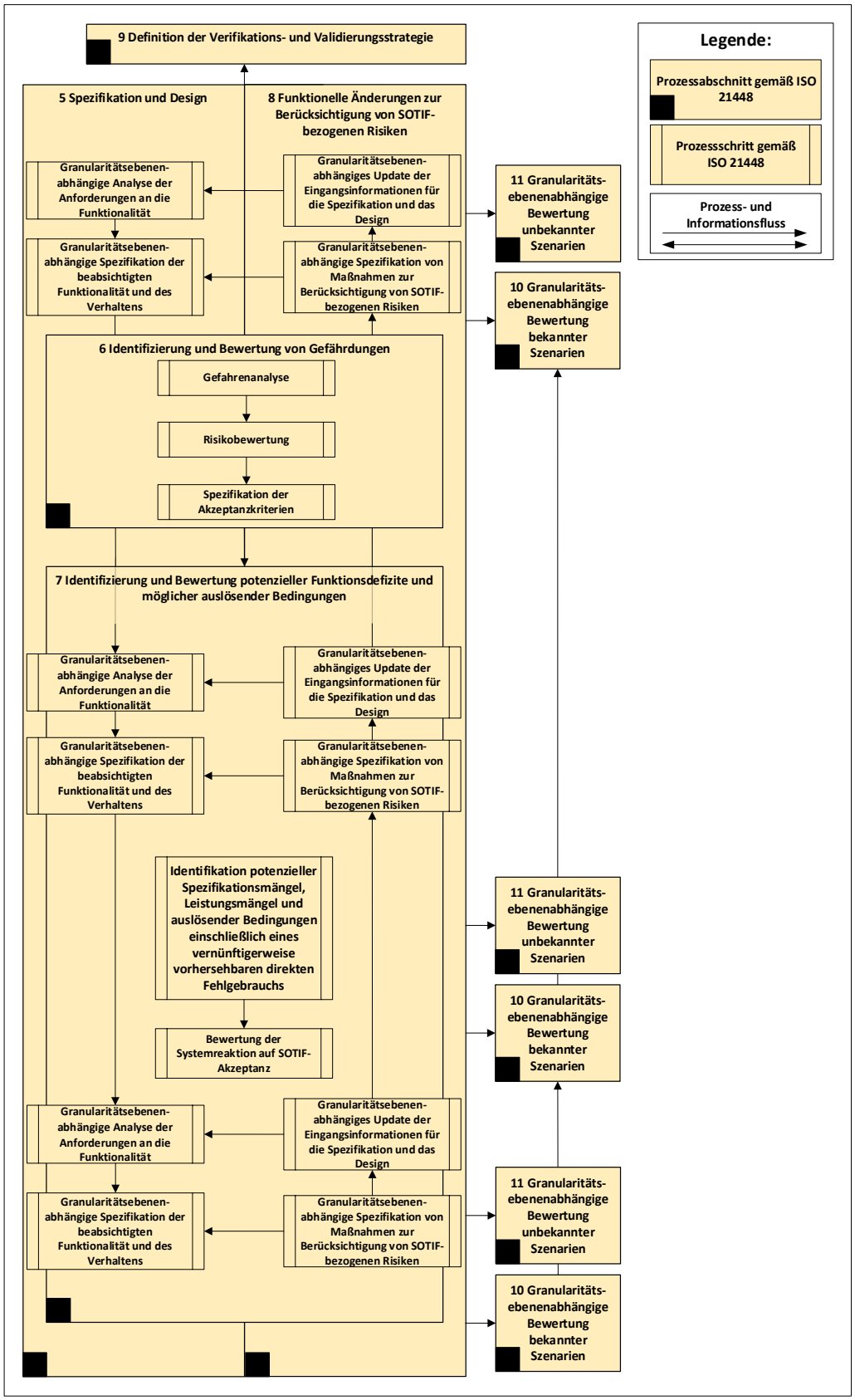


Abbildung A.8: Systementwicklungsbezogenen Prozessabschnitte und -schritte gemäß ISO 21448.

- **Teil 10 - „Bewertung bekannter Szenarien“:** Teil 10 der ISO 21448 steht in Zusammenhang mit der „Produktentwicklung auf Systemebene“ der ISO 26262 und den darin festgelegten Verifikationstätigkeiten (siehe Abbildung 5.5). Im Zuge dessen sind das System und die Komponenten (Sensoren, Algorithmen und Aktuatoren) zu verifizieren. Hierbei soll aufgezeigt werden, dass sich diese bei bekannten Gefährdungsereignissen und -szenarien sowie vernünftigerweise vorhersehbarem Missbrauch erwartungsgemäß verhalten (siehe Abbildung A.8) [55].

- **Teil 11 - „Bewertung unbekannter Szenarien“:** Teil 11 der ISO 21448 kann mit der „Produktentwicklung auf Systemebene“ der ISO 26262 assoziiert werden und bezieht sich im Speziellen auf die darin definierten Validierungstätigkeiten (siehe Abbildung 5.5). Hierbei müssen die Funktionen des Systems und der Komponenten (Sensoren, Algorithmen und Aktuatoren) validiert werden, um aufzuzeigen, dass diese in realen Anwendungsfällen kein unangemessenes Risiko hervorrufen (siehe Abbildung A.8) [55].

- **Teil 12 - „Bewertung des Erreichens der SOTIF“:** Teil 12 der ISO 21448 kann auf die Erteilung der Freigabe zur Produktion im Zuge der „Produktentwicklung auf Systemebene“ der ISO 26262 bezogen werden und umfasst Kriterien der Evaluierung der Verifikations- und Validierungsstrategie sowie dem Nachweis der notwendigen SOTIF-bezogenen Risikominimierung [55].

- **Teil 13 - „Betriebsphasenaktivitäten“:** Teil 13 der ISO 21448 kann mit Teil 7 der ISO 26262 „Produktion, Betrieb, Wartung und Außerbetriebnahme“ verknüpft werden. Insbesondere geht es darum, durch Feldüberwachungsverfahren das Erreichen der SOTIF während der Betriebsphase zu gewährleisten [55].

A.7 Methoden der Sicherheitsverifikation und -validierung

Um den Nachweis zu erbringen, dass der Systemarchitekturentwurf den Sicherheitsanforderungen entspricht, fordert die ISO 26262 die Durchführung von Integrationstests im Sinne der Fehlerbeseitigung. Dabei wird die Systemarchitektur hinsichtlich der korrekten Implementierung der funktionalen und technischen Sicherheitsanforderungen, der korrekten funktionalen Performanz, Genauigkeit und zeitlichen Abstimmung der Sicherheitsmechanismen, der konsistenten und korrekten Umsetzung der Schnittstellen als auch einer adäquaten Robustheit überprüft. Zudem muss aufgezeigt werden, dass unbeabsichtigte Verhaltensweisen, welche die Verletzung eines Sicherheitsziels hervorrufen können, ausgeschlossen sind. Hierfür ist eine Integrations- und Teststrategie festzulegen, welche den Entwurf der Systemarchitektur, das funktionale Sicherheitskonzept und das technische Sicherheitskonzept berücksichtigt. Um eine angemessene Spezifikation der Testfälle für die Integrationstests zu ermöglichen, müssen die Testfälle unter Verwendung einer geeigneten Kombination von Methoden und unter Berücksichtigung der Integrationsebene (System- oder Hardware- und Softwareebene) definiert werden. Die Testfälle werden aus den erhobenen Anforderungen, dem erwarteten Funktionsverhalten, Expertenwissen und Erfahrungswerten aus dem Feld, Grenzwerten, Wechselwirkungen an Schnittstellen oder der statistischen Verteilung von Umgebungsbedingungen abgeleitet. Dabei werden die definierten Testfälle mit „Pass/Fail-Kriterien“ verknüpft und mit reproduzierbaren Testmethoden wie Tests unter Laborbedingungen, Tests auf Prüfgeländen und Simulationsmethoden vollzogen. Darüber hinaus können auch Feldtests unter realen Bedingungen durchgeführt werden [50].

Im Anschluss an die Verifikationstätigkeiten erfolgt die Sicherheitsvalidierung. Der Zweck der vorangehenden Verifizierungsaktivitäten besteht in der Erbringung des Nachweises, dass die Ergebnisse jeder einzelnen Aktivität den erhobenen Anforderungen entsprechen. Dahingegen zielt die Sicherheitsvalidierung des integrierten Systems in repräsentativen Fahrzeugen darauf ab, die Eignung bzw. Tauglichkeit für den vorgesehenen Einsatz und Betrieb zu argumentieren als auch die Angemessenheit der Sicherheitsmaßnahmen für eine Fahrzeugreihe oder -klasse zu bestätigen. Infolgedessen soll durch die Sicherheitsvalidierung gewährleistet werden, dass die Sicherheitsziele auf der einen Seite geeignet sind, dem Stand der Technik entsprechen und auf der anderen Seite auch vollständig erreicht werden. Hierfür sind auf Fahrzeugebene Sicherheitsvalidierungsverfahren und Testfälle für jedes Sicherheitsziel, einschließlich detaillierten Pass/Fail-Kriterien sowie dem Anwendungsbereich zu definieren. Dies kann Aspekte wie Konfiguration, Umweltbedingungen, Fahrsituationen, betriebliche Anwendungsfälle usw. umfassen. Nachfolgend eine Darlegung der jeweiligen Testmethoden auf Systemebene, welche in erster Linie auf die Verifikation, Effektivität und Robustheit abzielen, gemäß der ISO 26262 (Teil 4-8 „Item Integration und Testen“) [50] wiedergegeben:

- **Anforderungsbasierter Test (engl. *Requirements-based Test*):** Ein anforderungsbasierter Test umfasst das Testen gegen funktionale und nichtfunktionale Anforderungen.

- **Fehlerinjektionstest (engl. *Fault Injection Test*):** Beim Fehlerinjektionstest werden spezifische Mittel eingesetzt, um Fehler in das System einzuprägen. Dies kann über eine gesonderte Testschnittstelle oder speziell präparierte Elemente bzw. Kommunikationsvorrichtungen erfolgen. Die Methode wird verwendet, um die Testabdeckung der Sicherheitsanforderungen zu erhöhen, da während des normalen bzw. fehlerfreien Betriebs die Sicherheitsmechanismen nicht aktiviert werden.

- **Back-to-Back Test:** Im Zuge des „Back-to-Back-Tests“ werden die Reaktionen des Testobjekts mit den Reaktionen eines Simulationsmodells (MiL, SiL und HiL Methoden vgl. Abschnitt 4.7) unter Einbeziehung derselben Stimuli gegenübergestellt, um Unterschiede zwischen dem Verhalten des Modells und seiner realen Implementierung zu identifizieren.

- **Performanztest (engl. *Performance Test*):** Mit Hilfe von Performanztests wird die Leistungsfähigkeit (z.B. Geschwindigkeit oder Belastbarkeit der Aktuatoren, Reaktionszeiten des Gesamtsystems) hinsichtlich der Sicherheitsmechanismen des Systems überprüft.

- **Error Guessing Test:** Beim „Error Guessing Test“ werden Expertenwissen und Daten genutzt, welche durch „Lessons Learned“ gesammelt wurden, um Fehler im System zu prognostizieren. Auf Grundlage dessen wird eine Reihe von Tests zusammen mit geeigneten Testmöglichkeiten entworfen, um derartige Fehler zu erfassen.

- **Test auf Basis von Felderfahrung (engl. *Test Derived From Field Experience*):** Hierbei handelt es sich um einen Test, welcher auf Erfahrungen und Daten aus der Praxis basiert.

- **Test externer Schnittstellen (engl. *Test of External Interfaces*):** Der Test externer Schnittstellen umfasst das Testen der analogen und digitalen Ein- und Ausgänge, Grenz- und Äquivalenzklassentests, um die spezifizierten Schnittstellen, die Kompatibilität, die zeitliche Abstimmung und andere spezifizierte Eigenschaften des Systems möglichst vollständig zu überprüfen.

- **Test interner Schnittstellen (engl. *Test of Internal Interfaces*):** Der Test interner Schnittstellen umfasst ebenfalls das Testen der analogen und digitalen Ein- und Ausgänge als auch Grenz- und Äquivalenzklassentests. Zudem können interne Schnittstellen sowohl durch statische Tests (z.B. Übereinstimmung von Steckverbindern) als auch durch dynamische Tests der Buskommunikation oder anderer Schnittstellen zwischen Systemelementen begutachtet werden.

- **Überprüfung der Schnittstellen auf Konsistenz (engl. *Interface Consistency Check*):** Die Überprüfung der Schnittstellen auf Konsistenz beruht auch auf dem Testen der analogen und digitalen Ein- und Ausgänge als auch auf Grenz- und Äquivalenzklassentests.

- **Test der Interaktion/Kommunikation (engl. *Test of Interaction/Communication*):** Der Kommunikations- und Interaktionstest beinhaltet Tests der Kommunikation zwischen den Systemelementen sowie zwischen dem Testobjekt und anderen Fahrzeugsystemen während der Laufzeit anhand der funktionalen und nichtfunktionalen Anforderungen.

- **Test der Ressourcennutzung (engl. *Resource Usage Test*):** Tests zur Ressourcennutzung werden in der Regel in dynamischen Umgebungen durchgeführt (z.B. in Laborfahrzeugen oder Prototypen). Zu den zu prüfenden Aspekten gehören beispielsweise Stromverbrauch und Buslast.

- **Stresstest (engl. *Stress Test*):** Mittels Stresstests wird der korrekte Betrieb des Systems unter hohen Betriebslasten oder hohen Anforderungen aus der Umgebung überprüft. Im Zuge dessen können extreme Benutzereingaben, hohe Anforderungen von anderen Systemen sowie Tests unter extremen Umweltbedingungen hinsichtlich Temperaturen, Feuchtigkeit als auch der Aufbringung mechanischer Stöße durchgeführt werden.

- **Test auf Störfestigkeit und Robustheit unter bestimmten Umweltbedingungen (engl. *Test for Interference Resistance and Robustness Under Certain Environmental Conditions*):** Hierbei handelt sich um einen Spezialfall des Stresstests, welcher Tests zur elektromagnetischen Verträglichkeit (EMV) und elektrostatischer Entladung enthält.

Des Weiteren muss im Zusammenhang mit den Sicherheitsvalidierungsaktivitäten gemäß der ISO 26262 (Teil 4-8 „Sicherheitsvalidierung“) [50] ein geeigneter Satz der folgenden Methoden angewendet werden:

- Wiederholbare Tests mit spezifizierten Testverfahren, Testfällen und Pass/Fail-Kriterien als Abnahmekriterien (Positivtests von Funktionen und Sicherheitsanforderungen, Black-Box-Tests, Tests unter Randbedingungen, Fehlerinjektion, Lebensdauertests, Stresstests, beschleunigte Grenzlastprüfungen (engl. Highly *Accelerated Life Testing*) und Simulationen von äußeren Einflüssen);

- Sicherheitsanalysemethoden, wie z.B. FMEA, FTA, Ereignisbaumanalysen (engl. *Event Tree Analysis {ETA}*) und Simulationen;

- Langzeittests, wie z.B. Fahrprogramme für Fahrzeuge und Erfassung von Testflotten;

- Betriebliche Anwendungsfälle und Anwendertests unter realen Bedingungen, Panel- oder Blindtests sowie Experten-Panels;

Reviews.

A.8 Scode for Open Context Analysis

Nachfolgend wird die Scode for Open Context Analysis (SOCA) Methode gemäß Butz et al. [325] zusammengefasst wiedergegeben. Für weitere Einzelheiten zu SOCA sei einerseits auf Butz et al. [325] sowie andererseits auf den Anhang der ISO 34502 [219] verwiesen.

SOCA ist eine Art morphologischer Kasten der es ermöglicht, den Entscheidungsraum (engl. *Decision Space*) eines hochautomatisierten Kraftfahrzeugs in Äquivalenzklassen systematisch zu zerlegen. Diese Äquivalenzklassen liefern in Kombination mit sogenannten Zonengraphen, welche von konkreten geometrischen Abmessungen des Fahrbahnbereichs und konkreten Verteilungen mit Objekten und anderen Verkehrsteilnehmern eines definierten Betriebsbereichs abstrahiert, einen Satz konsistenter, kontextabhängiger Anforderungen auf Ebene des hochautomatisierten Ego-Kraftfahrzeugs als Black-Box.

Abbildung A.9 repräsentiert eine schematische Vogelperspektive eines Fußgängerüberwegs mit einem hochautomatisierten Ego-Kraftfahrzeug sowie zwei Fußgängern im Sinne des zu betrachteten Zonengraphen. Diese Zonen repräsentieren sogenannte Fahrzonen (G, F) für das hochautomatisierte Ego-Kraftfahrzeug, Positionszonen für andere Verkehrsteilnehmer (L, M) oder aber Informationszonen, welche beispielsweise den Fußgängerüberweg beinhalten (F) (siehe Abbildung A.9). Darüber hinaus können die Fahrzonen für das hochautomatisierte Kraftfahrzeug in statische und dynamische Fahrzonen unterschieden werden. Statische Fahrzonen, wie z.B. F, ändern weder ihre Position noch ihre Größe und sind durch die Szenerie des Betriebsbereichs determiniert. Dahingegen hängen dynamische Fahrzonen vom aktuellen dynamischen Zustand des hochautomatisierten Kraftfahrzeugs ab und werden verwendet, um dessen Fähigkeiten auszudrücken, beispielsweise die Bremsfähigkeit vor der Vorfahrtslinie.

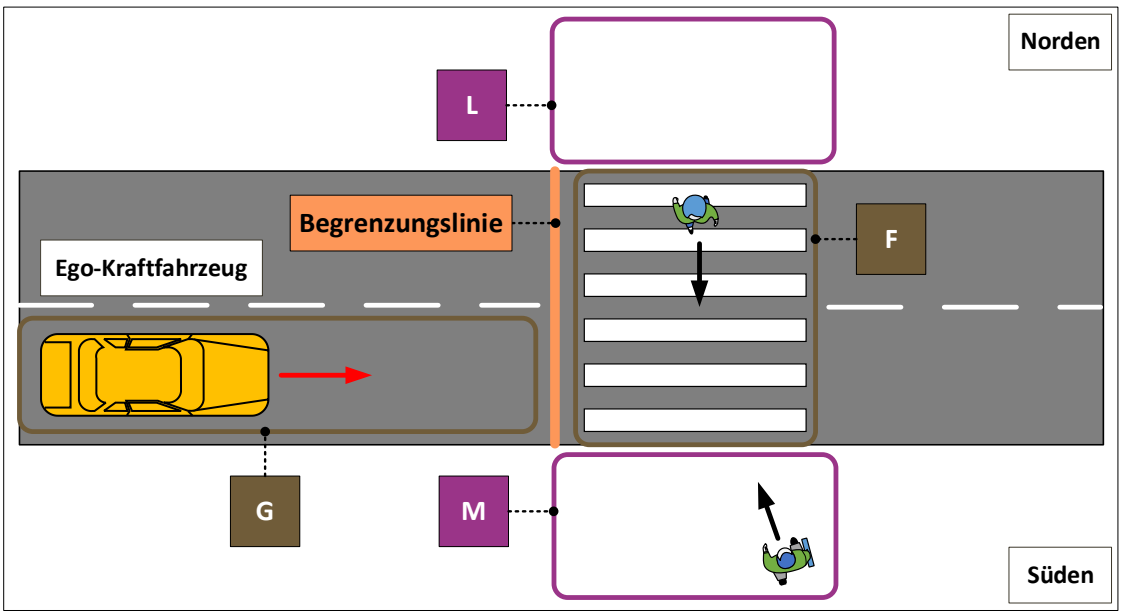


Abbildung A.9: Vogelperspektive bzw. Zonengraph für das Heranfahren an einen Fußgängerüberweg (in Anlehnung an [325]).

In Abbildung A.9 ist die Zone G als dynamische Zone identifiziert. Die Bildung der Fahrzonen fußt letztlich auf der jeweiligen Intention des hochautomatisierten Ego-Kraftfahrzeugs. Für jedes infrastrukturelle Element, das einen Einfluss auf die Verhaltensentscheidung des hochautomatisierten Ego-Kraftfahrzeugs haben kann (vorhersehbar oder nicht vorhersehbar), wird eine Informationszone hinzugefügt. Unter der Annahme, dass sich alle Verkehrsteilnehmer an die Verkehrsregeln halten, entstehen Positionszonen wie L und M, welche die Fahrzone F sozusagen bedrohen, da Fußgänger die Straße zur gleichen Zeit überqueren können, in der das hochautomatisierten Ego-Kraftfahrzeug die Fahrzone F passieren möchte.

Nach Beschreibung der Zonengraphen werden diese herangezogen, um einen Satz konsistenter, kontextabhängiger Verhaltensanforderungen an das hochautomatisierte Ego-Kraftfahrzeug als Black-Box abzuleiten. Während sich ein Fußgänger auf dem Überweg befindet, nähert sich ein anderer Fußgänger dem Überweg von Süden. Die resultierenden Zonen L, F und M aus dem Zonengraphen werden visualisiert (siehe Abbildung A.9). Die Basis für die Definition des qualitativen Entscheidungsraums des hochautomatisierten Ego-Kraftfahrzeug, in einen Straßenabschnitt einzufahren, wird dabei durch den Zonengraphen vorgegeben. Grundsätzlich kann jede Fahrzone für das hochautomatisierte Ego-Kraftfahrzeug befahrbar oder nicht befahrbar sein, in Abhängigkeit davon, ob diese blockiert oder durch einen anderen Verkehrsteilnehmer sozusagen bedroht wird.

Im Fall des Fußgängerüberwegs hängt der Entscheidungsraum für das Einfahren in die Fahrzone F davon ab, ob F blockiert oder von L oder M aus bedroht ist. Die Zone F gilt als blockiert, wenn sich ein Fußgänger innerhalb dieser Zone aufhält und voraussichtlich noch dort ist, wenn das hochautomatisierte Ego-Kraftfahrzeug ankommt. Bedrohung durch Fußgänger besteht, wenn sie sich auf dem Gehweg befinden und den Überweg betreten könnten, bevor das hochautomatisierte Ego-Kraftfahrzeug diesen passiert hat. Dieser Entscheidungsraum wird mit Hilfe einer Zwicky-Box innerhalb der SCODE-ANALYZER Toolbox [314] gemäß Tabelle A.1 dargestellt.

Eine Zwicky-Box oder morphologische Box [326] ist eine Darstellung eines diskreten Raums P_K. Jede Dimension $D_1, i = 1, \dots, n$ des Raums ist durch eine endliche Menge von paarweise disjunkten Alternativen $\{a_{i1,1}, \dots, a_{i,n}\}$ gegeben. Die vollständige Menge der kombinatorischen Punkte dieses Raums ist durch das kartesische Produkt der Dimensionen $P_K = D_1 \times \dots \times D_n$ gegeben, was anhand des Fußgängerwegs zu $1 \cdot 2 \cdot 2 \cdot 2 = 8$ möglichen Zuständen führt.

Tabelle A.1: Zwicky-Box im Hinblick auf den Entscheidungsraum des an einen Fußgängerüberweg heranfahrenden automatisierten Ego-Kraftfahrzeugs unter Hervorhebung (dunkelgrau) und Ausschluss (hellorange) der jeweiligen Alternativen (in Anlehnung an [325]).

Dimension	Alternativen	
Position Ego-Kraftfahrzeug	G	
Status Fußgängerüberweg F	Blockiert durch Fußgänger	Nicht blockiert
Status Annäherungszone L	Blockiert durch Fußgänger	Nicht blockiert
Status Annäherungszone M	Blockiert durch Fußgänger	Nicht blockiert

Im Folgenden wird vereinfachend angenommen, dass alle Zonen für das hochautomatisierte Ego-Kraftfahrzeug sichtbar sind. Jede Dimension repräsentiert einen Informationsaspekt des Betriebsbereichskontextes, der für Entscheidungen und das Verhalten des hochautomatisierten Ego-Kraftfahrzeugs relevant sein kann. Dabei werden die Äquivalenzklassen durch Kombinationen von einer oder mehreren Alternativen für jede Dimension definiert. In Tabelle A.1 sind die grau markierten Alternativen diejenigen, welches es dem hochautomatisierten Ego-Kraftfahrzeug erlauben, den Fußgängerüberweg zu passieren. Alle anderen Kombinationen dieses Entscheidungsraums erfordern, dass das hochautomatisierte Ego-Kraftfahrzeug vor dem Fußgängerüberweg anhält. Die beiden Äquivalenzklassen bzw. Modi

- "Fußgängerüberweg passieren"
- "Vor dem Fußgängerüberweg anhalten"

entsprechen dabei die zwei grundsätzlichen Verhaltensanforderungen an das hochautomatisierte Ego-Kraftfahrzeug.

Die SCODE-ANALYZER Toolbox [314] erzwingt und garantiert gleichzeitig, dass diese Äquivalenzklassen bzw. Modi sich gegenseitig ausschließen, was wiederum zur Folge hat, dass die Analyse konsistent ist. Außerdem wird sichergestellt, dass alle Modi zusammen den gesamten Entscheidungsraum abdecken, so dass jede mögliche Kombination einer Verhaltensanforderung zugeordnet ist. Im Beispiel des Fußgängerüberwegs könnten alle durch die Zwicky-Box induzierten Kombinationen tatsächlich in der Realität auftreten. Dies ist jedoch nicht immer der Fall, da es Kombinationen geben kann, die nur formal existieren und in der Realität keine Bedeutung haben. Solche sinnlosen Kombinationen werden in einem speziellen „Nicht-System-Modus“ zusammengefasst. Diese Klasse umfasst alle Fälle, die in der Realität nicht auftreten können und für die keine spezifischen Anforderungen festgelegt werden müssen.

Um dieses qualitative Verhalten zu quantifizieren, sind weitere Modelle und Parameter erforderlich, wobei die Parameter der Fahrzonen und Positionszonen formalisiert werden. Zur Quantifizierung der Äquivalenzklasse "Anhalten vor dem Fußgängerüberweg" wird ein Modell des hochautomatisierte Ego-Kraftfahrzeugs benötigt, welches die Berechnung des Anhaltewegs vor dem Fußgängerüberweg ermöglicht. Diese ermöglichen es wiederum, einen Bereich zu berechnen, in welchem das hochautomatisierte Ego-Kraftfahrzeug zum Stillstand kommt, basierend auf dessen aktueller Geschwindigkeit und Verzögerungsfähigkeiten unter Berücksichtigung der Reibung der Straße und möglicher anderer Parameter. Zusätzlich werden Modelle benötigt, welche die mögliche Bewegung von Fußgängern beschreiben und die Zonen L und M formalisieren.

Diese Äquivalenzklassen repräsentieren verschiedene Verhaltensweisen des hochautomatisierten Ego-Kraftfahrzeugs, welche durch die Dimensionen der Zwicky-Box möglich sind. Der SCODE-ANALYZER überprüft formal die Vollständigkeit, indem dieser sicherstellt, dass alle potenziellen Kombinationen durch mindestens eine Äquivalenzklasse abgedeckt sind. Zudem gewährleistet das Tool die Konsistenz, indem es sicherstellt, dass jede Kombination nur einer Äquivalenzklasse zugeordnet wird. Es ist zu beachten, dass die Entscheidungsräume für den Fußgängerüberweg hauptsächlich mit symbolischen Begriffen und nicht mit expliziten Werten formuliert werden. Infolgedessen bleibt die definierte Menge von Äquivalenzklassen für den Fußgängerüberweg stabil bzw. unverändert. Dies eröffnet die Möglichkeit, stabile qualitative Abstraktionen für eine große Klasse von konkreten Modellen herzuleiten. Im Hinblick darauf können die konkreten Modelle für verschiedene Typen von hochautomatisierten Kraftfahrzeugen unterschiedlich sein, die qualitative Unterteilung und dessen Semantik im Kontext der Analyse bleiben aber im Sinne der Generalisierbarkeit und Allgemeingültigkeit stabil bestehen.

B Anhang Betriebssicherheitslebenszyklusprozess

B.1 Prozessablauf der Teil 3 Betriebskonzeptphase

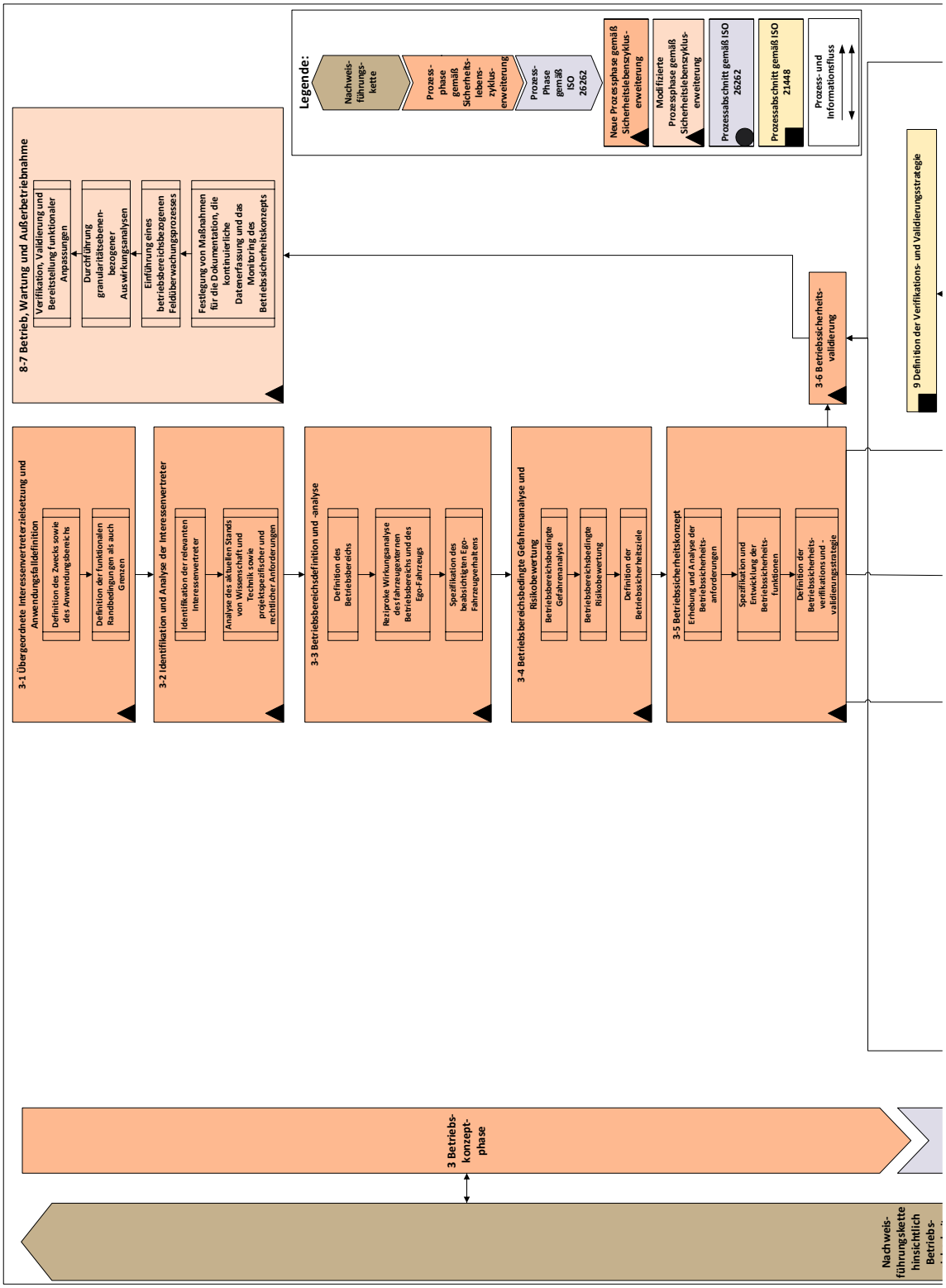


Abbildung B.1: Oberer Teil des Top-Down-Gesamtprozessablaufdiagramms des um der Betriebskonzeptphase nach oben geklappten V-Modells der ISO 26262 unter zusätzlicher Darstellung der jeweiligen Prozessphasen, -abschnitte und -schritte des Betriebssicherheitslebenszyklusprozesses, der ISO 26262 sowie der ISO 21448.

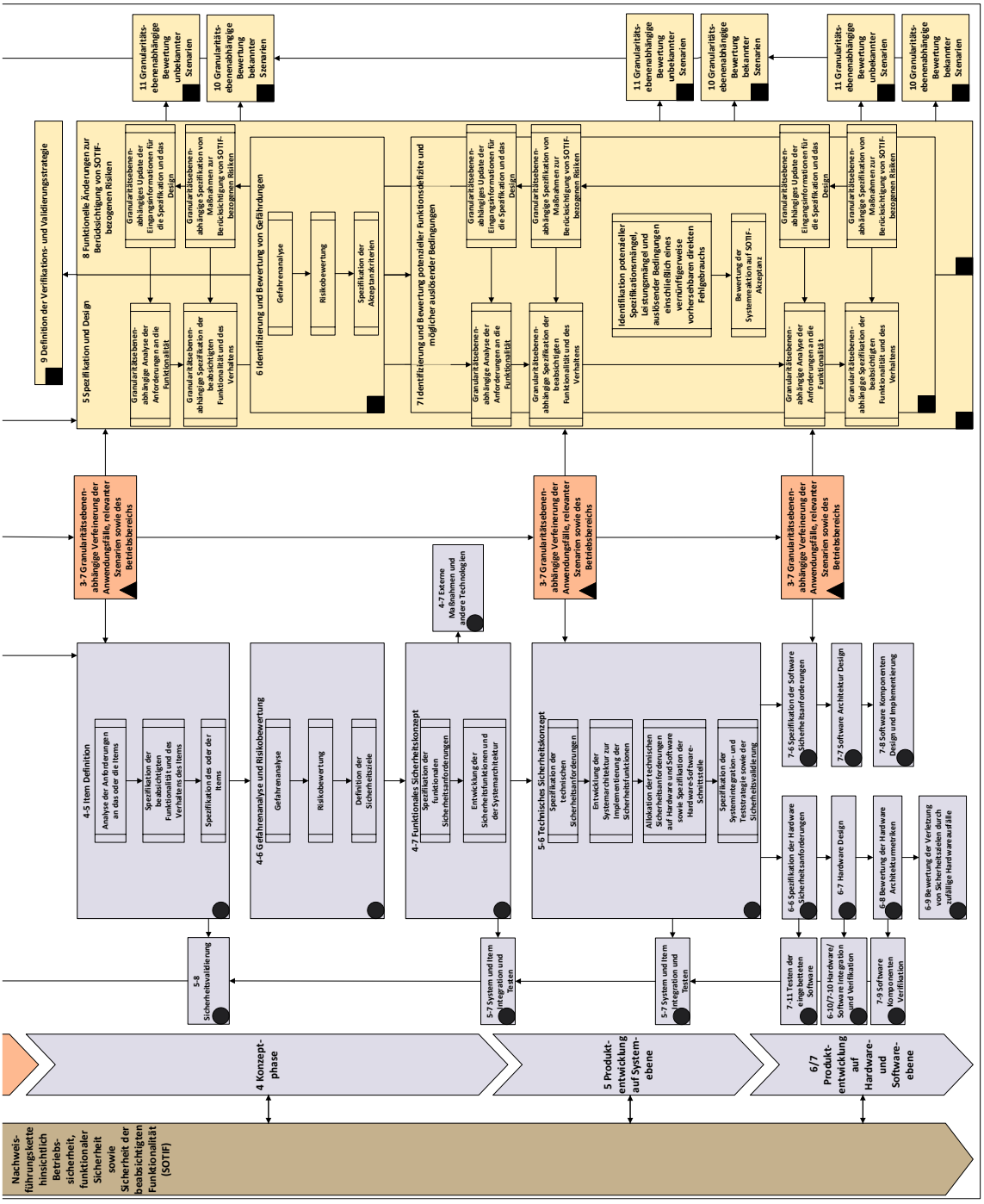


Abbildung B.2: Unterer Teil des Top-Down-Gesamtprozessablaufdiagramms des um der Betriebskonzeptphase nach oben geklappten V-Modells der ISO 26262 unter zusätzlicher Darstellung der jeweiligen Prozessphasen, -abschnitte und -schritte des Betriebssicherheitslebenszyklusprozesses, der ISO 26262 sowie der ISO 21448.

B.2 Arbeitsprodukte des Betriebssicherheitslebenszyklusprozesses

Nachfolgend werden die gemäß des Betriebssicherheitslebenszyklusprozesses zu generierenden Arbeitsprodukte unter Berücksichtigung der hierarchischen Strukturierung des Betriebssicherheitsnachweises (vgl. Unterabschnitt 7.2.4) anhand der Aspekte der Betriebssicherheit (OpSa), der funktionalen Sicherheit (FuSa) sowie der Sicherheit der beabsichtigten Funktionalität (SotiF) tabellarisch aufgelistet.

Tabelle B.1: Arbeitsprodukte im Hinblick auf Planungs- und Managementaktivitäten als Evidenzen des Betriebssicherheitsnachweises.

Spezifikationstyp	Betriebssicherheitslebens-zyklusprozessphase	Arbeitsprodukt (WP)
Planungs- und Management-aktivitäten	Übergreifendes Betriebs-sicherheitsmanagement	WP-1 Organisationsspezifische Vorgaben und Prozesse für OpSa inkl. FuSa und SotiF (2-5.3.1)
		WP-2 Evidenz eines Kompetenzmanagementsystems (2-5.3.2)
		WP-3 Evidenz eines Qualitätsmanagementsystems (2-5.3.3)
		WP-4 Bericht der identifizierten Betriebssicherheitsanomalien (2-5.3.4)
		WP-5 Auswirkungsanalyse auf System-Of-Systems-, System-, Subsystem-, Komponenten- oder Einheitenebene (2-6.3.1)
		WP-6 Betriebssicherheitsplan (2-6.3.2)
		WP-7 Evidenz eines Betriebssicherheitsmanagements hinsichtlich Produktion, Betrieb, Wartung und Außerbetriebnahme (2-7.3.1)

Tabelle B.2: Arbeitsprodukte im Hinblick auf Anforderungen und Testfälle als Evidenzen des Betriebssicherheitsnachweises.

Spezifikationstyp	Betriebssicherheitslebens-zyklusprozessphase	Arbeitsprodukt (WP)
Anforderungs- und Testfall-spezifikation	Betriebskonzeptphase	WP-8 Spezifikation der projektbezogenen Anforderungen (3-2.3.1)
		WP-9 Spezifikation der behördlichen Anforderungen (3-2.3.2)
		WP-10 Spezifikation der OpSa-bezogenen Sicherheitsziele und Anforderungen (3-4.3.2)
		WP-11 Spezifikation der OpSa-Validierung (3-6.3.1)
	Produktion, Betrieb, Wartung und Außerbetriebnahme	WP-12 Betriebssicherheitsrelevanter Inhalt des Produktionsplans, des Produktionslenkungsplans, einschließlich des Prüfplans sowie des Wartungsplans (8-5.3.1, 8-5.3.2 und 8-5.3.5)
		WP-13 Spezifikation der Herstellbarkeitsanforderungen (8-5.3.3)

		WP-14 Bericht der Produktionsprozessfähigkeit und Kontrollmaßnahmen (8-5.3.4, 8-6.3.1 und 8-6.3.2)
		WP-15 OpSa-relevante Instruktionen für Wartung, Nutzerinformationen, Rettungsdienste und Außerbetriebnahme (8-5.3.6, 8-5.3.7, 8-5.3.8 und 8-5.3.10)
		WP-16 OpSa-bezogener Feldüberwachungsprozess (8-7.3.1)
	Konzeptphase	WP-17 Spezifikation der FuSa-bezogenen Sicherheitsziele (ISO 26262:3-6.5.1)
		WP-18 Spezifikation der SotiF-bezogenen Sicherheitsziele (ISO 21448-6.6.3)
		WP-19 Spezifikation der funktionalen Sicherheitsanforderungen (ISO 26262:3-7.5.1)
		WP-20 Spezifikation der SotiF-bezogenen Anforderungen (ISO 21448-5.5)
	Produktentwicklung auf Systemebene	WP-21 Spezifikation der technischen Sicherheitsanforderungen (ISO 26262:4-6.5.1)
		WP-22 Spezifikation der Anforderungen für Produktion, Betrieb, Wartung und Außerbetriebnahme (8-5.3.9 und ISO 26262:4-6.5.5)
		WP-23 Spezifikation der SotiF-bezogenen Anforderungen auf Systemebene (ISO 21448-5.5)
		WP-24 FuSa-bezogene Integrations- und Teststrategie (ISO 26262:4-7.5.1)
		WP-25 FuSa-bezogene Spezifikation für die Sicherheitsvalidierung einschließlich der Beschreibung der Sicherheitsvalidierungsumgebung (ISO 26262:4-8.5.1)
		WP-26 Definition der SotiF-bezogenen Verifikations- und Validierungsstrategie (ISO 21448-9.4)
	Produktentwicklung auf Hardwareebene	WP-27 Spezifikation der Hardwaresicherheitsanforderungen (ISO 26262:5-6.5.1)
		WP-28 Spezifikation der Anforderungen für Produktion, Betrieb, Wartung und Außerbetriebnahme (ISO 26262:5-7.5.4)
		WP-29 Spezifikation der SotiF-bezogenen Anforderungen auf Hardwareebene (ISO 21448-5.5)
	Produktentwicklung auf Softwareebene	WP-30 Spezifikation der Softwaresicherheitsanforderungen (ISO 26262:6-6.5.1)
		WP-31 Spezifikation der SotiF-bezogenen Anforderungen auf Softwareebene (ISO 21448-5.5)

Tabelle B.3: Arbeitsprodukte im Hinblick auf den Architekturentwurf als Evidenzen des Betriebssicherheitsnachweises.

Spezifikationstyp	Betriebssicherheitslebens-zyklusprozessphase	Arbeitsprodukt (WP)
Architektur-entwurf	Betriebskonzeptphase	WP-32 Anwendungsfalldefinition (3-1.2.1)
		WP-33 Betriebsbereichsdefinition (3-3.3.1)
		WP-34 Bericht der OpSa-bedingten Gefahrenanalyse und Risikobewertung (3-4.3.1)
		WP-35 Betriebssicherheitskonzept (3-5.3.1)
	Konzeptphase	WP-36 Spezifikation der Item Definition und des Systementwurfs (ISO 26262:3-5.5.1 und ISO 21448-5.5)
		WP-37 Spezifikation der Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs gemäß der Konzeptphase (3-7.3.1)
		WP-38 Bericht der FuSa-bezogenen Gefahrenanalyse und Risikobewertung (ISO 26262:3-6.5.1)
		WP-39 SotiF-bezogene Identifizierung und Bewertung von Gefährdungen (ISO 21448-6.6.1/6.6.2)
		WP-40 Funktionales Sicherheitskonzept (ISO 26262:3-7.5.1)
		WP-41 Spezifikation systembezogener SotiF-Maßnahmen (ISO 21448-8.5)
	Produktentwicklung auf Systemebene	WP-42 Spezifikation des Subsystementwurfs (ISO 26262:4-6.5.3 und ISO 21448-5.5)
		WP-43 Spezifikation der Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs gemäß der Produktentwicklung auf Systemebene (3-7.3.1)
		WP-44 Technisches Sicherheitskonzept (ISO 26262:4-6.5.2)
		WP-45 Spezifikation der Hardware-Software Schnittstelle (ISO 26262:4-6.5.4)
		WP-46 Spezifikation subsystembezogener SotiF-Maßnahmen (ISO 21448-8.5)
		WP-47 Sicherheitsanalysebericht (ISO 26262:4-6.5.7)
		WP-48 Analysebericht subsystembezogener SotiF-Insuffizienzen (ISO 21448-7.5.1)
		WP-49 Bericht der Bewertung subsystembezogener Auslösebedingungen (ISO 21448-7.5.2)
	Produktentwicklung auf Hardwareebene	WP-50 Verfeinerung der Spezifikation der Hardware-Softwareschnittstelle (ISO 26262:5-6.5.2 bzw. ISO 26262:6-6.5.2)
		WP-51 Spezifikation des Hardwareentwurfs (ISO 26262:5-7.5.1 und ISO 21448-5.5)
		WP-52 Spezifikation der Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs gemäß der Produktentwicklung auf Hardwareebene (3-7.3.1)
		WP-53 Bericht der Hardwaresicherheitsanalysen (ISO 26262:5-7.5.2)

		WP-54 Bericht der Wirksamkeitsanalyse in Bezug auf die Bewältigung von zufälligen Hardwareausfällen (ISO 26262:5-8.5.1)
		WP-55 Bericht der Analyse von Sicherheitszielverletzungen aufgrund zufälliger Hardwareausfälle (ISO 26262:5-9.5.1)
		WP-56 Analysebericht hardwarebezogener SotiF-Insuffizienzen (ISO 21448-7.5.1)
		WP-57 Bericht der Bewertung hardwarebezogener Auslösebedingungen (ISO 21448-7.5.2)
		WP-58 Spezifikation dedizierter Hardwaremaßnahmen (ISO 26262:5-9.5.2)
		WP-59 Spezifikation hardwarebezogener SotiF-Maßnahmen (ISO 21448-8.5)
		WP-60 Spezifikation der Hardwareintegration und -verifikation (ISO 26262:5-10.5.1)
	Produktentwicklung auf Softwareebene	WP-61 Spezifikation des Softwarearchitekturentwurfs (ISO 26262:6-7.5.1 und ISO 21448-5.5)
		WP-62 Spezifikation der Verfeinerung der Anwendungsfälle, relevanter Szenarien sowie des Betriebsbereichs gemäß der Produktentwicklung auf Softwareebene (3-7.3.1)
		WP-63 Spezifikation softwarebezogener SotiF-Maßnahmen (ISO 21448-8.5)
		WP-64 Bericht der Softwaresicherheitsanalysen (ISO 26262:5-7.5.2)
		WP-65 Bericht der Fehlerabhängigkeitsanalyse (DFA) (ISO 26262:5-7.5.3)
		WP-66 Analysebericht softwarebezogener SotiF-Insuffizienzen (ISO 21448-7.5.1)
		WP-67 Bericht der Bewertung softwarebezogener Auslösebedingungen (ISO 21448-7.5.2)
		WP-68 Spezifikation des Softwareeinheitenentwurfs (ISO 26262:6-8.5.1 und ISO 21448-5.5)
		WP-69 Implementierung der Softwareeinheiten (ISO 26262:6-8.5.2 und ISO 21448-5.5)
		WP-70 Spezifikation der Softwareverifikation (ISO 26262:6-9.5.1)
		WP-71 Verfeinerte Spezifikation der Softwareverifikation (ISO 26262:6-10.5.1)
		WP-72 Eingebettete Software (ISO 26262:6-10.5.2 und ISO 21448-5.5)
		WP-73 Verfeinerte Spezifikation der eingebetteten Softwareverifikation (ISO 26262:6-11.5.1)

Tabelle B.4: Arbeitsprodukte im Hinblick auf durchzuführende V&V-Aktivitäten und Testfallresultate als Evidenzen des Betriebssicherheitsnachweises.

Spezifikationstyp	Betriebssicherheitslebens-zyklusprozessphase	Arbeitsprodukt (WP)
V&V-Aktivitäten und Testfall-resultate	Integration, Verifikation und Validierung gemäß der Betriebskonzeptphase	WP-74 Verifikationsbericht der OpSa-bedingten Gefahrenanalyse und Risikobewertung (3-4.3.3)
		WP-75 Verifikationsbericht des Betriebssicher-heitskonzepts (3-5.3.2)
		WP-76 Betriebssicherheitsvalidierungsbericht (3-6.3.2)
	Integration, Verifikation und Validierung gemäß der Produktentwicklung auf Systemebene	WP-77 Verifikationsbericht der Gefahrenanalyse und Risikobewertung (ISO 26262:3-6.5.2)
		WP-78 Verifikationsbericht des funktionalen Si-cherheitskonzepts (ISO 26262:3-7.5.2)
		WP-79 Verifikationsbericht der Systemspezifika-tion, des technischen Sicherheitskonzepts, der Spezifikation der Hardware-Software Schnittstelle sowie der Anforderungen für Produktion, Betrieb, Wartung und Außerbetriebnahme (ISO 26262:4-6.5.6 und ISO 21448-5.5)
		WP-80 Integrations- und Testbericht (ISO 26262:4-7.5.2)
		WP-81 Sicherheitsvalidierungsbericht (ISO 26262:4-8.5.2)
		WP-82 Verifikations- und Validierungsresultate bekannter Szenarien (ISO 21448-10.8)
		WP-83 Validierungsresultate unbekannter Szena-rien (ISO 21448-11.4.1)
		WP-84 Bewertung verbleibender Risiken (ISO 21448-11.4.2)
	Integration, Verifikation und Validierung gemäß der Produktentwicklung auf Hardwareebene	WP-85 Verifikationsbericht der Spezifikation der Hardwaresicherheitsanforderungen (ISO 26262:5-6.5.3)
		WP-86 Verifikationsbericht des Hardwareent-wurfs (ISO 26262:5-7.5.3)
		WP-87 Verifikationsbericht der Wirksamkeit in Be-zug auf die Bewältigung von zufälligen Hardware-ausfällen (ISO 26262:5-8.5.2)
		WP-88 Verifikationsbericht der Bewertung von Si-cherheitszielverletzungen aufgrund zufälliger Hardwareausfälle (ISO 26262:5-9.5.3)
		WP-89 Bericht der Hardwareintegration und -veri-fikation (ISO 26262:5-10.5.2)
		WP-90 Verifikations- und Validierungsresultate bekannter Szenarien auf Hardwareebene (ISO 21448-10.8)
	Integration, Verifikation und Validierung gemäß der Produktentwicklung auf Softwareebene	WP-91 Verifikationsbericht der Spezifikation der Softwaresicherheitsanforderungen (ISO 26262:6-6.5.3)
		WP-92 Verifikationsbericht des Softwarearchitek-turentwurfs (ISO 26262:6-7.5.4)

		WP-93 Verifikationsbericht des Softwareeinheitenentwurfs (ISO 26262:6-9.5.2)
		WP-94 Verifikationsbericht des verfeinerten Softwareeinheitenentwurfs (ISO 26262:6-10.5.3)
		WP-95 Verifikationsbericht der eingebetteten Software (ISO 26262:6-11.5.2)
		WP-96 Verifikations- und Validierungsresultate bekannter Szenarien auf Softwareebene (ISO 21448-10.8)

Tabelle B.5: Arbeitsprodukte im Hinblick auf die Behauptungen des Betriebssicherheitsnachweises.

Spezifikationstyp	Betriebssicherheitslebenszyklusprozessphase	Arbeitsprodukt (WP)
Behauptung	Übergreifendes Betriebssicherheitsmanagement	WP-97 OpSa-bezogener Bericht der Bestätigungsmaßnahmen (2-6.3.4)
		WP-98 OpSa-bezogener Bericht der Freigabe für die Produktion und den Betrieb (2-6.3.5)

B.3 Betriebsbereichsontologie

Die Inhalte der Betriebsbereichsontologie, welche durch den Autor der vorliegenden Dissertation in [306] publiziert wurde, werden nachfolgend dargestellt (siehe Abbildung B.3, Abbildung B.4 und Abbildung B.5):

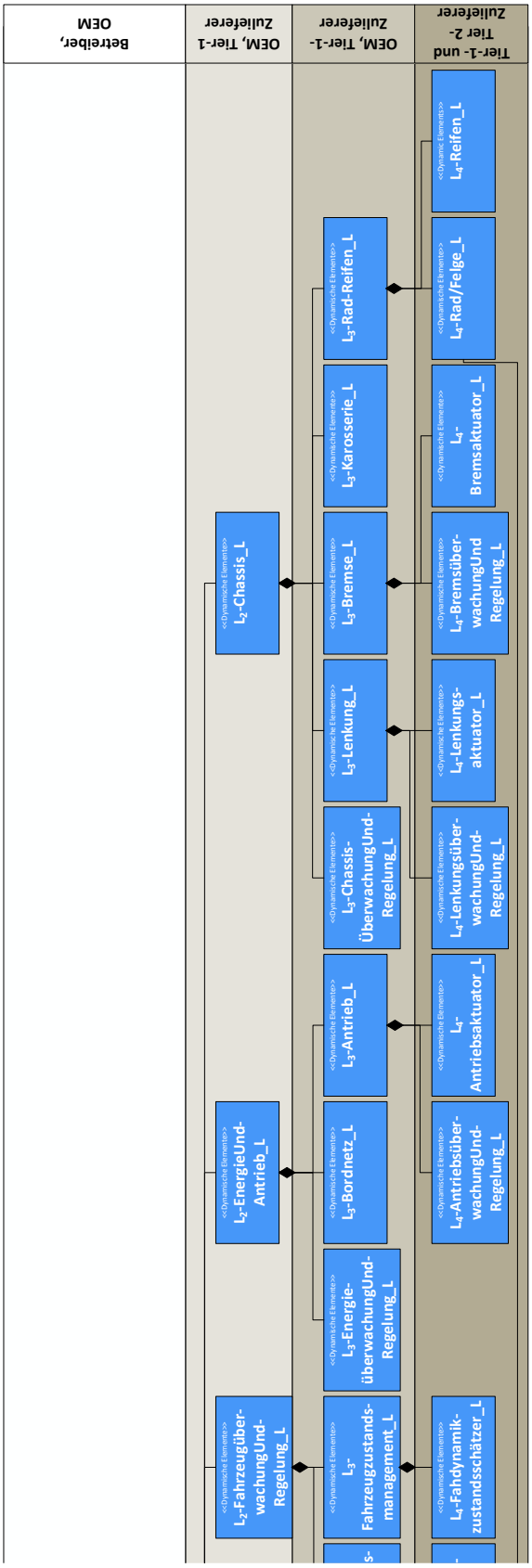


Abbildung B.3: Ausschnitt von Teil 1 der Betriebsbereichsontologie.

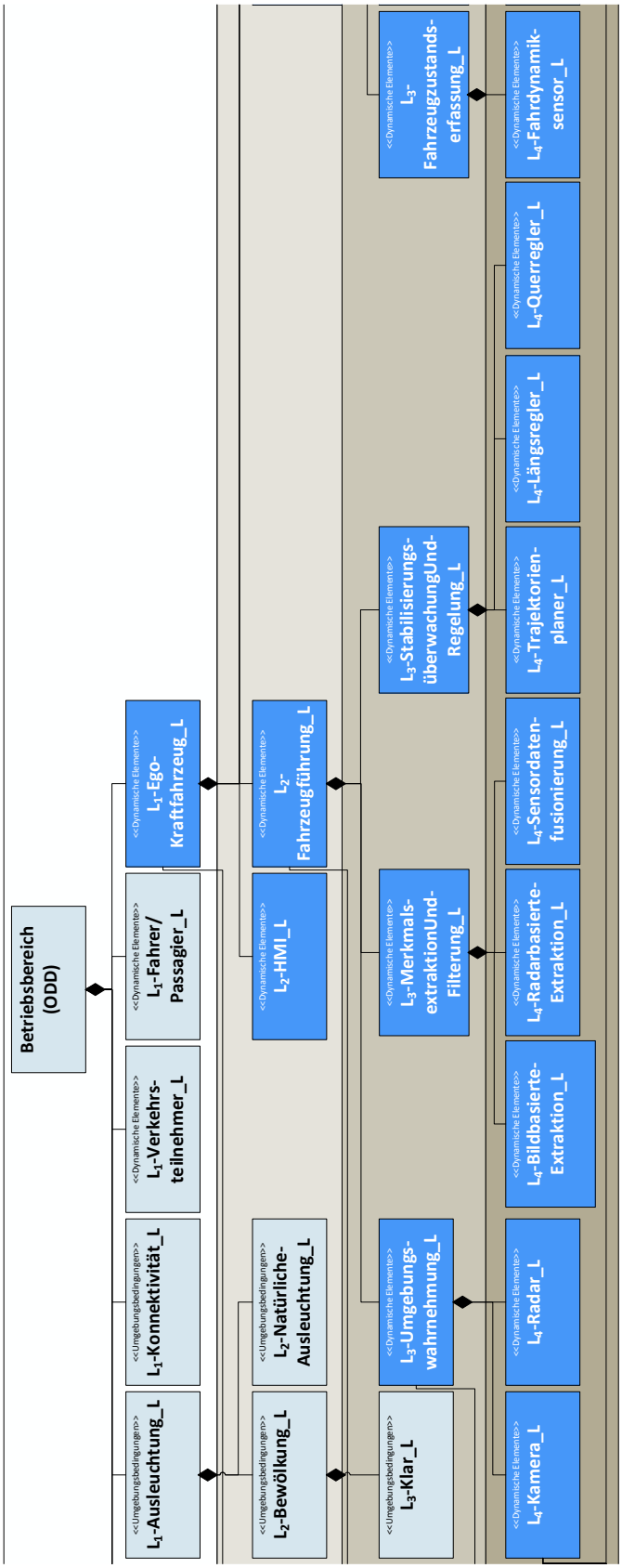


Abbildung B.4: Ausschnitt von Teil 2 der Betriebsbereichsontologie.

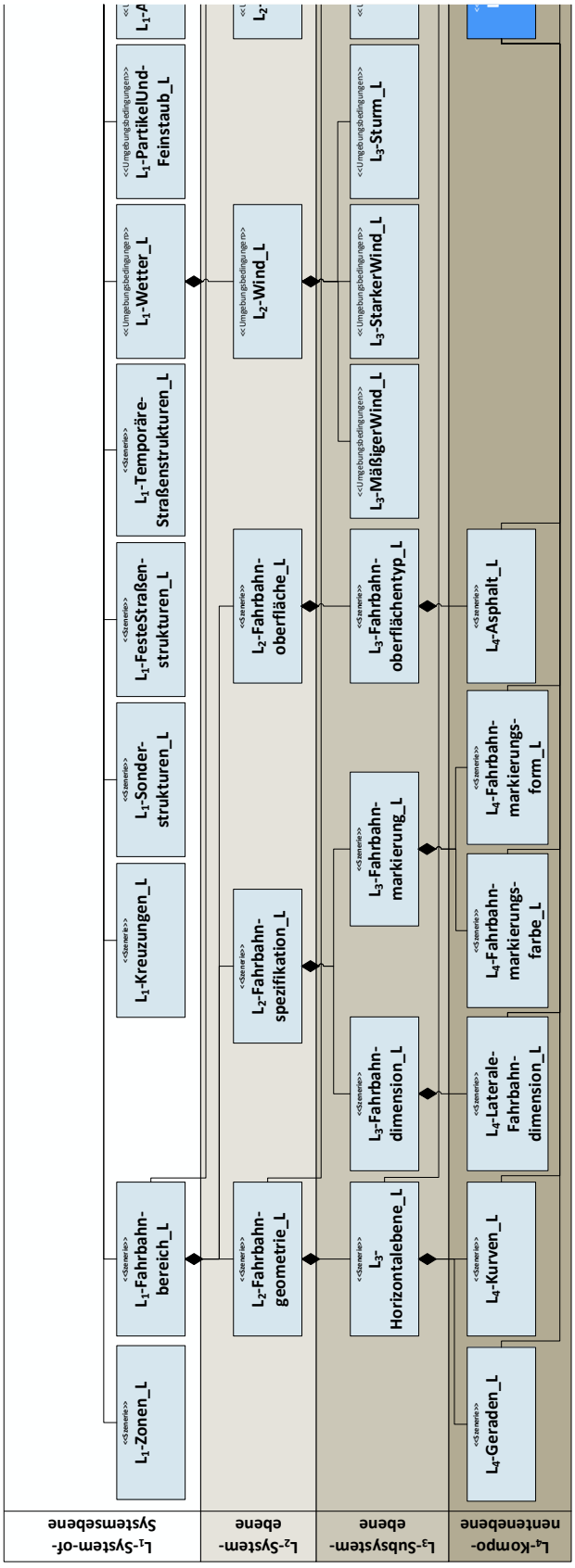


Abbildung B.5: Ausschnitt von Teil 3 der Betriebsbereichsontologie.

C Anhang Betriebssicherheitskonzept

C.1 Ergänzende Artefakte des Entwurfs- und Validierungszyklus gemäß der Betriebskonzeptphase

C.1.1 Artefakte der übergeordnete Interessenvertreterzielsetzung und Anwendungsfalldefinition

Tabelle C.1: Verhaltensbezogene Spezifikation des Anwendungsfalls „L_1-FolgeFahrstreifen…_UC“ anhand der involvierten Akteure als logische Aspekte, des Funktionsumfangs, des Automatisierungsgrads sowie der funktionalen Systemgrenzen und des Wunschverhaltens.

<<Anwendungsfall>>	
L1.1-UC „L_1-FolgeFahrstreifenHochautomatisiertAufDerAutobahn_UC“	
ID: L1.10000UC	
Akteure	• „L_1-Ego-Kraftfahrzeug_L“ • „L_1-Fahrer-Passagier_L“ • „L_1-Verkehrsteilnehmer_L“ • „L_1-FahrzeugexterneODDElemente_L“
Funktionsumfang und Automatisierungsgrad	• „L_1-Ego-Kraftfahrzeug_L“ verantwortet Durchführung der dynamischen Fahraufgabe • Ausschluss des „L_1-Fahrers/Passagiers_L“ als Rückfallebene in Bezug auf die dynamische Fahraufgabe • SAE-Level 4
Funktionale Systemgrenzen	• Maximale Geschwindigkeit „L_1-Ego-Kraftfahrzeug_L“: $36.11\ \frac{m}{s}\left(130\ \frac{km}{h}\right)$ • Ausschluss von Spurwechsel- oder Ausweichmanövern • Frontsichtbereich eingeschränkt auf Ego-Fahrstreifen • Betrieb eingeschränkt auf Autobahnabschnitten innerhalb Deutschlands • Betrieb eingeschränkt auf ideale Straßen- und Wetterbedingungen zur Tageszeit
Wunschverhalten	• Manöver der hochautomatisierten Längsführung: ○ „Freifahrt“ (engl. *Free Driving*) unter Einhaltung der Geschwindigkeitsbegrenzung ○ „Annähern“ (engl. *Approach*) an „L_1-Verkehrsteilnehmer_L“ ○ „Abstandshaltung“ (engl. *Gap Maintenance*) zum „L_1-Verkehrsteilnehmer_L“ • Manöver der hochautomatisierten Querführung: ○ „Fahrstreifen Folgen“ (engl. *Lane Maintenance*)

C.1.2 Artefakte der Identifikation und Analyse der relevanten Interessenvertreter

Tabelle C.2: Vorgenommene Einschränkungen in Bezug auf die Limitierung der Straßenverkehrsgesetzgebung als auch das Auslassen unternehmensbezogener, organisatorischer und projektspezifischer Rahmenbedingungen.

<<Einschränkung>>
ID: L1.10000CSTR
L1.1-CSTR Limitierung der Straßenverkehrsgesetzgebung auf deutsche StVO und UN-Regelung Nr. 157
Der Betrachtungsrahmen des zu generierenden Betriebssicherheitskonzepts im Hinblick auf die Straßenverkehrsgesetzgebung wird auf die deutsche StVO und die UN-Regelung Nr. 157 eingeschränkt.
ID: L1.20000CSTR
L1.2-CSTR Auslassen unternehmensbezogener, organisatorischer und projektspezifischer Rahmenbedingungen
Der Betrachtungsrahmen des zu generierenden Betriebssicherheitskonzepts beinhaltet keine Berücksichtigung unternehmensbezogener, organisatorischer und projektspezifischer Rahmenbedingungen.

Tabelle C.3: Ableitung von verhaltensbezogenen Betriebssicherheitsanforderungen gemäß dem Verhaltensaspekt Geschwindigkeit im Hinblick auf die StVO [309] als auch die UN-Regelung Nr. 157 [308] als Anforderungsquelle.

Verhaltensaspekt Geschwindigkeit	
Abschnitt bzw. Absatz der Verordnung/Richtlinie	Inhalt im Wortlaut
StVO § 3 Geschwindigkeit [309]	*„(1) Wer ein Fahrzeug führt, darf nur so schnell fahren, dass das Fahrzeug ständig beherrscht wird. Die Geschwindigkeit ist insbesondere den Straßen-, Verkehrs-, Sicht- und Wetterverhältnissen sowie den persönlichen Fähigkeiten und den Eigenschaften von Fahrzeug und Ladung anzupassen. […] Es darf nur so schnell gefahren werden, dass innerhalb der übersehbaren Strecke gehalten werden kann. […]“* *„(2) Ohne triftigen Grund dürfen Kraftfahrzeuge nicht so langsam fahren, dass sie den Verkehrsfluss behindern.“*
UN-Regelung Nr. 157 Abschnitt 5.2.3.2 [308]	*„Das aktivierte System muss die Fahrzeuggeschwindigkeit an die Infrastruktur- und Umgebungsbedingungen (z.B. enge Kurvenradien, schlechtes Wetter) anpassen.“*
Übergeordneter Anforderungstyp: <<Interessenvertreteranforderung>>	
ID: L1.10000SHReq	
L1.1-SHReq Fahrdynamische Beherrschbarkeit	
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll nur so schnell fahren, dass dieses ständig hinsichtlich der Fahrdynamik beherrscht wird.	
ID: L1.20000SHReq	
L1.2-SHReq Geschwindigkeitsanpassung	
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll die Geschwindigkeit den Straßen-, Verkehrs-, Sicht- und Wetterverhältnissen sowie dem aktuellen Fahrzeug- und Ladungszustand anpassen.	
ID: L1.30000SHReq	

L1.3-SHReq Geschwindigkeitsanpassung Sichtfeld
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll nur so schnell fahren, dass dieses innerhalb der übersehbaren Strecke noch anhalten kann.

Tabelle C.4: Ableitung von verhaltensbezogenen Betriebssicherheitsanforderungen gemäß dem Verhaltensaspekt Abstand im Hinblick auf die StVO [310] als auch die UN-Regelung Nr. 157 [308] als Anforderungsquelle.

Verhaltensaspekt Abstand	
Abschnitt bzw. Absatz der Verordnung/Richtlinie	Inhalt im Wortlaut
StVO § 4 Abstand [310]	*„(1) Der Abstand zu einem vorausfahrenden Fahrzeug muss in der Regel so groß sein, dass auch dann hinter diesem gehalten werden kann, wenn es plötzlich gebremst wird.* *Wer vorausfährt, darf nicht ohne zwingenden Grund stark bremsen.“*
UN-Regelung Nr. 157 Abschnitt 5.2.3.3 [308]	*„Das aktivierte System muss den Abstand zum nächsten vorausfahrenden Fahrzeug ermitteln und die Fahrzeuggeschwindigkeit anpassen, um einen Zusammenstoß zu vermeiden.* *Solange sich das ALKS-Fahrzeug nicht im Stillstand befindet, muss das System die Geschwindigkeit so anpassen, dass der Abstand zu einem vorausfahrenden Fahrzeug auf demselben Fahrstreifen gleich oder größer als der Mindestabstand ist.* *Kann der Mindestabstand wegen anderer Verkehrsteilnehmer (z.B. ein einfahrendes Fahrzeug, ein abbremsendes vorausfahrendes Fahrzeug usw.) vorübergehend nicht eingehalten werden, muss das Fahrzeug den Mindestabstand bei der nächsten sich bietenden Gelegenheit ohne starkes Abbremsen neu einstellen, es sei denn, ein Notfallmanöver wäre erforderlich.* *[…] Der Mindestabstand darf bei Geschwindigkeiten unter 2 m/s niemals weniger als 2 m betragen.“*
UN-Regelung Nr. 157 Abschnitt 5.2.4. [308]	*„Das aktivierte System muss in der Lage sein, das Fahrzeug hinter einem stehenden Fahrzeug, einem stehenden Verkehrsteilnehmer oder einer blockierten Fahrspur zum Stillstand zu bringen, um einen Zusammenstoß zu vermeiden.* *Dies muss bis zur maximalen Betriebsgeschwindigkeit des Systems gewährleistet sein.“*
UN-Regelung Nr. 157 Abschnitt 5.2.5. [308]	*„Das aktivierte System muss die Gefahr einer Kollision insbesondere mit einem anderen Verkehrsteilnehmer vor […] dem Fahrzeug aufgrund eines abbremsenden vorausfahrenden Fahrzeugs, eines einfahrenden Fahrzeugs oder eines plötzlich auftauchenden Hindernisses erkennen und automatisch geeignete Manöver durchführen, um die Risiken für die Sicherheit der Fahrzeuginsassen und anderer Verkehrsteilnehmer zu minimieren.“*

UN-Regelung Nr. 157 Abschnitt 5.3.1. [308]	*„Bei drohender Kollisionsgefahr muss ein Notfallmanöver durchgeführt werden."*
UN-Regelung Nr. 157 Abschnitt 5.3.1.1 [308]	*„Jede Längsverzögerung des Systems von mehr als 5,0 m/s^2 ist als Notfallbremsmanöver zu betrachten."*
UN-Regelung Nr. 157 Abschnitt 5.3.2. [308]	*„Beim Notfallbremsmanöver wird das Fahrzeug erforderlichenfalls bis zur Erreichung seiner vollen Verzögerungsleistung abgebremst […]"*
Übergeordneter Anforderungstyp: <<Interessenvertreteranforderung>>	
ID: L1.40000SHReq	
L1.4-SHReq Abstandshaltung	
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L" soll in der Regel einen ausreichenden Abstand zum vorausfahrenden „L_1-Verkehrsteilnehmer_L" einhalten, dass auch dann hinter diesem gehalten werden kann, wenn dieser plötzlich gebremst wird. Dies soll bis zur maximalen Betriebsgeschwindigkeit gewährleistet werden.	
ID: L1.4.10000SHReq	
L1.4.1-SHReq Einhaltung eines definierten Mindestabstands	
Befindet sich das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L" nicht im Stillstand, soll dieses die Geschwindigkeit so anpassen, dass der Abstand zum „L_1-Verkehrsteilnehmer_L" auf demselben Fahrstreifen gleich oder größer als der definierte Mindestabstand ist.	
ID: L1.4.20000SHReq	
L1.4.2-SHReq Einhaltung eines definierten Mindestabstands bei niedrigen Geschwindigkeiten	
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L" soll bei Geschwindigkeiten unter $2\ \frac{m}{s}\ \left(7.2\ \frac{km}{h}\right)$ einen Mindestabstand von $2\ m$ einhalten.	
ID: L1.4.30000SHReq	
L1.4.3-SHReq Einstellung eines definierten Mindestabstands	
Kann der Mindestabstand des „L_1-Verkehrsteilnehmers_L" (z. B. ein einfahrendes Fahrzeug, ein abbremsendes vorausfahrendes Fahrzeug usw.) vorübergehend nicht eingehalten werden, soll das „L_1-Ego-Kraftfahrzeug_L" den Mindestabstand bei der nächsten sich bietenden Gelegenheit ohne starkes Abbremsen neu einstellen, es sei denn, ein Notfallbremsmanöver wird erforderlich.	
ID: L1.50000SHReq	
L1.5-SHReq Durchführung Notfallabbremsmanöver	
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L" soll bei Kollisionsgefahr mit einem abbremsenden vorausfahrenden „L_1-Verkehrsteilnehmer_L" oder einem in die Ego-Fahrspur einfahrenden „L_1-Verkehrsteilnehmer_L" erkennen und ein geeignetes Notfallabbremsmanöver (engl. Emergency Braking) im Sinne einer Längsverzögerung von $< -5.0\ \frac{m}{s^2}$ durchführen und erforderlichenfalls bis zur Erreichung seiner vollen Verzögerungsleistung abbremsen.	

Tabelle C.5: Ableitung von verhaltensbezogenen Betriebssicherheitsanforderungen gemäß dem Verhaltensaspekt Spurführung im Hinblick auf die UN-Regelung Nr. 157 [308] als Anforderungsquelle.

Verhaltensaspekt Spurführung bzw. -haltung	
Abschnitt bzw. Absatz der Verordnung/Richtlinie	Inhalt im Wortlaut
UN-Regelung Nr. 157 Abschnitt 5.2.1 [308]	*„Das aktivierte System muss das Fahrzeug innerhalb seiner Fahrspur halten und sicherstellen, dass das Fahrzeug keine Fahrbahnmarkierung überfährt (Außenkante des Vorderreifens bis Außenkante der Fahrbahnmarkierung). Das System*

	muss darauf abzielen, das Fahrzeug innerhalb eines stabilen Querführungsbereichs innerhalb der Fahrspur zu halten, um andere Verkehrsteilnehmer nicht zu verwirren.“
Übergeordneter Anforderungstyp: <<Interessenvertreteranforderung>>	
ID: L1.60000SHReq	
L1.6-SHReq Spurhaltung	
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll sich innerhalb seiner Ego-Fahrspur halten und sicherstellen, dass keine Fahrbahnmarkierungen unzweckmäßig überfahren werden (Außenkante des Vorderreifens bis Außenkante der Fahrbahnmarkierung).	
ID: L1.70000SHReq	
L1.7-SHReq Stabiler Querführungsbereich	
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll sich innerhalb eines stabilen Querführungsbereichs hinsichtlich der Ego-Fahrspur halten, um den „L_1-Verkehrsteilnehmer_L“ nicht zu verwirren.	

Tabelle C.6: Betriebsbereichsbedingte Parameter der geometrischen Gestaltung von Autobahnen des Typs EKA 1 A und EKA 1 B gemäß der RAA [246].

Autobahnklassifikation	EKA 1 A	EKA 1 B
Funktion	Fernautobahn	Überregionalautobahn
Geschwindigkeitsbegrenzung	Keine	Keine
Kurvenmindestradius	$900\ m$	$720\ m$
Spurmindestbreite	$3.50\ m$	$3.50\ m$

C.1.3 Artefakte der Betriebsbereichsdefinition und -analyse

Tabelle C.7: Getroffene Annahme und vorgenommene Einschränkungen im Hinblick auf ideale Witterungsbedingungen und Temperaturen sowie den Ausschluss entsprechender Attribute und zusätzlicher Verkehrsteilnehmer aus dem Betrachtungsrahmen bzw. der Betriebsbereichsdefinition.

<<Annahme>>
ID: L1.10000ASMP
L1.1-ASMP Ideale Witterungsbedingungen und Temperaturen über dem Gefrierpunkt bei Tageslicht
Im Hinblick auf das Attribut „L_1-Wetter_L“ sowie „L_1-Ausleuchtung_L“ werden ideale Witterungsbedingungen sowie Temperaturen weit über dem Gefrierpunkt bei Tageslicht angenommen.
<<Einschränkung>>
ID: L1.30000CSTR
L1.3-CSTR Ausschluss Steigungen bzw. Gefälle des „L_1-Fahrbahnbereichs_L“
Innerhalb des Attributs „L_1-Fahrbahnbereich_L“ werden mögliche Gefälle und Steigungen aus dem Betrachtungsrahmen des definierten Betriebsbereichs ausgeschlossen.
ID: L1.40000CSTR
L1.4-CSTR Ausschluss der Attribute „L_1-Kreuzungen_L“, „L_1-Sonderstrukturen_L“ usw.

Die Attribute „L_1-Kreuzungen_L“, „L_1-Sonderstrukturen_L“, „L_1-FesteStraßenstrukturen_L“, „L_1-TemporäreStraßenstrukturen_L“, „L_1-PartikelUndFeinstaub_L“ sowie „L_1-Konnektivität_L“ werden aus der Betriebsbereichsdefinition exkludiert. Dies gilt auch für Fußgänger, Wildtieren etc. innerhalb des Attributs „L_1-Verkehrsteilnehmer_L“.
ID: L1.50000CSTR
L1.5-CSTR „L_1-Verkehrsteilnehmer_L“ bezieht sich auf nur ein vorausfahrendes Kraftfahrzeug
In Bezug auf das Kontextelement „L_1-Verkehrsteilnehmer_L“ wird lediglich ein vorausfahrendes bzw. ein sich parallel neben des Ego-Fahrstreifens befindendes Kraftfahrzeug berücksichtigt, wodurch weitere Verkehrsteilnehmer hinter dem „L_1-Ego-Kraftfahrzeug_L“ nicht in den Betrachtungsrahmen des definierten Betriebsbereichs fallen.

Tabelle C.8: Getroffene Annahme der Beschreibung des analytisch dynamischen Ego-Kraftfahrzeugverhaltens, des vorausfahrenden „L_1-Verkehrsteilnehmers_L“ sowie vorgenommene Einschränkung der Bewegungsfreiheitsgrade.

<<Annahme>>
ID: L1.20000ASMP
L1.2-ASMP Beschreibung des analytisch dynamischen Ego-Kraftfahrzeugverhaltens sowie des vorausfahrenden „L_1-Verkehrsteilnehmers_L“ anhand der Gesetzmäßigkeiten des Punktmassemodells
Es wird angenommen, dass das jeweils analytisch dynamische Verhalten des „L_1-Ego-Kraftfahrzeugs_L“ als auch des „L_1-Verkehrsteilnehmers_L“ mittels der kinematischen Gesetzmäßigkeiten des Punktmassemodells für die durchzuführenden Analysetätigkeiten während der Betriebskonzeptphase ausreichend genau beschrieben werden kann.
<<Einschränkung>>
ID: L1.60000CSTR
L1.6-CSTR Bewegungsfreiheitsgrade des „L_1-Ego-Kraftfahrzeugs_L“ sowie des „L_1-Verkehrsteilnehmers_L“ beschränken sich auf den dreidimensionalen Bereich
Der Betrachtungsrahmen der Bewegungsfreiheitsgrade des „L_1-Ego-Kraftfahrzeugs_L“ als auch des „L_1-Verkehrsteilnehmers_L“ wird auf den dreidimensionalen Bereich limitiert. Zudem wird der Betrachtungsumfang hinsichtlich des längsdynamischen Grenzbereichs auf $-10\,\frac{m}{s^2}$ sowie des querdynamischen Grenzbereichs auf $\pm 4\,\frac{m}{s^2}$ begrenzt.

Tabelle C.9: Definition des Basisszenarios „L_1-Freifahrt“.

<<Szenario>>		
ID: L1.10000SCEN		
L1.1-SCEN Basisszenario „L_1-Freifahrt“		
Szene	<<Dynamische Elemente>>	• „L_1-Ego-Kraftfahrzeug_L“ • „L_1-Fahrer/Passagier_L“
	<<Szenerie>>	• „L_1-Zone_L“ • „L_1-Fahrbahnbereich_L“
	<<Umgebungsbedingungen>>	• „L_1-Wetter_L“ • „L_1-Ausleuchtung_L“
	<<Selbstrepräsentation>>	• „L_1-Ego-Kraftfahrzeug_L“: ○ Maximale Längsgeschwindigkeit: $36.11\,\frac{m}{s}\left(130\,\frac{km}{h}\right)$ ○ Maximale Längsverzögerung: $-10\,\frac{m}{s^2}$

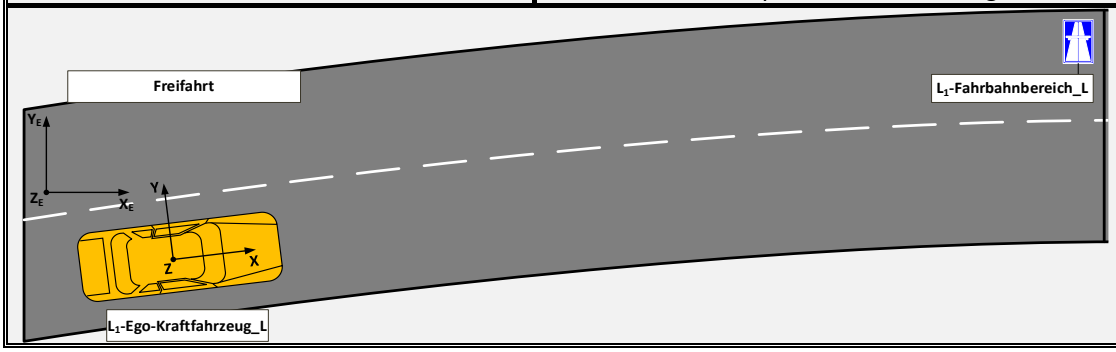
		○ Maximale Querbeschleunigung: $\pm 4\ \frac{m}{s^2}$ ○ Ausschluss von Spurwechsel- oder Ausweichmanövern ○ Frontsichtbereich eingeschränkt auf Ego-Fahrstreifen • „L_1-Fahrbahnbereich_L“: ○ Kurvenmindestradius: $720\ m$ ○ Spurmindestbreite: $3.50\ m$
Aktionen und Ereignisse		• „L_1-Ego-Kraftfahrzeug_L“: ○ „Freifahrt“ ○ „Fahrstreifen Folgen“
Ziele und Werte		• L1.1-SHReq Fahrdynamische Beherrschbarkeit • L1.2-SHReq Geschwindigkeitsanpassung • L1.3-SHReq Geschwindigkeitsanpassung Sichtfeld • L1.6-SHReq Spurhaltung • L1.7-SHReqStabiler Querführungsbereich
		

Tabelle C.10: Definition des Basisszenarios „L_1-Annähern“.

<<Szenario>>		
ID: L1.20000 SCEN		
L1.2-SCEN Basisszenario „L_1-Annähern“		
Szene	<<Dynamische Elemente>>	• „L_1-Ego-Kraftfahrzeug_L“ • „L_1-Fahrer/Passagier_L“ • „L_1-Verkehrsteilnehmer_L“
	<<Szenerie>>	• „L_1-Zone_L“ • „L_1-Fahrbahnbereich_L“
	<<Umgebungsbedingungen>>	• „L_1-Wetter_L“ • „L_1-Ausleuchtung_L“
	<<Selbstrepräsentation>>	• „L_1-Ego-Kraftfahrzeug_L“: ○ Maximale Längsgeschwindigkeit: $36.11\ \frac{m}{s}\left(130\ \frac{km}{h}\right)$ ○ Maximale Längsverzögerung: $-10\ \frac{m}{s^2}$ ○ Maximale Querbeschleunigung: $\pm 4\ \frac{m}{s^2}$

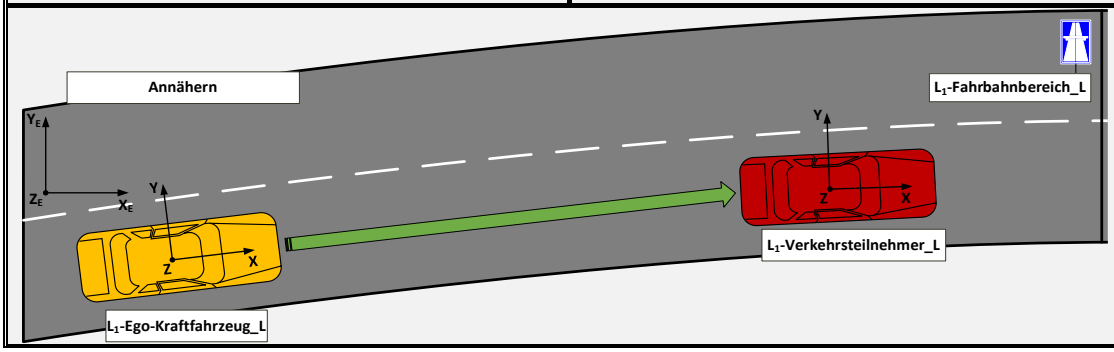
		○ Ausschluss von Spurwechsel- oder Ausweichmanövern ○ Frontsichtbereich eingeschränkt auf Ego-Fahrstreifen • „L_1-Verkehrsteilnehmer_L“: ○ Maximale Längsgeschwindigkeit: $36.11\ \frac{m}{s}\left(130\ \frac{km}{h}\right)$ ○ Maximale Längsverzögerung: $-10\ \frac{m}{s^2}$ ○ Maximale Querbeschleunigung: $\pm 4\ \frac{m}{s^2}$ • „L_1-Fahrbahnbereich_L“: ○ Kurvenmindestradius: $720\ m$ ○ Spurmindestbreite: $3.50\ m$
Aktionen und Ereignisse		• „L_1-Ego-Kraftfahrzeug_L“: ○ „Annähern“ an „L_1-Verkehrsteilnehmer_L“ ○ „Fahrstreifen Folgen“ • „L_1-Verkehrsteilnehmer_L“: ○ „Beschleunigen“ ○ „Geschwindigkeitsbeibehaltung“ ○ „Verzögern“ ○ „Stillstand“
Ziele und Werte		• L1.1-SHReq Fahrdynamische Beherrschbarkeit • L1.2-SHReq Geschwindigkeitsanpassung • L1.3-SHReq Geschwindigkeitsanpassung Sichtfeld • L1.4-SHReq Abstandshaltung • L1.5-SHReq Notfallabbremsmanöver • L1.6-SHReq Spurhaltung • L1.7-SHReq Stabiler Querführungsbereich
		

Tabelle C.11: Definition des Basisszenarios „L_1-Abstandshaltung“.

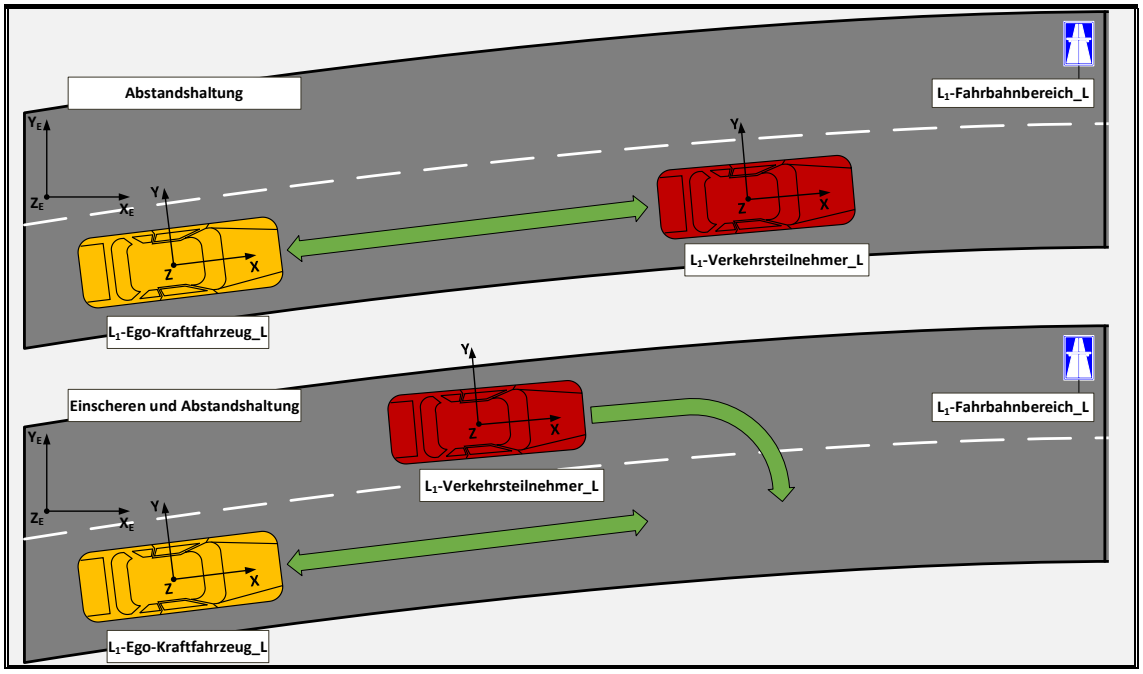
<<Szenario>>
ID: L1.30000SCEN
L1.3-SCEN Basisszenario „L_1-Abstandshaltung“

Szene	<<Dynamische Elemente>>	• „L_1-Ego-Kraftfahrzeug_L“ • „L_1-Fahrer/Passagier_L“ • „L_1-Verkehrsteilnehmer_L“
	<<Szenerie>>	• „L_1-Zone_L“ • „L_1-Fahrbahnbereich_L“
	<<Umgebungsbedingungen>>	• „L_1-Wetter_L“ • „L_1-Ausleuchtung_L“

	<<Selbstrepräsentation>>	• „L_1-Ego-Kraftfahrzeug_L“:
		  ○ Maximale Längsgeschwindigkeit: $36.11\ \frac{m}{s}\left(130\ \frac{km}{h}\right)$
		  ○ Maximale Längsverzögerung: $-10\ \frac{m}{s^2}$
		  ○ Maximale Querbeschleunigung: $\pm 4\ \frac{m}{s^2}$
		  ○ Ausschluss von Spurwechsel- oder Ausweichmanövern
		  ○ Frontsichtbereich eingeschränkt auf Ego-Fahrstreifen
		• „L_1-Verkehrsteilnehmer_L“:
		  ○ Maximale Längsgeschwindigkeit: $36.11\ \frac{m}{s}\left(130\ \frac{km}{h}\right)$
		  ○ Maximale Längsverzögerung: $-10\ \frac{m}{s^2}$
		  ○ Maximale Querbeschleunigung: $\pm 4\ \frac{m}{s^2}$
		• „L_1-Fahrbahnbereich_L“:
		  ○ Kurvenmindestradius: $720\ m$
		  ○ Spurmindestbreite: $3.50\ m$

Aktionen und Ereignisse		• „L_1-Ego-Kraftfahrzeug_L“:
		  ○ „Abstandshaltung“ bezüglich „L_1-Verkehrsteilnehmer_L“
		  ○ „Fahrstreifen Folgen“
		• „L_1-Verkehrsteilnehmer_L“:
		  ○ „Beschleunigen“
		  ○ „Geschwindigkeitsbeibehaltung“
		  ○ „Verzögern“
		  ○ „Spurwechsel („Einscheren“ und/oder „Ausscheren“)

Ziele und Werte		• L1.1-SHReq Fahrdynamische Beherrschbarkeit • L1.2-SHReq Geschwindigkeitsanpassung • L1.3-SHReq Geschwindigkeitsanpassung Sichtfeld • L1.4-SHReq Abstandshaltung • L1.5-SHReq Notfallabbremsmanöver • L1.6-SHReq Spurhaltung • L1.7-SHReq Stabiler Querführungsbereich



C.1.4 Artefakte der betriebsbereichsbedingten Gefahrenanalyse und Risikobewertung

Tabelle C.12: Identifizierte Verlustszenarien gemäß des ersten STPA-Schritts „Gegenstand der Analyse definieren“ im Hinblick auf den Betrieb des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“.

<<Verlustszenario>>
ID: L1.10000LSCEN
L1.1-LSCEN Personenschaden sowohl innerhalb als auch außerhalb des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“
ID: L1.20000LSCEN
L1.2-LSCEN Sachschaden am hochautomatisierten „L_1-Ego-Kraftfahrzeug_L“
ID: L1.30000LSCEN
L1.3-LSCEN Umwelt- bzw. Sachschaden an statischen und/oder dynamischen Objekten außerhalb des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“
ID: L1.40000LSCEN
L1.4-LSCEN Verletzung und/oder Missachtung der Verkehrsregeln gemäß der deutschen StVO durch das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“

Tabelle C.13: Übersicht über die ASIL-Klassifikation der betrachteten Gefährdungsereignisse anhand der Längsgeschwindigkeitsbereiche des „L_1-Ego-Kraftfahrzeugs_L“.

	Geschwindigkeitsbereiche des „L_1-Ego-Kraftfahrzeugs_L“				
Gefährdungsereignis	Sehr niedrig $\{0; 10\}\frac{km}{h}$	Niedrig $\{10; 40\}\frac{km}{h}$	Mittel $\{40; 70\}\frac{km}{h}$	Hoch $\{70; 100\}\frac{km}{h}$	Sehr hoch $\{100; 130\}\frac{km}{h}$

Frontkollision mit beweglichem Hindernis auf dem Ego-Fahrstreifen	QM S0, E2, C3	QM S0, E2, C3	QM S1, E2, C3	ASIL B S3, E2, C3	ASIL B S3, E2, C3
Frontkollision mit „L_1-Verkehrsteilnehmer_L“	QM S0, E4, C3	QM S0, E4, C3	ASIL B S1, E4, C3	ASIL D S3, E4, C3	ASIL D S3, E4, C3
Seitliche/schräge Kollision mit unbeweglichem Objekt Rande des „L_1-Fahrbahnbereichs_L“	QM S0, E4, C3	ASIL B S1, E4, C3	ASIL C S2, E4, C3	ASIL D S3, E4, C3	ASIL D S3, E4, C3
Seitliche/schräge Kollision mit „L_1-Verkehrsteilnehmer_L“ durch Verlassen des Ego-Fahrstreifens	QM S1, E4, C0	QM S1, E4, C1	ASIL B S1, E4, C3	ASIL D S3, E4, C3	ASIL D S3, E4, C3

Tabelle C.14: Identifizierte gefährdende Verhaltensweisen einschließlich vorgenommener ASIL-Klassifikation und dazugehörige Gefährdungsereignisse des ersten STPA-Schritts „Gegenstand der Analyse definieren“ im Hinblick auf den Betrieb des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“.

<<Gefährdende Verhaltensweise>>
ID: L1.10000HB
L1.1-HB Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ unterschreitet den sicheren Abstand zu Hindernissen
ASIL B
<<Gefährdungsereignis>>
ID: L1.10000HE
L1.1-HE Frontkollision mit beweglichem Hindernis auf dem Ego-Fahrstreifen
<<Gefährdende Verhaltensweise>>
ID: L1.20000HB
L1.2-HB Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ unterschreitet den sicheren Abstand zum „L_1-Verkehrsteilnehmer_L“
ASIL D
<<Gefährdungsereignis>>
ID: L1.20000HE
L1.2-HE Frontkollision mit vorausfahrendem „L_1-Verkehrsteilnehmer_L“
<<Gefährdende Verhaltensweise>>
ID: L1.30000HB
L1.3-HB Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ verlässt den vorgesehenen Ego-Fahrstreifen bzw. die vorgesehene Trajektorie

ASIL D
<<Gefährdungsereignis>>
ID: L1.30000HE
L1.3-HE Seitliche/Schräge Kollision mit unbeweglichem Objekt am Rande des „L_1-Fahrbahnbereichs_L“
ID: L1.40000HE
L1.4-HE Seitliche und/oder schräge Kollision mit „L_1-Verkehrsteilnehmer_L“

Tabelle C.15: Erhobene Betriebssicherheitsziele im Hinblick auf das „L_1-Ego-Kraftfahrzeug_L“.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsziel>>
ID: L1.10000OpSaG
L1.1-OpSaG Vermeidung der Unterschreitung sicherer Abstände zu Hindernissen
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll die Unterschreitung sicherer Abstände zu Hindernissen vermeiden.
ASIL D
ID: L1.20000OpSaG
L1.2-OpSaG Vermeidung der Unterschreitung sicherer Abstände zum „L_1-Verkehrsteilnehmer_L“
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll die Unterschreitung sicherer Abstände zum vorausfahrenden „L_1-Verkehrsteilnehmer_L“ vermeiden.
ASIL D
ID: L1.30000OpSaG
L1.3-OpSaG Vermeidung eines unbeabsichtigten Verlassens des Ego-Fahrstreifens
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll ein unbeabsichtigtes Verlassen des vorgesehenen Ego-Fahrstreifens bzw. der vorgesehenen Trajektorie vermeiden.
ASIL D

Tabelle C.16: Herbeigeführte Entwurfsentscheidung und deren Rechtfertigung bezüglich des Stillstands auf dem aktuellen bzw. rechten Ego-Fahrstreifen als sicherer Zustand.

<<Entwurfsentscheidung>>
ID: L1.20000DECN
L1.2-DECN Stillstand auf dem aktuellen bzw. rechten Ego-Fahrstreifen als sicherer Zustand
<<Rechtfertigung>>
ID: L1.10000JSTF
L1.1-JSTF Begrenzung Frontsichtbereich des „L_1-Ego-Kraftfahrzeugs_L“ auf den Ego-Fahrstreifen etc. als Rechtfertigung für die Einnahme des Stillstands als sicheren Zustand
Die Begrenzung des Frontsichtbereich des „L_1-Ego-Kraftfahrzeugs_L“ auf den Ego-Fahrstreifen (vgl. L1.1-UC), die Nichtberücksichtigung von weiteren „L_1-Verkehrsteilnehmern_L“ hinter dem „L_1-Ego-Kraftfahrzeug_L“ gemäß Einschränkung L1.5-CSTR als auch der Ausschluss von Fahrstreifenwechseln (vgl. L1.1-UC) rechtfertigt den Stillstand auf dem Ego-Fahrstreifen als sicheren Zustand.

C.1.5 Artefakte des Betriebssicherheitskonzepts

Tabelle C.17: Überblick der jeweiligen Fahrzonen als auch der zonenabhängigen Maximalverzögerung und Abstandszeitkonstante im Hinblick auf den Entscheidungsraum der Fahrzeugverhaltensspezifikation des „L_1-Ego-Kraftfahrzeugs_L“ im Zuge der Durchführung von SOCA.

Bezeichnung der Fahrzone	Fahrzone	Zonenabhängige Maximalverzögerung $[\frac{m}{s^2}]$	Vektor Zonenabhängigen Abstandszeitkonstante $[s]$
Notfallabbremsungsfahrzone	A_5	$a_5 = -10$	$\boldsymbol{t_5} = [1.1: 0.1: 2.3]$
Harte Abbremsungsfahrzone	A_4	$a_4 = -5$	$\boldsymbol{t_4} = 1.2 \cdot \boldsymbol{t_5}$
Komfortable Abbremsungsfahrzone	A_3	$a_3 = -2$	$\boldsymbol{t_3} = 1.4 \cdot \boldsymbol{t_5}$
Zielabstandsfahrzone	A_2	$a_2 = -0.75$	$\boldsymbol{t_2} = 1.6 \cdot \boldsymbol{t_5}$
Annäherungsfahrzone	A_1	$a_1 = -0.5$	$\boldsymbol{t_1} = 1.8 \cdot \boldsymbol{t_5}$
Maximalsichtbereichsfahrzone	A_0	$a_0 = 0$	Nichtzutreffend

Tabelle C.18: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf die Durchführung der „Notfallabbremsung“ als Modus 1.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.10000OpSaReq
L1.1-OpSaReq Verhaltensregel 1 im Hinblick auf die Durchführung einer Notfallabbremsung (Modus 1)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A5$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = ($TTC \leq TTC_{min}$ ODER $TTC > TTC_{min}$)
ASIL D
ID: L1.20000OpSaReq
L1.2-OpSaReq Verhaltensregel 2 im Hinblick auf die Durchführung einer Notfallabbremsung (Modus 1)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = ($A4$ ODER $A3$ ODER $A2$) UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = $TTC \leq TTC_{min}$
ASIL D
ID: L1.30000OpSaReq
L1.3-OpSaReq Verhaltensregel 3 im Hinblick auf die Durchführung der „Notfallabbremsung“ (Modus 1)
Ego-Kraftfahrzeug Modus = Annähern UND Fahrzone = $A1$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = $TTC \leq TTC_{min}$
ASIL D

Tabelle C.19: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf die Durchführung der „Harten Abbremsung“ als Modus 2.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.40000OpSaReq
L1.4-OpSaReq Verhaltensregel 1 im Hinblick auf die Durchführung der „Harten Abbremsung“ (Modus 2)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A4$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = TTC > TTCmin
ASIL D

Tabelle C.20: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf die Durchführung der „Komfortablen Abbremsung“ als Modus 3.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.50000OpSaReq
L1.5-OpSaReq Verhaltensregel 1 im Hinblick auf die Durchführung der „Komfortablen Abbremsung“ (Modus 3)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A3$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = TTC > TTCmin
ASIL D
ID: L1.60000OpSaReq
L1.6-OpSaReq Verhaltensregel 2 im Hinblick auf die Durchführung der „Komfortablen Abbremsung“ (Modus 3)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = (A5 ODER A4) UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} == 0$ UND Time To Collision = Nichtzutreffend
ASIL D

Tabelle C.21: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf die Durchführung des „Segelns“ als Modus 4.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.70000OpSaReq
L1.7-OpSaReq Verhaltensregel 1 im Hinblick auf die Durchführung des „Segelns“ (Modus 4)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A3$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} == 0$ UND Time To Collision = Nichtzutreffend
ASIL D
ID: L1.80000OpSaReq
L1.8-OpSaReq Verhaltensregel 2 im Hinblick auf die Durchführung des „Segelns“ (Modus 4)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A2$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = $TTC > TTC_{min}$

ASIL D

Tabelle C.22: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf die Beibehaltung des „Stillstands“ als Modus 5.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.90000OpSaReq
L1.9-OpSaReq Verhaltensregel 1 im Hinblick auf die Beibehaltung des „Stillstands“ (Modus 5)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = ($A5$ ODER $A4$ ODER $A3$) UND Ego-Längsgeschwindigkeit = $v_{sub} == 0$ UND Relativgeschwindigkeit = ($v_{rel} == 0$ ODER $v_{rel} > 0$) UND Time To Collision = Nichtzutreffend
ASIL D
ID: L1.100000OpSaReq
L1.10-OpSaReq Verhaltensregel 2 im Hinblick auf die Beibehaltung des „Stillstands“ (Modus 5)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A2$ UND Ego-Längsgeschwindigkeit = $v_{sub} == 0$ UND Relativgeschwindigkeit = $v_{rel} == 0$ UND Time To Collision = Nichtzutreffend
ASIL D

Tabelle C.23: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf „Geschwindigkeitsbeibehaltung“ als Modus 6.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.110000OpSaReq
L1.11-OpSaReq Verhaltensregel 1 im Hinblick auf „Geschwindigkeitsbeibehaltung“ (Modus 6)
Ego-Kraftfahrzeug Modus = Freie Fahrt UND Fahrzone = $A0$ UND Ego-Längsgeschwindigkeit = $v_{sub} = v_{sub,max}$ UND Relativgeschwindigkeit = Nichtzutreffend UND Time To Collision = Nichtzutreffend
ASIL D
ID: L1.120000OpSaReq
L1.12-OpSaReq Verhaltensregel 2 im Hinblick auf „Geschwindigkeitsbeibehaltung“ (Modus 6)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = ($A5$ ODER $A4$ ODER $A3$) UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} > 0$ UND Time To Collision = Nichtzutreffend
ASIL D
ID: L1.130000OpSaReq
L1.13-OpSaReq Verhaltensregel 3 im Hinblick auf „Geschwindigkeitsbeibehaltung“ (Modus 6)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A2$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} == 0$ UND Time To Collision = Nichtzutreffend
ASIL D
ID: L1.140000OpSaReq
L1.14-OpSaReq Verhaltensregel 4 im Hinblick auf „Geschwindigkeitsbeibehaltung“ (Modus 6)
Ego-Kraftfahrzeug Modus = Annähern Fahrzone = $A1$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = $TTC > TTC_{min}$
ASIL D

Tabelle C.24: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf die Durchführung der „Beschleunigung“ als Modus 7.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.150000OpSaReq
L1.15-OpSaReq Verhaltensregel 1 im Hinblick auf die Durchführung der „Beschleunigung“ (Modus 7)
Ego-Kraftfahrzeug Modus = Freie Fahrt UND Fahrzone = $A0$ UND Ego-Längsgeschwindigkeit = ($v_{sub} == 0$ ODER $0 < v_{sub} < v_{sub,max}$) UND Relativgeschwindigkeit = Nichtzutreffend UND Time To Collision = Nichtzutreffend
ASIL D
ID: L1.160000OpSaReq
L1.16-OpSaReq Verhaltensregel 2 im Hinblick auf die Durchführung der „Beschleunigung“ (Modus 7)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A1$ UND Ego-Längsgeschwindigkeit = ($v_{sub} == 0$ ODER $0 < v_{sub} < v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} == 0$ UND Time To Collision = Nichtzutreffend
ASIL D
ID: L1.170000OpSaReq
L1.17-OpSaReq Verhaltensregel 3 im Hinblick auf die Durchführung der „Beschleunigung“ (Modus 7)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = ($A2$ ODER $A1$) UND Ego-Längsgeschwindigkeit = ($v_{sub} == 0$ ODER $0 < v_{sub} < v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} > 0$ UND Time To Collision = Nichtzutreffend
ASIL D

Tabelle C. 25: Getroffene Annahmen des Bremsverhaltens des „L_1-Verkehrsteilnehmers_L“, der Bekanntheit relevanter Parameter und Bewegungsmodelle als auch deren perfekte Wahrnehmung sowie eine ausreichend niedrige Längsgeschwindigkeit bei Kurveneinfahrt.

<<Annahme>>
ID: L1.30000ASMP
L1.3-ASMP Keine unzulässigen bzw. vernünftigerweise unvorhersehbar starken Bremsmanöver des „L_1-Verkehrsteilnehmers_L“
Im Zuge der Deduktion der Fahrzeugverhaltensspezifikation des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“ wird angenommen, dass der „L_1-Verkehrsteilnehmer_L“ keine unzulässigen bzw. vernünftigerweise unvorhersehbar starken Bremsmanöver durchführt.
ID: L1.40000ASMP
L1.4-ASMP Bekanntheit der relevanten statischen Parameter der Szenerie und der Bewegungsmodelle sowie perfekte Wahrnehmung und Fehlerfreiheit des „L_1-Ego-Kraftfahrzeugs_L“
Im Zuge der Deduktion der Fahrzeugverhaltensspezifikation des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“ wird angenommen, dass alle relevanten statischen Parameter der Szenerie und der Bewegungsmodelle bekannt sind, der „L_1-Verkehrsteilnehmer_L“ bis zu einer Entfernung von $150\ m$ perfekt wahrgenommen und der gesamte operative Systemzustand des „L_1-Ego-Kraftfahrzeugs_L“ fehlerfrei ist.
ID: L1.50000ASMP
L1.5-ASMP Ausreichend niedrige Längsgeschwindigkeit bei Kurveneinfahrt im Hinblick auf die Einhaltung der Gesetzmäßigkeiten kombinierter Reifenlängs- und querkräfte
Im Zuge der Deduktion der Fahrzeugverhaltensspezifikation des hochautomatisierten „L_1-Ego-Kraftfahrzeugs_L“ wird angenommen, dass die Längsgeschwindigkeit bei Kurveneinfahrt ausreichend niedrig ist, so dass diese unter Berücksichtigung von idealen Straßenbedingungen nicht dazu führt, dass das „L_1-Ego-Kraftfahrzeug_L“ die Ego-Fahrspur ungewollt verlässt.

Tabelle C.26: Modusübergangsmatrix der jeweiligen Ausgangs- und Zielmodi im Hinblick auf die Fahrzeugverhaltensspezifikation des „L_1-Ego-Kraftfahrzeugs_L“ im Zuge der Durchführung von SOCA.

		Zielmodi							
		Notfallabbremsung	Harte Abbremsung	Komfortable Abbremsung	Segeln	Stillstand	Geschwindigkeits-beibehaltung	Beschleunigung	Keine Transition
Ausgangsmodi	Notfallabbremsung	*	E1	E2	E3	E4	E5	E6	E7
	Harte Abbremsung	E8	*	E9	E10	E11	E12	E13	E14
	Komfortable Abbremsung	E15	E16	*	E17	E18	E19	E20	E21
	Segeln	E22	E23	E24	*	E25	E26	E27	E28
	Stillstand	-	-	-	-	*	-	E29	E30
	Geschwindigkeits-beibehaltung	E31	E32	E33	E34	-	*	E35	E36
	Beschleunigung	E37	E38	E39	E40	-	E41	*	E42

Nach dem oben dargestellten Verfahren in Bezug auf die Durchführung von SOCA werden die Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln der jeweiligen Modusübergänge erhoben. Aus Gründen des Umfangs werden diese innerhalb der vorliegenden Dissertation allerdings nicht weiter tabellarisch erfasst bzw. dargestellt (siehe Tabelle C.27).

Tabelle C.27: Gemäß der Durchführung von SOCA erhobene Betriebssicherheitsanforderungen an das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ im Sinne von Verhaltensregeln im Hinblick auf die Durchführung eines Modusübergangs „Notfallabbremsung“ zur „Harten Abbremsung“.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.180000OpSaReq
L1.18-OpSaReq Verhaltensregel 1 im Hinblick auf die Durchführung des Modusübergangs von der „Notfallabbremsung“ zur „Harten Abbremsung“ (E1)
Ego-Kraftfahrzeug Modus = Abstandshaltung UND Fahrzone = $A4$ UND Ego-Längsgeschwindigkeit = ($0 < v_{sub} < v_{sub,max}$ ODER $v_{sub} = v_{sub,max}$) UND Relativgeschwindigkeit = $v_{rel} < 0$ UND Time To Collision = TTC > TTCmin
ASIL D

Tabelle C.28: Überblick der jeweiligen Modi und der dadurch vollständig erfassten Zustände im Hinblick auf den Entscheidungsraum der Fahrzeugverhaltensspezifikation des „L_1-Ego-Kraftfahrzeugs_L“ im Zuge der Durchführung von SOCA.

Modus	Erfasste Zustände
Modus 1: Notfallabbremsung	12
Modus 2: Harte Abbremsung	2
Modus 3: Komfortable Abbremsung	6
Modus 4: Segeln	4
Modus 5: Stillstand	7
Modus 6: Geschwindigkeitsbeibehaltung	11
Modus 7: Beschleunigung	8
Modus 8: Nicht-System-Modus	598
Gesamtanzahl der durch die Modi erfassten Zustände	648
Gesamtanzahl möglicher Zustände des betrachteten Entscheidungsraums	648

Tabelle C.29: Berechnung der zonenabhängigen minimalen Abstandszeitkonstante sowie des Mindestabstandes gemäß der UN-Regelung Nr. 157 [271] einschließlich linearer Interpolation bis zur maximalen Längsgeschwindigkeit des „L_1-Ego-Kraftfahrzeugs_L“.

„L_1-Ego-Kraftfahrzeug_L“ Längsgeschwindigkeit $[\frac{km}{h}]$	„L_1-Ego-Kraftfahrzeug_L“ Längsgeschwindigkeit $[\frac{m}{s}]$	Zonenabhängigen Abstandszeitkonstante $[s]$	Zonenabhängigen Mindestabstand $[m]$
$v_{sub} = 10$	$v_{sub} = 2.78$	$t_5 = 1.1$	$A_5 = 3.1$
$v_{sub} = 20$	$v_{sub} = 5.56$	$t_5 = 1.2$	$A_5 = 6.7$
$v_{sub} = 30$	$v_{sub} = 8.33$	$t_5 = 1.3$	$A_5 = 10.8$
$v_{sub} = 40$	$v_{sub} = 11.11$	$t_5 = 1.4$	$A_5 = 15.6$
$v_{sub} = 50$	$v_{sub} = 13.89$	$t_5 = 1.5$	$A_5 = 20.8$
$v_{sub} = 60$	$v_{sub} = 16.67$	$t_5 = 1.6$	$A_5 = 26.7$
$v_{sub} = 70$	$v_{sub} = 19.44$	$t_5 = 1.7$	$A_5 = 33.0$
$v_{sub} = 100$	$v_{sub} = 27.78$	$t_5 = 2.0$	$A_5 = 55.6$
$v_{sub,max} = 130$	$v_{sub,max} = 36.11$	$t_5 = 2.3$	$A_5 = 83.1$

Tabelle C.30: An das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ gestellte Betriebssicherheitsanforderungen im Sinne von funktionalen L_1-System-Of-Systems-Fähigkeiten.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L1.200000OpSaReq
L1.20-OpSaReq Wahrnehmung und Erkennung relevanter statischer und dynamischer Objekte
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll innerhalb des Betriebsbereichs die relevanten Attribute der „L_1-Zone_L“, des „L_1-Fahrbahnbereichs_L“ sowie des „L_1-Verkehrsteilnehmers_L“ wahrnehmen, klassifizieren und deren Bedeutung verstehen.
Relevante Eingangsschnittstellen: • *„Zonenbedingungen“* • *„Fahrbahnbereichsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
ASIL D
ID: L1.210000OpSaReq
L1.21-OpSaReq Wahrnehmung und Erkennung der Umgebungsbedingungen

Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll innerhalb des Betriebsbereichs die gegebenen Bedingungen gemäß den Attributen „L_1-Wetter_L“ und „L_1-Ausleuchtung_L“ wahrnehmen, klassifizieren und deren Bedeutung verstehen.
Relevante Eingangsschnittstellen: • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“*
ASIL D
ID: L1.220000OpSaReq
L1.22-OpSaReq Vorhersage des zukünftigen Verhaltens relevanter statischer und dynamischer Objekte
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll situationsbedingte Vorhersagen des zukünftigen Verhaltens des „L_1-Fahrbahnbereichs_L“ und insbesondere des „L_1-Verkehrsteilnehmers_L“ treffen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
ASIL D
ID: L1.230000OpSaReq
L1.23-OpSaReq Erstellung einer kollisionsfreien und gesetzeskonformen Trajektorienplanung und Regelung in Längs- und Querrichtung
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll eine kollisionsfreie (soweit wie praktikabel möglich) und gesetzeskonforme Trajektorienplanung und Regelung in Längs- und Querrichtung durchführen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L1.240000OpSaReq
L1.24-OpSaReq Trajektorienplanung und Regelung unter Berücksichtigung von Unsicherheiten
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll die Trajektorienplanung und Regelung unter Berücksichtigung von Unsicherheiten des fahrzeugexternen Betriebsbereichs sowie der eigenen Leistungsfähigkeit durchführen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L1.250000OpSaReq
L1.25-OpSaReq Folgenminderung bei unvermeidlichen Kollisionen
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll bei einer unvermeidlichen Kollision deren Folgen soweit wie praktikabel möglich minimieren.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*

ASIL D
ID: L1.260000OpSaReq
L1.26-OpSaReq Überwachung des Ego-Zustands und der Erreichung des beabsichtigten Nominalverhaltens
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll den Ego-Zustand im Sinne der Leistungsfähigkeit bzgl. des aktuell erreichbaren Sensorsichtbereichs als auch der Reaktionszeit auf wahrgenommene statische und dynamische Attribute des „L_1-Fahrbahnbereichs_L“, des „L_1-Wetters_L“ sowie des „L_1-Verkehrsteilnehmers_L“ überwachen und feststellen, wenn das beabsichtigte Nominalverhalten nicht erreicht werden kann.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L1.270000OpSaReq
L1.27-OpSaReq Degradation im Falle unzureichenden Nominalverhaltens oder eintretenden Ausfällen
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll im Falle unzureichenden Nominalverhaltens und/oder eintretenden Ausfällen einen sicheren Degradationsmodus und -übergänge durchführen sowie die Manöverplanung in Längs- und Querrichtung bedarfsgerecht anpassen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L1.280000OpSaReq
L1.28-OpSaReq Erkennung des Betriebsmodus und Gewährleistung sicherer Betriebsmodusübergänge
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll den aktuellen Betriebsmodus erkennen und die Durchführung sicherer Betriebsmodusübergänge im Degradationsfall umsetzen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L1.290000OpSaReq
L1.29-OpSaReq Einnahme eines Zustands minimalen Risikos bzw. eines sicheren Zustands
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll im Falle schwerwiegender Systemausfälle die sichere Überführung in einen Zustand minimalen Risikos bzw. sicheren Zustand realisieren.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“*

• *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L1.300000OpSaReq
L1.30-OpSaReq Korrekte Ausführung der Trajektorienplanung und Regelung
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll die durchgeführte Trajektorienplanung und Regelung hinsichtlich der Längs- und Querführung korrekt umsetzen.
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L1.310000OpSaReq
L1.31-OpSaReq Kenntnis der aktuell erreichbaren Beschleunigungen und Verzögerungen
Das hochautomatisierte „L_1-Ego-Kraftfahrzeug_L“ soll die aktuell erreichbaren Beschleunigungen und Verzögerungen in Längs- und Querrichtung sowie um die vertikale Achse kennen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D

Tabelle C.31: Testfallspezifikation für das „L_1-Ego-Kraftfahrzeug_L“ als Testobjekt im Hinblick auf die Überprüfung der Spurhaltung bei konstanter Längsgeschwindigkeit.

<<Testfall>>	
ID: L1.10000TC	
L1.1-TC Spurhaltung bei konstanter Längsgeschwindigkeit	
Basisszenario	L1.1-SCEN „L_1-Freifahrt”
Testobjekt	„L_1-Ego-Kraftfahrzeug_L”
Wunschverhalten	• Manöver der hochautomatisierten Längsführung: ○ „Freifahrt“ unter Einhaltung der Geschwindigkeitsbegrenzung • Manöver der hochautomatisierten Querführung: ○ „Fahrstreifen Folgen“
Beschreibung	• Die Spurhaltung bzw. das Folgen des Ego-Fahrstreifens des „L_1-Ego-Kraftfahrzeugs_L“ wird auf einem geradlinigen und/oder gekrümmten „L_1-Fahrbahnbereich_L“ mit verschiedenen konstanten Längsgeschwindigkeiten getestet.
Vorbedingungen	• „L_1-Ego-Kraftfahrzeug_L“ fährt mit konstanter Längsgeschwindigkeit • „L_1-Ego-Kraftfahrzeug_L“ befindet sich innerhalb des Ego-Fahrstreifens
Testvektoren	• Testvektor initiale Längsgeschwindigkeit „L_1-Ego-Kraftfahrzeug_L“: $[11.11 \quad 19.44 \quad 27.78 \quad 36.11]\ \frac{m}{s}$ $\left([40 \quad 70 \quad 100 \quad 130]\ \frac{km}{h}\right)$ • Testvektor Fahrbahnradius: $[0 \quad 720]\ m$ • Testvektor Spurbreite: $[3.50]\ m$
Pass/Fail-Kriterien	• Gemäß den Manövern „Freifahrt“ und „Fahrstreifen Folgen“ hält das „L_1-Ego-Kraftfahrzeug_L“ hält die Spur ohne unzulässige Querabweichungen von $\pm 0.7\ m$.

Zugehörige zu erfüllende Betriebssicherheitsziele	• L1.1-OpSaG Vermeidung der Unterschreitung sicherer Abstände zu Hindernissen • L1.3-OpSaG Vermeidung eines unbeabsichtigten Verlassens des Ego-Fahrstreifens
UN-Regelung Nr. 157 Abschnitte 4.1, 4.1.1 [308]	• *„4.1. Beibehaltung der Fahrspur: 4.1.1. Mit der Prüfung ist nachzuweisen, dass das ALKS seine Spur nicht verlässt und über den gesamten Geschwindigkeitsbereich und bei unterschiedlichen Kurvenverläufen innerhalb seiner Systemgrenzen eine stabile Position innerhalb seiner Ego-Spur beibehält. […]“*

Tabelle C.32: Testfallspezifikation für das „L_1-Ego-Kraftfahrzeug_L“ als Testobjekt im Hinblick auf die Überprüfung der Kollisionsvermeidung mit vorausfahrendem „L_1-Verkehrsteilnehmer_L“ im Stillstand und Spurhaltung.

<<Testfall>>	
ID: L1.20000TC	
L1.2-TC Kollisionsvermeidung mit vorausfahrendem „L_1-Verkehrsteilnehmer_L“ im Stillstand und Spurhaltung	
Basisszenario	L1.2-SCEN „L_1-Annähern”
Testobjekt	„L_1-Ego-Kraftfahrzeug_L”
Beschreibung	• Die Kollisionsvermeidung des „L_1-Ego-Kraftfahrzeug_L“ mit dem auf der Ego-Fahrspur sich im Stillstand befindenden „L_1-Verkehrsteilnehmer_L“ wird auf einem geradlinigen und/oder gekrümmten „L_1-Fahrbahnbereich_L“ mit verschiedenen Längsgeschwindigkeiten getestet.
Vorbedingungen	• „L_1-Ego-Kraftfahrzeug_L“ fährt mit konstanter Längsgeschwindigkeit • „L_1-Ego-Kraftfahrzeug_L“ befindet sich innerhalb des Ego-Fahrstreifens • „L_1-Verkehrsteilnehmer_L“ befindet sich mit einem entsprechenden Relativabstand auf dem Ego-Fahrstreifen im Stillstand
Testvektoren	• Testvektor initialer Relativabstand: $[5\colon 5\colon 150]\ m$ • Testvektor initiale Längsgeschwindigkeit „L_1-Ego-Kraftfahrzeug_L“: $[11.11 \quad 19.44 \quad 27.78 \quad 36.11]\ \frac{m}{s}\ \left([40 \quad 70 \quad 100 \quad 130]\ \frac{km}{h}\right)$ • Testvektor initiale Längsgeschwindigkeit „L_1-Verkehrsteilnehmer_L“: $[0]\ \frac{m}{s}\ \left([0]\ \frac{km}{h}\right)$ • Testvektor Fahrbahnradius: $[0 \quad 720]\ m$ • Testvektor Spurbreite: $[3.50]\ m$
Pass/Fail-Kriterien	• Gemäß dem Manöver „Annähern“ kommt das „L_1-Ego-Kraftfahrzeug_L“ bis einschließlich des physikalischen Grenzbereichs vor dem „L_1-Verkehrsteilnehmer_L“ zum Stillstand und vermeidet eine Kollision. • Gemäß dem Manöver „Fahrstreifen Folgen“ hält das „L_1-Ego-Kraftfahrzeug_L“ die Spur ohne unzulässige Querabweichungen von $\pm 0.7\ m$.
Zugehörige zu erfüllende Betriebssicherheitsziele	• L1.1-OpSaG Vermeidung der Unterschreitung sicherer Abstände zu Hindernissen • L1.2-OpSaG Vermeidung der Unterschreitung sicherer Abstände zum „L_1-Verkehrsteilnehmer_L“ • L1.3-OpSaG Vermeidung eines unbeabsichtigten Verlassens des Ego-Fahrstreifens

UN-Regelung Nr. 157 Abschnitte 4.2, 4.2.1, 4.2.2 [308]	• *„4.2. Vermeidung einer Kollision mit einem Verkehrsteilnehmer […] 4.2.1. Bei der Prüfung ist nachzuweisen, dass das ALKS eine Kollision mit einem stehenden Fahrzeug […] bis zur angegebenen Höchstgeschwindigkeit des Systems vermeidet. 4.2.2. Diese Prüfung muss mindestens durchgeführt werden: a) Mit einem stehenden Fahrzeug; […] (h) Auf einem kurvenreichen Straßenabschnitt.“*

Tabelle C.33: Testfallspezifikation für das „L_1-Ego-Kraftfahrzeug_L“ als Testobjekt im Hinblick auf die Überprüfung der Abstandshaltung zum vorausfahrenden „L_1-Verkehrsteilnehmer_L“ und Spurhaltung.

<<Testfall>>	
ID: L1.30000TC	
L1.3-TC Abstandshaltung zu vorausfahrendem „L_1-Verkehrsteilnehmer_L“ und Spurhaltung	
Basisszenario	L1.3-SCEN „L_1-Abstandshaltung”
Testobjekt	„L_1-Ego-Kraftfahrzeug_L”
Beschreibung	• Die Abstandshaltung des „L_1-Ego-Kraftfahrzeug_L“ und das Folgen eines sich auf der Ego-Fahrspur befindenden „L_1-Verkehrsteilnehmers_L“ wird auf einem geradlinigen und/oder gekrümmten „L_1-Fahrbahnbereich_L“ mit verschiedenen Längsgeschwindigkeiten getestet.
Vorbedingungen	• „L_1-Ego-Kraftfahrzeug_L“ fährt mit konstanter Längsgeschwindigkeit • „L_1-Ego-Kraftfahrzeug_L“ befindet sich innerhalb des Ego-Fahrstreifens • „L_1-Verkehrsteilnehmer_L“ befindet sich mit einem entsprechenden Relativabstand auf dem Ego-Fahrstreifen und fährt mit konstanter Längsgeschwindigkeit
Testvektoren	• Testvektor initialer Relativabstand: $[5{:}\,5{:}\,150]\ m$ • Testvektor initiale Längsgeschwindigkeit „L_1-Ego-Kraftfahrzeug_L“: $[11.11 \quad 19.44 \quad 27.78 \quad 36.11]\ \frac{m}{s}\ \left([40 \quad 70 \quad 100 \quad 130]\ \frac{km}{h}\right)$ • Testvektor initiale Längsgeschwindigkeit „L_1-Verkehrsteilnehmer_L“: $[0{:}\,1.39{:}\,36.11]\ \frac{m}{s}\ \left([0{:}\,5{:}\,130]\ \frac{km}{h}\right)$ • Testvektor Längsbeschleunigung „L_1-Verkehrsteilnehmer_L“: $[0]\ \frac{m}{s^2}$ • Testvektor Längsverzögerung „L_1-Verkehrsteilnehmer_L“: $[0]\ \frac{m}{s^2}$ • Testvektor Fahrbahnradius: $[0 \quad 720]\ m$ • Testvektor Spurbreite: $[3.50]\ m$
Pass/Fail-Kriterien	• Gemäß dem Manöver Abstandshaltung hält das „L_1-Ego-Kraftfahrzeug_L“ bis einschließlich des physikalischen Grenzbereichs einen sicheren Mindestabstand zum „L_1-Verkehrsteilnehmer_L“ ein und folgt diesem. • Gemäß dem Manöver „Fahrstreifen Folgen“ hält das „L_1-Ego-Kraftfahrzeug_L“ die Spur ohne unzulässige Querabweichungen von $0.7\ m$.
Zugehörige zu erfüllende Betriebssicherheitsziele	• L1.1-OpSaG Vermeidung der Unterschreitung sicherer Abstände zu Hindernissen • L1.2-OpSaG Vermeidung der Unterschreitung sicherer Abstände zum „L_1-Verkehrsteilnehmer_L“

	• L1.3-OpSaG Vermeidung eines unbeabsichtigten Verlassens des Ego-Fahrstreifens
UN-Regelung Nr. 157 Abschnitte 4.3, 4.3.1, 4.3.2 [308]	• *„4.3. Abstandshaltung zum vorausfahrenden Fahrzeug: 4.3.1. Mit der Prüfung ist nachzuweisen, dass das ALKS in der Lage ist, den erforderlichen Sicherheitsabstand zu einem vorausfahrenden Fahrzeug einzuhalten und wiederherzustellen und eine Kollision mit einem vorausfahrenden Fahrzeug, das bis zu seiner maximalen Verzögerung abbremst, zu vermeiden. 4.3.2. Diese Prüfung ist mindestens wie folgt durchzuführen: a) Über den gesamten Geschwindigkeitsbereich des ALKS. […] (d) Für gerade und gekrümmte Straßenabschnitte. (f) Bei einer Verzögerung des führenden Fahrzeugs von mindestens 6 $\frac{m}{s^2}$ mittlere Vollverzögerung bis zum Stillstand.“*

Tabelle C.34: Testfallspezifikation für das „L_1-Ego-Kraftfahrzeug_L“ als Testobjekt im Hinblick auf die Überprüfung der Abstandshaltung zu einscherendem „L_1-Verkehrsteilnehmer_L“ und Spurhaltung.

<<Testfall>>	
ID: L1.40000TC	
L1.4-TC Abstandshaltung zu einscherendem Verkehrsteilnehmer und Spurhaltung	
Basisszenario	L1.1-SCEN „L_1-Freifahrt“ und L1.3-SCEN „L_1-Abstandshaltung“
Testobjekt	„L_1-Ego-Kraftfahrzeug_L”
Beschreibung	• Die Abstandshaltung des „L_1-Ego-Kraftfahrzeugs_L“ und das Folgen eines von der linken Nachbarspur auf die Ego-Fahrspur einscherenden „L_1-Verkehrsteilnehmers_L“ wird auf einem geradlinigen und/oder gekrümmten „L_1-Fahrbahnbereich_L“ mit verschiedenen Längsgeschwindigkeiten getestet.
Vorbedingungen	• „L_1-Ego-Kraftfahrzeug_L“ fährt mit konstanter Längsgeschwindigkeit • „L_1-Ego-Kraftfahrzeug_L“ befindet sich innerhalb des Ego-Fahrstreifens • „L_1-Verkehrsteilnehmer_L“ befindet sich mit einem entsprechenden Relativabstand auf der linken Nachbarspur und fährt mit konstanter Längsgeschwindigkeit
Testvektoren	• Testvektor initialer Relativabstand: $[5{:}\,5{:}\,150]\ m$ • Testvektor initiale Längsgeschwindigkeit „L_1-Ego-Kraftfahrzeug_L“: $[11.11 \quad 19.44 \quad 27.78 \quad 36.11]\ \frac{m}{s}$ $\left([40 \quad 70 \quad 100 \quad 130]\ \frac{km}{h}\right)$ • Testvektor initiale Längsgeschwindigkeit „L_1-Verkehrsteilnehmer_L“: $[0{:}\,1.39{:}\,36.11]\ \frac{m}{s}$ $\left([0{:}\,5{:}\,130]\ \frac{km}{h}\right)$ • Testvektor Längsbeschleunigung „L_1-Verkehrsteilnehmer_L“: $[0]\ \frac{m}{s^2}$ • Testvektor Längsverzögerung „L_1-Verkehrsteilnehmer_L“: $[0]\ \frac{m}{s^2}$ • Testvektor Fahrbahnradius: $[0 \quad 720]\ m$ • Testvektor Spurbreite: $[3.50]\ m$
Pass/Fail-Kriterien	• Gemäß dem Manöver „Abstandshaltung“ hält das „L_1-Ego-Kraftfahrzeug_L“ bis einschließlich des physikalischen Grenzbereichs einen sicheren Mindestabstand zum „L_1-Verkehrsteilnehmer_L“ ein und folgt diesem.

	• Gemäß dem Manöver „Fahrstreifen Folgen“ hält das „L_1-Ego-Kraftfahrzeug_L“ die Spur ohne unzulässige Querabweichungen von $\pm 0.7\ m$.
Zugehörige zu erfüllende Betriebssicherheitsziele	• L1.1-OpSaG Vermeidung der Unterschreitung sicherer Abstände zu Hindernissen • L1.2-OpSaG Vermeidung der Unterschreitung sicherer Abstände zum „L_1-Verkehrsteilnehmer_L“ • L1.3-OpSaG Vermeidung eines unbeabsichtigten Verlassens des Ego-Fahrstreifens
UN-Regelung Nr. 157 Abschnitte 4.4, 4.4.1, 4.3.2 [308]	• *„4.4. Fahrspurwechsel eines anderen Fahrzeugs in die Ego-Fahrspur: 4.4.1. Die Prüfung soll zeigen, dass das ALKS-Fahrzeug in der Lage ist, eine Kollision mit einem Fahrzeug, das in die Fahrspur des ALKS-Fahrzeugs einschert, bis zu einer bestimmten Kritikalität des Einschermanövers zu vermeiden. […] 4.4.3. Bei dieser Prüfung sind mindestens die nachstehenden Bedingungen zu berücksichtigen: (a) für unterschiedliche TTC-, Abstands- und Relativgeschwindigkeitswerte des Einschermanövers, wobei sowohl Einscherszenarien, bei denen ein Zusammenstoß vermieden werden kann, als auch solche, bei denen ein Zusammenstoß nicht vermieden werden kann, abgedeckt werden; (b) für einscherende Fahrzeuge, die mit konstanter Längsgeschwindigkeit fahren und dabei beschleunigen oder abbremsen;“*

C.2 Ergänzende Artefakte des Entwurfs- und Verifikationszyklus gemäß der Konzeptphase

C.2.1 Artefakte der Item Definition respektive der Spezifikation und des Designs gemäß der Konzeptphase

Tabelle C.35: An das System „L_2-Fahrzeugführung_L“ gestellte Betriebssicherheitsanforderungen im Sinne von funktionalen L_2-Systemfähigkeiten.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L2.10000OpSaReq
L2.1-OpSaReq Wahrnehmung und Erkennung relevanter statischer und dynamischer Objekte
Das Element „L_2-Fahrzeugführung_L“ soll das Attribut „L_2-Regionen/Staaten_L“, die Attribute „L_2-Fahrbahntyp_L“, „L_2-Fahrbahngeometrie_L“, „L_2-Fahrbahnspezifikation_L“ sowie „L_2-Fahrbahnoberfläche_L“ sowie die Attribute des „L_1-Verkehrsteilnehmers_L“ wahrnehmen, klassifizieren und deren Bedeutung verstehen.
Relevante Eingangsschnittstellen: • *„Zonenbedingungen“* • *„Fahrbahnbereichsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
ASIL D
ID: L2.20000OpSaReq

L2.2-OpSaReq Wahrnehmung und Erkennung der Umgebungsbedingungen
Das Element „L_2-Fahrzeugführung_L“ soll die Attribute „L_2-Bewölkung_L“ und „L_2-NatürlicheAusleuchtung_L“ wahrnehmen, klassifizieren und deren Bedeutung verstehen.
Relevante Eingangsschnittstellen: • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“*
ASIL D
ID: L2.30000OpSaReq
L2.3-OpSaReq Prädiktion des zukünftigen Verhaltens relevanter statischer und dynamischer Objekte
Das Element „L_2-Fahrzeugführung_L“ soll situationsbedingte Vorhersagen des zukünftigen Verhaltens der dem „L_1-Fahrbahnbereich_L“ untergeordneten Attribute „L_2-Fahrbahngeometrie_L“, „L_2-Fahrbahnspezifikation_L“ sowie „L_2-Fahrbahnoberfläche_L“ und insbesondere des „L_1-Verkehrsteilnehmers_L“ treffen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
ASIL D
ID: L2.40000OpSaReq
L2.4-OpSaReq Erstellung einer kollisionsfreien und gesetzeskonformen Trajektorienplanung und Regelung in Längs- und Querrichtung
Das Element „L_2-Fahrzeugführung_L“ soll eine kollisionsfreie (soweit wie praktikabel möglich) und gesetzeskonforme Trajektorienplanung und Regelung in Längs- und Querrichtung durchführen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“*
Relevante Ausgangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D
ID: L2.50000OpSaReq
L2.5-OpSaReq Trajektorienplanung und Regelung unter Berücksichtigung von Unsicherheiten
Das Element „L_2-Fahrzeugführung_L“ soll die Trajektorienplanung und Regelung unter Berücksichtigung von Unsicherheiten der Wahrnehmung der Attribute „L_2-Fahrbahngeometrie_L“, „L_2-Fahrbahnspezifikation_L“ und „L_2-Fahrbahnoberfläche_L“ sowie dem Attribut „L_2-Wind_L“ als auch der eigenen Leistungsfähigkeit durchführen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“* • *„ChassisInformation“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
Relevante Ausgangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D
ID: L2.60000OpSaReq

L2.6-OpSaReq Folgenminderung bei unvermeidlichen Kollisionen
Das Element „L_2-Fahrzeugführung_L“ soll bei einer unvermeidlichen Kollision deren Folgen soweit wie praktikabel minimieren.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“* • *„ChassisInformation“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
Relevante Ausgangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D
ID: L2.70000OpSaReq
L2.7-OpSaReq Überwachung des Ego-Zustands und der Erreichung des beabsichtigten Nominalverhaltens
Das Element „L_2-Fahrzeugführung_L“ soll den Ego-Zustand im Sinne der Leistungsfähigkeit bzgl. des aktuell erreichbaren Sensorsichtbereichs als auch der Reaktionszeit auf wahrgenommene statische und dynamische Attribute „L_2-Fahrbahngeometrie_L“, „L_2-Fahrbahnspezifikation_L“, „L_2-Fahrbahnoberfläche_L“ sowie „L_2-Wind_L“ überwachen und feststellen, wenn das beabsichtigte Nominalverhalten nicht erreicht werden kann.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“* • *„ChassisInformation“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
Relevante Ausgangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D
ID: L2.80000OpSaReq
L2.8-OpSaReq Degradation im Falle unzureichenden Nominalverhaltens oder eintretenden Ausfällen
Das Element „L_2-Fahrzeugführung_L“ soll im Falle unzureichenden Nominalverhaltens und/oder eintretenden Ausfällen einen sicheren Degradationsmodus und -übergänge durchführen sowie die Manöverplanung in Längs- und Querrichtung bedarfsgerecht anpassen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“* • *„ChassisInformation“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
Relevante Ausgangsschnittstellen:

• *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D
ID: L2.90000OpSaReq
L2.9-OpSaReq Erkennung des Betriebsmodus und Gewährleistung sicherer Betriebsmodusübergänge
Das Element „L_2-Fahrzeugführung_L“ soll den aktuellen Betriebsmodus erkennen und die Durchführung sicherer Betriebsmodusübergänge im eigenen Degradationsfall oder im Falle der Degradation der Elemente „L_2-EnergieUndAntrieb_L“ und „L_2-Chassis_L“ umsetzen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“* • *„ChassisInformation“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
Relevante Ausgangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D
ID: L2.100000OpSaReq
L2.10-OpSaReq Einnahme eines Zustands minimalen Risikos bzw. eines sicheren Zustands
Das Element „L_2-Fahrzeugführung_L“ soll im Falle schwerwiegender Systemausfälle seiner selbst oder der Elemente „L_2-EnergieUndAntrieb_L“ und „L_2-Chassis_L“ die sichere Überführung in einen Zustand minimalen Risikos bzw. sicheren Zustand einleiten.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“* • *„ChassisInformation“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
Relevante Ausgangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D

Tabelle C.36: An das System „L_2-EnergieUndAntrieb_L“ gestellte Betriebssicherheitsanforderungen im Sinne von funktionalen L_2-Systemfähigkeiten.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L2.110000OpSaReq
L2.11-OpSaReq Korrekte Ausführung der Trajektorienplanung und Regelung in Längsrichtung
Das Element „L_2-EnergieUndAntrieb_L“ soll die durchgeführte Trajektorienplanung und Regelung hinsichtlich der Längsführung korrekt umsetzen.

Relevante Eingangsschnittstellen: • *„Beschleunigungsbefehl“*
Relevante Ausgangsschnittstellen: • *„Antriebsmoment“*
ASIL D
ID: L2.120000OpSaReq
L2.12-OpSaReq Bereitstellung einer sicheren Energieversorgung
Das Element „L_2-EnergieUndAntrieb_L“ soll eine sichere Energieversorgung für die Elemente „L_2-Fahrzeugführung_L“ sowie „L_2-Chassis_L“ bereitstellen.
Relevante Ausgangsschnittstellen: • *„ElektrischeEnergieversorgung“*
ASIL D
ID: L2.130000OpSaReq
L2.13-OpSaReq Degradation im Falle unzureichenden Nominalverhaltens oder eintretenden Ausfällen
Das Element „L_2-EnergieUndAntrieb_L“ soll im Falle unzureichenden Nominalverhaltens und/oder eintretenden Ausfällen einen sicheren Degradationsmodus und -übergänge durchführen und die Elemente „L_2-Fahrzeugführung_L“ sowie „L_2-Chassis_L“ diesbezüglich informieren.
Relevante Ausgangsschnittstellen: • *„Antriebsmoment“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
ASIL D

Tabelle C.37: An das System „L_2-Chassis_L“ gestellte Betriebssicherheitsanforderungen im Sinne von funktionalen L_2-Systemfähigkeiten.

Übergeordneter Anforderungstyp: <<Funktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L2.140000OpSaReq
L2.14-OpSaReq Korrekte Ausführung der Trajektorienplanung und Regelung in Längsrichtung
Das Element „L_2-Chassis_L“ soll die durchgeführte Trajektorienplanung und Regelung hinsichtlich der Längsführung korrekt umsetzen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Antriebsmoment“* • *„Verzögerungsbefehl“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L2.150000OpSaReq
L2.15-OpSaReq Kenntnis der aktuell erreichbaren Beschleunigungen und Verzögerungen in Längsrichtung
Das Element „L_2-Chassis_L“ soll die aktuell erreichbaren Beschleunigungen und Verzögerungen in Längsrichtung unter Berücksichtigung der Attribute „L_2-Fahrbahngeometrie_L“, „L_2-Fahrbahnspezifikation_L“ und „L_2-Fahrbahnoberfläche_L“ kennen und dem Element „L_2-Fahrzeugführung_L“ bereitstellen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“*
Relevante Ausgangsschnittstellen: • *„Antriebsmoment“*

• *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
ASIL D
ID: L2.160000OpSaReq
L2.16-OpSaReq Korrekte Ausführung der Trajektorienplanung und Regelung in Querrichtung
Das Element „L_2-Chassis_L“ soll die durchgeführte Trajektorienplanung und Regelung hinsichtlich der Querführung korrekt umsetzen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Lenkbefehl“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“*
ASIL D
ID: L2.170000OpSaReq
L2.17-OpSaReq Kenntnis der aktuell erreichbaren Beschleunigungen in Querrichtung
Das Element „L_2-Chassis_L“ soll die aktuell erreichbaren Beschleunigungen in Querrichtung sowie um die vertikale Achse unter Berücksichtigung der Attribute „L_2-Fahrbahngeometrie_L“, „L_2-Fahrbahnspezifikation_L“ und „L_2-Fahrbahnoberfläche_L“ als auch dem Attribut „L_2-Wind_L“ kennen und dem Element „L_2-Fahrzeugführung_L“ bereitstellen.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“*
Relevante Ausgangsschnittstellen: • *„EnergieUndAntriebInformationen“*
ASIL D
ID: L2.180000OpSaReq
L2.18-OpSaReq Degradation im Falle unzureichenden Nominalverhaltens oder eintretenden Ausfällen
Das Element „L_2-Chassis_L“ soll im Falle unzureichenden Nominalverhaltens und/oder eintretenden Ausfällen einen sicheren Degradationsmodus und -übergänge durchführen und die Elemente „L_2-Fahrzeugführung_L“ sowie „L_2-EnergieUndAntrieb_L“ diesbezüglich informieren.
Relevante Eingangsschnittstellen: • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„ElektrischeEnergieversorgung“* • *„Antriebsmoment“*
Relevante Ausgangsschnittstellen: • *„EnergieUndAntriebInformationen“*
ASIL D

Tabelle C.38: Erhobene Betriebssicherheitsanforderungen im Hinblick auf die Gesamtreaktions- und -ausführungszeit sowie der Kommunikationslatenz der L_2-Systeme.

Übergeordneter Anforderungstyp: <<Nichtfunktionale Anforderung>>
Spezifischer Anforderungstyp: <<Betriebssicherheitsanforderung>>
ID: L2.190000OpSaReq
L2.19-OpSaReq Gesamtausführungszeit und Kommunikationslatenz des Systems „L_2-Fahrzeugführung_L“ im Hinblick auf die Umsetzung der Funktion „L_2-RegleAutomatisierte…F“
Die Gesamtausführungszeit des Systems „L_2-Fahrzeugführung_L“ im Hinblick auf dessen Verhaltensrepräsentation „L_2-RegleAutomatisierteFahraufgabe_LB“ soll $0.59\ \mathrm{s}\ (590\ \mathrm{ms})$ *nicht überschreiten. Des*

Weiteren soll die auf die Übermittlung der Ausgangsgrößen bezogene Kommunikationslatenz nicht mehr als $0.01\ \mathrm{s}\ (10\ \mathrm{ms})$ *betragen.*
Relevante Eingangsschnittstellen: • *„Zonenbedingungen“* • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“* • *„Ausleuchtungsbedingungen“* • *„VorausfahrenderVerkehrsteilnehmerdynamik“* • *„ChassisInformation“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
Relevante Ausgangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Beschleunigungsbefehl“*
ASIL D
ID: L2.200000OpSaReq
L2.20-OpSaReq Gesamtausführungszeit und Kommunikationslatenz des Systems „L_2-EnergieUndAntrieb_L“ im Hinblick auf die Umsetzung der Funktion „L_2-StelleNotwendige…F“
Die Gesamtausführungszeit des Systems „L_2-EnergieUndAntrieb_L“ im Hinblick auf dessen Verhaltensrepräsentation „L_2-StelleNotwendigeLeistungsUndEnergieformenBereit_LB“ soll $0.19\ \mathrm{s}\ (190\ \mathrm{ms})$ *nicht überschreiten. Des Weiteren soll die auf die Übermittlung der Ausgangsgrößen bezogene Kommunikationslatenz nicht mehr als* $0.01\ \mathrm{s}\ (10\ \mathrm{ms})$ *betragen.*
Relevante Eingangsschnittstellen: • *„Beschleunigungsbefehl“*
Relevante Ausgangsschnittstellen: • *„Antriebsmoment“* • *„ElektrischeEnergieversorgung“* • *„EnergieUndAntriebInformationen“*
ASIL D
ID: L2.210000OpSaReq
L2.21-OpSaReq Gesamtausführungszeit und Kommunikationslatenz des Systems „L_2-Chassis_L“ im Hinblick auf die Umsetzung der Funktion „L_2-BefördereP assagiere…F“
Die Gesamtausführungszeit des Systems „L_2-Chassis_L“ im Hinblick auf dessen Verhaltensrepräsentation „L_2-BefördereP assagiereUndRealisiereFahrzeugbewegung_LB“ soll $0.19\ s\ (190\ ms)$ *nicht überschreiten. Des Weiteren soll die auf die Übermittlung der Ausgangsgrößen bezogene Kommunikationslatenz nicht mehr als* $0.01\ s\ (10\ ms)$ *betragen.*
Relevante Eingangsschnittstellen: • *„Lenkbefehl“* • *„Verzögerungsbefehl“* • *„Antriebsmoment“* • *„ElektrischeEnergieversorgung“* • *„Fahrbahnbereichsbedingungen“* • *„Wetterbedingungen“*
Relevante Ausgangsschnittstellen: • *„EgoKraftfahrzeugdynamik“* • *„ChassisInformation“*
ASIL D

Tabelle C.39: Testfallspezifikation im Hinblick auf die Gesamtausführungszeit des Systems „L_2-Fahrzeugführung_L“ sowie dessen Kommunikationslatenz.

<<Testfall>>	
ID: L2.10000TC	
L2.1-TC Sprungantwort und Übermittlung der Ausgangsgrößen des Systems „L_2-Fahrzeugführung_L“	
Testobjekt	• „L_2-Fahrzeugführung_L”
Beschreibung	• Die Gesamtausführungszeit des Systems „L_2-Fahrzeugführung_L“ einschließlich der Kommunikationslatenz wird getestet.
Vorbedingungen	• Das System „L_2-Fahrzeugführung_L“ liefert die konstanten Ausgangsgrößen „Beschleunigungsbefehl“ bzw. „Verzögerungsbefehl“ und befindet sich in einer dynamischen Ruhelage.
Testvektoren/Sprungfunktionen	• Sprungfunktionsanregung „Beschleunigungsbefehl“: $H(t) = \begin{cases} [0]\frac{m}{s^2} & (t < 0\ s) \\ [1]\frac{m}{s^2} & (t \geq 0\ s) \end{cases}$ • Sprungfunktionsanregung „Verzögerungsbefehl“: $H(t) = \begin{cases} [0]\frac{m}{s^2} & (t < 0\ s) \\ [-1]\frac{m}{s^2} & (t \geq 0\ s) \end{cases}$
Pass/Fail-Kriterien	• Das System „L_2-Fahrzeugführung_L“ überträgt die im Anschluss eines eingangsseitigen Sollwertsprungs zu generierenden Ausgangsgrößen „Beschleunigungsbefehl“ bzw. „Verzögerungsbefehl“ innerhalb der Gesamtreaktions- und -ausführungszeit von $0.59\ \mathrm{s}\ (590\ \mathrm{ms})$ und hält die maximale Kommunikationslatenz von $0.01\ \mathrm{s}\ (10\ \mathrm{ms})$ ein.
Zugehörige zu erfüllende Betriebssicherheitsanforderungen	• L2.19-OpSaReq Gesamtausführungszeit und Kommunikationslatenz „L_2-Fahrzeugführung_L“

Tabelle C.40: Testfallspezifikation im Hinblick auf die Gesamtausführungszeit des Systems „L_2-EnergieUndAntrieb_L“ sowie dessen Kommunikationslatenz.

<<Testfall>>	
ID: L2.20000TC	
L2.2-TC Sprungantwort und Übermittlung der Ausgangsgrößen des Systems „L_2-EnergieUndAntrieb_L“	
Testobjekt	• „L_2-EnergieUndAntrieb_L“
Beschreibung	• Die Gesamtausführungszeit des Systems „L_2-EnergieUndAntrieb_L“ einschließlich der Kommunikationslatenz wird getestet.
Vorbedingungen	• Das System „L_2-EnergieUndAntrieb_L“ liefert die konstante Ausgangsgröße „Antriebsmoment“ als Informationsbestandteil der Schnittstelle „EnergieUndAntriebsInformationen“ und befindet sich in einer dynamischen Ruhelage.
Testvektoren/Sprungfunktionen	• Sprungfunktionsanregung „Antriebsmoment“: $H(t) = \begin{cases} [0]\ Nm\ (t < 0\ s) \\ [600]\ Nm\ (t \geq 0\ s) \end{cases}$
Pass/Fail-Kriterien	• Das System „L_2-EnergieUndAntrieb_L“ überträgt die im Anschluss eines eingangsseitigen Sollwertsprungs zu generierenden Ausgangsgröße „Antriebsmoment“ als Informationsbestandteil der

	Schnittstelle „EnergieUndAntriebsInformationen“ innerhalb Gesamtreaktions- und -ausführungszeit von $0.19\ \mathrm{s}\ (190\ \mathrm{ms})$ und hält die maximale Kommunikationslatenz von $0.01\ \mathrm{s}\ (10\ \mathrm{ms})$ ein.
Zugehörige zu erfüllende Betriebssicherheitsanforderungen	• L2.20-OpSaReq Gesamtausführungszeit und Kommunikationslatenz „L_2-EnergieUndAntrieb_L“

Tabelle C.41: Testfallspezifikation im Hinblick auf die Gesamtausführungszeit des Systems „L_2-Chassis_L“ sowie dessen Kommunikationslatenz.

<<Testfall>>	
ID: L2.30000TC	
L2.3-TC Sprungantwort und Übermittlung der Ausgangsgrößen des Systems „L_2-Chassis_L“	
Testobjekt	• „L_2-Chassis_L“
Beschreibung	• Die Gesamtausführungszeit des Systems „L_2-Chassis_L“ einschließlich der Kommunikationslatenz wird getestet.
Vorbedingungen	• Das System „L_2-Chassis_L“ liefert die konstante Ausgangsgrößen „Chassisbeschleunigung“ bzw. „Chassisverzögerung“ als Informationsbestandteile der Schnittstelle „ChassisInformationen“ und befindet sich in einer dynamischen Ruhelage.
Testvektoren/Sprungfunktionen	• Sprungfunktionsanregung „Chassisbeschleunigung“: $H(t) = \begin{cases} [0]\ \frac{m}{s^2}\ (t < 0\ s) \\ [1]\ \frac{m}{s^2}\ (t \geq 0\ s) \end{cases}$ • Sprungfunktionsanregung „Chassisverzögerung“: $H(t) = \begin{cases} [0]\ \frac{m}{s^2}\ (t < 0\ s) \\ [-1]\ \frac{m}{s^2}\ (t \geq 0\ s) \end{cases}$
Pass/Fail-Kriterien	• Das System „L_2-Chassis_L“ überträgt die im Anschluss eines eingangsseitigen Sollwertsprungs zu generierenden Ausgangsgrößen „Chassisbeschleunigung“ bzw. „Chassisverzögerung“ als Informationsbestandteile der Schnittstelle „ChassisInformationen“ innerhalb Gesamtreaktions- und -ausführungszeit von $0.19\ \mathrm{s}\ (190\ \mathrm{ms})$ und hält die maximale Kommunikationslatenz von $0.01\ \mathrm{s}\ (10\ \mathrm{ms})$ ein.
Zugehörige zu erfüllende Betriebssicherheitsanforderungen	• L2.21-OpSaReq Gesamtausführungszeit und Kommunikationslatenz „L_2-Chassis_L“

C.3 Ergänzende Artefakte des virtuellen Integrations- und Validierungszyklus

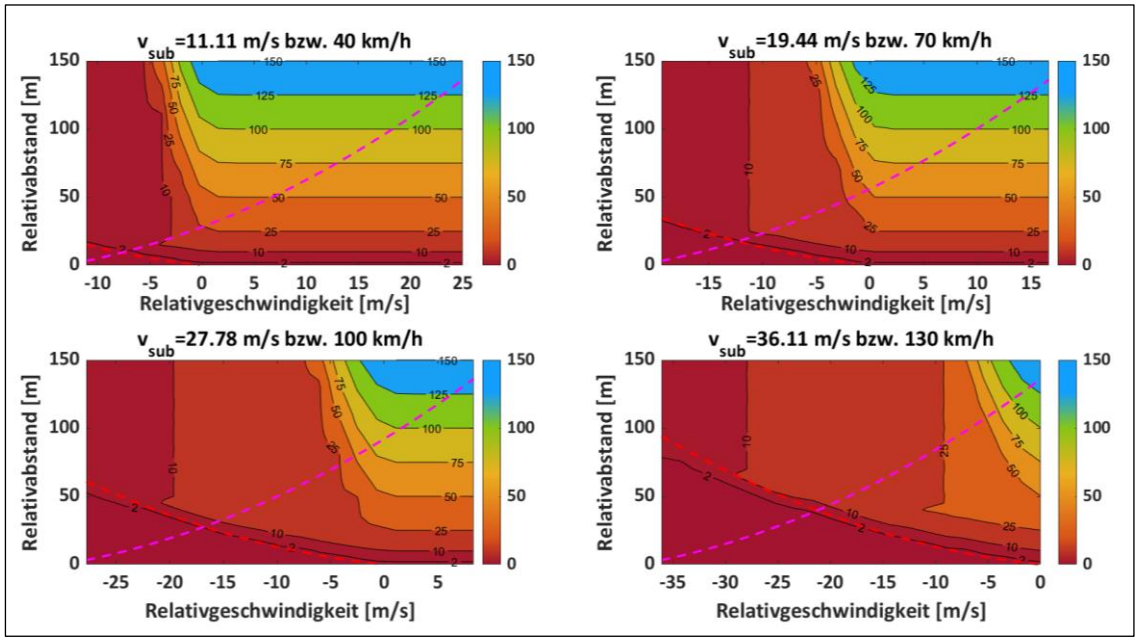


Abbildung C.1: Minimaler Relativabstand im Hinblick auf die Durchführung der Testfälle L1.2-TC, L1.3-TC und L1.4-TC auf L_1-Granularitätsebene. Das Ganze erfolgt unter Berücksichtigung des L_1/L_2-Simulationsmodells einschließlich des analytisch dynamischen Verhaltens der beteiligten L_2-Systeme.

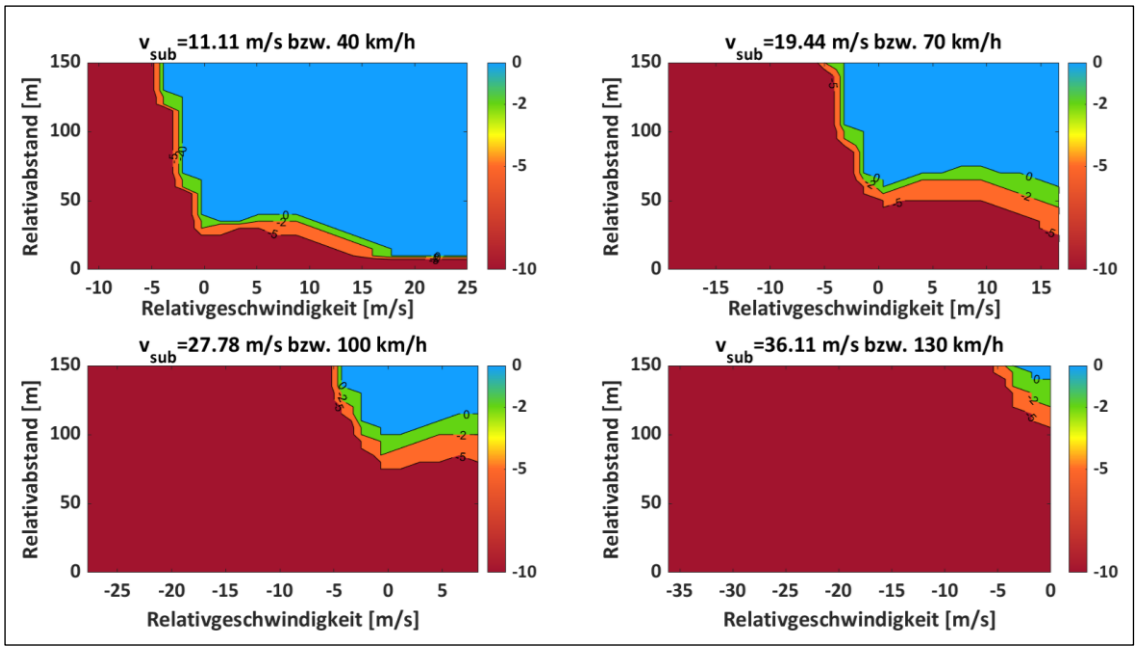


Abbildung C.2: Maximale Ego-Verzögerung im Hinblick auf die Durchführung der Testfälle L1.2-TC, L1.3-TC und L1.4-TC auf L_1-Granularitätsebene. Das Ganze erfolgt unter Berücksichtigung des L_1/L_2-Simulationsmodells einschließlich des analytisch dynamischen Verhaltens der beteiligten L_2-Systeme.

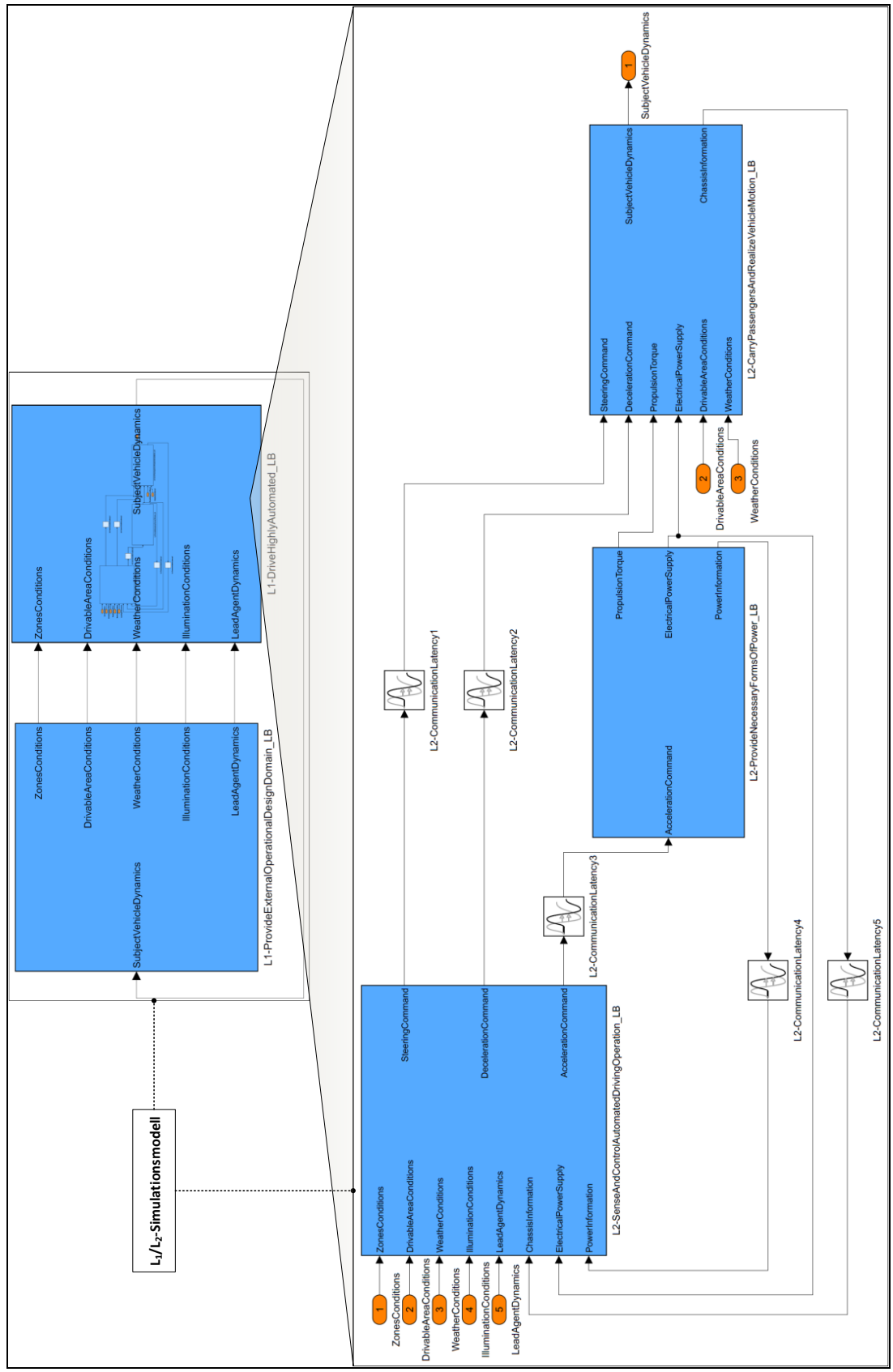


Abbildung C.3: Übergang L_1-Simulationsmodell zu L_1/L_2-Simulationsmodell.

D Abkürzungen und Symbole

D.1 Abkürzungen

ABS	Antiblockiersystem
ACC	Adaptive Cruise Control
ADL	Architecture Description Language
AI	Artificial Intelligence
ALARP	As Low As Reasonably Practicable
ALKS	Automated Lane Keeping System
ANSI	American National Standards Institute
ARG	Argument
ASIL	Automotive Safety Integrity Level
ASMP	Assumption
ASPICE	Automotive Software Process Improvement and Capability Determination
AUTOSAR	AUTomotive Open System Architecture
B	Verhaltensvariable
BASt	Bundesanstalt für Straßenwesen
BCOND	Boundary Condition
C	Controllability
CAE	Computer-Aided Engineering
CAN	Controller Area Network
CAPS	Controller, Actuator, Process, Sensor
CD	Continuous Deployment
CI	Continuous Integration
CL	Claim
CMMI	Capability Maturity Model Integration
CSTR	Constraint

CT	Continuous Test
CUBE	Compositional Unified System-Based Engineering
DECN	Decision
DevOps	Development & Operations
E	Exposure
E/E	Elektrisch/Elektronisch
E/E/EP	Elektrisch/Elektronisch/Elektronisch Programmierbar
EG-Richtlinien	Europäische Gemeinschafts-Richtlinien
EMV	Elektromagnetische Verträglichkeit
EPS	Electric Power Steering
ESP	Elektronisches Stabilitätsprogramm
F	Funktionale Architekturvariable
FB	Funktional spezifische Verhaltensvariable
FeV	Fahrerlaubnisverordnung
FF	Forschungsfrage
FFG-L	Fahrfreigabe-Level
FMEA	Failure Mode and Effects Analysis
FMI	Functional Mock-Up Interface
FMU	Functional Mock-Up Unit
FReq	Functional Requirement
FRAM	Functional Resonance Analysis Method
FuSa	Functional Safety
FSC	Functional Safety Concept
FSReq	Functional Safety Requirement
FTA	Fault Tree Analysis
FTTI	Fault Tolerant Time Interval
F-VP	Functional Viewpoint

FZI	Forschungszentrum Informatik
FZV	Fahrzeug-Zulassungsverordnung
GG	Grundgesetz
GIDAS	German In-Depth Accident Study
Gl	Gleichung
HARA	Hazard and Risk Analysis
HAZOP	Hazard and Operability Study
HB	Hazardous Behaviour
HE	Hazardous Event
HF	Herausforderung
HiL	Hardware-in-the-Loop
HMI	Human-Machine Interface
HSI	Hardware-Software Interface
HWCR	Hardware Component Release
I-HiL	Integrations-HiL
INCOSE	International Council on Systems Engineering
IoT	Internet of Things
IR	Item Release
IT	Informationstechnik
ITIV	Institut für Technik der Informationsverarbeitung
JSTF	Justification
K-HiL	Komponenten-HiL
KI	Künstliche Intelligenz
KIT	Karlsruher Institut für Technologie
KM	Konfigurationsmanagement
KPI	Key Performance Indicator
L	Logische Architekturvariable

LB	Logisch spezifische Verhaltensvariable
LIN	Local Interconnect Network
LKAS	Lane Keeping Assistance System
L_n	Layer bzw. Level der Granularitätsebene
LSCEN	Loss Scenario
L-VP	Logical Viewpoint
MATLAB	MATrix LABoratory
MiL	Model-in-the-Loop
ML	Maturity Level
MOST	Media Oriented Systems Transport
NFReq	Non-functional Requirement
NHTSA	National Highway Traffic Safety Administration
ODD	Operational Design Domain
ODDR	Operational Design Domain Release
ODE	Ordinary Differential Equation
OEDR	Object and Event Detection Reaction
OEM	Original Equipment Manufacturer
OpSa	Operational Safety
OpSaG	Operational Safety Goal
OpSaReq	Operational Safety Requirement
OTA	Over-the-Air
P-Anteil	Proportionalanteil
PEGASUS	Project for the Establishment of Generally Accepted quality criteria, tools and methods as well as Scenarios and Situations
PEP	Produktentstehungsprozess
PiL	Processor-in-the-Loop
PL	Plan
PM	Projektmanagement

PMT	Prozesse, Methoden und Tools
QM	Qualitätsmanagement
QS	Qualitätssicherung
QUASAR	Quality Assessment of Software-Intensive System Architectures
R	Release
RAA	Richtlinien für die Anlage von Autobahnen
Req-VP	Requirements Viewpoint
RGA-MS	Reifegradabsicherungsmeilenstein
S	Severity
SAE	Society of Automotive Engineers
SceML	Scenario Modeling Language
SCEN	Scenario
SE	Systemerstellung
SET	Simulative dEvelopment and Testing
SIFAD	Safety Integrity Framework for Automated Driving
SiL	Software-in-the-Loop
SOCA	System Co-Design for Open Context Analysis
SOP	Start of Production
SotiF	Safety Of The Intended Functionality
SSR	Subsystem Release
STPA	System-Theoretic Process Analysis
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
StVZO	Straßenverkehrszulassungsordnung
SUT	System Under Test
SWCR	Software Component Release
SWUR	Software Unit Release

T	Technische Architekturvariable
TB	Technisch spezifische Verhaltensvariable
TC	Test Case
TSC	Technical Safety Concept
TSReq	Technical Safety Requirement
TTC	Time To Collision
TÜV	Technischer Überwachungsverein
T-VP	Technical Viewpoint
UC	Use Case
UL	Underwriters Laboratories
UNECE	United Nations Economic Commission for Europe
V&V	Verifikation und Validierung
V2I	Vehicle-to-Infrastructure-Communication
V2V	Vehicle-to-Vehicle-Communication
V2X	Vehicle-to-Everything-Communication
VDA	Verband der Automobilindustrie e.V.
ViL	Vehicle-in-the-Loop
VP	Viewpoint
VVM	VV-Methoden
WP	Work Product
X-Domain	Cross-Domain
XiL	X-in-the-Loop
XML	Extensible Markup Language
XP	Extreme Programming
XT	Extreme Tailoring

D.2 Formelzeichen und Symbole

Allgemein

x	Skalar x
$\boldsymbol{x}$	Vektor x
$\boldsymbol{X}$	Matrix X
$\dot{}$	Zeitliche Ableitung
$\lvert \quad \rvert$	Betrag eines Skalars
$\lVert \quad \rVert$	Norm eines Vektors (hier: euklidische Norm)
∇	Gradient einer Funktion

Indize

$(...)_n$	Index des Layers bzw. des Levels der Granularitätsebene

Koordinaten- und Achsensysteme

X, Y, Z	Horizontiertes Achsensystem
X_E, Y_E, Z_E	Ortsfestes Koordinatensystem

Griechische Symbole

α	Schräglaufwinkel (Reifenschräglaufwinkel)
α_f, α_r	Schräglaufwinkel der Vorder- bzw. Hinterachse
β	Fahrzeugschwimmwinkel
δ	Radlenkwinkel
δ_f, δ_r	Radlenkwinkel der Vorder- bzw. Hinterachse
δ_f^*	Sollradlenkwinkel der Vorderachse
η_{tot}	Gesamtwirkungsgrad Antriebsstrang
θ	Fahrzeugnickwinkel
κ	Krümmung des Bahnverlaufs
κ^*	Krümmung des Sollbahnverlaufs
κ_{max}^*	Maximale Krümmung des Sollbahnverlaufs
μ	Allgemeiner Kraftschlussbeiwert
ρ	Luftdichte
φ	Fahrzeugwankwinkel
ψ	Fahrzeuggierwinkel
$\dot{\psi}$	Gierwinkelrate
$\dot{\psi}_{nec}$	Notwendige Gier- bzw. Kurswinkelrate
$\dot{\psi}_{req}$	Gier- bzw. Kurswinkelratenbefehl
$\ddot{\psi}$	Gierwinkelbeschleunigung
ψ^*	Richtungswinkel der Sollbahn
ψ_e	Kurswinkelabweichung

Lateinische Symbole

A	Fahrzone
A_n	Sichtbereichsbezogene Fahrzone
A_f	Querspantfläche Fahrzeugfront
A_0	Maximalsichtbereichsfahrzone
A_1	Annäherungsfahrzone
A_2	Zielabstandsfahrzone
A_3	Komfortable Abbremsungsfahrzone
A_4	Harte Abbremsungsfahrzone
A_5	Notfallabbremsungsfahrzone
a	Fahrzeugbeschleunigung
a_X	Längsbeschleunigung in Längsrichtung des horizontierten Koordinatensystems
a_{X_E}	Beschleunigung in Längsrichtung des ortsfesten Koordinatensystems
$a_{X,accel,max}$	Absolute Maximalbeschleunigung in Längsrichtung
$a_{X,accel,req}$	Beschleunigungsbefehl in Längsrichtung
$a_{X,decel,max}$	Absolute Maximalverzögerung in Längsrichtung
$a_{X,decel,req}$	Verzögerungsbefehl in Längsrichtung
$a_{X,decel,n}$	Zonenabhängige Maximalverzögerung in Längsrichtung
a_Y	Querbeschleunigung in Querrichtung des horizontierten Koordinatensystems
a_{Y_E}	Beschleunigung in Querrichtung des ortsfesten Koordinatensystems
$a_{Y,max}$	Absolute Maximalbeschleunigung in Querrichtung
$a_{Y,nec}$	Notwendige Querbeschleunigung bzgl. eines gekrümmten Sollbahnverlaufs
$a_{i,n}$	Disjunkte Alternative
a_{rel}	Relativbeschleunigung
B	Sollbahn
$B_{X/Y/\alpha/\kappa}$	Steifigkeitsfaktor des Magic-Formula-Reifenmodells (Längs/Quer)
$C_{X/Y/\alpha/\kappa}$	Formfaktor des Magic-Formula-Reifenmodells (Längs/Quer)
c_R	Rollwiderstandsbeiwert
c_{WX}	Luftwiderstandsbeiwert in Längsrichtung
c_{test}	Testfallkombinatorik
$D_{X/Y/\alpha/\kappa}$	Maximalwert des Magic-Formula-Reifenmodells (Längs/Quer)
D_n	Dimension gemäß SOCA-Methode
d_{rel}	Relativabstand
d_{rel}^*	Sollrelativabstand
$d_{rel,min}^*$	Minimaler Sollrelativabstand
$d_{rel,phys,min}$	Minimaler Relativabstand, um eine Kollision noch vermeiden zu können
d_{sight}	Maximale Sichtweite (maschinelle Wahrnehmung) des Ego-Kraftfahrzeugs
$E_{X/Y/\alpha/\kappa}$	Krümmungsfaktor des Magic-Formula-Reifenmodells (Längs/Quer)
e	Exponentialfunktion
F_{RX}	Rollwiderstandskraft in Längsrichtung
F_{WX}	Luftwiderstandskraft in Längsrichtung
F_{XT}	Reifenumfangskraft (Reifenlängskraft)
$F_{XT,f}, F_{XT,r}$	Reifenumfangskraft der Vorder- bzw. Hinterachse
$F_{XT,max}$	Maximale Reifenumfangskraft
F_{YT}	Reifenseitenkraft (Reifenquerkraft)
$F_{YT,f}, F_{YT,r}$	Reifenseitenkraft der Vorder- bzw. Hinterachse

$F_{YT,max}$	Maximale Reifenseitenkraft
F_{ZT}	Reifennormalkraft
$F_{ZT,f}, F_{ZT,r}$	Reifennormalkraft der Vorder- bzw. Hinterachse
f	Funktion
$G(s)$	Übertragungsfunktion
$G_{M_B}(s)$	Übertragungsfunktion des Bremsmoments
$G_{M_{BS}}(s)$	Übertragungsfunktion Bremse
$G_{M_D}(s)$	Übertragungsfunktion des Antriebsmoments
$G_{M_M}(s)$	Übertragungsfunktion Antrieb
$G_{PT_1}(s)$	Übertragungsfunktion PT_1-Glied
$G_{PT_1T_t}(s)$	Übertragungsfunktion PT_1T_t-Glied
$G_{T_t}(s)$	Übertragungsfunktion T_t-Glied
$G_{a_{X,accel,req},a_{X,decel,req}}(s)$	Übertragungsfunktion der Beschleunigungs- sowie Verzögerungsbefehle
$G_{a_Y}(s)$	Übertragungsfunktion der Querbeschleunigung
$G_{a_{Y,req},\psi,req}(s)$	Übertragungsfunktion des Querbeschleunigungs- und Gierratenbefehls
$G_{\delta_f}(s)$	Übertragungsfunktion Lenkung
$G_{\dot{\psi}}(s)$	Übertragungsfunktion der Gierrate
g	Erdbeschleunigung
$H(t)$	Sprungfunktion bzw. Heaviside-Funktion
i_{tot}	Gesamtübersetzungsverhältnis des Antriebsstrangs
J_Z	Fahrzeugmassenträgheitsmoment um Fahrzeughochachse
K	Proportionalparameter PT_1-Glied
$K_{M_{BS}}$	Proportionalparameter Bremse
K_{M_M}	Proportionalparameter Antrieb
K_{a_Y}	Proportionalparameter der Querbeschleunigung
$K_{a_{Y,req},\psi,req}$	Proportionalparameter des Querbeschleunigungs- und Gierratenbefehls
K_{δ_f}	Verstärkungsfaktor bzw. Proportionalparameter Lenkung
$K_{\dot{\psi}}$	Proportionalparameter der Gierrate
l	Radstand
l_f, l_r	Radstand Fahrzeugschwerpunkt zur Vorder- bzw. Hinterachse
M	Fahrzeuggesamtmoment
M_B	Bremsmoment
M_{BS}	Bremsmoment Bremse
M_D	Antriebsmoment
M_M	E-Maschinenmoment Antrieb
m	Fahrzeuggesamtmasse
n	Anzahl
$\boldsymbol{n}^*$	Normalvektor
P_K	Kartesisches Produkt
$\boldsymbol{p}_E$	Hinterachsmittelpunkt
$\boldsymbol{p}_E^*$	Referenzpunkt Sollbahn
R_P	Bahnradius
r_{dyn}	Dynamischer Rollradius
s	Komplexe Laplace-Variable im Frequenz- bzw. Bildbereich
$\boldsymbol{s}_e^T$	Differenzvektor

s_i	Komplexe Polstelle
s_{Xe}	Tangentialer Abstand bzw. Längsabweichung
s_{Ye}	Orthogonaler Abstand bzw. Querabweichung
T	Zeitkonstante PT_1-Glied
T_{M_B}	Ausführungszeitkonstante des Bremsmoments
$T_{M_{BS}}$	Ausführungszeitkonstante Bremse
T_{M_D}	Ausführungszeitkonstante des Antriebsmoments
T_{M_M}	Ausführungszeitkonstante Antrieb
T_{a_Y}	Ausführungszeitkonstante der Querbeschleunigung
$T_{a_{Y,req,\psi,req}}$	Ausführungszeitkonstante der Querbeschleunigungs- sowie Gierratenbefehle
T_{δ_f}	Ausführungszeitkonstante Lenkung
$T_{\dot{\psi}}$	Ausführungszeitkonstante der Gierrate
T_t	Totzeit
$T_{t,L_{2,com}}$	Kommunikationstotzeit der L_2-Systeme
$T_{t,M_{BS}}$	Ausführungstotzeit der Bremse
T_{t,M_M}	Ausführungstotzeit des Antriebs
$T_{t,a_{X,accel,decel,req}}$	Ausführungstotzeit der Beschleunigungs- sowie Verzögerungsbefehle
$T_{t,a_{Y,req,\psi,req}}$	Ausführungstotzeit der Querbeschleunigungs- sowie Gierratenbefehle
T_{t,δ_f}	Ausführungstotzeit der Lenkung
TTC	Time To Collision
TTC_{min}	Minimale Time To Collision
t	Zeit
$\boldsymbol{t}^*$	Tangentialvektor
t_c	Testabdeckung
t_{gap}	Zeitlücke
t_n	Fahrzonenabhängige Zeitkonstante
t_{react}	Ego-Reaktionszeit
t_{1-5}	Vektor der fahrzonenabhängigen Abstandszeitkonstante
u	Eingangsgröße
v	Fahrzeuggeschwindigkeit
v_{lead}	Geschwindigkeit des vorausfahrenden Verkehrsteilnehmers
v_{rel}	Relativgeschwindigkeit
v_{sub}	Ego-Kraftfahrzeuggeschwindigkeit
$v_{sub,max}$	Maximale Ego-Kraftfahrzeuggeschwindigkeit
$v_{T,f}$, $v_{T,r}$	Reifengeschwindigkeit der Vorder- bzw. Hinterachse
v_X	Längsgeschwindigkeit
v_X^*	Wunsch- bzw. Sollgeschwindigkeit in Längsrichtung
v_Y	Quergeschwindigkeit
x	Zustandsgröße
y	Ausgangsgröße

Implementierte Wertebereiche der Parameter

Parameter	**Wert**	**Einheit**
η_{tot}	0.95	$[-]$

κ^*_{max}	0.0014	$\left[\frac{1}{m}\right]$
μ	1.00	$[-]$
ρ	1.20	$\left[\frac{kg}{m^3}\right]$
A_f	2.20	$[m^2]$
$a_{X,accel,max}$	2.00	$\left[\frac{m}{s^2}\right]$
$a_{X,decel,max}$	-10.00	$\left[\frac{m}{s^2}\right]$
$a_{Y,max}$	± 4.00	$\left[\frac{m}{s^2}\right]$
$C_{X,\kappa,f}$, $C_{X,\kappa,r}$	1.50, 1.50	$[-]$
$C_{Y,\alpha,f}$, $C_{Y,\alpha,r}$	1.30, 1.30	$[-]$
c_R	0.015	$[-]$
c_{WX}	0.29	$[-]$
$d^*_{rel,min}$	2.00	$[m]$
d_{sight}	150.00	$[m]$
$E_{X,\kappa,f}$, $E_{X,\kappa,r}$	$-1.00, -1.00$	$[-]$
$E_{Y,\alpha,f}$, $E_{Y,\alpha,r}$	$-1.00, -1.00$	$[-]$
g	9.81	$\left[\frac{m}{s^2}\right]$
i_{tot}	8.28	$[-]$
J_Z	3400.00	$[kgm^2]$
$K_{M_{BS}}$	1.00	$[-]$
K_{M_M}	1.00	$[-]$
K_{a_Y}	1.00	$[-]$
$K_{a_{Y,req,\psi,req}}$	1.00	$[-]$
K_{δ_f}	1.00	$[-]$
$K_{\dot{\psi}}$	1.00	$[-]$
l	2.97	$[m]$
l_f, l_r	1.42, 1.55	$[m]$
m	2036.00	$[kg]$
r_{dyn}	0.30	$[m]$
T_{M_B}	0.20	$[s]$
$T_{M_{BS}}$	0.18	$[s]$
T_{M_D}	0.20	$[s]$
T_{M_M}	0.18	$[s]$
T_{a_Y}	0.08	$[s]$
$T_{a_{Y,req,\psi,req}}$	0.12	$[s]$
T_{δ_f}	0.10	$[s]$
$T_{\dot{\psi}}$	0.08	$[s]$
$T_{t,L_{2,com}}$	0.01	$[s]$
$T_{t,M_{BS}}$	0.02	$[s]$
T_{t,M_M}	0.02	$[s]$
$T_{t,a_{X,accel,decel,req}}$	0.60	$[s]$
$T_{t,a_{Y,req,\psi,req}}$	0.60	$[s]$
T_{t,δ_f}	0.02	$[s]$

TTC_{min}	2.00	$[s]$
t_{react}	0.80	$[s]$
$v_{sub,max}$	36.11	$\left[\frac{m}{s}\right]$