Entwicklung von Tests für die Freigabe des Dynamikmoduls als Teil der Absicherung eines automatisierten Fahrzeugs

Bachelorthesis Nr. 1364/20

Bearbeiter: Johannes Krause | 2683629
Betreuer: Björn Klamann, M. Sc.

TECHNISCHE UNIVERSITÄT DARMSTADT

FZD FAHRZEUGTECHNIK TU DARMSTADT

Johannes Krause
Matrikelnummer: 2683629
Studiengang: Bachelor Wirtschaftsingenieurwesen – technische Fachrichtung Maschinenbau

Bachelorthesis Nr. 1364/20
Thema: Entwicklung von Tests für die Freigabe des Dynamikmoduls als Teil der Absicherung eines automatisierten Fahrzeugs

Eingereicht: 05.03.2021

Technische Universität Darmstadt
Fachgebiet Fahrzeugtechnik
Prof. Dr. rer. nat. Hermann Winner
Otto-Berndt-Straße 2
64287 Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

Bachelorthesis Nr. 1364/20 im Studiengang Wirtschaftsingenieurwesen Maschinenbau (12 CP)

von Johannes Krause

Beginn:	05.10.2020
Zwischenkolloquium:	01.12.2020
Ende:	05.03.2021

Thema: **Entwicklung von Tests für die Freigabe des Dynamikmoduls als Teil der Absicherung eines automatisierten Fahrzeugs**

Topic: ***Development of tests for the release of the dynamic module as part of the validation of an automated vehicle***

Fachgebiet Fahrzeugtechnik

FZD

Prof. Dr. rer. nat. Hermann Winner

Otto-Berndt-Straße 2
64287 Darmstadt

Bearbeiter:

Björn Klamann, M. Sc.
Tel. +49 6151 16 – 24235
Fax +49 6151 16 – 24205
bjoern.klamann@tu-darmstadt.de
www.fahrzeugtechnik-darmstadt.de

Datum
03.10.20

Am Fachgebiet Fahrzeugtechnik der TU Darmstadt (FZD) wird für das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt UNICAR*agil* in Zusammenarbeit mit mehreren deutschen Universitäten an modularen und diensteorientierten automatisierten Fahrzeugen geforscht. Der Fokus liegt dabei auf der Vermeidung technologischer Altlasten und darauf, diese durch neue, disruptive Konzepte zu ersetzen. Das zu entwickelnde Fahrzeug verfügt über vier elektrische Radnabenantriebe, die eine radindividuelle Vorgabe von Lenkwinkeln und Antriebs- bzw. Bremsmomenten ermöglichen. Antrieb, Lenkung und Bremse werden dabei als eigenständiges Dynamikmodul entwickelt. Im Rahmen von UNICARagil wird ein Verfahren entwickelt, um solche Module unabhängig von anderen Komponenten individuell abzusichern.

Zur Entwicklung eines modularen Absicherungskonzepts sollen sowohl Modultests als auch Fahrzeugtests für eine Freigabe der Dynamikmodule beschrieben und durchgeführt werden.
Ziel dieser Arbeit ist es, Risiken durch den Betrieb der Dynamikmodule zu identifizieren und anhand dessen Tests zur Freigabe der Dynamikmodule abzuleiten. Hierzu ist zuerst eine ausführliche Beschreibung und die Aufstellung einer Anforderungsliste anzufertigen. Mit deren Hilfe werden Risiken und daraufhin herausfordernde Tests zur Freigabe der Dynamikmodule ermittelt. Die Durchführung der Tests erfolgt durch Projektpartner.

Als Ergebnisse der Bachelorthesis sind nachzuweisen:

1. Der grundlegende technische und funktionale Aufbau der Software und Hardware des Dynamikmoduls mit der Beschreibung der Schnittstellen und der Spezifikation von Anforderungen sind in einer Modul Definition dargestellt.

CP	Dauer Zwischenkolloq (Vortrag / gesamt)	Dauer Abschlusskolloq (Vortrag / gesamt)
< 18	5 - 7 / 15 min	15 / 45 min
> 18	10 / 20 min	20 / 60 min

2. Mögliche Testaufbauten für die Durchführung von Tests für die Absicherung sind beschrieben.
3. Risiken des Dynamikmoduls sind anhand der zusammengetragenen Informationen methodisch identifiziert.
4. Allgemeine Bestehens- bzw. Versagenskriterien für die Freigabe der Dynamikmodule sind ermittelt.
5. Konkrete Testfälle sind anhand der identifizierten Risiken für die verschiedenen Testaufbauten definiert und priorisiert.
6. Erste durchgeführte Tests sind anhand der Testkriterien bewertet.
7. Potentielle Unzulänglichkeiten in den Modultests im Vergleich zu den Systemtests sind identifiziert und beschrieben.
8. Die Methodik und Ergebnisse des Vorgehens sowie vorhandene Unzulänglichkeiten sind dokumentiert und diskutiert.

Schwerpunkte der Bewertung:

- Methodik des Vorgehens
- Vollständigkeit
- Belastbarkeit der Argumentation
- Nachvollziehbarkeit

Die Arbeit bleibt Eigentum des Fachgebiets. Auf das Merkblatt des Fachgebiets wird hingewiesen.

Prof. Dr. rer. nat. Hermann Winner

Björn Klamann, M. Sc.
(Betreuer)

Erklärung

Erklärung zur Abschlussarbeit gemäß § 23 Abs. 7 APB der TU Darmstadt

Hiermit versichere ich, Johannes Krause, die vorliegende Bachelor-Thesis ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Mir ist bekannt, dass im Falle eines Plagiats (§38 Abs.2 APB) ein Täuschungsversuch vorliegt, der dazu führt, dass die Arbeit mit 5,0 bewertet und damit ein Prüfungsversuch verbraucht wird. Abschlussarbeiten dürfen nur einmal wiederholt werden.

Bei der abgegebenen Thesis stimmen die schriftliche und die zur Archivierung eingereichte elektronische Fassung überein.

English translation for information purposes only:

Thesis Statement pursuant to § 23 paragraph 7 of APB TU Darmstadt

I herewith formally declare that I, Johannes Krause, have written the submitted thesis independently. I did not use any outside support except for the quoted literature and other sources mentioned in the paper. I clearly marked and separately listed all of the literature and all of the other sources, which I employed when producing this academic work, either literally or in content. This thesis has not been handed in or published before in the same or similar form.

I am aware, that in case of an attempt at deception based on plagiarism (§38 Abs. 2 APB), the thesis would be graded with 5,0 and counted as one failed examination attempt. The thesis may only be repeated once.

In the submitted thesis, the written copies and the electronic version for archiving are identical in content.

Matrikelnummer: 2683629

Datum / Date: 05.03.2021

Unterschrift / Signature:

Zusammenfassung

Automatisierte Fahrfunktionen entwickeln sich kontinuierlich weiter. Maßgeblich für deren Zulassung ist ein belastbarer Nachweis ihrer Sicherheit. Mit zunehmendem technischem Fortschritt der Fahrzeugautomatisierung, wird es schwieriger und komplexer diese Funktionen für einen Einsatz im Straßenverkehr abzusichern. So stoßen auch in der Entwicklung hochautomatisierter Fahrzeuge gängige Absicherungsansätze an Grenzen. Das Forschungsprojekt UNICAR*agil* verfolgt daher unter anderem im Umgang mit funktionaler Fahrzeugsicherheit neue Herangehensweisen. Mit diesem Hintergrund liefert diese Arbeit eine Methodik für eine Testentwicklung aus modularer Perspektive. Der hierfür untersuchte Gegenstand ist das Dynamikmodul des Forschungsprojekts, welches in allen Varianten der entwickelten Konzeptfahrzeuge für die Bereitstellung der Fahrfunktionen sorgen wird. Dabei wird das übergeordnete Ziel verfolgt, Aufwand und Komplexität der Absicherung durch modulares Testen zu reduzieren.

Zunächst wird dafür die Modulumgebung, das Konzeptfahrzeug, beschrieben. Anschließend erfolgt eine Beschreibung des Dynamikmoduls mit seinem Aufbau und seinen Funktionen. Schnittstellen, funktionale Zusammenhänge aber auch vorgesehene Einsatzbedingungen werden dabei erklärt. Im nächsten Schritt werden für eine Testentwicklung relevante Grundbegriffe und deren Bedeutung erläutert. Um eine breite Informationsgrundlage aus testbaren Anforderungen zu entwickeln, wird daraufhin eine kombinierte Arbeitsweise für eine Risikoanalyse abgeleitet. Den Rahmen hierfür liefern Ansätze und analytische Methoden der ISO 26262, welche durch die Perspektive der *Systems Theoretic Process Analysis* (STPA) ergänzt werden. Mit kombinierten Analysen werden innere Zusammenhänge und mögliche Gefährdungen des Dynamikmoduls unabhängig von äußeren Einsatzbedingungen und Betriebssituationen erfasst. Funktionsbereiche und Beziehungen innerhalb des Dynamikmoduls werden dafür durch jeweilige Methoden unterschiedlich untersucht. Zunächst liefert die *Failure Mode and Effects Analysis* (FMEA) mögliche Gefährdungen aus einzelnen Ausfällen innerhalb des Moduls. Wechselwirkungen und Zusammenhänge einzelner Ausfälle werden durch Fehlerbaumanalysen ergründet. Zuletzt lassen sich anhand eines Kontrollflussdiagramms der STPA Gefährdungen durch unsichere Wechselwirkungen ermitteln. Gemeinsam mit bekannten Anforderungen aus existierenden Unterlagen werden die Ergebnisse der Analysen in einer Anforderungsliste gesammelt. Mit Angaben über ihre Bedeutung in der funktionalen Modularchitektur, lassen sich diese anschließend sortieren und einzelnen Testumgebungen priorisiert zuordnen. Unter Berücksichtigung bekannter Möglichkeiten wurde dafür ein einfaches Testkonzept erstellt, mit dem einzelne Testfälle entsprechend ihrer Eigenschaften und Priorität den verfügbaren Testumgebungen zugeordnet wurden.

Mit der beschriebenen Vorgehensweise und gewonnenen Ergebnissen lassen sich auch in der Zukunft des Forschungsprojekts Testfälle entwickeln. Grafische und tabellarische Ergebnisse durchgeführter Analysen liefern dafür Informationsgrundlagen über die Struktur des Dynamikmoduls. Auch lassen sich die gesammelten Anforderungen strukturiert neuen Testumgebungen zuweisen. Darüber hinaus bietet die Arbeit mit ihrem Aufbau Orientierung für andere Testentwicklungen und liefert zuletzt mögliche Anknüpfungspunkte für weitere Arbeiten über modulares Testen.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABS	Antiblockiersystem
ASIL	*Automotive Safety Integrity Level*
ASOA	*automotive service-oriented architecture,* Softwarearchitektur im Projekt UNICAR*agil*
C	*Programmiersprache, keine Abkürzung*
CAN	*Controller Area Network,* (Bussystem)
DIN	Deutsches Institut für Normung
E/E	Elektrisch/ Elektronisch
EN	Europäische Norm
ETA	*Event Tree Analysis,* Ereignisbaumanalyse
FMEA	*Failure Mode and Effects Analysis,* Fehlermöglichkeits- & Einflussanalyse
FMECA	*Failure Modes, Effects and Criticality Analysis,* Abwandlung der FMEA
FMEDA	*Failure Modes, Effects and Diagnostics Analysis,* Abwandlung der FMEA
FTA	*Fault Tree Analysis,* Fehlerbaumanalyse
FZD	Fahrzeugtechnik Darmstadt
HARA	*Hazard Analysis and Risk Assessment,* Gefährdungs- und Risikoanalyse
HAZOP	*Hazard and Operability [Analysis],* deutsch auch: PAAG-Verfahren
ID	Identifikator
ISO	Internationale Ordnung für Normung (von griechisch: *isos,* deutsch: gleich)
IT	Informationstechnik
MoSCoW	Akronym: *must*, *should*, *could* und *won't*
MTBF	*Mean Time Between Failures,* mittlere Betriebsdauer zwischen Ausfällen
MTTF	*Mean Time To Failure* Mittlere Betriebsdauer bis zu einem Erstausfall
NASA	*National Aeronautics and Space Administration,* Bundesbehörde der Vereinigten Staaten von Amerika
PAS	*Publicly Available Specification,* öffentlich verfügbare Spezifikation

QM	Qualitätsmanagement
RWTH	Rheinisch-Westfälische Technische Hochschule [Aachen]
SAE	*Society of Automotive Engineers*, Verband der Automobilingenieure
SFMEA	*Software-FMEA,* Abwandlung der FMEA
SG#-DM	Sicherheitsziel Nummer #, des Dynamikmoduls
STPA	*Systems Theoretic Process Analysis,* Systemtheoretische Prozessanalyse
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TU	Technische Universität

Physikalische Größen und Zwischengrößen

V	Volt	Einheit der elektrischen Spannung
°	Grad	Winkeleinheit
mm	Millimeter	Längeneinheit
s	Sekunde	Zeiteinheit
km/h	Kilometer pro Stunde	gängige Einheit für die Fahrzeuggeschwindigkeit
m/s^2	Meter pro (Sekunde)²	Einheit der Beschleunigung
%	Prozent	Gradiente, Höhenzunahme pro Streckenverlauf
Nm	Newtonmeter	Einheit für Drehmoment
kW	Kilowatt	Einheit der Leistung
“	Zoll	Längeneinheit, üblich für Kreisdurchmesser
kg	Kilogramm	Einheit der Masse
1/min	hier: Umdrehungen pro 60s	Einheit für Rotationsgeschwindigkeit

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

1.1 Motivation

Die meisten Unfälle im Straßenverkehr werden derzeit durch menschliche Fahrer verursacht. So ist es eine naheliegende Annahme, dass ein Teil der heutigen Unfälle durch Fahrzeugautomatisierung verhindert werden könnte.[1] Deshalb treibt die "Vision Zero", eine Welt ohne Verkehrstote und Verletzte, die Entwicklungen in der Fahrzeugautomation voran. Mit zunehmendem Einsatz vernetzter Systeme besteht das Potential, diesem Ausblick Stück für Stück näher zu kommen.[2a]

Seit dem ersten Einsatz des Antiblockiersystems in einem Serienfahrzeug 1978 konnten sich viele weitere Fahrassistenzsysteme etablieren. Moderne elektronische Helfer unterstützen an unterschiedlichsten Stellen die allgemeine Fahrsicherheit und den Fahrkomfort. In kleinen aber deutlichen Schritten wird dem Fahrer dadurch Arbeit abgenommen.[3a] Setzt man die bisherigen Entwicklungen im Zusammenspiel mit der zunehmenden technischen Konnektivität gedanklich fort, bleibt es nur noch eine Frage der Zeit, bis Kraftfahrzeuge in der Lage sind autonom zu fahren.

Die computergesteuerte Mobilität hätte revolutionäre Auswirkungen auf diverse Industriezweige, unsere Städte und unsere alltäglichen Gewohnheiten.[3b] Sobald ihre Zuverlässigkeit, Langzeitqualität und Wirtschaftlichkeit hinreichend nachgewiesen ist, kann sie auch tatsächlich eingesetzt werden. Ansonsten kommt sie nur in vereinzelten Nischenbereichen eingeschränkt zur Anwendung.[4]

Erst wenn die Technologien des autonomen Fahrens in Serienfahrzeugen mit großer Stückzahl zum Einsatz kommen, sind sie in der Lage den Straßenverkehr grundlegend zu verändern. Die dafür notwendigen Freigaben erfolgen, wenn die technischen Systeme alle an sie gestellten Anforderungen hinreichend erfüllen. Grundlagen liefern dafür unter anderem diverse Normen und Gesetze, aber auch die Kundenbedürfnisse. Insbesondere relevant für autonome Fahrzeuge sind die Sicherheitsanforderungen für eine Typgenehmigung und erfüllbare Produkthaftung.[5] Darüber hinaus spielen auch ethische Fragestellungen in der Entwicklung der Fahrzeugautomation eine Rolle. Um Menschen vor Schäden zu schützen, wird für den Einsatz automatisierter Systeme grundsätzlich eine Verbesserung in der Risikobilanz aller Fahrzeuge verlangt. In einem Schadensfall mit einem autonomen Fahrzeug, kämen Grundsätze der Produkthaftung zur Anwendung. Somit sind Hersteller in der Pflicht, sogar ausgelieferte Wagen fortlaufend in einem zumutbaren Rahmen zu verbessern. Maßnahmen zur Vermeidung von Unfällen sind damit in vielen Bereichen der Entwicklung von Bedeutung.[2b]

---

[1] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 440.

[2] Jipp, M.; Schneider, L.: Fahrtests unter Realbedingungen (2020), a: S. VII; b: 5-9.

[3] Lalli, M.: Autonomes Fahren und die Zukunft (2020), a: S. 7–8; b: 8-9.

[4] Braess, H.-H.; Seiffert, U.: Vieweg Handbuch Kraftfahrzeugtechnik (2013), S. 44.

[5] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 440.

1.2 Problembeschreibung

Als grundlegende Annahme bezüglich funktionaler Systemsicherheit lässt sich sagen:

„Wenn alle erdenkbaren Fehler eines Systems beherrschbar sind, gilt das System als sicher."[6]

Um eine solche Sicherheit zu gewährleisten, erfolgt in der Automobilindustrie üblicherweise eine Absicherung durch Testfahrten mit menschlichen Fahrern. Besonderheit bei dem Einsatz automatisierter Fahrfunktionen ist allerdings die eingeschränkte oder fehlende Beaufsichtigung durch Menschen. Auch wenn zunehmend virtuelle Simulationsumgebungen zum Einsatz kommen, erfolgen abschließende Freigaben immer noch auf der Grundlage realer Fahrtests. Wenn die Verantwortung für Fahreraufgaben von technischen Systemen übernommen wird, nimmt der Aufwand für eine solche Absicherung mit abnehmender menschlicher Kontrolle zu. Folglich steht das Reaktionsverhalten dieser Systeme unter besonders genauer Beobachtung. Zusätzlich wird auch dem Degradationsverhalten mehr Bedeutung beigemessen. Der erweiterte Sicherheitsfokus, auch in einzelnen Komponenten, führt schlussendlich zu erhöhtem Absicherungsaufwand.[7a]

Besonders das städtische Umfeld setzt Fahrassistenzsysteme vor komplexe Szenarien. Eine große Menge variierender Faktoren wirkt hier beeinflussend.[8] So entstehen Herausforderungen aus situationsabhängigen Anforderungen und der unstrukturierten Natur eines Umfelds mit vielen möglichen Interaktionskombinationen. Auch das resultierende Fahrzeugverhalten lässt sich wegen komplexen Wechselwirkungen zwischen Systemkomponenten nur schwer vorhersagen.[9] Allein ein einfacher Fahrstreifenwechsel erzeugt unzählige Kombinationen von Einflussparametern. Abstände zu anderen Verkehrsteilnehmern, Geschwindigkeiten, Beschleunigungen, Kurvenkrümmung, Wetterbedingungen und weitere Einflüsse erlauben viele Variationen möglicher Betriebsszenarien. Diese alle zu testen würde sehr lange dauern.[7b] Darüber hinaus würden bauliche Veränderungen des Gesamtfahrzeugs immer wieder neue Sicherheitsvalidationen erfordern.[10]

Wie zuvor bemerkt, wird für eine Freigabe des autonomen Fahrens nicht nur eine dadurch reduzierte Unfallhäufigkeit vorausgesetzt. Zusätzlich wird ein gesellschaftlich annehmbares Verhältnis von den durch autonome Systeme zusätzlich erzeugten Risiken zu den dadurch vermiedenen Risiken gefordert.[11a] So liegt die Schlussfolgerung nahe, dass der Sicherheitsnachweis für eine Freigabe autonomer Fahrzeuge nach herkömmlichen Methoden mehrere Milliarden Testkilometer verlangen würde und damit ökonomisch nicht umsetzbar ist.[11b]

---

[6] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 119.

[7] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), a: S. 3–4; b: 4-5.

[8] Schuldt, F. et al.: Test Case Generation for DAS (2018), S. 149.

[9] Stellet, J. E. et al.: Validation of automated driving (2020), S. 64.

[10] Stolte, T. et al.: Safety Concepts for Automated Vehicles (2020), S. 1584.

[11] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 442; b: 457-458.

1.3 Lösungsansatz

Allgemein ist es bei der Arbeit mit komplexen Systemen ein gängiges Bestreben diese zu vereinfachen. Ansätze, wie das Reduzieren einzelner Elemente, die Definition von Akzeptanzbereichen statt Akzeptanzwerten, das Zerlegen in Einzelteile, Strukturieren von Problemen, aber auch das Einnehmen verschiedener Perspektiven wirken dabei unterstützend. Durch ein Beschränken auf einzelne Systemfunktionen können diese gezielter bearbeitet werden. Ist ein annehmbarer Wertebereich bekannt, vereinfacht sich dadurch die Bewertung quantitativer Größen. Einzelne Abschnitte eines komplexen Systems lassen sich strukturiert betrachten. Auch strukturiertes Vorgehen an sich schafft Klarheit. Zuletzt stellt das Einnehmen verschiedener Sichtweisen tieferes Verständnis und erhöhte Informationsqualität in Aussicht.[12] Das Forschungsprojekt UNICAR*agil* verfolgt in diesem Sinne einen modularen Ansatz. Wenn sich hier die Fahrzeugmodule hinreichend einzeln testen ließen, könnte man auf Tests am Gesamtfahrzeug verzichten. Zusätzlich würde sich die Anzahl relevanter Parameter in den einzelnen Tests verringern, was die allgemeine Komplexität des Testvorgehens reduzieren würde. Insofern sieht die Zielsetzung des Projekts vor, den bisherigen Umfang von Integrations- und Fahrzeugtests durch modulare Einzeltests abzudecken. Dafür werden Testkriterien und Testfälle auf modularer Ebene definiert.[13] Die einzelnen dafür durchgeführten Prozesse ließen sich besser verwalten, wodurch auch eine gewisse Flexibilität bei der Wahl der eingesetzten Methoden entstünde. Die Zuordnung von Risiken bleibt jedoch eine Herausforderung. Schließlich sind nicht alle Komponenten von einer jeweiligen Gefährdung gleichermaßen betroffen.[14]

1.4 Aufgabe

Diese Arbeit beschäftigt sich mit der Entwicklung von Tests für das Dynamikmodul, welches baugleich in allen Konzeptfahrzeugen des Forschungsprojekts zum Einsatz kommt. Nach einem Überblick über das Fahrzeugkonzept wird der Aufbau des Moduls technisch und funktional beschrieben. Sowohl Hardware als auch Softwarekomponenten werden mit ihren Schnittstellen und Anforderungen erläutert. Um daraus eine Informationsgrundlage für die Testentwicklung zu bestimmen, werden nach einer integrativen Methodik Gefährdungen und Risiken ermittelt. Risikobetrachtungen priorisieren und unterstützen die abschließende Ableitung von testbaren Anforderungen. Auch wenn im Rahmen dieser Arbeit keine Testdurchführung erfolgt, sind verfügbare Testaufbauten beschrieben und einbezogen. Eine abschließende Diskussion ergänzt das Vorgehen und bietet Anknüpfungspunkte für nachfolgende Untersuchungen und Testvorhaben.

[12] Dittes, F.-M.: Komplexität reduzieren (2012), S. 133–138.

[13] Woopen, T. et al.: UNICARagil - Disruptive Modular Architectures (2018), S. 22.

[14] Philipp, R. et al.: Decomposition of Automated Driving Systems (2020), S. 93.

2 Technische Rahmenbedingungen

Um alle weiteren Inhalte der Arbeit mit einem Bezug zu einem technischen System erfassen zu können, erfolgt in diesem Kapitel eine kurze Beschreibung des Forschungsprojekts UNICAR*agil* und der darin entwickelten Dynamikmodule. Vor allem auch für die erfolgte Testentwicklung liefert der folgende Abschnitt ein kontextuelles Verständnis. Nach einer kurzen Beschreibung des Forschungsprojekts wird dafür das Dynamikmodul mit seinen technischen Bereichen Radantrieb (1), Bremse (2), Lenkung (3) und Steuergerät (4) genauer erklärt. Zuletzt werden außerdem mögliche Situationen im Betrieb des Dynamikmoduls mit ihrer Bedeutung für die Testentwicklung genauer beschrieben.

2.1 Das Forschungsprojekt UNICAR*agil*

Das Forschungsprojekt UNICAR*agil* verfolgt einen disruptiven und modularen Ansatz bei der Entwicklung einer Architektur für automatisierte und elektrische Stadtfahrzeuge.[15a] Um die entstehenden Möglichkeiten zu demonstrieren, werden auf Basis der gemeinsamen Fahrzeugarchitektur vier verschiedene Prototypvarianten entwickelt. Als „autoTAXI“ entsteht ein vollautomatisiertes Taxi, das Passagiere per Smartphone-Bestellung bedient. Privat dient „autoELF“ dem familiären Bedarf, für Einkaufs- oder auch Schulfahrten. Mit dem „autoCARGO“ wird eine „mobile Packstation“ mit intelligenter Fördertechnologie für eine unabhängige Paketaufnahme und -ablieferung entwickelt. Zuletzt stellt das „autoSHUTTLE“ eine Fahrzeuglösung für die Beförderung kleiner Gruppen im öffentlichen Nahverkehr dar.[15b&16]

Damit umfasst das Projekt Themenbereiche der Fahrzeugtechnik, Elektrotechnik bis hin zu Computerwissenschaften. Bedeutende Kerngebiete sind Automatisierung, Sicherheit, Verifikation & Validierung und Modularisierung.[15c] Gemeinsam arbeiten daran die RWTH Aachen, TU Darmstadt, TU Braunschweig, das Karlsruher Institut für Technologie, die TU München, Universität Stuttgart und die Universität Ulm. Darüber hinaus beteiligen sich die Industrieunternehmen Atlatec GmbH, fly-Xdrive GmbH, iMAR Navigation GmbH, IPG Automotive GmbH, Schaeffler Technologies AG & Co. KG und Vires Simulationstechnologie GmbH.[15d]

Der gemeinsam verfolgte Architekturentwurf und die darin fehlende menschliche Rückfallebene schaffen neue Herausforderungen. Deswegen verfolgt das Projekt ein Sicherheitskonzept über bisherige Ansätze der ISO 26262 hinaus. Während dem Betrieb stehen alle Systemzustände unter dauerhafter Überwachung. So beobachtet sich das System selbst und bewertet seinen eigenen Zustand.[15e] Beispielsweise berücksichtigt die Routenplanung des Fahrzeugs auch die aktuell verfügbaren technischen Kapazitäten. Straßen, die das Fahrzeug nicht beherrscht, werden prinzipiell vermieden.[17] Kommt es zu einem Versagensfall, wird von dem Fahrzeug ein Übergang in einen sicheren Zustand gefordert. In schweren Fällen sorgt dann ein sicheres Anhalten für einen Fahrzeugstillstand bei der nächsten sicheren Gelegenheit.[15f] Da die menschliche Rückfallebene ab SAE Ebene 3 oder höher

[15] Woopen, T. et al.: UNICARagil - Disruptive Modular Architectures (2018), a: S. 665; b: S. 669; c: S.665; d: S.665; e: S. 668; f: 668.

[16] Unbekannte Autoren: Homepage des Projekts UNICARagil (2021).

[17] Reschka, A.: Sicherheitskonzept für autonome Fahrzeuge (2015), S. 501.

fehlt, wird an ihrer Stelle mit einer Rückfalltrajektorie gearbeitet. Stellt die Selbstwahrnehmung des Fahrzeugs einen Fehler fest wird auf diese Rückfallebene zurückgegriffen.[18a] Zusätzlich ist das Fahrzeug in Situationen mit eingeschränkter Funktion ausgehend von einem Kontrollzentrum fernsteuerbar. Aus dem Fahrzeugstillstand ist hierfür ein menschlicher Bediener in der Lage, mit Zugriff auf alle verfügbaren Sensordaten die Fahrzeugbewegungen vorzugeben.[18a] Sobald die Selbstwahrnehmungsfunktion des Fahrzeugs ein reguläres Fortsetzen des autonomen Betriebs erlaubt, darf die menschliche Leitwartenaufsicht die Kontrolle an das Fahrzeug zurückgeben.[18b]

Grundlage aller dafür notwendigen Softwarefunktionen legt eine sogenannte ASOA (*automotive service-oriented software architecture*). Sie ermöglicht die flexible Integration einzelner Komponenten und unterstützt dadurch das verfolgte Prinzip der Modularität. Module und Subsysteme sind mit ihr in der Lage, erforderliche Funktionen als Dienste anzubieten und abzufragen. Diese Umsetzung erlaubt im Übrigen flexible Anpassungsmöglichkeiten des Fahrzeugsystems.[18c]

Mit der Absicht Verifikation und Validation einzelner Systemkomponenten modular durchzuführen, wird das technische Gesamtsystem, wie durch Abbildung 2-1 veranschaulicht, strukturell in die Teilbereiche „Großhirn“, „Stammhirn“ und „Rückenmark“ aufgeteilt. Dazwischen trennen klar definierte Schnittstellen die einzelnen Bereiche.[18d]

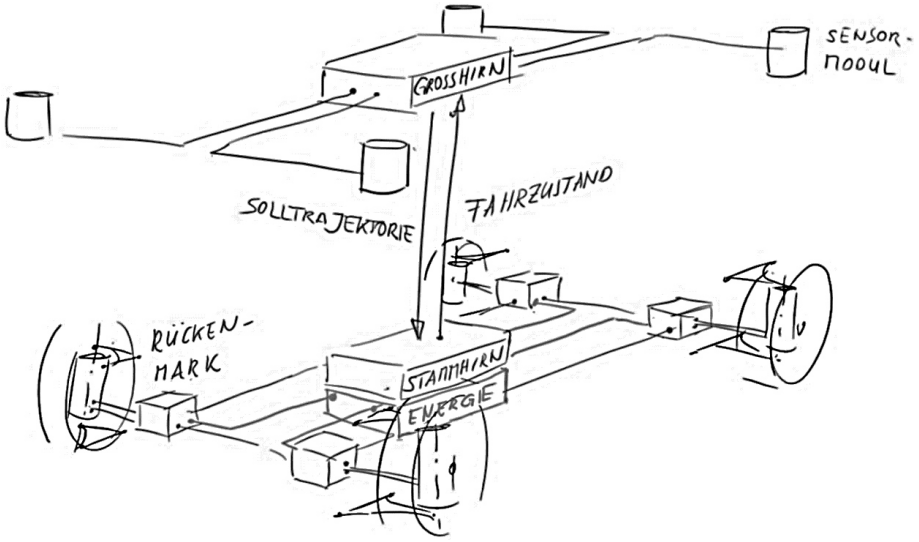

Abb. 2-1: Systemstruktur UNICAR*agil* [19]

Im Betrieb erfassen Sensormodule die Umgebung des Fahrzeugs. Gesammelte Informationen werden verarbeitet an das *Großhirn* weitergeleitet. Dort findet die hauptsächliche Datenverarbeitung in der Verhaltens- und Trajektorienplanung statt. In der nachfolgenden *Stammhirn*-Ebene werden diese geplanten Trajektorien zu Fahrmanövern umgesetzt. Notwendige Lenkwinkel, Brems- und Antriebsmomente werden berechnet und über das *Rückenmark* an die einzelnen Dynamikmodule kommuniziert. Das *Rückenmark* reagiert auch auf Defekte oder Ausfälle des *Stammhirns* und sichert damit, dank einer eigenen redundanten Stromversorgung, die Ausfallsicherheit des Gesamtsystems.[18e]

[18] Woopen, T. et al.: UNICARagil - Disruptive Modular Architectures (2018), a: S. 668; b: 673; S. 673–674; c: 668; d: 671; e: 667.

[19] Ackermann, S.; Winner, H.: Sicheres Anhalten Modularer Automatisierter Fahrzeuge (2020), S. 146.

Mehrere Schnittstellen sind an der Kontrolle von Fahrzeugverhalten, Vorgaben und Steuerbefehlen beteiligt. Sollten Funktionen im *Großhirn* ausfallen, wäre damit unter Umständen auch die Trajektorienplanung eingeschränkt. In diesem Fall dient die zuvor berechnete Rückfalltrajektorie als Grundlage, um trotzdem Vorgaben an die Dynamikmodule zu liefern. Auch wenn einzelne Funktionen ausfallen, findet damit nach wie vor ein Abgleich zwischen Umgebungsmodell und Dynamikmodulen statt.[20a] Die Umsetzung der vorgegebenen Trajektorie erfolgt durch einen Soll- / Ist-Vergleich mit einem Dynamikcontroller des *Rückenmarks*. Die Dynamikmodule erlauben hierfür neuartige Fahrmanöver durch unabhängig steuerbare Lenkwinkel und Momente. Es wird beabsichtigt, diese neuen Steuerungsmöglichkeiten für mehr Fahrkomfort und Sicherheit zu nutzen. So werden bei der Umsetzung der Trajektorien auch der aktuelle Bewegungsstatus und die Straßenreibung berücksichtigt.[20b] Durch Abgleich zwischen dem aktuellen dynamischen Fahrzeugzustand und dem Sollzustand, wird das Fahrzeug entlang berechneter Trajektorien gesteuert.

Für die Nutzung der vielen Freiheitsgrade werden individuelle Fahr- und Lenkmomentvorgaben an die einzelnen Dynamikmodule geleitet.[20c] Vier individuelle Kontrollsignale werden im *Stammhirn* anhand der Trajektorien berechnet und über das *Rückenmark* an die Aktorik der Dynamikmodule übermittelt. Ebenfalls zum *Rückenmark* gehörende Steuergeräte regeln dafür die geforderten Kräfte durch Bereitstellung gesteuerter Ströme und Spannungen.[20d]

In diesem beschriebenen System stellen die Dynamikmodule die grundlegenden Fahrfunktionen Lenken, Beschleunigen und Bremsen zu Verfügung. Jedes Modul verfügt dafür über einen 48 V Radnabenmotor und kann Lenkwinkel bis 90° stellen.[20e] Für die Stromversorgung sorgen vier verbaute Batterien, die ringförmig miteinander verbunden sind. Mit dieser dezentralen Stromversorgung ist das Fahrzeug auch bei einem lokalen Ausfall immer noch in der Lage, mit den restlichen Dynamikmodulen sicher anzuhalten.[21] So ist die Stromversorgung der Module auch allgemein auf eine maximale Spannung von 48 Volt ausgelegt. Das erlaubt Wartungsarbeiten ohne spezielle Hochspannungsunterweisungen. Allerdings gehen damit vergleichsweise stärkere Stromstärken als in einem Hochvoltsystem einher. Es entsteht so ein neuer Zusammenhang der den Bauraum bestimmt, denn Verbindungen zwischen Akku und elektrischen Motoren sind demzufolge möglichst kurz.[20f]

[20] Woopen, T. et al.: UNICARagil-Disruptive Modular Architectures (2018), a: S. 672;b: S. 674-675; c: 674; d: S. 672 e: S.665;f: 673.

[21] Woopen, T. et al.: UNICARagil - Where We Are (2020), S. 296.

2.2 Das Dynamikmodul und seine Funktionsbereiche

Auch wenn der Radstand in einer kurzen Variante der Konzeptfahrzeuge 2800 mm, in einer langen 3400 mm beträgt, besteht das Fahrwerk in allen Fällen aus vier identischen Dynamikmodulen.[22a] Für einen technischen Überblick, zeigt Abbildung 2-2 den Aufbau eines solchen Moduls. Die einzelnen Subsysteme werden nachfolgend in vier Abschnitten, geordnet nach funktionalen Bereichen, beschrieben. An erster Stelle stehen dabei Radantrieb (1), Perimeterbremse (2) und Lenkeinheit (3). Im Kontext der Lenkeinheit wird auch auf eingesetzte Fahrwerkskomponenten und das speziell entwickelte Rad eingegangen. Zuletzt folgt die Beschreibung des verbauten Steuergeräts (4).

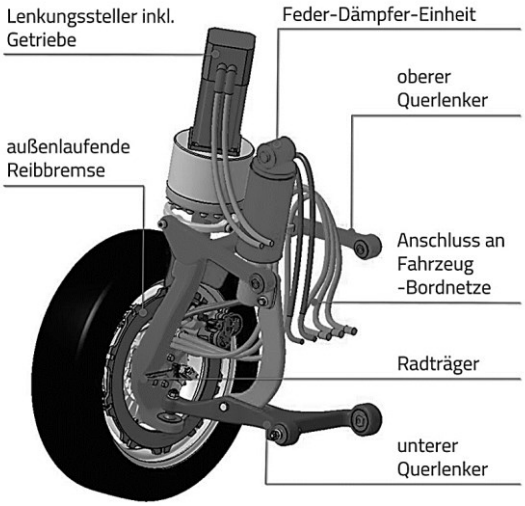

Abb. 2-2: Das Dynamikmodul[23]

Radantrieb

Die Verwendung von Radnabenantrieben ermöglicht sehr große Lenkwinkel bis zu 90°. Da die Steuerung der Dynamikmodule einzeln und ohne direkte mechanische Verbindung erfolgt, kann der Antrieb so mit identischer Geschwindigkeit bidirektional und auch seitwärts erfolgen.[22b]

Relevante Größen bei der Auslegung des Antriebsmotors waren die maximale Beschleunigung, das Vermögen für Rekuperation und die maximale Steigrate.[22c] Vorgesehen ist eine Fahrzeughöchstgeschwindigkeit von 70 km/h. Da die Kühlsysteme jedoch nur für den Luftstrom in eine Fahrtrichtung ausgelegt werden, ist die Geschwindigkeit entgegen der Vorzugsrichtung auf 30 km/h beschränkt. Um den Fahrzeugantrieb dafür angemessen dimensioniert zu entwickeln, fand die Auslegung entsprechend des vorgesehenen städtischen Einsatzgebiets statt.[22d] Dafür wurden Gradienten der geplanten Teststrecken herangezogen. Das zu stellende Spitzenmoment orientiert sich an der dort gewünschten Fahrzeugbeschleunigung, während das dauerhaft verfügbare Moment nach der gewünschten Steigrate ausgelegt wurde.[22e]

[22] Martens, T. e.: UNICARagil Dynamics Module (2020), a: S. 869; b: S. 864; c: S. 868; d: S. 865; e: S. 868 .

[23] Struth, M. et al.: Dynamikmodul (2020).

So ist das Fahrzeug in der Lage, bis zu einer Geschwindigkeit von grob 42 km/h mit 1,3 m/s² beschleunigen. Bei einer Geschwindigkeit von 50 km/h ist immer noch eine Beschleunigung von 1 m/s² möglich. Auch wenn der Motor seine Spitzenleistung nur auf Intervalle von 20 Sekunden begrenzt liefert, ist darin eine Beschleunigung mit voller Leistung von 0 auf 50 km/h mit 1,3 m/s² möglich. Der größte Anstieg der berücksichtigten Teststrecken liegt in Aachen mit einer maximale Steigrate von 7 %. Damit diente diese Steigung als Zielwert der Auslegung. Schlussendlich lässt sich mit den dauerhaften Leistungswerten des Motors eine solche Steigung von 7 % kontinuierlich mit 50 km/h fahren. Aber auch Anstiege mit höheren Steigungswerten von 19 % lassen sich unter Aufbringen der Maximalleistung kurzzeitig befahren.[22e]

Nach Übersetzung durch ein Planetengetriebe ist der Motor entsprechend seiner Auslegung in der Lage, ein kurzzeitiges Spitzenmoment von 500 Nm bei einer Spitzenleistung von 14 kW an das Rad zu liefern. Im dauerhaften Betrieb liegen die Werte bei 280 Nm Drehmoment am Rad und 10 kW Dauerleistung. So leistet das Gesamtfahrzeug mit vier Modulen die addierten Spitzenwerte 56 kW und 2000 Nm und dementsprechend dauerhafte Leistungen mit 40 kW bei maximal 1120 Nm.[24a]

Perimeterbremse

Mit dem Einsatz von 20“ Rädern und einer darin verbauten umlaufenden Perimeterbremse wurde die Nutzbarkeit des radinneren Bauraums optimiert. Bremsklotz, Radträger und der 14“ Radnabenmotor passen so in diesen verfügbaren Raum.[24b] Laut der deutschen StVZO muss mit dieser Bremskonfiguration eine durchschnittliche Verzögerung von 5 m/s² erreicht werden. Ähnlich sieht die europäische Regel No. 13-H eine Verzögerung von mindestens 5,76 m/s² vor. Im Rahmen des Projekts werden diese Notbremsungen jedoch als Ausnahmefall angenommen. Im regulären Betrieb gilt ein Richtwert von 1,3 m/s² für elektrisches Beschleunigen und rekuperatives Bremsen. Also wird die Perimeterbremse nur für das schnelle Anhalten in Notsituationen und als Rückfallebene eingeplant.[24c]

Lenkeinheit

Das vorgesehene Fahrwerkkonzept mit einem steer-by-wire System unterscheidet sich grundlegend von konventionellen Fahrwerken. Da keine Antriebswellen und Lenkgestänge angreifen, lassen sich größere Lenkwinkel erreichen. Basis für die Entwicklung der Dynamikmodule ist der Aufbau der Vorderachse aus dem Forschungsfahrzeug SpeedE, welches bereits zuvor am Institut für Kraftfahrzeuge in Aachen entwickelt wurde. Ebenso wie UNICAR*agil* verfügt es über ein steer-by-wire System mit großen Lenkwinkeln bis zu 60° am kurvenäußeren und 90° am -inneren Rad.[24d] Damit wird das Fahrzeugkonzept in der Lage sein, spezielle und neuartige Lenkmanöver auszuführen. In Abbildung 2-3 wird neben der Fahrt geradeaus, zunächst die vorgesehene Seitwärtsfahrt mit einem Lenkwinkel von 90° an allen Rädern dargestellt. Außerdem sind auch Wendemanöver mit einem Radmittelpunkt als Momentanpol und Wenden auf der Stelle beabsichtigt.

[24] Martens, T. e.: UNICARagil Dynamics Module (2020), a: 868; b: S. 871; c: S. 867; d: S. 869.

Um diese tatsächlich realisieren zu können, ist der maximal erreichbare Lenkwinkel an den Rädern auf 66° außen und 93° innen festgelegt.[25a]

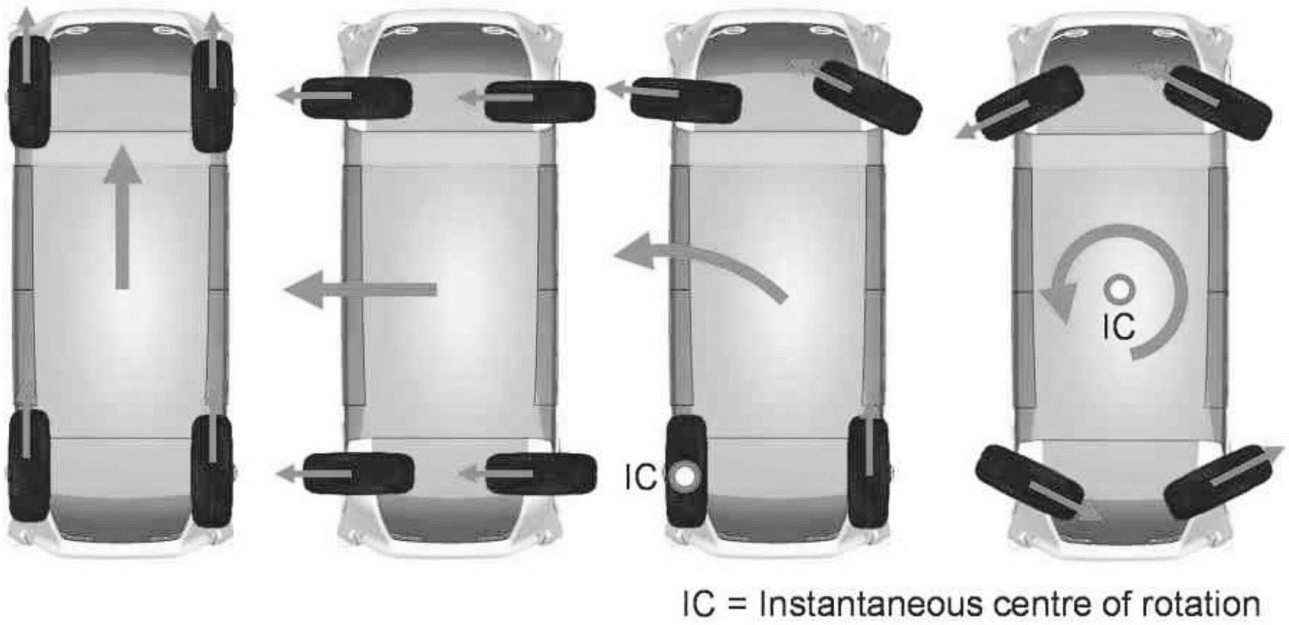

Abb. 2-3: Lenkmanöver der Konzeptfahrzeuge[25b]

Elektromotor, Sensorik für Lenkwinkel und -momente, eine Haltebremse und ein Spannungswellengetriebe bilden gemeinsam das steer-by-wire-System. Das Spannungswellengetriebe ist mit einem Adapter am Radträger befestigt. So können Lenkmomente über das Kardangelenk und den oberen Querlenker an der Fahrzeugkarosse abgestützt werden, während Rotationsbewegungen auch bei Ein- und Ausfedern möglich bleiben.[25c] Ein oberer und ein unterer Querlenker bilden dafür eine Doppelquerlenkeraufhängung. Beide sind über vibrationsdämpfende Gelenke am Gehäuse befestigt. Radträger und Gelenke schließen die kinematische Kopplung und bestimmen die Position der Lenkachse. Spurstange und oberes Kugelgelenk werden durch ein Kardangelenk ersetzt. Dieses bietet zwei definierte Rotationsachsen und besteht aus einem inneren und einem äußeren Kardanring. Der äußere Kardanring ist mit dem oberen Querlenker verbunden. Der untere Ring ist am Gehäuse des Lenksystems befestigt.[25d] Ein Feder-Dämpfer-System ist am unteren Querlenker angebracht. Eine spezielle Sichelform dieses Feder-Dämpfer-Elements ermöglicht den geforderten Lenkwinkelbereich bei gleichzeitiger Rollstabilisierung. Außerdem bleibt damit Platz für die Bremse bei Lenk- und Federbewegungen. Die Auslegung resultiert in einer Federspurweite von 778,55 mm bei einer Spurbreite von 1700 mm.[25e] In der modularen Architektur des Konzepts sind hierbei keine Stabilisatoren im Fahrzeug vorgesehen. Rollstabilisation erfolgt rein über das Feder-Dämpfer-System.[25f]

Die Lenkung des Dynamikmoduls wurde entsprechend dem geplanten Lenkwinkelbereich, einem Fahrzeuggewicht von 3200 kg in schwerster Ausführung, gemäß der bidirektionale Auslegung, nach verschiedenen Fahrzeuglängen und letztlich der gewählten Reifendimension ausgelegt.[25g]

[25] Martens, T. e.: UNICARagil Dynamics Module (2020), a: S. 870; b: S.870; c: S. 872; d: S. 871-872; e: S. 872; f: S. 871; g: S. 874.

Wieder orientiert sie sich an realen Manövern. Die Auslegung der Spitzenanforderungen des Lenkantriebs erfolgte nach notwendigen Kräften bei Lenken im Stillstand mit angezogener Bremse und Vollbremsungen aus Höchstgeschwindigkeit. Die Auslegung dauerhafter Standhaftigkeit erfolgte nach den auftretenden Kräften in konstanten Kurvenfahrten.[26a] Somit stellt der Lenkantrieb ein Spitzenmoment von 1290 Nm bei mindestens 5 Umdrehungen pro Minute am Rad. Um die Lenkung nicht zu überlasten, wird dieses Moment jedoch nur fünfmal innerhalb von 70 Sekunden gestellt. Erreichen Lenkantrieb oder Inverter kritische Temperaturen, folgt vor der nächsten vollen Leistungsabgabe eine Abkühlphase von 3 Minuten.[26b] Dauerhafte Leistungskapazitäten der Lenkung wurden anhand zulässiger Querbeschleunigungen in Kurvenfahrten ausgelegt. Für schnelle Kurvenfahrten mit höchster auftretender Querbeschleunigung ist der Antrieb somit in der Lage, Lenkmomente von 340 Nm bei Winkelgeschwindigkeiten von 15 1/min dauerhaft zu stellen.[26c]

Fällt die Lenkung bei einem Fahrzeug aus, ist ein Unfall nahezu unvermeidbar. Die sichere Funktion eines automobilen Steer-by-Wire Systems ist daher allgemein sehr wichtig.[27] Deswegen wurden besondere Sicherheitsvorkehrungen für das Lenksystem des Dynamikmoduls vorgesehen. Eine Bremse mit 24 V Spannungsversorgung blockiert die Lenkung im Fall einer erkannten Fehlfunktion. Zusätzlich erfassen Temperatursensoren kritische Wärmeentwicklungen. Die Temperaturwerte liefern damit Informationen über den Zustand des Lenkantriebs. Außerdem erfasst ein Drehmomentsensor die Momente am Ausgang des Lenksystems. Störmomente am Rad und Störungen im Spannungswellengetriebe lassen sich damit erkennen.[26d]

Das besondere Lenksystem erfordert ein speziell entwickeltes Rad. Es wurde dafür nach Reifendimensionen, Anschlusspunkten und verfügbarem Bauraum konstruiert. Die verwendeten Reifendimensionen betragen 195/55R20. Montiert wird das Rad mit vier M12 Schrauben in einem Lochkreis von 100 mm. Für eine veranschlagte Traglast von 800 kg erfolgte bereits eine Validation dieses Rades nach üblichen Industriestandards.[26e]

[26] Martens, T. e.: UNICARagil Dynamics Module (2020), a: S. 881; b: S. 874; c: S. 875; d: S. 876-877; e: S. 877.

[27] Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011), S. 7.

Steuergerät

Für den geplant flexiblen Einsatz, besitzt jedes Dynamikmodul ein eigenes Steuergerät, wie es in Abbildung 2-4 dargestellt ist.[28a]

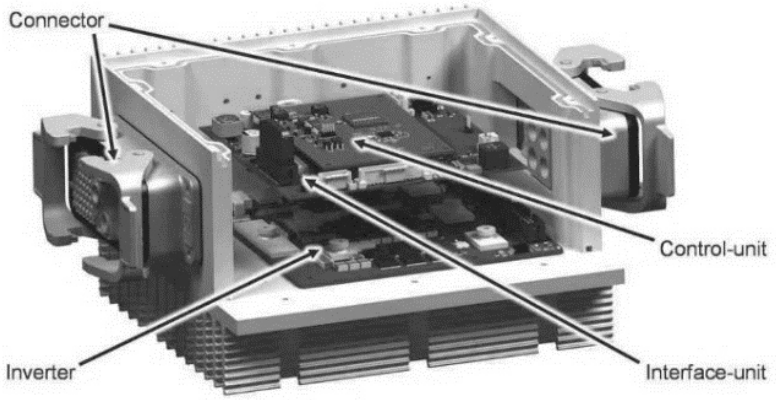

Abb. 2-4: Das Steuergerät eines Dynamikmoduls (Teil des *Rückenmarks*)[28b]

Die Steuergeräte der Dynamikmodule bilden gemeinsam das *Rückenmark*. Jedes einzelne dieser Steuerungsmodule enthält neben einer Steuereinheit, eine Schnittstelleneinheit und einen Inverter für die Leistungsbereitstellung.[28c] Die Steuereinheit bewältigt die grundlegenden Berechnungs- und Kommunikationsaufgaben für ein Dynamikmodul. Ein Aurix™ TriCore™ Microcontroller führt hierfür simultan Sicherheitsanwendungen und die Steuerung der Elektromotoren aus. Insgesamt verfügt die Einheit dafür über mehrere Kommunikationsschnittstellen. Dabei enthält die Schnittstelleneinheit als weitere Komponente alle Anschlüsse für interne Sensoren, externe Kommunikationsschnittstellen und die Stromversorgung.

Der verbaute Inverter stellt als Leistungseinheit mit einer Spannung von 48 V die Phasenströme des Lenkmotors. Für optimierte thermische Eigenschaften ist der Inverter mit einer Leiterplatte aus Aluminium ausgestattet. So wird eine gleichmäßige Wärmeabfuhr der einzelnen Komponenten unterstützt. Ergänzend leiten zusätzliche Rippenkühlkörper und ein ebenfalls geripptes Aluminiumgehäuse die Wärme ab. Um dem modularen Leitgedanken treu zu bleiben, sind diese Gehäuse für alle Dynamikmodule und Fahrzeugvarianten identisch.[28d]

Auch in der eingesetzten Steuerungssoftware kommt das modulare Grundprinzip zur Anwendung. Zunächst findet darin eine Signalaufbereitung für Steuergeräte der Längs- und Querdynamik statt. Dafür werden Eingangswerte nach ihrer Plausibilität beurteilt und gegebenenfalls gefiltert. Der dabei verwendete Code wurde mit Simulink erstellt in den restlichen Softwarerahmen eingegliedert. Diese Rahmensoftware wiederum ist in C geschrieben. Veranschaulichend stellt die Abbildung 2-5 den gesamten Aufbau der Steuerungs-Software dar.

[28] Martens, T. e.: UNICARagil Dynamics Module (2020), a: S. 863–864; b: S. 879; c: S. 878; d: S. 878-879.

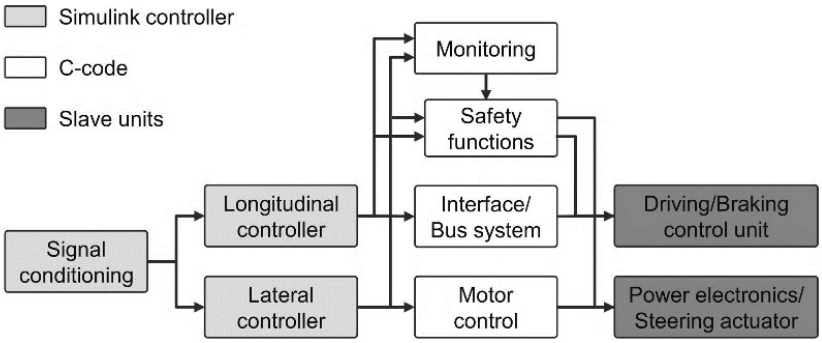

Abb. 2-5: Softwarestruktur der Steuergeräte[29a]

Die Software bildet damit die Schnittstelle zwischen den Steuerungseinheiten und der Aktorik des Dynamikmoduls. Zusätzliche Überwachungs- und Sicherheitsfunktionen, aber auch die Steuerung des Lenkmotors wurden hier ebenfalls in C programmiert.

Zusammengefasst, werden Steuerungsvariablen aus der Fahrzeugdynamiksteuerung in der Signalaufbereitung vorbehandelt und an die Steuerung für Längs- und Querdynamik weitergeleitet. Daraus resultierende Werte werden entweder an die Steuerung des Lenkmotors oder per CAN-Bus an Radnabenmotor und Bremse übertragen. Für erhöhte Sicherheit findet dabei die Ausführung von Überwachungs- und Sicherheitsprozessen auf einem separaten Steuergerät statt.[29b] Über die ASOA werden Radgeschwindigkeiten und Lenkwinkel für die Schätzung des dynamischen Fahrzustands zurück an die Steuergeräte des *Stammhirns* übermittelt.[30a] Einhaltung gesetzter Obergrenzen für Fahrzeugbeschleunigung oder den Anfahrruck werden ebenfalls in vorangestellten Planungssystemen geregelt. Auch die Anpassungen vorgegebener Lenkwinkel und Geschwindigkeiten für genaues Einhalten der geplanten Trajektorie, erfolgen außerhalb des Dynamikmoduls.[30b] Die eigentliche Kontrolle, ob die Dynamikmodule ihren jeweiligen Vorgaben folgen, erfolgt damit innerhalb des *Stammhirns*.[30c]

2.3 Betriebssituationen des Dynamikmoduls

Im Allgemeinen beeinflusst der geplante Einsatzbereich eines autonomen Fahrzeugs seine Anforderungen maßgeblich. Werden Passagiere befördert, fallen generell detailliertere Anforderungen an. Die Sicherheit der Passagiere ist schließlich beim Anhalten, aber auch insbesondere im Fahrbetrieb zu berücksichtigen.[31a] So sieht auch eine Item Definition nach der Norm ISO 26262 eine Beschreibung von Systemumgebung und Betriebsbedingungen vor.[31b] Generell ist das Vorgehen bei einer solchen Beschreibung jedoch nicht ausführlich in der Norm definiert.[31c]

In seiner Dissertation präsentiert Reschka deswegen eine eigene Stuktur für eine Item Definition nach der Norm.[32] Er sieht darin eine Beschreibung des Anwendungsfalls und eine Klassifikation des Automatisierungsgrads vor. Davon ausgehend empfiehlt er mögliche Anwendungsszenarien und

[29] Martens, T. e.: UNICARagil Dynamics Module (2020), a: S. 880; b: S. 880.

[30] Buchholz, M. et al.: Automation of the UNICARagil Vehicles (2020), S. 6–7.

[31] Reschka, A.: Sicherheitskonzept für autonome Fahrzeuge (2015), a: S. 500; b: S.95; c: S. 98.

[32] Reschka, A.: Dissertation, Fertigkeiten- und Fähigkeitengraphen (2016), S. 102.

darin erwartetes Sollverhalten zu bestimmen. Mit einer Identifikation sicherer Betriebszustände und einer Beschreibung der vorgesehenen Fahrmanöver, aber auch der geplanten Fertigkeiten, sieht er alle notwendigen Grundlagen für den Konzeptentwurf einer Entwicklung als vorhanden an.

Wie im ersten Grundlagenkapitel beschrieben, soll das Dynamikmodul in einem autonomen Fahrzeug für den städtischen Verkehr zum Einsatz kommen. Generell ist dessen Betrieb in verschiedenen Automatisierungsstufen möglich. Deren übliche Einteilung erfolgt häufig in fünf Stufen.[33] In gewisser Hinsicht verteilt sich der Betriebsbereich der Konzeptfahrzeuge situationsabhängig über alle dieser fünf Stufen, von reinem Fahrerbetrieb bis hin zu vollautomatisiertem Fahren. Um dabei mögliche Funktionsgrenzen zu berücksichtigen, wird im Betrieb eine Verwaltung mit vier verschiedenen Betriebsmodi vorgesehen. Im automatischen Modus fährt das Fahrzeug selbstständig ohne menschliche Eingriffe. In einem manuellen Modus ist einfaches Rangieren möglich. Als Sicherheitsvorkehrung ist das bereits erwähnte „Sichere Anhalten“ vorgesehen, nach dessen erfolgreicher Ausführung beispielsweise ein Wechsel in den vierten Modus, den Leitwartenbetrieb, möglich ist.[34a]

Der manuelle Betrieb ist vor allem für Reparatur- und Wartungsarbeiten vorgesehen. Einfaches manövrieren nach menschlichen Vorgaben ist hierbei nützlich. Dafür erfolgen die Vorgaben entweder über Steuerknüppel und Bremspedal oder alternativ über eine externe Steuerung.[34b] Wichtigere Bedeutung in der Fahrzeugsicherheit hat der Betriebsmodus "Sicheres Anhalten". Darin wird die Rückfallebene aktiviert. Nach Betriebsstart läuft der automatisierte Betrieb grundsätzlich nur, wenn dafür alle Notwendigkeiten erfüllt sind. Ein Wechsel zwischen den Betriebsmodi erfolgt nur im Stillstand. Ausnahme ist nur ein Wechsel in das "Sichere Anhalten", der auch in Bewegung möglich ist.[34c] In Situationen, in denen das Fahrzeug aus dem Sicheren Halt nicht alleine weiterfahren kann, kommt der Leitwartenbetrieb zum Einsatz. Menschliches Eingreifen per Fernsteuerung löst dann möglicherweise eine problematische Situation auf.[34d]

Bei Absicherungsansätzen mit Szenarien, würde die Berücksichtigung dieser Betriebsmodi möglicherweise die Definition von Testfällen erschweren. Ähnliche Verkehrssituationen müssten möglicherweise für alle Betriebsmodi getestet werden. Fahrzeuge in autonomem Betrieb könnten grundsätzlich ein anderes Fahrverhalten aufweisen als Menschen und mit ihrer Umgebung somit auch anders in Wechselwirkung treten. Beispielsweise könnten konsequent eingehaltene Sicherheitsabstände autonomer Fahrzeuge vermehrtes Abschneiden durch menschliche Fahrer verursachen.[35] Auch wenn ein Testvorgehen mit Szenarien vielversprechend ist, ließe sich hier der Umgang mit Einflussparametern durch ein Vorgehen mit partikulären Tests vereinfachen. Das gezielte Testen von einzelnen Funktionen liefert hier möglicherweise auch schnellere Ergebnisse.[36] Es besteht die Möglichkeit, ähnliche Einsatzbereiche im Testvorgehen für schnellere Fortschritte als gleichwertig zu behandeln. Bei gleichbleibender Funktion in gleichem Einsatzgebiet ließe sich dann eine zuvor erteilte Freigabe übernehmen. Neue Einsatzbereiche erforderten dann nur noch eine Absicherung in dem dafür jeweils

[33] Jipp, M.; Schneider, L.: Fahrtests unter Realbedingungen (2020), S. 3–4.

[34] Buchholz, M. et al.: Automation of the UNICARagil Vehicles (2020), S. 4.

[35] Stellet, J. E. et al.: Validation of automated driving (2020), S. 67.

[36] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 1.

nötigen Umfang. Eine Einteilung nach Geschwindigkeitsbereichen oder Automatisierungsgrad wäre dafür beispielsweise denkbar. Zusätzlich liegen Testergebnisse schneller vor, wenn die Anzahl durchzuführender Testfälle möglichst klein gehalten wird.

Virtuelle Testumgebungen anstelle von Fahrversuchen stellen zusätzlich schnellere Ergebnisse in Aussicht. Die Beobachtung von Interaktionen zwischen künstlichen und realen Elementen ist einfacher variierbar und schafft Vorteile. Eine Testdurchführung auf ausschließlich virtueller Ebene bietet in dem Kontext das größte Optimierungspotential.[37]

Wie beschrieben, wird von dem Dynamikmodul erwartet, geforderte Fahrleistungen umzusetzen. Die Quelle der jeweiligen Vorgaben liegt dabei außerhalb des Moduls. Grundsätzlich ist somit die Annahme naheliegend, dass die Anforderungen an die Leistungserbringung in allen Betriebssituationen ähnlich ausfallen. Auch wenn keine Höchstgeschwindigkeiten im manuellen Rangieren zu erwarten sind, bietet sich eine Zusammenfassung dieser Anforderungen an um eine Vereinfachung zu treffen.

Für eine angemessene Regelung der Fahrgeschwindigkeit ist es notwendig, dass ein autonomes Fahrzeug in der Lage ist seine eigene Leistungsfähigkeit zu erkennen.[38] Das Fahrzeugkonzept implementiert in diesem Zusammenhang die drei grundlegende Sicherheitsmechanismen der Selbstwahrnehmung, des Sicheren Anhaltens und der kapazitätsbasierten Routenplanung.[39] Aktiviert wird die Rückfallebene des sicheren Anhaltens, wenn die primären Fahrfunktionen ihre dynamische Fahraufgabe nicht mehr erfüllen können. Dann überführt die Rückfallebene das Fahrzeug in einen risikominimalen Zustand.[40a] Die vier nachfolgend beschriebenen Fahrmanöver der vorgesehenen Rückfallebene stellen deswegen auch besonders relevante Situationen für das Dynamikmodul dar:

1. Starke Verzögerung (6 m/s²) bei konstantem Lenkwinkel bis der sichere Fahrzeugstillstand erreicht ist.
2. Abfahrt der geplanten Bahn bei gleichzeitiger Verzögerung bis zum Stillstand ohne weitere Berücksichtigung des Umfelds.
3. Das Fahrzeug hält an einer geeigneten Stelle an. Dabei werden Hindernisse immer noch wahrgenommen und berücksichtigt.
4. Verfolgen einer zusätzlich zur Solltrajektorie geplanten Notbahn, die ausfallsicher an das Stammhirn übertragen wurde. Reichen die Planungskapazitäten, endet die Bahn an einem risikominimalen Ort außerhalb des fließenden Verkehrs auch ohne genaue Wahrnehmung der Umgebung. Diese Bahn wird nicht verlassen, nur die Geschwindigkeit reduziert.[40b]

[37] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 458–462.

[38] Reschka, A.: Sicherheitskonzept für autonome Fahrzeuge (2015), S. 501.

[39] Stolte, T. et al.: Safety Concepts for Automated Vehicles (2020), S. 1563.

[40] Ackermann, S.; Winner, H.: Sicheres Anhalten Modularer Automatisierter Fahrzeuge (2020), a: S. 146; b: S. 146-147.

Als Gegenstück zu den antreibenden Fähigkeiten stehen kognitive Fähigkeiten autonomer Fahrzeuge. Diese lassen sich kategorisierend neben der Selbstwahrnehmung und der Wahrnehmung der Umgebung auch der Planung von Entscheidungen und Trajektorien zuordnen. Zukünftig wird daneben auch der Informationsaustausch mit anderen Fahrzeugen eine Rolle spielen.[41] Die damit verknüpften Funktionen spielen eine große Rolle in der Fahrzeugsicherheit. Auch die wahrnehmenden und kommunizierenden Funktionen des Dynamikmoduls sind für sicherheitsrelevante Entscheidungen außerhalb des Dynamikmoduls von Bedeutung. An der Stelle lässt sich argumentieren, dass diese Funktionen eine untergeordnete Rolle spielen, sobald in einem Notfall Sicherheitsmaßnahmen eingeleitet werden und Sicherheitsprioritäten bei den ausführenden Funktionen liegen. Allerdings blieben dann die vorgesehenen Eingriffsmöglichkeiten der Leitwarte unberücksichtigt.[42] Damit das Fahrzeug von der Leitwarte möglichst sicher bedient werden kann, ist die Sensorik und Kommunikation aller Fahrzeugkomponenten stets von Bedeutung.

Aus diesem Grund lassen sich auch Funktionen der Kommunikation und Sensorik in allen Betriebssituationen gleichermaßen wichtig einstufen. Dennoch ist es für vorgesehene Sicherheitsmechanismen wichtig, einzelne Komponenten des Dynamikmoduls, wie beispielsweise die *fail-silent* Bremse, unter Sonderbedingungen zu testen. Vereinfachend bietet es sich für das Dynamikmodul dabei jedoch an, die Anforderungen aller Betriebssituationen gleichwertig zu testen und sich dabei die jeweils strengsten Maßstäbe anzuwenden.

[41] Reschka, A. et al.: Ability and Skill graphs (2015), S. 935.

[42] Woopen, T. et al.: UNICARagil - Disruptive Modular Architectures (2018), S. 673–674.

3 Theoretische Grundlagen

Ausgehend von technischen Informationen lassen sich bereits intuitive Tests definieren. Für ein strukturierteres Vorgehen bietet es sich an, zunächst einen theoretischen Rahmen zu definieren, mit dem sich Informationen für eine Testentwicklung einordnen lassen. Deswegen beschreibt dieses Kapitel in vier Abschnitten Grundlagen im Umgang mit Anforderungen, zerlegende und strukturierende Ansätze für funktionale Dekomposition, Grundbegriffe der funktionalen Sicherheit und zuletzt die Bedeutung von Tests im allgemeinen Entwicklungsprozess.

3.1 Anforderungen

Unter einer Anforderung versteht man im Allgemeinen eine Bedingung oder Fähigkeit, die zur Lösung eines Problems oder dem Erreichen eines Ziels benötigt wird.[43] Tests untersuchen, ob das Testobjekt eine geforderte Eigenschaft erfüllt. Somit besteht ein direkter Zusammenhang zwischen Anforderungen und einer Testentwicklung.[44a] Ganz allgemein dienen Anforderungen der Beschreibung von Systemen. Sie definieren welche Eigenschaften von einem System verlangt werden und unterstützen damit auch die Kontrolle der Systemumsetzung.[44b] Exakt definierte Anforderungen, die auch von Dritten verstanden werden, sind eine wichtige Grundlage für die Erstellung von Testfällen. Unpräzise Anforderungen lassen sich schwerer testen und beeinträchtigen sowohl die Aussagekraft als auch die Bewertbarkeit der damit erzielbaren Testergebnisse. Allgemein werden Anforderungen klarer, indem man offene Punkte mehrfach überarbeitet. Für die Handhabung der Anforderungen innerhalb von Testprozessen ist außerdem eine eindeutige Kennzeichnung mit zusätzlichen Attributen wie Priorität oder Komplexität hilfreich.[45]

Im Automobilbereich werden Verbundsysteme aus Steuergeräten, Sensoren, Aktuatoren, Software und deren Wechselwirkungen mit Systemanforderungen beschrieben. Diese Anforderungen an Gesamtsysteme sind gemeinsam in Systemlastenheften gesammelt. Unabhängig von dem Schwerpunkt des Lastenhefts beschreibt es eine Systemvision mit einer funktionalen und einer qualitativen Beschreibung der Systemziele.[44c] Zusätzliche technische Sicherheitsanforderungen erweitern die Angaben über das untersuchte Bauteil. Sie beschreiben konkret, wie der jeweilige Entwicklungsgegenstand auf Störungen bei der Erfüllung seiner Sicherheitsziele reagieren soll.[46]

Eine solche Systemspezifikation berücksichtigt also grundsätzlich mehrere Elemente. Einflussfaktoren aus der Umgebung lassen sich meist durch eine genauere Betrachtung der relevanten Schnittstellen ermitteln. Auch die Einsatzarten und Betriebsmodi fließen in die Spezifikation ein. Unterschiede in der Konfiguration oder den Regelbetrieben werden ebenfalls berücksichtigt. Relevante Eingangs- und Ausgangsgrößen werden definiert. Ursprung und Empfänger dieser Werte, aber auch eventuelle Informationsformate und Geltungsbereiche, werden beschrieben. Eine Spezifikation der inneren

[43] Martin Glinz: Spezifikation von Anforderungen, S. 91.

[44] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), a: S. 13; b: S. 5; c: S. 6.

[45] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), S. 74.

[46] G. Bagschik et al.: Entwicklung, Absicherung & Test automatisierter Fahrzeuge (2017), S. 130.

Zusammenhänge und Systembedingungen gibt Aufschluss über deren Beziehungen. Störeinflüsse und veränderbare Beziehungen sind zuletzt ebenfalls von Bedeutung.[47]

Um keine Missverständnisse zu erlauben wird grundsätzlich eine möglichst eindeutige Formulierung angestrebt. Vielfache Interpretationsmöglichkeiten werden so ausgeschlossen.[48a] Besonders bei umfangreichen Systemen bietet sich eine Priorisierung der Anforderungen an. Eine einfache Einteilung nach Priorität erfolgt in drei Stufen. An erster Stelle unverzichtbare *Muss-Anforderungen,* an zweiter Stelle unter Kosten vernachlässigbare *Soll-Anforderungen* und drittens im Fall unerheblicher Zusatzkosten zu erfüllende *Wunsch-Anforderungen.*[49] Eine derartige Kategorisierung in drei Stufen findet sich auch in dem MoSCoW-Prinzip wieder. Dieses Akronym steht dabei für eine Einteilung in die Kategorien M wie *MUST*, S wie *SHOULD*, C wie *COULD* und W wie *WON'T.* [50]

Für die allgemeine Lesbarkeit, ist die Anforderungsliste aus den Ergebnissen der in Kapitel 4 erläuterten Analysen weitestgehend in natürlicher Sprache verfasst worden. Jeder Eintrag verfügt zusätzlich über eine Angabe über seinen Ursprung und lässt sich nach beteiligten Subsystemen und Einflüssen kategorisiert anzeigen. Zusätzlich sind alle Einträge mit einer Priorisierung nach den drei vorgestellten Kategorien versehen.

3.2 Dekomposition

Ein Gesamtfahrzeug setzt sich aus mehreren Systemen zusammen. Jedes einzelne System lässt sich durch ein eigenes Systemlastenheft beschreiben. Neben organisatorischen Bestimmungen sind darin auch abstrakte Fahrzeugfunktionen aufgeführt. Hier bilden einzelne Funktionen mögliche Unterkapitel mit Systemanforderungen einer untergeordneten Ebene.[48b] Noack schlägt in seiner Dissertation vor diese einzelnen Anforderungen durch beschreibende Verknüpfungen zu ergänzen. In Vorwärtsrichtung lassen sich Anforderungen mit Testfällen verknüpfen. In Rückwärtsrichtung dokumentieren sie den Ursprung einer Anforderung. Zusätzlich untereinander verknüpfte Anforderungen machen Abhängigkeiten deutlich.[48c]

Anforderungen lassen sich ganz allgemein in funktionale und nicht-funktionale Anforderungen kategorisieren. Nichtfunktionale Anforderungen werden in der Literatur auch als Qualitätsanforderungen beschrieben. Unabhängig von den Begrifflichkeiten beschreiben diese nichtfunktionalen Anforderungen qualitative Systemeigenschaften in Form von bezifferbaren Anforderungen.[48d] Nichtfunktionale Anforderungen sind oft weniger ersichtlich als die Anforderungen der grundlegenden Funktionserfüllung. So ist die Entscheidung, wann die Nichtfunktionalität eines Systems genau genug beschrieben und abgesichert ist, eine häufige Schwierigkeit bei der Spezifikation von nichtfunktionalen Anforderungen. Mögliche Hilfestellung ist hier eine präzise Testplanung, die bestimmt welche nichtfunktionalen Qualitätsmerkmale in welchem Umfang abzusichern sind.[48e] Eine kategorisierte

[47] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 160.

[48] Noack, T.: Automatische Verlinkung von Testfällen & Anforderungen (2015), a: S. 12; b: S. 31; c: S. 25-26; d: S.11; e: S.19.

[49] Martin Glinz: Spezifikation von Anforderungen, S. 95.

[50] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), S. 75.

Betrachtung stellt dafür eine mögliche Hilfestellung dar. So schlagen Lippert et al. für Sicherheitsanforderungen automatisierter Fahrzeuge beispielsweise eine Aufteilung in eine makroskopische und eine mikroskopische Ebene vor.[51a] Makroskopische Anforderungen an Sicherheit und Unfallrisiko sind für eine gesellschaftliche Akzeptanz autonomer Fahrzeuge im Straßenverkehr zu erfüllen.[51b] Auf mikroskopischer Ebene lassen sich Anforderungen Bereichen der Verhaltenssicherheit, funktionaler Sicherheit, passiver Sicherheit, Gebrauchssicherheit und zusätzlich auch der IT Sicherheit zuordnen.

Verhaltenssicherheit ist gegeben, wenn ein Fahrzeug im Betrieb keine Gefährdungen verursacht. Relevant sind dafür die Bewegungen und Wechselbeziehungen im Verkehrsgeschehen. Das System muss Gefahren im Verkehrsbetrieb generell vermeiden und minimieren. Auf der Ebene funktionaler Sicherheit gilt es, Fehler von Fahrzeugkomponenten zu vermeiden. Hier unterstützt eine Risikobewertung und Gefahrenanalyse nach ISO 26262 bei der Feststellung möglicher Gefahren. Passive Sicherheit entsteht durch Vorkehrungen die das Ausmaß von Unfallauswirkungen minimieren. Besonders wichtig sind dabei Personenschäden. So sind für eine Typzulassung auch per Gesetz Unfallsicherheitsanforderungen vorgeschrieben. An nächster Stelle umfasst die Gebrauchssicherheit verschiedene Aspekte, die bei Interaktionen zwischen Personen und Fahrzeug eine Rolle spielen. Ganz konkret sind Systeminteraktionen außerhalb der Hauptfunktionen von Bedeutung. Anforderungen an die Gebrauchssicherheit beeinflussen demzufolge Reparaturen, Wartungen und auch den Schutz vor scharfen Kanten oder elektrischen Schocks. Zuletzt hat auch die Sicherheit der eingesetzten informationstechnischen Systeme wechselseitig Einfluss auf die Sicherheit automatisierter Fahrzeuge.[51c]

Bei einer funktionalen Betrachtung lassen sich automatisierte Robotersysteme oft in wahrnehmende, planende und handelnde Komponenten aufteilen.[52] Vergleichbar werden Software-basierte Systeme branchenübergreifend nach dem sogenannten "EVA-Prinzip" beschrieben. "EVA" steht hier als Akronym für die Funktionsbereiche Eingabe, Verarbeitung und Ausgabe.[53] An diese kategorisierte Betrachtung in seiner Dissertation knüpft Amersbach an, indem er für autonome Fahrfunktionen eine Dekomposition in 6 Ebenen vorschlägt. Die erste Funktionsebene beschäftigt sich mit dem Informationszugang (1). Auf nächster Ebene befinden sich alle Funktionen für den Informationsempfang (2). Die empfangenen Informationen gehen weiter an die Funktionen in der Informationsverarbeitung (3). Darin findet Informationsfusion für eine modellhafte Erfassung der Umgebung statt. Funktionen für das Situationsverständnis (4) strukturieren die Informationen zu einer anwendbaren Entscheidungsgrundlage für nachfolgende Ebenen. Daraufhin finden sich in den letzten Ebenen alle Funktionen für die Verhaltenswahl (5) und entsprechende Ausführung (6).[54]

Für eine noch detailliertere Beschreibung funktionaler Systemarchitekturen in automatisierten Fahrzeugen präsentieren Reschka, Bagschik und Kollegen die Einsatzmöglichkeiten von *"Fähigkeitsgraphen".* Damit lassen sich auch die Abhängigkeiten und Interaktionen einzelner Systemkomponenten

[51] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), a: S. 2; b: S. 2; c: S. 2-3.

[52] Philipp, R. et al.: Decomposition of Automated Driving Systems (2020), S. 96.

[53] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 240.

[54] Amersbach, C. T.: Dissertation, Decomposition Approach - Reducing Validation Effort (2020), S. 53–55.

mit ihrer Bedeutung für die Systemanforderungen visualisieren.[55] Ein *"Fähigkeits-Knoten"* stellt darin als Ausgangspunkt eine grundlegende Fähigkeit dar, die von anderen Knoten untergeordneter Fähigkeiten abhängig ist. Diese untergeordneten Fähigkeiten sind im Einzelfall möglicherweise auch durch Abhängigkeiten in mehreren Ebenen miteinander verknüpft. Jeweils notwendige Datenquellen und Datenempfänger vervollständigen die schematische Darstellung, wie sie in Abbildung 3-1 beispielhaft abgebildet ist.[56a]

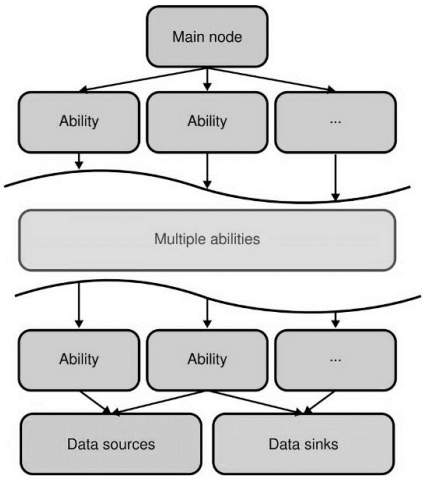

Abb. 3-1: Aufbau eines *Fähigkeitengraphs*[56b]

Diese *Fähigkeitsgraphen* liefern eine vielseitig nutzbare Informationsgrundlage. Jedoch weisen die Autoren auch auf Herausforderungen bei der Identifikation der relevanten Fähigkeiten, der Verknüpfung ihrer Abhängigkeiten und dem Auffinden passender Metriken hin, denen sie sich in ihrem Forschungsbeitrag für das Projekt „Stadtpilot“ intensiver widmen.[56c]

Die Gliederung einer Systemspezifikation ist allgemein von den Methoden abhängig, die bei ihrer Bestimmung eingesetzt wurden. Grundsätzlich ist Verständlichkeit von Anforderungen in allen Fällen ein wichtiges Qualitätsmerkmal. Ganz prinzipiell sind fehlende oder unverständliche Gliederungen immer unvorteilhaft für deren Leser.[57]

Mit einem funktionsorientierten Verknüpfungssystem, das in Abschnitt 5.4 genauer erklärt wird, flossen Noacks Gedanken in die erstellte Anforderungsliste mit ein. Es dient sowohl bei der strukturierten Darstellung zusammenhängender Anforderungen als auch bei der Zuordnung zu einem genaueren Sicherheitsziel. Eine Kategorisierung der einzelnen Anforderungen in funktionale Anforderungen und Sicherheitsanforderungen wurde ebenfalls einbezogen. In Anlehnung an Amersbach funktionale Zerlegung automatisierter Fahrfunktionen wurde in 5.3 ebenfalls eine Einteilung der Funktionsbereiche des Dynamikmoduls vorgenommen. Diese lieferte eine grundlegende Struktur für weitere Untersuchungen mit *Fähigkeitengraphen,* ähnlich zu der hier beschriebenen Form.

[55] Reschka, A. et al.: Ability and skill graphs (2015), S. 935.

[56] Reschka, A. et al.: Ability and skill graphs (2015), a: S. 936; b: S. 936; c: S. 938-939.

[57] Martin Glinz: Spezifikation von Anforderungen, S. 96.

3.3 Grundbegriffe in der funktionalen Sicherheit

Bei der Durchführung von sicherheitsorientierten Systemanalysen spielen die Begriffe „Fehler“, „Gefährdung“ und „Risiko“ eine wichtige Rolle. Um ihre Abstraktheit ein wenig zu reduzieren, werden sie deshalb mit diesem Unterkapitel in knapper Weise erklärend beschrieben.

Fehler

Der allgemeine Fehlerbegriff ist vielseitig. So finden sich beispielsweise in der englischen Sprache mehrere Worte für *Fehler*. Das englische Wort *fault* steht im Deutschen für die Fehlerursache und beschreibt einen Auslöser für einen Fehlerzustand. Ein Fehlerzustand, im Englischen *error* genannt, ist ein Systemzustand, der für einen Ausfall oder eine Fehlerauswirkung verantwortlich ist. Diese Fehlerauswirkungen oder Ausfälle, englisch *failures* genannt, stellen Abweichungen zwischen dem erbrachten und dem erwarteten Systemzustand dar. Der genauere Zusammenhang dieser Begriffe besteht hier also wie folgt: Eine Fehlerursache in einer Systemkomponente erzeugt einen Ausfall, der im Gesamtsystem einen Fehlerzustand hervorruft.[58a]

Für eine einfache kategorisierte Betrachtung von Fehlern bietet sich eine Unterscheidung nach ihrer Ursache an. Häufige Fehlerursachen liegen im Entwurf, in mangelhafter Spezifikation, in der Implementierung, Dokumentation, Herstellung, im Betrieb, in Störungen, Verschleiß oder anderen physikalischen Zusammenhängen. Auch in der Bedienung oder Wartung sind häufig Fehler begründet.[58b] Noch einfacher lassen sich Fehler nach ihrem Entstehungsort unterscheiden, beispielsweise in Hardwarefehler und Softwarefehler.[58c]

Gefährdungen

Mit dem Begriff der Gefährdung (englisch: *hazard*) wird Auskunft über das Ausmaß eines möglichen Schadens geliefert. Bei einer Sicherheitsklassifizierung eines Systems unterstützt diese Informationsangabe somit eine Einteilung mit Sicherheitsstufen vorzunehmen.[58d]

Zusätzlich kategorisierend im technischen Bereich, stellt etwa die Norm DIN EN ISO 121-1 verschiedene Gefährdungsarten vor. Mechanische Gefährdungen entstehen durch kinetische Energien von Teilen und Massen, aber auch durch potentielle Energien elastischer Elemente, wie beispielsweise Federn. In strombetriebenen Systemen entstehen elektrische Gefährdungen durch Hochspannung, aber auch durch ungeeignete Isolierung oder chemische Reaktionen bei Kurzschlüssen. Für Menschen bestehen häufig auch thermische Gefährdungen. Berührungen heißer Bauteile, aber auch extreme Umgebungstemperaturen sind hier von Bedeutung. Darüber hinaus entstehen mögliche Gefährdungen durch Lärm. Für Serienprodukte existiert eine weitere Kategorisierung. Gefährdungen durch Schwingungen, wie sie beispielsweise bei handgeführten Maschinen auftreten können, bilden eine dieser Gruppen. Ebenfalls stellen Auswirkungen von Strahlungen, wie Laser- oder Röntgenstrahlen, aber auch elektromagnetische Felder eine mögliche Gefährdungsquelle dar. Ferner gibt es

[58] Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011), a: S. 48; b: S. 48-49; c: S. 49; d: S.44.

Gefährdungen durch Materialien, die produziert oder bei der Produktion verwendet werden. Auch vernachlässigte ergonomische Grundsätze sind eine mögliche Gefährdungsursache. Hier sind generell auch Gefährdungen durch Ausrutschen, Stolpern und Stürzen zu berücksichtigen.[59]

Vereinfachend stellt Ross eine kompakte Kategorisierung nach Gefahrenursachen mit fünf Bereichen gegenüber. An erster Stelle stehen Gefährdungen durch chemische Reaktionen (1). An zweiter Stelle folgen Gefährdungen elektrischen Ursprungs (2) durch hohe Ströme und Spannungen. Ebenfalls führt er Gefährdungen durch Strahlungen (3) auf. Überhitzung, Verbrennung, Feuer und Rauch fasst er unter dem Begriff thermischer Gefährdungen (4) zusammen. Zuletzt schließt er mit der Kategorie kinetischer Gefährdungen (5) die Auswirkungen von Deformationen, Bewegungen und beschleunigten Massen ein.[60]

Risiken

Eine Risikoangabe liefert allgemein eine kombinierte Information über die Eintrittswahrscheinlichkeit eines gefährlichen Ereignisses und das dabei zu erwartende Schadensausmaß.[61] Die Akzeptanz für Risiken scheint grundsätzlich mit dem einhergehenden persönlichen Nutzen verknüpft zu sein.[62a] Im Bereich automatisierter Fahrzeuge ist sie darüber hinaus auch von der jeweils betrachteten Zielgruppe abhängig. So ist aus Sicht der gesamten Gesellschaft, nicht das Schicksal einzelner Personen, sondern vielmehr die gesamte Unfallquote von Bedeutung.[62b]

Für erste Risikozuordnungen genügt oft eine grobe Unterscheidung zwischen geringen und großen Risiken. So werden Scheingenauigkeiten vermieden. In anschließend umfangreicheren Untersuchungen lassen sich weitere Gruppen bilden, beispielsweise mit A-, B- und C-Risiken. Dabei bietet es sich besonders an, eine Kategorie für nicht tolerierbare Risiken zu bilden. Diese Kategorie, die beispielsweise Bedrohungen von Menschenleben enthält, erfährt anschließend besondere Berücksichtigung, wodurch sich enthaltene Gefährdungen verhindern lassen.[63] Erweiterte Risikobetrachtungen schließen neben der Eintrittswahrscheinlichkeit und dem Schadensausmaß ergänzend die Kontrollierbarkeit von auftretenden Gefährdungen ein. Abhängig von vorhandenen Möglichkeiten zur Einflussnahme, erfolgt so eine Zuordnung in höhere oder niedrigere Risikoklassen.

Nach üblicher Vorgehensweise werden aus Risikobewertungen Sicherheitsmaßnahmen abgeleitet, um mögliche Lücken zwischen vorhandenen und akzeptierten Risiken zu überbrücken. Im automobilen Kontext erfolgt deswegen für elektrische oder elektronische Sicherheitsmechanismen eine ASIL (*Automotive Safety Integrity Level*) Bewertung. Risikobewertungen sind damit grundsätzlich von der

[59] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), S. 157–158.

[60] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 38.

[61] Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011), S. 43.

[62] Junietz, P. et al.: Macroscopic Requirements for Automated Driving (2019), a: S. 3; b: S.6.

[63] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), S. 46.

eingesetzten Technologie beeinflusst. Beispielsweise lassen sich für E/E-Systeme durch alternativen Einsatz hydraulischer Sicherheitsmechanismen niedrigere ASIL Bewertungen erzielen.[64]

Nutzer automatisierter Fahrzeuge tragen Risiko üblicherweise nur in einer passiven Rolle. Aus Herstellersicht muss das Ausmaß des zu tragenden Risikos jedoch für alle betroffenen Parteien in einem verträglichen Rahmen gehalten werden.[65a] Bei Untersuchungen autonomer Fahrzeuge lassen sich Fahrzeug, Passagier und Verkehrsteilnehmer als soziotechnisches System betrachten. Drei Risikoebenen lassen sich in dessen Betrieb unterscheiden. An erster Stelle steht hier das innere Systemverhalten. Von dem System wird in allen Betriebsszenarien sicheres Arbeiten erwartet. Dafür muss der innere Systemzustand und der dynamische Fahrzustand in Zusammenhang mit der Verkehrssituation betrachtet werden. Weder Passagiere noch Verkehrsteilnehmer sollen durch das Fahrzeug gefährdet werden. Zweitens entstehen Risiken im Zusammenspiel zwischen Fahrzeug und Umfeld. Eine Vollbremsung des Fahrzeugs könnte beispielsweise eine gefährliche Halteposition des Fahrzeugs zur Folge haben. Deswegen berücksichtigt die Sicherheitsdefinition für das Fahrzeug nicht nur innere Systemzustände und dynamische Fahrzustände mit der aktuellen Verkehrssituation, sondern auch mögliche Konsequenzen von denkbaren Zukunftsentscheidungen. Zuletzt entstehen Risiken auch aus mangelhafter Funktionserfüllung von Fahrzeugkomponenten. Ausfälle von Bestandteilen oder Subsystemen schaffen Unsicherheiten für das Gesamtsystem.[65b]

Eine Zuordnung der für die Testentwicklung des Dynamikmoduls gesammelten Anforderungen nach verschiedenen Sicherheitszielen, schafft hier eine gewisse Kategorisierbarkeit. Anforderungen lassen sich damit auch nach den hier beschriebenen Risikoebenen unterscheiden. Je nach verknüpftem Sicherheitsziel stehen verletzte Anforderungen direkt mit der Gefährdung einer Person in Verbindung oder indirekt über resultierende Konsequenzen. Genauere Beschreibung dieser Sicherheitsziele erfolgt im Kontext der Testentwicklung in Abschnitt 5.2. Neben der Zuordnung von Anforderungen dienen sie auch als Ausgangspunkt für die in 4.2 beschriebene Fehlerbaumanalyse.

3.4 Tests in der Entwicklung

Verifikation und Validierung

Bei der Entwicklung technischer Systeme für autonomes Fahren, spielen Sicherheitsanforderungen eine wichtige Rolle. Deswegen sind in allen Phasen der Entwicklungsprozesse Methoden und Maßnahmen erforderlich, die qualitative Aussagen über die Sicherheit der entwickelten Systeme erlauben. So wird für Entwicklungsvorhaben häufig das V-Modell herangezogen. Das Entwicklungsmodell existiert generell in mehreren Varianten, neben anderen somit auch für den automobilen Bereich.[66] Ursprünglich stammt der Entwicklungsstandard aus der IT-Branche, wobei die erste Version aus dem

[64] Ross, H.-L.: Functional Safety for Road Vehicles (2016), S. 86–90.

[65] Reschka, A. et al.: System-Wide Functional Safety (2018), a: S. 126; b: S. 126.

[66] Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011), S. 8.

Jahr 1992 inzwischen mehrfach weiterentwickelt wurde.[67a] Wie Abbildung 3-2 im Anschluss zeigt, veranschaulicht das V-Modell die Arbeitsschritte in einem strukturierten Entwicklungsprozess.[67b]

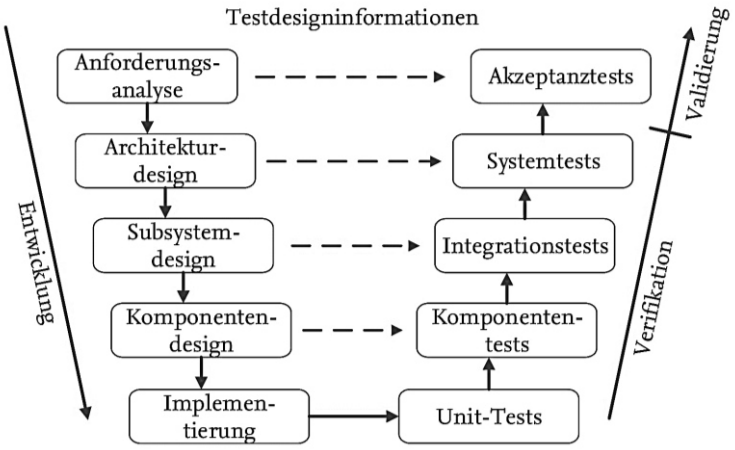

Abb. 3-2: Entwicklungsprozess im V-Modell[68a]

Tests haben hier einen besonderen Stellenwert. Auch wenn die verwendeten Bezeichnungen für Testtypen variieren, unterscheidet man mit zunehmender Abstraktion generell Modultests (in der Abbildung 3-2 von Schuldt als Unit- und Komponententests abgebildet), Integrationstests, Systemtests und Abnahmetests. Die ersten drei werden dem Bereich der Verifikation zugeordnet, wobei abschließende Abnahmetests der Validierung dienen. Getestet werden immer die Spezifikationen, die auf der jeweils gegenüberliegenden Seite des V-Modells bereits entwickelt wurden.[67c]

Als Ergebnis von Verifikationsprozessen stehen allgemein Auskünfte über die Erfüllung der zuvor formulierten Anforderungen. So liefert die Verifikation eine Aussage darüber, ob das System entsprechend seiner Anforderungsspezifikation *richtig* entwickelt wurde.[68b] Bei der abschließenden Validierung wird untersucht, ob das entwickelte System mit seinen formulierten Anforderungen für einen bestimmten Gebrauch geeignet ist. Das heißt es wird überprüft, ob das *richtige* System für die vorgesehene Anwendung entwickelt wurde.[68c]

Voraussetzungen für die Validität eines Fahrzeugsystems entstehen aus verschiedenen Bereichen. Der alltägliche Gebrauch des Fahrzeugs erfordert einen sicheren Umgang des Fahrers und anderer Personen mit den fahrzeugspezifischen Funktionen und Eigenschaften. Möglichen Missbrauch und unsachgemäßen Gebrauch gilt es zu verhindern. Gesetzliche Bestimmungen verlangen die Funktionalität von Schutzfunktionen wie ABS, Airbag und weiteren Subsystemen. Unzureichende Leistungen und Funktionalitäten gilt es daher in verschiedenen Bereichen zu untersuchen. Im automobilen Kontext kommen der Aktorik, Systemleistung, Sensorik und der Algorithmik besonderes Gewicht zu. Aber auch die Eignung eingesetzter Schnittstellen ist von Bedeutung.

Eine ausreichend gesicherte Verfügbarkeit sicherheitsrelevanter Funktionen wie Bremsen und Lenken ist grundsätzlich erforderlich. Das gilt gleichermaßen für alle daran beteiligten Systeme,

[67] Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011), a: S. 38; b: S. 8; c: S. 39.

[68] Schuldt, F.: Dissertation, Test automatisierter Fahrfunktionen (2016), a: S. 55; b: S. 23; c: S. 24.

Sensoren, Aktuatoren. Deren Untersuchungen schließen alle logischen Zustände, Betriebszustände, und Verkehrssituationen ein. In modernen Fahrzeugen mit umfangreicher E/E-Architektur werden alle Systembestandteile berücksichtigt. Auch Geometrien, falsche Verbauung im Fahrzeug oder fehlerhafte Integration werden behandelt. Die Umgebung liefert mögliche Einflüsse in Form von elektromagnetischen Effekten, möglicher Überspannung oder starken Strömen aber auch verschiedenen Temperaturen. Resultierend sind Störungen der Sensorik denkbar. Alle unerwarteten Systemeinflüsse, auch in verschiedenen Ereigniskombinationen, spielen eine mögliche Rolle. Zusätzlich bestimmen zeitliche Vorgaben die geforderten Systemreaktionsfähigkeiten und angemessen rechtzeitigen Aktionen.[69]

Allgemeines Testvorgehen

Effektives und effizientes Testen erfordert ein systematisches Vorgehen. Angemessene Testabdeckung ist erwünscht, wobei mehrfache Testdurchführung prinzipiell vermieden wird. Deswegen werden Verantwortlichkeiten für einzelne Tests oft verteilt. Das Testen einzelner Elemente findet meistens schon bei ihren jeweiligen Zulieferern statt.[70a] Anschließende Integrationstests kontrollieren das Zusammenwirken der eingesetzten Komponenten und Teilsysteme. Sie weisen nach, ob die gemeinsamen Funktionen im Zusammenwirken korrekt ausgeführt werden. Dafür werden Schnittstellen der einzelnen Komponenten untersucht und auch Softwarefehler finden Berücksichtigung.[71] Üblicherweise stehen Systemtests an vorletzter Stelle im Testprozess. Dabei kommen häufig Black-Box-Testmethoden zum Einsatz. Das heißt anhand der vorhandenen Spezifikationen werden nur Eingangs- und Ausgangsdaten untersucht, ohne die innere Struktur des Systems zu beachten. Primäres Ziel der Systemtests ist das Aufdecken unvorhergesehener Fehler, die aus der Systemintegration oder unklar formulierten Anforderungen resultieren. An abschließender Stelle im Testprozess stehen Abnahmetests. Anders als in den vorherigen Stufen ist hier eine Validation das Ziel der Tests. Ein Abnahmetest stellt in einzelnen Fällen somit auch den Freigabetest eines Systems dar.[72]

Alle Tests untersuchen grundsätzlich gleichermaßen, ob ein Produkt in der Lage ist, die spezifizierten Eigenschaften unter gestellten Bedingungen zu erfüllen. Problematisch ist dabei oft die begrenzt verfügbare Zeit für das Testen. Auch sind Produktspezifikationen grundsätzlich unvollständig. Ein Nachweis *vollständiger Korrektheit* ist so in der Realität nicht umsetzbar. Allerdings lässt sich die Anzahl vorstellbarer Fehler minimieren, indem durch das Testen möglichst viele Unzulänglichkeiten entdeckt werden.[70b]

In einem allgemeinen Testprozess, werden zuerst vorbereitend relevante Informationen ermittelt und notwendige Gerätschaften bereitgestellt. Grundlagen dieser Testvorbereitung bildet oft ein Lastenheft, das gewünschte Produkteigenschaften spezifiziert. Davon ausgehend werden konkrete Testziele abgeleitet. Bei der Bestimmung dieser Ziele erfahren Fehlerarten und -bereiche häufig zusätzlich eine

[69] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 389–390.

[70] Baumann, G.: Was verstehen wir unter Tests? (2006), a: S. 6; b: S. 3-4.

[71] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), S. 294.

[72] Schuldt, F.: Dissertation, Test automatisierter Fahrfunktionen (2016), S. 57.

Priorisierung. Im nächsten Schritt wird das angewendete Testverfahren bestimmt und die Testausrüstung vorbereitet. Um die Testergebnisse später zu bewerten ist außerdem eine Referenz notwendig. Dafür wird üblicherweise eine Testreferenz (auch Orakel genannt) definiert, die für jeden Eingabewert die korrekte Ausgabe mit Soll- und Grenzwerten liefert. Anschließend werden die Testfälle mit einzelnen Durchführungs- und Auswertungsvorschriften bestimmt. Jeder Anforderung des Lastenhefts wird dafür im gesamten Testvorgehen mindestens ein Testfall zugeordnet. Bei jeder Testdurchführung ist ein initialisierter und bekannter Anfangszustand wichtig. Ist dieser Zustand vorhanden, werden die Eingänge des Systems mit Signalen bespielt. Reaktionen und Auswirkungen werden daraufhin an entsprechender Stelle am Prüfgegenstand gemessen oder beobachtet. Die abschließende Phase beschäftigt sich mit der Auswertung dieser Beobachtungen. Ein Vergleich zwischen Messwerten und der Referenz wird gemäß definierter Vergleichsvorschrift durchgeführt. Daraus ergibt sich ein klares Ergebnis (Test bestanden oder nicht bestanden) mit weiteren Informationen über Art und Umfang der erzielten Abweichung. Diese Ergebnisse werden anschließend in einem Testbericht eingetragen und dokumentiert.[73a] Grundlage für die Definition von Testendekriterien, den zu erfüllenden Voraussetzungen für einen Testabschluss, liefern häufig Systemtestfälle, welche die Funktionalität prüfen. Oft lassen sich diese direkt aus den Systemanforderungen ableiten.[74a]

Die Definition von Testfällen beinhaltet dabei keine Wertung. Es findet ein reiner Vergleich zwischen Ist- und Sollverhalten statt. Ein Ergebnis heißt demzufolge "bestanden" oder "nicht bestanden". Nicht-Bestehen weist somit nicht unbedingt auf eine mangelhafte Sache hin. Es kann auch auf zu hohe Erwartungen, ungünstige Rahmenbedingungen oder fehlerhafte Ausrüstung zurückzuführen sein.[73b] Die jeweils zulässigen Werte sind grundsätzlich abhängig von dem Aufbau des gesamten Fahrzeugsystems. Auch die Funktion und Leistungsfähigkeit anderer Module haben einen Einfluss. Deswegen besteht bei der Definition von Bestehens- und Versagenskriterien ein starker Bezug auf zuvor festgelegte Anforderungen und technische Spezifikationen.[75a] Zunächst genügt für diese Kriterien eine rein qualitative Beschreibung wie "fehlerhaft". Für eine genaue Testauswertung sind jedoch zugehörige Metriken für untersuchte Werte notwendig. Diese Werte können extern und intern vorliegen. Darüber hinaus sind dafür neben den erzielten Ausgangsdaten auch Werte in vorhandenen Schnittstellen von Interesse.[75b]

In der Praxis existieren grundsätzlich mehr Testfälle als Anforderungen.[74b] Deswegen ist es naheliegend bei der Entwicklung von Tests gewisse Kriterien zu beachten. Diese lassen sich in Effektivitäts- und Effizienzanforderungen kategorisieren. Für ein effektives Vorgehen sind Tests (1) repräsentativ, (2) variierbar, (3) beobachtbar. Repräsentative Tests schließen durch Vereinfachungen der Realität keine relevanten Aspekte aus. Verschiedene mögliche Gegebenheiten werden hinreichend detailliert untersucht. Variierbar definierte Testfälle lassen sich in der Durchführung auch mit kleinen Veränderungen umsetzen. Dabei sind alle entscheidenden Parameter für eine Auswertung beobachtbar. So liefert ein klares Ergebnis Auskunft über das Bestehen oder Nicht-Bestehen des Tests. Zusätzlich

[73] Baumann, G.: Was verstehen wir unter Tests? (2006), a: S. 4–5; b: S.3.

[74] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), a: S. 18; b: S. 32.

[75] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), a: S. 10; b: S. 9-10.

werden Tests (4) ökonomisch, (5) reproduzierbar, (6) frühzeitig, (7) sicher und damit effizient durchgeführt. Eine ökonomische Testdurchführung erfolgt schnell, gut vorbereitet und kostengünstig. Jeder Test ist reproduzierbar. Dadurch ist beispielsweise der Aufwand für Regressionstests minimiert. Nach einem erkannten Fehler können in gleichem Szenario direkt weitere Tests folgen. Frühzeitig im Entwicklungsprozess werden Fehler gesucht. Korrekturen sind damit ohne viele zusätzliche Entwicklungsschritte umsetzbar. Für eine sichere Durchführung wird das akzeptierte Risiko der Testbeteiligten konsequent eingehalten. Das ist vor allem bei realen Testfahrten relevant.[76]

Ganz im Sinne einer effizienten Vorgehensweise, kommen beim Testen vermehrt Simulationsumgebungen zum Einsatz. So ist eine Durchführung mehrerer Testfälle parallel und schneller als in Echtzeit möglich. Die Elemente einer Simulation sind außerdem deterministisch. Kosten und Zeitaufwand lassen sich damit durch die Anzahl durchgeführter Testfälle begrenzen.[77] Eine Simulation stellt dafür eine durch Abstraktion vereinfachte Nachbildung des untersuchten Systems dar. So liefert sie ein Modell für Experimente und die Untersuchung relevanter Eigenschaften. Damit gesammelte Erkenntnisse lassen sich anschließend auf das reale System übertragen.[78] Finden Tests mit einem geschlossenen Regelkreis statt, handelt es sich um ein *Closed-Loop*- oder auch *In-the-Loop*-Verfahren.[79a] Im Gegensatz sind *Open-Loop*-Tests vor allem für reaktive Systeme geeignet, die nicht in Regelkreise mit kurzen Zeitkonstanten eingebunden sind. Damit lassen sich beispielsweise viele Systeme der Innenraum- und Karosserieelektronik mit einfachen Mitteln testen. Sind allerdings schnellere Regelungen von Bedeutung, gilt es *Closed-Loop*-Tests zu bevorzugen. Dies trifft insbesondere auf Schlupf- und Fahrdynamikregelungen zu. Erzielbare Testergebnisse hängen hier stark von der Qualität des Streckenmodells ab. Deswegen muss je nach Art des untersuchten Streckenmodells abgewogen werden, ob aufwendiges Testen mit einer hochwertigen Echtzeit-Simulation gerechtfertigt ist, oder ob Tests durch frühe Fahrversuchen eine Alternative darstellen.[79b]

In höheren Teststufen kommen auch häufig Black-Box-Methoden zum Einsatz. Diese untersuchen Eingangs- und Ausgangsparameter, ohne dabei innere Strukturen der Teilsysteme zu berücksichtigen.[80] Besonders in Fällen, in denen die inneren Zusammenhänge des Prüfgegenstands unvollständig vorhanden sind, bietet sich ein solches Vorgehen an. Grundsätzlich werden die Eingangsschnittstellen des Prüfgegenstands mit Signalkombinationen beaufschlagt. Resultierende Ausgangssignale lassen sich anschließend bezüglich ihrer Plausibilität beurteilen. Die Menge möglicher Eingangssignalkombinationen ist meistens sehr hoch, weshalb oft eine stichprobenartige Durchführung stattfindet.[79c]

[76] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 447–448.

[77] Schuldt, F. et al.: Test Case Generation for DAS (2018), a: S. 152.

[78] Schuldt, F.: Dissertation, Test automatisierter Fahrfunktionen (2016), S. 17.

[79] Baumann, G.: Was verstehen wir unter Tests? (2006), a: S. 11–12; b: S. 14; c: S. 9-10.

[80] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), S. 295.

4 Methodische Testentwicklung

Mit der modularen Betrachtungsweise des Forschungsprojekts UNICAR*agil* lässt sich der Testaufwand durch die Betrachtung einzelner Subsysteme möglicherweise reduzieren. Um dabei möglichst vollständig testbare Fehlerursachen aufzufinden, schlagen Lippert et al. einen kombinierten Methodeneinsatz vor. Durch die Verknüpfung unterschiedlicher Herangehensweisen ließen sich Fehlerursachen in hoher Vollständigkeit ermitteln.[81] Daher werden Informationsgrundlagen für die Testentwicklung dieser Arbeit mit den gesammelten Ergebnissen verschiedener Systemanalysen gebildet. Deren Ursprung und Herangehensweise, aber auch ihre ergänzenden Eigenschaften, werden im nachfolgenden Kapitel erklärt. Zum Abschluss ergänzen allgemeingültige Bemerkungen über Testfalldefinitionen und strukturierende Maßnahmen den methodischen Werkzeugkasten, den dieses Kapitel für die Testentwicklung des Dynamikmoduls darstellt.

4.1 Ausgangspunkt: Sicherheitsnormen

Eine allgemeine Vorgehensweise für eine nachweisliche Erreichung von Sicherheitszielen ist in der Norm DIN EN 61508 beschrieben und kommt auch in anderen Normen vergleichbar zur Anwendung. Vorgesehen ist darin die Durchführung einer Risikoanalyse und die Spezifikation von Sicherheitszielen. Sie verlangt außerdem das Erkennen und Beherrschen von Fehlern durch zufällige Hardwareausfälle. Systematische Fehler gilt es durch bestimmte Analysen, Entwurfsmethoden und Testverfahren zu vermeiden. Auch das Erbringen eines Sicherheitsnachweises ist vorgesehen.[82a] Im Gegensatz zu der Norm DIN EN 61508 stellt die ISO 26262 viele Aspekte noch detaillierter, praxistauglicher und eigenständiger dar.[82b] So liefert sie auch Richtlinien für das Testvorgehen. Beispielsweise sieht sie ein Testkonzept vor, in dem Systemanforderungen, Testziele, Teststufen und Testplattformen festgelegt sind.[83] Hier stellt die Spezifikation verwendeter Eingangsdaten allgemein eine große Aufgabe in der Testfallerstellung dar. Parameter, die das untersuchte Objektverhalten bestimmen, enthalten zeitliche Verläufe und es dürfen keine widersprüchlichen Vorgaben gesetzt werden.[84a]

Die Norm ISO 26262 bietet Rahmenbedingungen für den gesamten Entwicklungsprozess von sicherheitskritischen elektrischen und elektronischen Systemen. Damit liefert sie auch Anhaltspunkte zur funktionalen Sicherheit bei der Entwicklung automatisierter Fahrzeugsysteme.[84b] In 10 Abschnitten liefert sie Richtlinien und Hilfestellungen für die sicherheitsbezogene Produktentwicklung im automobilen Bereich. Sieben dieser Abschnitte (3 bis 9) beschreiben Sicherheitsaktivitäten. Abschnitt 3 bezieht sich auf das Vorgehen während der Konzeptphase. Dabei wird eine genaue Beschreibung des Entwicklungsgegenstands und die HARA (*Hazard and Risk Assessment*) empfohlen. So entstehen klare Sicherheitsziele für Risiken, die nach ASIL (*Automotive Safety Integrity Levels*) bewertet werden. In Abschnitt 4 werden Anforderungen auf Ebene des Gesamtsystems festgelegt. Diese

[81] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 9.

[82] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), a: S. 324; b: S. 150.

[83] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), S. 102.

[84] G. Bagschik et al.: Entwicklung, Absicherung & Test automatisierter Fahrzeuge (2017), a: S. 129; b: S. 125-126.

Anforderungen werden mit den Abschnitten 5 und 6 auf Hard- und Software-Ebene erweitert. Bei der Entwicklung zusätzlicher Anforderungen für Produktion, Betrieb, Wartung und Entsorgung unterstützt Abschnitt 7. Weitere begleitende Prozesse liefert Abschnitt 8. Die Risikobewertung nach ASIL ist in Abschnitt 9 beschrieben.[85]

Bei einer Entwicklung nach der Norm wird der Entwicklungsgegenstand also schon vor der technischen Entwicklung in der Konzeptphase definiert (englisch: *item definition*). Nach ersten Sicherheitsüberlegungen erfolgt eine Gefährdungsanalyse mit Risikobewertung. Aus diesen Ergebnissen wird dann ein funktionales Sicherheitskonzept erstellt. Dabei geht die Beschreibung des entwickelten Gegenstands auf funktionale Zusammenhänge, Systemgrenzen, Einsatzgebiete, rechtliche Rahmenbedingungen und auch auf Abhängigkeiten zu angrenzenden Entwicklungsgegenständen ein.[86]

HARA: Gefahrenanalyse mit Risikobewertung

Die Gefahrenanalyse mit Risikobewertung der Norm ISO 26262 dient der Identifikation und Kategorisierung von Gefahren, die durch Fehlverhalten eines untersuchten Gegenstands verursacht werden können. Im Englischen wird sie *Hazard and Risk Assessment* genannt, nachfolgend also kurz: HARA.

Mit dieser Methode ermittelte Gefahren werden mit Risiken nach *Automotive Safety Integrity Levels* (ASIL) bewertet. Dabei fließen Einflussfaktoren wie deren Schwere, ihre Wahrscheinlichkeit und deren Kontrollierbarkeit ein. Grundlage hierfür ist allein das funktionale Systemverhalten. Deswegen ist eine genaue Kenntnis des untersuchten Gegenstands nicht zwingend dafür notwendig.[87]

Als Informationsbasis dafür liefert die *item definition* Angaben zu den beabsichtigen Funktionen und Eigenschaften. Auch Annahmen über die Systemarchitektur, Grenzen, Einschränkungen und Angaben zum Anwendungsbereich sind darin von Bedeutung. Ebenfalls die vorgesehene Handhabung und das Anwendungsprofil werden eingeschlossen.[88]

Die HARA beschäftigt sich also in einem Teilbereich mit Situationsanalysen und Gefährdungsidentifikation. In dem zweiten Teilbereich erfolgt eine Klassifikation von gefährlichen Ereignissen. In Rahmen der Situationsanalyse werden alle Betriebssituationen und -zustände, in denen Fehlverhalten zu Schäden führen kann, identifiziert. Jedes Verhalten, das nicht dem definierten funktionalen Sollverhalten entspricht, gilt als fehlerhaft. Erkannte gefährliche Szenarien werden mit dem Sicherheitsintegritätslevel für Automobile bewertet (ASIL). In diese Bewertung nehmen Auftrittswahrscheinlichkeit, mögliches Schadensausmaß und die Beherrschbarkeit Einfluss.

Die formelle Vorgehensweise bei der Durchführung einer HARA lässt sich in sechs Arbeitsschritte gliedern. Zunächst werden funktionale Zusammenhänge einer Gegenstandsbeschreibung entnommen. Anschließend werden mögliche Fehler identifiziert und denkbare Gefährdungen ermittelt. Ermittelte Fehler und Gefährdungen werden anschließend kombiniert in Form von Gefahrensituationen

[85] Abdulkhaleq, A. et al.: STPA Compliance with ISO 26262 (2017), S. 13.

[86] G. Bagschik et al.: Entwicklung, Absicherung & Test automatisierter Fahrzeuge (2017), S. 127.

[87] Ross, H.-L.: Functional Safety for Road Vehicles (2016), S. 81.

[88] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 202.

formuliert. Daraufhin erfolgt deren Bewertung und Klassifizierung nach ASIL. Abschließend werden aus den Ergebnissen konkrete Sicherheitsziele abgeleitet.[89a]

Insgesamt definiert die Norm ISO 26262 mehr als 100 Begriffe im Kontext der funktionalen Sicherheit. Als Gefährdung gelten alle möglichen Schadensursachen. Die Norm geht hier davon aus, dass Gefährdungen durch Fehler verursacht werden. Gefahrensituationen bilden immer eine Kombination aus einer Betriebssituation mit einer vorhandenen Gefahr. Betriebssituationen sind dabei alle Situationen, die im Lebenszyklus des Fahrzeugs vorkommen können. Die hier betrachteten Fehler entstehen durch Systemversagen oder ein ungewünschtes Systemverhalten.[89b]

Grundsätzlich beziehen sich die ermittelten Sicherheitsziele jeweils nicht nur auf eine Gefahr. Auch mehrere Gefahren können unter einem Ziel berücksichtigt werden. Insofern bietet sich die allgemeine Formulierung *„Vermeide Fehlfunktionen, die zu einer Gefährdung führen können“* an, ohne dabei weitere Angaben der potentiellen Gefahr zu nennen.[90] Allgemein formulierte Sicherheitsziele sind laut ISO 26262 prinzipiell kein Problem. Bei der Integration von Komponenten und Subsystemen sorgen sie jedoch möglicherweise für Verwirrung.[91] So beinhaltet jeder Steuerbefehl grundsätzlich zwei Sicherheitsziele. Erstens muss jede Steueraktion ausgeführt werden, wenn sie für einen sicheren Betrieb erforderlich ist. Zweitens darf eine Steueraktion nur dann ausgeführt werden, wenn sie für den sicheren Betrieb erforderlich ist. Der Begriff "erforderlich" gilt in diesem Zusammenhang sowohl auf logischer als auch auf zeitlicher Ebene.[92]

Ergebnisse der Risikoanalysen werden üblicherweise in einem Sicherheitsplan zusammengefasst. Eingeschlossen werden dabei anzuwendende (interne) Richtlinien, verantwortliche Personen und Abteilungen, Spezifikation und Entwurf des Systems und das geplante Vorgehen zur Verifikation und Validierung inklusive Abnahmekriterien. Auch anzuwendende Verfahren und Prozeduren werden erwähnt. Es erfolgen geplante Vorkehrungen für bestimmte Betriebsarten, wie beispielsweise Anlaufen nach Anhalten, Wiederanlauf nach Unterbrechungen oder nach Stillsetzen im Notfall. Fehler werden eindeutig angezeigt. Auch Maßnahmen zur Verhinderung unerwarteter Befehle, die möglicherweise zu gefährdendem Maschinenverhalten führen, werden beschrieben.[93] Resultierende Arbeitsergebnisse werden üblicherweise nicht veröffentlicht. Deswegen finden sich in wissenschaftlicher Literatur, auch auf dem Gebiet der Fahrzeugautomation, nur wenige Praxisbeispiele.[89c]

[89] Stolte, T. et al.: HARA for Automated Unmanned Vehicle (2017), a: S. 1849; b: S. 1849; c: S. 1848.

[90] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 214.

[91] Ross, H.-L.: Functional Safety for Road Vehicles (2016), S. 91.

[92] Stolte, T. et al.: Safety goals and functional Safety (2016), S. 2194.

[93] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), S. 160–162.

Testbegriff der ISO 26262

Für die Planung von Verifikationsaktivitäten sieht die Norm verschiedene Teilaufgaben vor. Beschreibungen definieren die abzusichernden Gegenstände, absichernde Methoden (Simulationen, Tests, …), dabei geltende Bestehens- und Versagenskriterien, die eingesetzte Umgebung (Simulations- oder Testumgebung) und eingesetzte Werkzeuge. Neben diesen Beschreibungen werden außerdem Maßnahmen für entdeckte Anomalien und auch Abschlussaktivitäten geplant. Die Angemessenheit der verwendeten Methoden und die Komplexität des untersuchten Gegenstands werden darin berücksichtigt. Wichtiger Ausgangspunkt hierfür sind bereits vorhandene Erkenntnisse. Bei allen Arbeitsschritten wird darüber hinaus der Reifegrad der eingesetzten Technologien mit eventuell verbundenen Risiken bedacht.[94a] Damit erfolgen neben einer Beschreibung der Testumgebung auch Angaben zu logischen und zeitlichen Abhängigkeiten und den eingesetzten Ressourcen.[94b] Eine Testspezifikation in Anlehnung an die ISO 26262 sieht insbesondere gewisse Informationsangaben vor, die nachfolgend knapp beschrieben sind. Erstens sorgt eine einzelne Identifikation für jeden Testfall für eine gewisse Nachvollziehbarkeit. Außerdem wird die Version des betrachteten Gegenstands grundsätzlich angegeben. Einzelne Startbedingungen und Konfigurationen sind enthalten. Auch beeinflussende Umweltbedingungen sind dokumentiert. Einzuspielende Eingangsdaten werden mit zeitlicher Abfolge und Wertangaben beschrieben. Dem steht das erwartete Systemverhalten, mit Ausgangsdaten und akzeptierten Ausgangswerten, Zeitverhalten und tolerierten Verhaltensweisen gegenüber. Hier schaffen genau definierte Initialwerte die Vergleichbarkeit für erzielte Ausgangswerte. Redundante Datenspeicherung lässt sich hier durch die Verwendung von eindeutigen Referenzbezeichnungen für Startbedingungen, Konfigurationen und Umweltbedingungen vermeiden.[94c]

4.2 Methoden für eine HARA nach ISO 26262

Das Vorgehen bei der Ermittlung von Risiken automatisierter Fahrzeuge wird wissenschaftlich nach wie vor diskutiert. Für das Auffinden möglicher Fehlverhalten bieten sich grundsätzlich mehrere Techniken an. Der Sicherheitsstandard der Norm ISO 26262 stellt allgemein neben anderen Methoden den Einsatz einer FMEA (*Failure Mode and Effects Analysis*) vor. [95] Darüber hinaus erwähnt sie die Fehlerbaumanalyse (FTA), Ereignisbaumanalyse (ETA) und die HAZOP Analyse (*Hazard and Operability*). Zusätzlich werden Markov Modelle und Zuverlässigkeitsblockdiagramme erwähnt.[94d] Die einzelnen Methoden werden nachfolgend vorgestellt. Im weiteren Vorgehen verarbeitete Ansätze werden dabei ausführlicher beschrieben. So wird ebenfalls die Risikobewertung nach *Automotive Safety Integrity Levels* (ASIL) kurz erklärt.

[94] Ross, H.-L.: Functional Safety for Road Vehicles (2016), a: S. 225; b: S. 227; c: S.226; d: S. 124-125.

[95] Stolte, T. et al.: Functional Safety of Vehicle Actuation (2016), S. 577.

FMEA: Fehlermöglichkeits- und Einflussanalyse

Die FMEA (englisch: *Failure Mode and Effects Analysis*) wird im deutschen auch Fehlermöglichkeits- und Einflussanalyse genannt. Sie findet ihren Einsatz häufig in frühen Gestaltungsphasen von Systemen oder Produkten, um mögliche Schwierigkeiten frühzeitig zu entdecken. Einschränkungen der Sicherheit oder auch der Leistungsfähigkeit lassen sich so schon in der Gestaltung minimieren.[96] Frühe bekannte Einsatzbeschreibungen der FMEA existieren seitens der NASA, mit Analysen des Projekts Apollo, bereits aus dem Jahr 1963.[97] Seit 1980 ist die Methode der FMEA auch in der DIN 25 448 unter der Bezeichnung "Ausfalleffektanalyse" genormt.[98]

Als Bottom-Up Analysemethode leitet die FMEA aus möglichen Fehlerursachen einzelner Komponenten potentielle Fehlermodi ab. Dabei beginnt sie mit untergeordneten Bauteilen und schließt daraus auf Fehlereffekte des Gesamtsystems. Ein untergeordneter Fehlereffekt wird also zu einem Fehlermodus des übergeordneten Systems. Darüber hinaus berücksichtigt die FMEA Ausmaße, Auftrittshäufigkeiten und Entdeckungswahrscheinlichkeiten um Risikoprioritätsziffern für die einzelnen Fehlermodi zu bestimmen.[99] So lässt sich die funktionale Sicherheit eines Systementwurfs analysieren. Geprüft werden alle möglichen Ausfallquellen des untersuchten Gegenstands mit ihren resultierenden Auswirkungen auf Systemverhalten und -sicherheit. In der Praxis findet sie häufig im Rahmen einer Teamsitzung mit Systemexperten statt. Einzelne Bauteile werden dabei der Reihe nach analysiert und daraus Verbesserungsmaßnahmen ermittelt. So unterstützt die Methode durch Fehlervermeidung die Funktionssicherheit und Zuverlässigkeit von Produkten. Es lassen sich dadurch störungsärmere Serienanläufe, bessere Termintreue oder auch wirtschaftlichere Fertigung erreichen.[100a]

Die Analyse schließt funktionale und nicht-funktionale Anforderungen, inklusive Sicherheitsanforderungen ein. Dafür werden mechanische und elektronische Bauteile in die Betrachtungen einbezogen.[100b] Hierfür übliche Informationsgrundlagen sind Lastenhefte, Pflichtenhefte, Systemkonzepte, Konstruktionspläne, Schaltpläne, Stücklisten aber auch Fertigungs- und Prüfpläne. Ergebnisse der Analysen werden typischerweise in einer Datenbank oder in Tabellenform dokumentiert.[100c] Eine Produktbezogene FMEA untersucht bei Systemfunktionen und Systemschnittstellen mit möglichen Umwelteinflüssen, ob die gestellten Systemanforderungen erfüllt werden können. Ebenfalls einzelne Bauteilfunktionen, -eigenschaften und Bauteilversagen werden untersucht.[100d] Abwandlung der FMEA ist die FMECA (*Failure Modes and Effects and Criticality Analysis*). Sie sortiert entdeckte Fehlermodi zusätzlich nach ihren Ausmaßen und erlaubt so ein Priorisieren der Gegenmaßnahmen. In einer nochmals anderen Variante, der *Failure Mode, Effects and Diagnostic Analysis* (kurz: FMEDA), werden Hardware und Elektroniksysteme auf Bauelement oder Blockschaltebene beurteilt. Wieder liegt der Fokus jedoch auf möglichen Ausfallquellen und daraus denkbaren Auswirkungen.[100e] Alternative Möglichkeiten durch zusätzliche Wahrscheinlichkeitsbetrachtungen, bietet eine

[96] Sulaman, S. M. et al.: Comparison of FMEA and STPA (2019), S. 350.

[97] Ross, H.-L.: Functional Safety for Road Vehicles (2016), S. 115.

[98] Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau (2004), S. 107.

[99] Sulaman, S. M. et al.: Comparison of FMEA and STPA (2019), S. 351.

[100] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), a: S. 263; b: S.264; c: S.264; d: S. 264; e: S. 266 .

probabilistic FMEA. Sie schließt noch einmal formell die Auftrittswahrscheinlichkeiten der einzelnen Fehlermodi in die Analyse ein. Besonders häufige Fehlermodi lassen sich so gesondert untersuchen. Auch eine Variante für Softwareintensive Systeme existiert. Die SFMEA (*Software FMEA*) berücksichtigt softwarespezifische Aspekte somit besonders. Unter anderem fällt darunter die Tatsache, dass Software nicht in traditionellem Sinne versagt, sondern stattdessen eher ungewünschte Verhaltensweisen aufweist.[101a]

Ganz allgemein erfolgt bei der Durchführung einer FMEA nach planender Vorbereitung zunächst eine Strukturanalyse. Danach werden die enthaltenen Funktionen analysiert. Nach der anschließenden Fehleranalyse, werden diese mit Risiken bewertet. Schlussendlich folgen Optimierungsansätze und eine Ergebnisdokumentation.[102] Bertsche und Lechner präsentieren eine Vorgehensweise zur Durchführung einer FMEA in ihrem Buch mit noch detaillierteren Schritten. Am Ende des Vorgehens steht typischerweise eine Ergebnistabelle mit einer baumartigen Struktur, wie sie Abb. 4-1 zeigt.

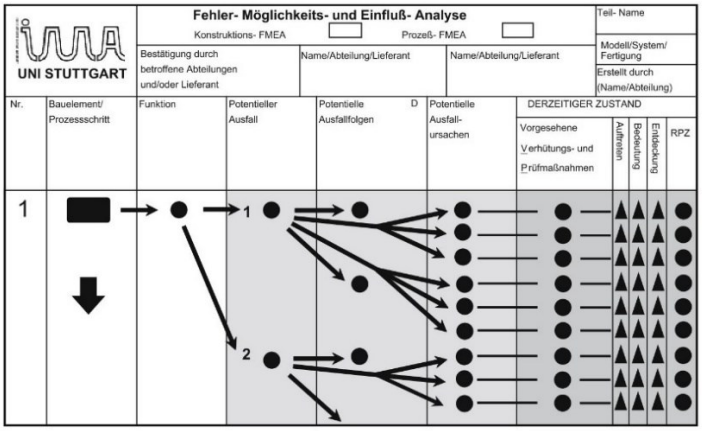

Abb. 4-1: FMEA Formblatt der VDA 86 mit typischer "Baumstruktur"[103]

Das Zurückführen von Fehlereffekten auf immer genau einen Grund schränkt die Nutzbarkeit der FMEA jedoch ein.[101b] Man geht hier grundsätzlich von kausalen Ereignisketten aus, die zu Unfällen führen. So basiert die Methode auf der Annahme, dass ein System sicher betrieben wird, wenn diese Ereignisketten verhindert werden. Aus dieser Perspektive müssten alle denkbaren Fehlerursachen berücksichtigt werden. Allerdings ist deren vollständige Ermittlung vor allem in interaktiven Systemen nahezu undenkbar. Im Übrigen sind die Ergebnisse der üblich eingesetzten Methoden, wie die der FMEA oder auch der *Hazard and Operability Analysis* (kurz: HAZOP-Analyse), stark von vorhandenem Expertenwissen zu ihrer Durchführung abhängig. Von weniger erfahrenen Analysten sind demzufolge andere Ergebnisse zu erwarten. Das lässt sich darauf zurückführen, dass die Methoden auf Brainstorming basieren und an sich eher wenig Verständnis für strukturierte Systemanalysen vermitteln.[104]

[101] Sulaman, S. M. et al.: Comparison of FMEA and STPA (2019), a: S. 351; b: S. 351-352.

[102] Tietjen, T.; Decker, A.: FMEA-Praxis (2020), S. 57.

[103] Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau (2004), S. 113.

[104] Stolte, T. et al.: Functional Safety of Vehicle Actuation (2016), S. 577.

FTA und ETA: Analysen mit Strukturbäumen

Hier stellen Analysen mit Strukturbäumen eine mögliche Ergänzung dar. Der ursprüngliche Hintergrund der FTA (*Fault Tree Analysis*, deutsch auch: Fehlerbaumanalyse) liegt im militärischen Bereich. Anfang der 1960er Jahre wurde die Methodik erstmals von der U.S. Airforce eingesetzt und verbreitete sich von dort aus in andere Gebiete, wie die Luftfahrt und den Nuklearenergiesektor.[105a] Schließlich führte Ford 1977 die Fehlerbaumanalyse, ebenso dynamische Ereignisbäume, in der Automobilindustrie ein.[105b]

Die FTA untersucht anders als die FMEA auch Ausfallkombinationen. Während die FMEA als induktive Methode einen systematisch bewerteten Katalog möglicher Ausfälle liefert, erbringt die FTA deduktiv auch Fehlerketten mit mehreren Komponenten.[106a] Methoden der FMEA eignen sich damit hauptsächlich für Analysen auf Systemebene und Hardwareanalysen, wohingegen sich Fehlerbaumanalysen auch universell für Softwareanalysen einsetzen lassen.[107a] Absicht der FTA Methodik ist das systematische Auffinden aller möglichen Ausfälle und Ausfallkombinationen aus Ursachen, die zu unerwünschten Ereignissen in einem System führen. Sie ermittelt so besonders kritische Ereignisse und Ereigniskombinationen. Dadurch werden zusätzliche objektive Beurteilungskriterien für Systemkonzepte geschaffen und es erfolgt eine übersichtliche Dokumentation von Ausfallmechanismen und funktionalen Zusammenhängen.[106b]

Startpunkte für eine FTA, auch *initiale Ereignisse* genannt, ergeben sich unter anderem aus Sicherheitszielen.[107b] Ein initiales Ereignis führt anschließend zu weiteren Gefährdungen. Diese werden in der Analyse in Form von Zweigen ausgeführt und beschreiben so alle denkbaren Gefahrenursachen. Kombinationen der Ursachen werden dabei mit Logikoperatoren (UND, ODER) vervollständigt. Ein Zweig endet mit der Festlegung von Basisereignissen, denen keine weitere Untersuchung folgt.[107c] So wird eine systematische Vorgehensweise für die Aufstellung eines Fehlerbaums folgendermaßen in der DIN 25424 beschrieben:

1. Das unerwünschte Ereignis wird festgelegt.

2. Ist dieses Ereignis bereits eine Ausfallart einer Komponente, so wird die Vorgehensweise mit Schritt 4 fortgesetzt. Ansonsten folgt die Ermittlung aller Ausfälle, die zu dem unerwünschten Ereignis führen.

3. Die Ausfälle werden in Kommentarrechtecke eingetragen und mit Hilfe der Fehlerbaumsymbolik logisch verknüpft. Stellen die Ausfälle eine Ausfallart dar, so wird die Bearbeitung mit Schritt 4 fortgesetzt, andernfalls wird wieder mit Schritt 2 begonnen.

4. In den häufigsten Fällen sind die einzelnen Ausfälle durch eine *ODER*-Verknüpfung verbunden, da jedes Eingangsereignis das Ereignis am Ausgang hervorruft. Diese Eingänge sind dabei dann mit Primärausfall, Sekundärausfall und kommandiertem Ausfall belegt. Primärausfälle können mit Hilfe

[105] Ross, H.-L.: Functional Safety for Road Vehicles (2016), a: S. 117; b: S.115.

[106] Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau (2004), a: S. 166; b: S. 164.

[107] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), a: S. 281; b: S. 278; c: S. 277.

der Fehlerbaumanalyse nicht weiter untersucht werden und stellen damit einen Standardeingang des Systems dar. Hingegen müssen Sekundärausfälle und kommandierte Ausfälle nicht unbedingt vorhanden sein. Liegen sie allerdings vor und ist der Ausfall kein Funktionselementausfall, so wird dieser Ausfall noch weiter untergliedert und die Bearbeitung beginnt wieder bei Schritt 2.[108a]

Eine gebräuchliche Darstellungsweise der eingesetzten Symbolik wird hier durch die nachfolgende Abbildung 4-2 illustriert. Das Symbol des *Standardeingangs* steht für ein Funktionsversagen. Diesem Bildzeichen für die Fehlerursache lassen sich auch weitere Angaben und Kenngrößen zuordnen. Die *Übertragungseingänge und -ausgänge* brechen einen Fehlerbaum ab oder setzen ihn an einer anderen Stelle fort. *Kommentare* in Rechtecken beschreiben Ein- und Ausgänge zwischen Verknüpfungssymbolen. Als logischer Operator drückt die *UND-Verknüpfung* aus, dass das Ereignis am Ausgang nur dann auftritt, wenn alle Ereignisse am Eingang stattfinden. Dementsprechend besagt die *ODER-Verknüpfung*, dass nur eines der Ereignisse am Eingang auftreten muss, damit das Ereignis am Ausgang eintrifft. Negationen werden mit der *NICHT-Verknüpfung* dargestellt. Damit hier das Ereignis am Ausgang passiert, darf die Bedingung am Eingang also nicht erfüllt sein.[108b]

Vergleichbar zu der FTA untersucht man bei einer Ereignisbaumanalyse, kurz ETA (*Event Tree Analysis*), einen Ereignisablauf und entdeckt damit die Folgen von Fehlern.[108c] Wie die FTA untersucht auch die ETA mögliche Initialereignisse und deren Auswirkungen auf das betrachtete System. Ergebnisse der Analyse werden ebenfalls grafisch dargestellt.[109] Häufiger Einsatzbereich der ETA sind Fahrsituationen im Rahmen einer System-FMEA. Dabei entstehen schnell hochkomplexe Diagramme. Für die Bestimmung initialer Fehlereignisse in verschiedenen Fahrsituationen kann sie sich dabei als nützlich erweisen. In diesem Fall überschneidet sie sich oft mit der HARA.[110]

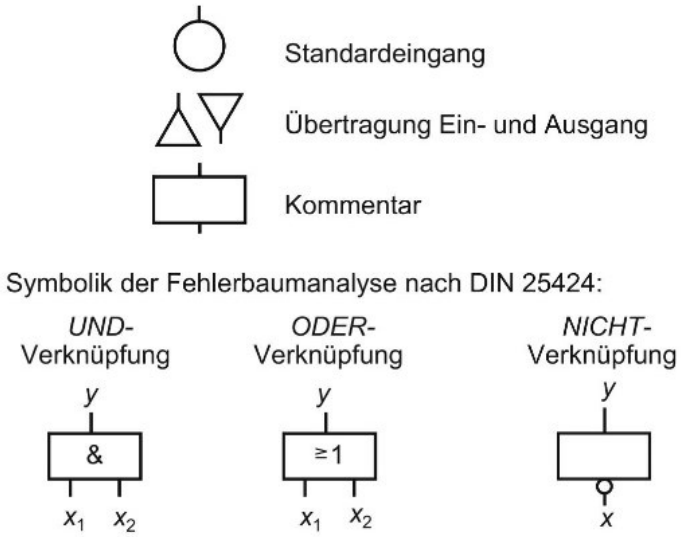

Abb. 4-2: Symbolik der FTA[108d]

[108] Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau (2004), a: S. 165; b: S. 162-263; c: S. 167; d: S.163.

[109] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), S. 156.

[110] Ross, H.-L.: Functional Safety for Road Vehicles (2016), S. 118.

Risikobewertung nach ASIL

Eine HARA nach ISO 26262 enthält neben der Identifikation auch die Bewertung von Risiken. In diese Bewertung fließen Schadensschwere, Häufigkeit und Kontrollierbarkeit einer Gefährdung in deren Bewertung ein. Abgeleitet erfolgt eine Kategorisierung des Risikos nach sogenannten *Automotive Safety Integrity Levels* (ASIL).[111] Die genaue Zuordnung der einzelnen Bewertungen zu der abschließenden Ebenen erfolgt nach dem Muster aus der nachfolgenden Tabelle 4-1.

In dieser Arbeit wurde die im Anschluss erklärte ASIL Risikobewertung anstelle der in der FMEA üblichen Risikoprioritätsziffer eingesetzt. Die Ergebnisse der FMEA mit dieser Risikobewertung finden sich im Anhang von Tabelle 7-1 bis Tabelle 7-11. Die Bewertung nach ASIL schafft hier auch unabhängig von der eingesetzten Analysemethode eine gewisse Vergleichbarkeit mit Risikobewertungen anderer Arbeiten. Bei Bewertungen die durch verschiedene Personen ausgeführt wurden, besteht jedoch die Möglichkeit, dass subjektive Einschätzungen die Vergleichbarkeit einschränken. Auch der Erfahrungshorizont der bearbeitenden Person beeinflusst die einzelnen Bewertungen und sorgt so für mögliche Unterschiede.

(S) Schwere	**(E) Häufigkeit**	**(C) Kontrollierbarkeit**		
		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**

Tabelle 4-1: Automotive Security Integrity Levels[112]

[111] Jipp, M.; Schneider, L.: Fahrtests unter Realbedingungen (2020), S. 14.

[112] Eigene Tabelle nach: Chen, L. et al.: HARA through STPA with FMEA (2020), S. 4.

In einer Bewertung nach ASIL erfährt das Schadensausmaß (englisch: *Severity*) eine Einteilung in drei Kategorien. An erster Stelle beschreibt S1 leichte und mäßige Verletzungsgefahren. Darüber steht S2 für ernsthafte Verletzungsgefahren. Sie sind zwar unter Umständen lebensgefährlich, jedoch bleibt ein Überleben wahrscheinlich. An oberster Stelle stehen mit S3 lebensbedrohliche Verletzungsgefahren, die das Überleben gefährden oder tödliche Verletzungen zur Folge haben.[113a] Die nächste Bewertungsdimension, die Eintrittswahrscheinlichkeit gefährdender Ereignisse (englisch: *Exposure Probability*) beziffert mit E, beinhaltet folgende Kategorien: E0 für unglaubhafte Eintrittswahrscheinlichkeiten, E1 für sehr geringe Eintrittswahrscheinlichkeit, E2 für geringe Eintrittswahrscheinlichkeit, E3 für mittlere Eintrittswahrscheinlichkeiten und zuletzt E4 für hohe Eintrittswahrscheinlichkeit der gefährdenden Ereignisse.[113b] Zuletzt beziffert man die Kontrollierbarkeit (englisch: *Controllability*) der gefährdenden Ereignisse. Hier steht C0 für allgemein kontrollierbare, C1 für einfach kontrollierbare, C2 für gewöhnlich kontrollierbare und C3 für schwer kontrollierbare, auch unkontrollierbare Ereignisse.[114] Abschließend sind die Klassen mit Buchstaben von A bis D beziffert. Hier ist A die verträglichste Bewertung und D die strengste. Der zusätzliche verwendete Eintrag "QM" ordnet Risiken nur dem Qualitätsmanagement zu und stellt keine ASIL Bewertung dar.[113c]

Alternative Analysemethoden der ISO 26262

Neben den vorgestellten Ansätzen schlägt die Norm ISO 26262 für Sicherheitsanalysen auch HAZOP Analysen, Markov Modelle und Zuverlässigkeitsblockdiagramme vor.[115a] Auch wenn die Methoden im weiteren Verlauf der Arbeit keine Rolle spielen, werden sie im folgenden Abschnitt für eine verbesserte Nachvollziehbarkeit der abschließend getroffenen Methodenauswahl knapp beschrieben.

Für eine Durchführung der HAZOP Analyse ist in der Norm DIN EN 61882 ein kompletter Prozess vorgesehen. Vergleichbar zu der ISO 26262 mit ihrer *item definition*, beginnt man dafür mit einer Beschreibung des Betrachtungsbereichs (auch: *scope*). Auch weitere vorbereitende Maßnahmen sind vergleichbar. Im weiteren Vorgehen wird die Betrachtungseinheit zerlegt und eine Zielfunktion (*Intended Function*) definiert.[113d] Während der Durchführung, wird die beabsichtigte Funktion auf mögliche Fehlfunktionen und Fehlverhalten durch strukturiertes Hinterfragen untersucht.[115b] So lässt sich in der Planungsphase einer Systementwicklung untersuchen, wie Abweichungen von der Systemspezifikation entstehen.[116] Ursprung der Methode liegt jedoch in der chemischen Industrie. Darüber hinaus findet sie ihren Einsatz in der Öl- und Gasindustrie.[115c]

Markov-Methoden beschränken sich auf Systeme, deren Elemente konstante Ausfall- und Reparaturraten besitzen. Sie erzeugen Modelle aus Zustandsdifferentialgleichungen, mit denen die Verfügbarkeit des untersuchten Gegenstands als Funktion der Zeit vorliegt.[117] So lassen sich dann mathematisch

[113] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), a: S. 210; b: S. 212; c: S. 60; d: S. 253.

[114] Chen, L. et al.: HARA through STPA with FMEA (2020), S. 3.

[115] Ross, H.-L.: Functional Safety for Road Vehicles (2016), a: S. 124–125; b: S. 120-121; c: S. 115.

[116] Sulaman, S. M. et al.: Comparison of FMEA and STPA (2019), S. 354.

[117] Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau (2004), S. 377.

anspruchsvoll Wahrscheinlichkeiten zuvor definierter Systemzustände berechnen.[118] Auch wenn Markov Analysen häufig zur Beurteilung von Übergängen genutzt werden, lassen sich eingesetzte Annahmen und Prinzipien nicht immer bei automobilen Systemen anwenden. Alterseffekte, Fehlerkombinationen, Abhängigkeiten und latente Fehler bleiben oft unberücksichtigt. Nützlich bleibt die Methode für Abschätzungen oder auch ergänzend zu anderen Analysemethoden.[119a]

Zuverlässigkeitsblockdiagramme (*englisch: RBD: Reliability-Block-Diagrams*) ähneln mit ihren logischen Verknüpfungsoperatoren den Fehlerbaumdiagrammen.[119b] Sie untersuchen, welche Elemente zur Erfüllung einer Funktion funktionieren müssen und welche ausfallen dürfen. Dafür wird der betrachtete Gegenstand in klare Aufgabenbereiche zerlegt, bis Zuverlässigkeitsangaben für jedes Elements bestimmt werden können. Ergebnisse dieser Analyse werden abschließend grafisch in dem Zuverlässigkeitsblockdiagramm dargestellt.[120] So illustrieren diese Blockdiagramme die Beziehungen und Einflussverhältnisse zwischen Systemkomponenten.[121] Ihr Einsatz zielt darauf ab, mögliche Fehler noch vor gestalterischen Entscheidungen zu entdecken.[119c]

4.3 Ergänzende Perspektive der STPA

Durch die Norm ISO 26262 werden vor allem Risiken durch mögliches Fehlverhalten und das Versagen von Hard- und Software adressiert. Mit ihrer HARA (*Hazard and Risk Assessment*) lassen sich diese identifizieren. Damit ist die Produktsicherheit jedoch nicht vollständig sichergestellt. Es bestehen auch Risiken ohne Fehlverhalten. Diese gilt es bei der Entwicklung eines sicheren Produkts ebenso zu berücksichtigen.[122a] Hier bietet die STPA *(Systems Theoretic Process Analysis*) einen breiteren Blickwinkel an. Sie betrachtet Sicherheit dabei als ein Steuerungsproblem. Für eine Systembeschreibung greift sie ebenfalls auf eine hierarchische Struktur zurück, verzichtet jedoch auf eine Abschätzung von Risiken.[123] Die Methoden FMEA und STPA wenden beide eine Zerlegung des Systems an. Auch identifizieren beide Fehler mit Ursachen und Auswirkungen. Grundsätzlich verfolgen sie jedoch unterschiedliche Schwerpunkte. Während die FMEA die Architektur und Komponenten eines Systems analysiert, sucht die STPA eher nach Ursachen für bereits identifizierte Risiken.[124]

Der Einsatz der STPA hat sich neben dem Automobilbereich auch in der Cybersicherheit und Softwaresicherheit etabliert.[122b] In ihrer Durchführung verläuft die Vorgehensweise in drei Schritten. Zu Beginn werden Systemgrundlagen für eine Analyse ermittelt. Als Ergebnis werden Versagensmöglichkeiten auf Systemebene mit ihren Risiken in Form einer hierarchischen Kontrollstruktur

[118] Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011).

[119] Ross, H.-L.: Functional Safety for Road Vehicles (2016), a: S. 120; b: S. 118; c: S. 141.

[120] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), S. 156.

[121] Ertas, A.: Systemic Thinking & Problem Solving (2018), S. 17.

[122] Abdulkhaleq, A. et al.: STPA Compliance with ISO 26262 (2017), a: S. 12; b: S.13.

[123] Chen, L. et al.: HARA through STPA with FMEA (2020), S. 5–6.

[124] Sulaman, S. M. et al.: Comparison of FMEA and STPA (2019), S. 383.

dargestellt. In diesem Diagramm werden anschließend potentielle Fehlerursachen identifiziert. Zuletzt wird untersucht, wie mögliche Ausfälle in diesen Kontrollpfaden entstehen.[125a]

Bei der Identifikation von kausalen Fehlerursachen unterstützt ein systematisches Vorgehen. Eine wichtige Fragestellung ist dabei, ob die Kontrollstruktur eine Überwachung der Sicherheitsfunktionen zulässt. Auch fehlende Steuerungsaktionen sind eine mögliche Fehlerursache. Darüber hinaus besteht die Möglichkeit, dass andere Steuergeräte einzelne Sicherheitsfunktionen stören oder einschränken könnten.[126]

Lippert und Kollegen schlagen für die Durchführung einer STPA im Forschungsprojekt UNICAR*agil* grundsätzlich allgemein formulierte Kausalfaktoren vor. Die Struktur der Analysen ließe sich so für andere oder weiterentwickelte Module wiederverwenden, sofern deren funktionale Architektur bestehen bleibt. Sie empfehlen jedoch Kausalfaktoren immer auf Modulebene zu definieren. Ansonsten sei eine unabhängige Betrachtung und Absicherung möglicherweise nur eingeschränkt möglich. Sie weisen deshalb auf eine klare Zuweisung zwischen dem Modul und den ermittelten Kausalfaktoren hin. Auf Modulebene ermöglichten allgemeine Formulierungen jedoch eine höhere erreichbare Vollständigkeit, indem Detailverlust durch frühes Eingrenzen vermieden wird.[127]

Wie auch die FTA (*Fault Tree Analysis*) ist die STPA eine Top-Down Methode. Im Gegensatz zu anderen Methoden der Risikoanalyse arbeitet sie jedoch mit einem "funktionalen Kontrolldiagramm" als Systemmodell. Hauptaugenmerk liegt dabei auf dem dynamischen Systemverhalten. Anders als die FMEA basiert die Methode auf Systemtheorie anstelle von Wahrscheinlichkeitstheorie. Außerdem betrachtet die STPA die Sicherheit als Abhängigkeit von der Steuerung und anstelle von Komponentenversagen.[128] Sie erweitert damit den Blickwinkel der funktionalen Sicherheit einer HARA. Mit dem Blick auf Steuerverhalten untersucht die STPA Aspekte der Betriebssicherheit, wie Steuerungsfehler durch Menschen, falsche Interaktionen, Umwelt oder auch Softwarefehler. Fehler durch unangemessene Steuerung ohne ein Komponentenversagen werden so ebenfalls entdeckt.[125b]

4.4 Kombinierte Betrachtungsweise

Ohne menschliche Verantwortung für die Ausführung der Fahraufgaben gelten veränderte Maßstäbe für das Testen. Demzufolge ist die Aussagekraft üblicher Testfälle eingeschränkt und die herkömmliche Vorgehensweise bei der Testfallgenerierung anpassungsbedürftig.[129]

Für die eindeutige Auswertung von Tests an hochautomatisierten Fahrzeugen sind genaue Testkriterien erforderlich. Dabei reicht es nicht, allein aus Anforderungen der Verhaltenssicherheit Definitionen für Bestehen oder Versagen abzuleiten. Eine mögliche Hilfestellung liefert eine HARA nach der

[125] Abdulkhaleq, A. et al.: STPA Compliance with ISO 26262 (2017), a: S. 13; b: S. 16.

[126] Thomas, J. et al.: Requirements Development and Hazard Analysis (2019), S. 106.

[127] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 9.

[128] Sulaman, S. M. et al.: Comparison of FMEA and STPA (2019), S. 350.

[129] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 454.

ISO 26262.[130a] Wie bereits erläutert bietet die STPA hier jedoch eine erweiternde Perspektive. Für eine Integration der STPA in eine HARA existieren bereits mehrere Ansätze. Beispielhaft sei hier auf den Ansatz von Abdulkhaleq und seinen Kollegen[131] oder eine neuere Variante von Thomas et al. in Zusammenarbeit mit General Motors verwiesen.[132a]

Ganz allgemein liefert eine Vielzahl von Normen Rahmenbedingungen für Tests. Der Einsatz dieser Normen ist jedoch nur dann gerechtfertigt, wenn er mit hoher Wahrscheinlichkeit zu qualitativen Verbesserungen führt. Auch wirtschaftliche Überlegungen sind bei ihrer Anwendung angebracht. Dokumente ohne Mehrwert gilt es zu vermeiden. Die Inhalte verschiedener Normen bilden allerdings eine Art Tool-Box nützlicher Vorgehensweisen. In jedem konkreten Einzelfall entsteht Qualität durch deren richtige Anwendung. Stumpfes Vorgehen nach Normen führt nur zu einem Realitätsverlust und lenkt ab von dem eigentlichen Ziel der Qualitätssicherung. Dennoch bleibt es von Bedeutung, den Einsatz von Normen konstruktiv zu diskutieren, um Konflikte zu vermeiden.[133]

Winner erwähnt drei verschiedene Herangehensweisen an eine Testfallentwicklung für autonome Fahrzeuge. Zum einen lassen sich aus vorhandenen Lastenheften und Systemspezifikationen Testfälle ableiten. Auch Risikobetrachtungen zeigen notwendige Testfälle auf. Zuletzt bietet sich eine genaue Schnittstellenbetrachtung an, um Testfälle zu deren relevanten Wertebereiche abzuleiten.[134] So finden sich diese drei Ansätze auch in dem nachgehend verfolgten Ansatz wieder. Mit einem konkreteren Vorschlag für eine Testentwicklung einzelner Module schlagen Lippert et al. ein strukturiertes Vorgehen ausgehend von Sicherheitszielen einer HARA vor. Dafür empfehlen sie ergänzenden Einsatz von FTA, STPA und eventuell weiteren Analysemethoden. Aus den damit ermittelten Anforderungen ließen sich anschließend klare Bestehens- und Versagenskriterien definieren.[130b]

In stark vernetzten Systemen werden unbeabsichtigte Interaktionen von herkömmlichen, fehlerorientierten Analysen möglicherweise übersehen. "Komponenteninteraktionsunfälle", die mit zunehmender Häufigkeit auftreten, stellen eine neue Klasse von Unfällen dar. Ursache für diese Unfälle ist ein dysfunktionales oder unbeabsichtigtes Zusammenspiel von Komponenten, auch ohne dabei auftretendes Komponentenversagen. Mögliche Ursache sind beispielsweise unkorrekte, unvollständige oder auch mehrdeutig definierte Softwareanforderungen. Auch wenn Softwarekomponenten einzeln für sich wie beabsichtigt arbeiten, ist nach dem Zusammenwirken mehrerer Komponenten ein unerwartetes Fahrzeugverhalten möglich.[132b]

Daher wird das Dynamikmodul in dieser Arbeit aus mehreren Perspektiven betrachtet, wie es die Abbildung 4-3 veranschaulicht. Die eingesetzten Methoden ergänzen sich dabei einander durch ihre unterschiedlichen Herangehensweisen.

---

[130] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), a: S. 5–6; b: S.7.

[131] Abdulkhaleq, A. et al.: STPA Compliance with ISO 26262 (2017), S. 16–18.

[132] Thomas, J. et al.: Requirements Development and Hazard Analysis (2019), a: S. 103–104; b: S.100.

[133] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), S. 58.

[134] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 445.

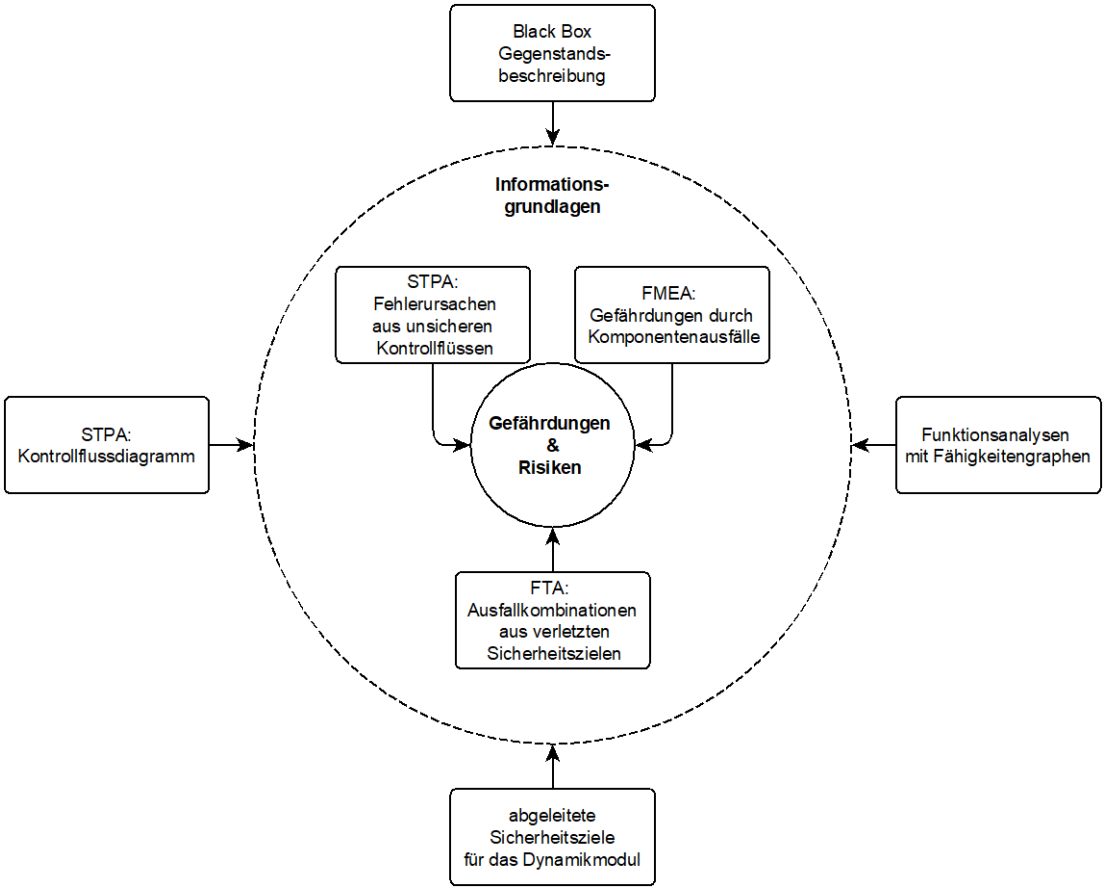

Abb. 4-3: Ermittlung von Gefährdungen und Risiken

Im allerersten Schritt wird eine kompakte Informationsgrundlage auch für die weiteren Arbeitsschritte geschaffen. Zum Einsatz kommt dafür eine „Black-Box"-Betrachtung, wie sie als Abbildung 4-4 von Bertsche und Lechner als Hilfsmittel für die Durchführung einer FMEA präsentiert wird.[135a] Die tabellenartige Darstellung liefert in kompakter Form einen allgemeinen Überblick über die Funktionen des Dynamikmoduls und seine Schnittstellen.

Black-Box

Eingang	Funktionen	Ausgang	
Drehzahl Hydraulik Druck Signale	- Drehmoment-/ Drehzahl wandeln - Gang wechseln - Gang wählen	gewandelte Drehzahl gewandeltes Moment anderer Gang	Getriebe
Signal Strom	- Signale verknüpfen - Licht erzeugen	Licht	Anzeige
Vorgabe von Top - funktionen	spezielle Funktion	führt zur Erfüllung der Topfunktion	Allgemein

Abb. 4-4: Struktur einer "Black Box"-Betrachtung[135b]

[135] Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau (2004), a: S. 139; b: S. 129.

Ausgehend von dieser Darstellungsstruktur lässt sich im nächsten Schritt ein Kontrollflussdiagramm im Sinne einer STPA ableiten. Dieses Diagramm unterstützt maßgeblich bei der Erstellung von funktionsbeschreibenden Fähigkeitsgraphen, wie sie im Kapitel der theoretischen Grundlagen unter Ansätzen für eine Dekomposition bereits vorgestellt wurden. Ergänzend werden aus einer bereits durchgeführten HARA der Gesamtfahrzeuge Sicherheitsziele für die Dynamikmodule abgeleitet. Mit diesen Informationen werden anhand der vorgestellten Methoden Risiken und Gefährdungen für das Dynamikmodul ermittelt, die sich in einer Anforderungsliste gesammelt zu Tests verarbeiten lassen.

4.5 Vorgehen in der Testentwicklung

Zu Beginn eines Testvorhabens finden üblicherweise planende Aktivitäten statt. Dabei wird beispielsweise bestimmt, auf welcher Plattform, in welcher Teststufe, welche Objekte mit welchen Testzielen untersucht werden. Die Fragen „Wo?“, „Wann?“, „Was?“ und „Wozu?“ liefern damit möglicherweise relevante Testplanungsdimensionen. Als Ergebnis dieser Planung entsteht schließlich ein Testkonzept.[136a] Gemäß der Norm ISO 26262-3 wird dieses sogar gefordert. Aus diesem gehen ganz konkret auch Testendekriterien hervor.[136b] Es wird beschrieben welche Testfälle für die jeweils vorgesehene Absicherung notwendig sind.[136c] Das Testkonzept definiert dafür jedoch keine Systemanforderungen oder Testfälle. Es bestimmt stattdessen, welche Testfälle mit welchen Eigenschaften für eine ausreichende Absicherung durchgeführt werden. Vorangegangene Sicherheitseinstufungen der Anforderungen werden dabei berücksichtigt. Für die Absicherung sicherheitskritischer Anforderungen gilt es daher beispielsweise mehr Testfälle vorzusehen als für unkritische Anforderungen.[136d] In einem vereinfachten Testkonzept werden also für jede Funktion Testziele, die angewendete Teststufe und die dabei eingesetzte Testplattform bestimmt.[137a] Testziele beschreiben den Zweck des Testens und liefern damit auch Qualitätsmerkmale. Denkbare Testziele sind Robustheit, Absicherung einer Funktionalität, Benutzbarkeit oder eine zu erfüllende Effizienz. Für einen Nachweis eines robusten Systems wird beispielsweise ein zuverlässig vorhersehbares Systemverhalten verlangt. Funktionale Absicherung untersucht die korrekte Erfüllung der geforderten Funktion. Auch Nutzerfreundlichkeit im Betrieb oder das Zeitverhalten einzelner Vorgänge können zu erreichende Testziele darstellen.[137b]

So wird auch in dieser Arbeit ein knappes Testkonzept in tabellarischer Form erstellt, mit dem sich Testfälle auf vorhandene Testumgebungen zuordnen lassen. Grundlage für einzelne Testfälle stellen existierende Anforderungsspezifikationen und analytisch ermittelte Gefährdungen dar.

Spezifikation von Testfällen

Bestimmende Angaben einer Testfallspezifikation sind eine eindeutige Kennung, ein genannter Bezug auf das Testobjekt, relevante Startbedingungen und Konfigurationen, Umgebungsbedingungen, Eingangsdaten mit gegebenenfalls zeitlichem Verlauf und das erwartete Verhalten mit definierten

[136] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), a: S. 15; b: S. 33; c: S. 2; d: S. 33.

[137] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), a: S. 83; b: S. 20.

Wertebereichen.[138a] Neben Testdaten ist also neben anderen Informationen auch eine Erwartung mit resultierenden Werten und Akzeptanzbereichen beschrieben.[139] Die erstellte tabellarische Testfallspezifikation dieser Arbeit orientiert sich schematisch an diesen Angaben.

Grundlagenliefernde testbare Anforderungen bestehen allgemein aus einem funktionalen Aspekt, einem Leistungsaspekt, einem Qualitätsaspekt und möglichen Randbedingungen. Funktionale Aspekte beschreiben Funktionen und verknüpfte Daten, aber auch das Systemverhalten und mögliche Fehler. Genauere Angaben der Daten, über ihre Struktur, Verwendung, Erzeugung, Übertragung oder Veränderung, spezifizieren diese jeweils genauer. Die Beschreibung der Funktion erklärt anschließend was mit den jeweiligen Daten passiert, wie sich das System dabei verhält und welche Fehler dabei für Abweichungen zum Normalverhalten sorgen können. Mit Leistungsaspekten von Anforderungen werden umgesetzte Datenmengen, Verarbeitungs- und Reaktionsgeschwindigkeiten aber auch Zeiten und Intervalle mit möglichst messbaren Angaben beschrieben. Dabei erwünschte Qualitäten, wie beispielsweise die Zuverlässigkeit ergänzen die Anforderung mit Qualitätsaspekten. Einzuhaltende Randbedingungen vervollständigen die Spezifikation. Darunter fallen einzuhaltende Schnittstellenwerte, Bedingungen aus Normen oder Gesetzen aber auch mögliche Vorgaben eines Auftraggebers.[140] Ergänzend werden Anforderungen in der Praxis auch mit Ursprungsangaben, Begründungen ihrer Relevanz oder auch Bewertungen ihrer Kritikalität und Priorität erweitert.[141]

Systematische Testbeschreibung erfolgt generell in einer semi-formalen, oder auch tabellarischen Darstellung. Wichtig für die Verständlichkeit ist dabei grundsätzlich die Verwendung einer für menschliche Experten verständlichen Fachsprache. Auch Parameterbereiche für Zustandsgrößen gilt es anzugeben. Erleichternd für deren Umsetzung hält sich ihre Definition an eine formale Ordnung (z.B. ein Dateiformat). Der gewählte Detailgrad ist dabei möglicherweise entscheidend für spätere Reproduzierbarkeit ohne Interpretationsspielräume. Im idealsten Fall ist eine Darstellung darüber hinaus effizient maschinenlesbar. Die geforderte Lesbarkeit für menschliche Experten und Maschinen stellt dann jedoch einen möglichen Widerspruch dar.[138b] Umfangreiche Vorschläge für eine dennoch formelle Spezifikation liefern beispielsweise die „SOPHISTen“ mit sprachlichen Anforderungsschablonen.[142] Ihre Herangehensweise, Anforderungen in natürlicher Sprache zu formulieren wurde auch bei der Erstellung der hier entwickelten Anforderungsliste verfolgt. Funktionale Aspekte, Leistungsaspekte, aber auch Qualitätsaspekte, wurden nach einem festen Muster in natürlicher Sprache ausgedrückt. Angaben über Randbedingungen, Ursprung, Sicherheitsbegründung und Bewertungen sind daneben nur ergänzend tabellarisch aufgeführt.

[138] G. Bagschik et al.: Entwicklung, Absicherung & Test automatisierter Fahrzeuge (2017), a: S. 129; b: S. 130-131.

[139] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 378.

[140] Martin Glinz: Spezifikation von Anforderungen, S. 96.

[141] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), S. 147.

[142] Die SOPHISTen: MASTeR (2019), S. 10.

Strukturierende Maßnahmen

Schon eine einfache Klassifizierung nach Komplexität und Priorität schafft Überblick. Anforderungen hoher Komplexität erfordern generell eine höhere Anzahl an Testfällen und somit mehr Aufwand als Anforderungen mit geringer Komplexität. Außerdem wird es damit möglich, Tests mit geringerer Priorität bewusst auszuschließen.[143a] In Anlehnung and das im Abschnitt über Anforderungen erwähnte MosCow-Prinzip, erfolgt die Priorisierung von Anforderungen und Testfällen in dieser Testentwicklung mit drei Kategorien. Anforderungen der Kategorie A müssen unbedingt umgesetzt werden. Wird die Anforderung nicht erfüllt darf keine Massenproduktion erfolgen. Der Buchstabe B bewertet Anforderungen mit mittlerer Priorität. Wird eine solche Anforderung nicht umgesetzt, wäre der Betrieb nicht unmöglich aber eingeschränkt. Abschließend stehen unter Kategorie C Anforderungen mit niedriger Priorität, die gegebenenfalls auch vernachlässigbar sind. Zur Erreichung der Projektziele ist ihre Erfüllung nicht erforderlich. Ein Nichterfüllen würde im schlimmsten Fall geringe Einschränkungen hervorrufen. Zahlen von 1 bis 3 erweitern diese Klassifizierung mit einer Angabe der verknüpften Komplexität. Dabei steht 1 für hohe Komplexität und die folgenden Ziffern für absteigende Komplexitäten bis hin zu niedriger Komplexität.[143b] Eine quantifizierbare Beschreibung von Komplexität gestaltet sich möglicherweise schwierig. Abgrenzung zwischen komplizierten und komplexen Systemen bietet dafür jedoch einen möglicherweise hilfreichen Bezug. Beide besitzen zwar eine Vielzahl interaktiver Komponenten, jedoch ist das Verhalten komplizierter Systeme gut zu verstehen. In komplexen Systemen fehlt dieses klare Verständnis.[144] Anforderungen mit intensivem Bezug zu informationstechnischen Systemen werden in dieser Arbeit daher unter Kategorie 1 zusammengefasst. Genaue Zusammenhänge lassen sich für sie oft nicht ohne weiteres ergründen. Anforderungen mit mechatronischem Schwerpunkt werden mittlerer Komplexität zugeordnet, da sich dadurch beschriebene Sachverhalte mit technischem Fachwissen generell nachvollziehen lassen. Anforderungen an rein mechanische Zusammenhänge bilden die Kategorie geringster Komplexität. Auch ohne Fachwissen lassen sich damit verknüpfte Sachverhalte erfassen.

In erster Linie liefert schon eine Gruppierung nach Aktuatoren eine strukturgebende Vereinfachung.[145] So verfolgt auch die Testentwicklung in dieser Arbeit durchgehend eine Einteilung nach den Aktorik-Systemen des Dynamikmoduls.

[143] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), a: S. 76; b: S. 75-76.

[144] Ertas, A.: Systemic Thinking & Problem Solving (2018), S. 2.

[145] Stolte, T. et al.: Functional Safety of Vehicle Actuation (2016), S. 579.

5 Testentwicklung für das Dynamikmodul

Ausgehend von technischen Rahmenbedingungen, theoretischen Grundlagen und einem methodischen Werkzeugkasten aus Kapitel 4, werden in diesem Kapitel Tests für das Dynamikmodul entwickelt. Dafür wird zunächst im Sinne der ISO 26262 ein einfaches Testkonzept aufgestellt, das die vorhandenen Testmöglichkeiten beschreibt. Um dafür testbare Anforderungen zu entwickeln, werden die in Abschnitt 4.4 vorgestellten Analysen eingesetzt, wie es Abb. 5-1 veranschaulicht. Darin enthaltene Pfeilverbindungen zeigen Informationsflüsse zwischen den verschiedenen Informationsentitäten dar. Zunächst werden Informationen über das Modul strukturiert gesammelt und grafisch dargestellt. Auch wenn alle resultierenden Darstellungen den Testprozess des Dynamikmoduls informierend unterstützen, sind sie in jeweils einzelnen Analysemethoden besonders nützlich. Die Black-Box Betrachtung, darauf aufbauende funktionale Dekomposition und der Einsatz der *Fähigkeitengraphen* eignet sich vor allem für die FMEA. Das Kontrollflussdiagramm unterstützt bei der Untersuchung von Kontrollflüssen der STPA. Abgeleitete Sicherheitsziele liefern initiale Ereignisse für Fehlerbaumanalysen. Vorgehensweisen der eingesetzten Analysen sind in den Abschnitten 4.2 und 4.3 bereits aus allgemeiner Perspektive beschrieben worden. Erfolgte Durchführungen werden hier daher ausschließlich ergänzend und verständnisfördernd beschrieben. Erzielte Ergebnisse dieser Untersuchungen fließen daraufhin gemeinsam in eine Anforderungsliste ein. Aus diesen Anforderungen werden daraufhin ausgewählte Testfälle gemäß dem definierten Testkonzept abgeleitet und beschrieben. Die tabellarische Darstellung der gesammelten Anforderungen und Tests liegt dem Darmstädter Fachgebiet für Fahrzeugtechnik gesondert vor. In dieser schriftlichen Ausarbeitung wird die Erstellung, der Inhalt und Aufbau der darin enthaltenen Tabellen dennoch beschrieben.

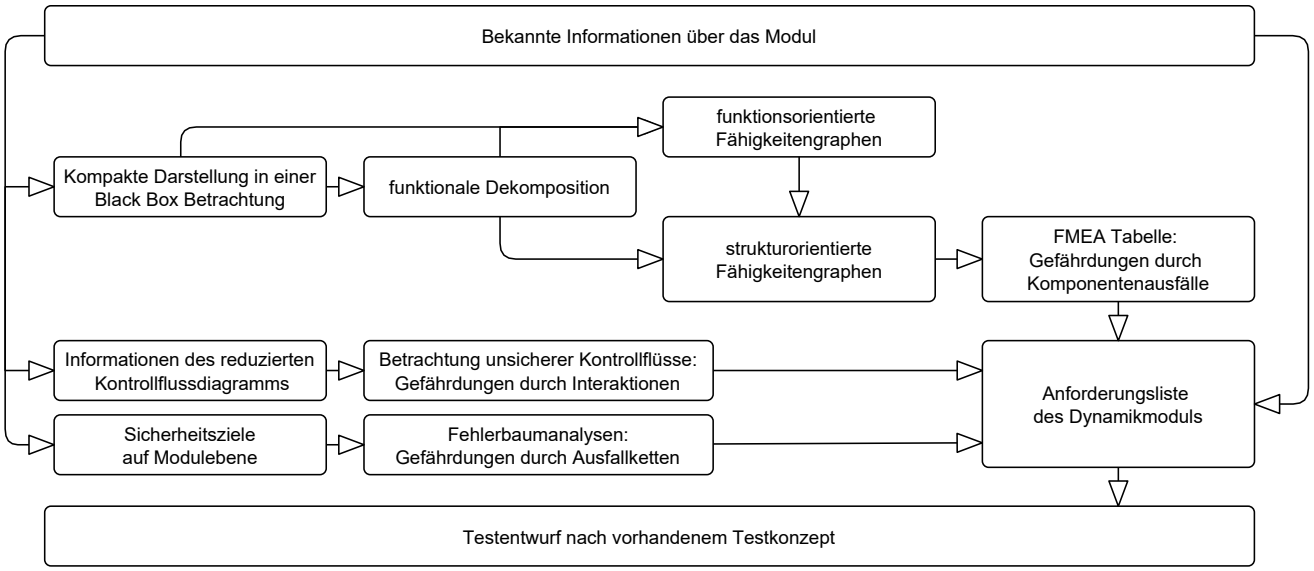

Abb. 5-1: Vorgehen für eine modulare Testentwicklung

Neben der Durchführung der kombinierten Methodik wird die Ableitung von drei verschiedenen Testfällen exemplarisch beschrieben. Dabei wird jeweils auf Anforderungen aus unterschiedlichen Analysemethoden zurückgegriffen. Auch die Spezifikation dieser Anforderungen wird beschrieben. So lässt sich der Ursprung aller Anforderungen und der bereits erstellten Testfälle nachvollziehen.

Mit der dadurch beschriebenen Vorgehensweise, lassen sich aus bestehenden Anforderungen weitere Tests auch für andere Testumgebungen ableiten. Zum Abschluss des Kapitels wird auf mögliche Unzulänglichkeiten der Methodik hingewiesen und Chancen für Verbesserungen erwogen.

5.1 Testkonzept

Anhand der bekannten Testmöglichkeiten ist nachfolgend in Tabelle 5-1 ein vereinfachtes Testkonzept in Anlehnung an die Darstellungsweise in Noacks Dissertation beschrieben.[146]

Funktion	Testziel	Teststufe	Testumgebung
Lenkung	Funktionalität	Komponente	Prüfstand des Lenkantriebs
Informationsfunktionen	Funktionalität	Integration	Simulink Modelle
Beschleunigung, Verzögerung, Lenkung	Funktionalität	Integration	Modultests auf Hebebühne
Alle	Funktionalität	Abnahme	Gesamtfahrzeug, Testgelände

Tabelle 5-1: Einfaches Testkonzept

Das Konzept orientiert sich an bekannten Ressourcen, wie sie nachfolgend beschrieben sind. Scheffel beschreibt in seiner Masterthesis bereits existierende Simulationsmodelle der Dynamikmodule. Er greift in seiner Arbeit auf ein Modell zurück, das zuvor von Elster erstellt wurde.[147] Dieses bildet im Detail den Antrieb, die Lenkung, die Bremse sowie den Reifen ab. Die einzelnen Teilmodelle wurden über Matlab/Simulink Plug-ins in CarMaker umgesetzt. Außerdem gäbe es ein Dynamikmodell zur Simulation der Radaufhängung. Ohne näher darauf einzugehen verweist er auf dessen Betreuung durch Projektpartner aus Aachen.[148]

Zum Zeitpunkt dieser vorliegenden Arbeit sind in Aachen ein physischer Prüfstand für den Lenkantrieb und diverse virtuelle Modelle in MATLAB Simulink vorhanden. Genutzt wurde der Prüfstand bisher für Auslegungen.[149] Dafür wurde bereits die endgültig vorgesehene Leistungselektronik eingesetzt. Zukünftig wird der Prüfstand außerdem mit einem angeschlossenen Sidestick ergänzt, um damit auch manuell Lenkbewegungen vorgeben zu können. Mit weiterem Entwicklungsfortschritt lässt sich das Dynamikmodul am Fahrzeug montiert auch auf einer Hebebühne testen. Ohne gegenwirkende Lasten lassen sich dort die grundlegenden Funktionen prüfen. Abschließende Tests sind mit dem Gesamtfahrzeug auf einem Testgelände vorgesehen. Von dem Dynamikmodul wird dort erwartet, sowohl programmierten Vorgaben als auch manuellen Vorgaben per Sidestick zu folgen.[150]

[146] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), S. 83.

[147] Elster, L.: Master Thesis, Simulationsmodelle für elektrische Radnabenantriebe (2020).

[148] Scheffel, T.: Masterthesis, Entwicklung und Implementierung von Ausfallmodellen für elektrische Radnabenantriebe (2020).

[149] Martens, T.; Pouansi, B.: Interview: Testmöglichkeiten und Hintergründe (2020).

[150] Klamann, B.: Interview: Aktuelle Möglichkeiten in Aachen (2021).

Das modulare Sicherheitskonzept des Forschungsprojekts sieht vor, die Validierung im Idealfall bereits durch Modultests und Integrationstests vorzunehmen.[151] Zusätzlich zu den modularen Ansätzen sollen virtuelle Testumgebungen den gesamten Testaufwand reduzieren. Da nicht für alle Komponenten virtuelle Modelle existieren bleiben reale Tests dennoch notwendig. Tests einzelner Module sind mit Simulationen ausgehend von ihren Eingabeschnittstellen geplant. Um den Simulationsrahmen selbst zu validieren, ist ein Vergleich zwischen Ergebnissen einer realen und einer virtuellen Umgebung vorgesehen. Eine digital geklonte Testumgebung soll dies ermöglichen.[152] Dieser validierende Vergleich liegt zum Zeitpunkt dieser Verfassung jedoch noch nicht vor. Es besteht dennoch die Möglichkeit, Ergebnisse des hier entwickelten Testkonzepts dabei vergleichend einzubinden.

5.2 Informationen über das Dynamikmodul

Bei der Aufdeckung möglichst vieler und detaillierter Fehlermöglichkeiten ist eine gute Kenntnis des Dynamikmoduls hilfreich.[153] Bevor also mögliche Risiken und Gefährdungen des Dynamikmoduls nach der vorgestellten kombinierten Methodik ermittelt werden, wird das Modul hier noch einmal kompakt beschrieben. Genauere Spezifikationen vervollständigen erst später die Testfallentwicklung. So bleiben funktionale Zusammenhänge überschaubar und verständlich. Die eingesetzten Informationsgrundlagen stammen dabei nicht ausschließlich aus öffentlich verfügbaren Quellen. Schnittstellen des Dynamikmodul sind bereits anschaulich durch ein intern verfügbares „Boundary Diagramm“ beschrieben. [154] Da dieses die Zusammenhänge der einzelnen Subsysteme des Dynamikmoduls aufzeigt, diente es hier unter anderem bei der Erstellung der „Black-Box“ Betrachtung und des Kontrollflussdiagramms. Weitere Informationen stammen aus einer internen Leistungsbeschreibung, welche Bauteile der Lenkeinheit näher beschreibt. Sie spezifiziert explizit den Lenkmotor, eine Bremse, das Lenkgetriebe, Flanschanschlüsse und die enthaltene Sensorik.[155]

An erster Stelle beschreibt eine Tabelle in Form von Abb. 5-2 das Dynamikmodul als „Black-Box“. In der Bereitstellung aktiver Funktionen des Dynamikmoduls spielt das Fahrwerk grundsätzlich eine untergeordnete Rolle, da hier ohne Aktoren eine rein passive Einflussnahme auf das Fahrgeschehen erfolgt. Das verwendete Rad wurde darüber hinaus bereits nach Industriestandards validiert.[156] So sind in dieser Tabelle nur die Subkomponenten des Dynamikmoduls beschrieben, die im automatisierten Betrieb für die maßgebliche Erfüllung der aktiven Funktionen verantwortlich sind. Darunter fallen Radnabenantrieb und Lenkantrieb mit ihrer jeweiligen Leistungselektronik, die Perimeterbremse und das Steuergerät. Jeweils relevante Eingangsgrößen lassen sich in Vorgaben, Signale, Energieversorgung und Umwelteinflüsse kategorisieren. An den Ausgängen setzen sich die Werte vereinfacht aus physikalischen Größen und Signalen zusammen. Die kompakte Darstellung

[151] Stolte, T. et al.: Safety Concepts for Automated Vehicles (2020), S. 1584.

[152] Woopen, T. et al.: UNICARagil - Disruptive Modular Architectures (2018), S. 685.

[153] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 9.

[154] Wolf, C.: Dynamikmodul: Boundary Diagramm mit Kontakten.

[155] Pouansi, B.: Leistungsbeschreibung der Aktoreinheiten des Dynamikmoduls (2020).

[156] Martens, T. e.: UNICARagil Dynamics Module (2020), S. 877.

beinhaltet dabei jedoch ausschließlich das Dynamikmodul, ohne innere Zusammenhänge der Subkomponenten zu untersuchen. Diese ergänzenden Informationen sind jedoch in einer umfangreicheren Black Box Betrachtung als Abb. 7-1 im Anhang zu finden.

Black Box Betrachtung des Dynamikmoduls

Subsystem — **Eingangsgrößen** — **Funktionen** — **Ausgangsgrößen**

Steuergerät	Vorgaben Energie Umwelt	Soll-Radgeschwindigkeit Soll-Lenkwinkel 48V DC Bordstrom Einflüsse und Störgrößen	Wertevorgaben empfangen; erreichte Leistungswerte, Zustand und Leistungskapazitäten an Stammhirn kommunizieren	Umwelt: Wärmeabgabe Signal: Hydrauliksteuerung Signal: Temperatur Lenkung Signal: Ist-Raddrehzahl Signal: Ist-Antriebsmoment Signal: Ist-Lenkwinkel Signal: Ist-Lenkmoment
Perimeter-bremse	Energie Umwelt	hydraulischer Druck 12V DC Bordstromnetz Einflüsse und Störgrößen	mechanisches Bremsen; Notbremsfunktion mit Bremspedal in der Fahrgastzelle; Parkbremsfunktion, Positionssicherung im Stillstand	Moment: Perimeterbremse Umwelt: Wärmeabgabe
Radantrieb	Energie Umwelt	48V DC Bordstromnetz Einflüsse und Störgrößen	Radgeschwindigkeit halten; Radgeschwindigkeit erhöhen; Radgeschwindigkeit rekuperativ verzögern	Moment: Antrieb / Bremse Leistung: Strom rekuperiert Umwelt: Wärmeabgabe
Lenkeinheit	Energie Umwelt	48V DC 12V DC für Fail Silent Bremse Einflüsse und Störgrößen auch: Widerstandsmomente	statische & dynamische Lenkwinkelvorgaben einhalten; Feststellbremse für Ausfallsituationen	Moment: Lenkmoment Moment: FS Bremse Umwelt: Wärmeabgabe

Abb. 5-2: Tabellenstruktur der Blackbox Betrachtung des Dynamikmoduls

An nächster Stelle erweitert das Kontrollflussdiagramm aus Abb. 5-3 die Perspektive, indem Komponenten des Moduls mit ihren Schnittstellen und Interaktionen dargestellt werden. Sowohl die Zusammenhänge als auch die verwendeten Kategorien der Kontrollflüsse orientieren sich an einem bereits existierenden Boundary Diagramm des Dynamikmoduls.[157] Mit dem Ziel einer übersichtlichen Darstellung, sind auch darin die Ströme zwischen den Komponentenschnittstellen kategorisiert. Unterschieden werden somit auch in der Darstellung dieser Arbeit Ströme der Wirkenergien, Kommunikationsverbindungen, Verbindungen der Wasserkühlung, mechanische Verbindungen und Umweltinteraktionen. Eine erweiterte Variante im Anhang zeigt die Zusammenhänge beteiligter Komponenten mit weiteren Einzelheiten.

[157] Wolf, C.: Dynamikmodul: Boundary Diagramm mit Kontakten.

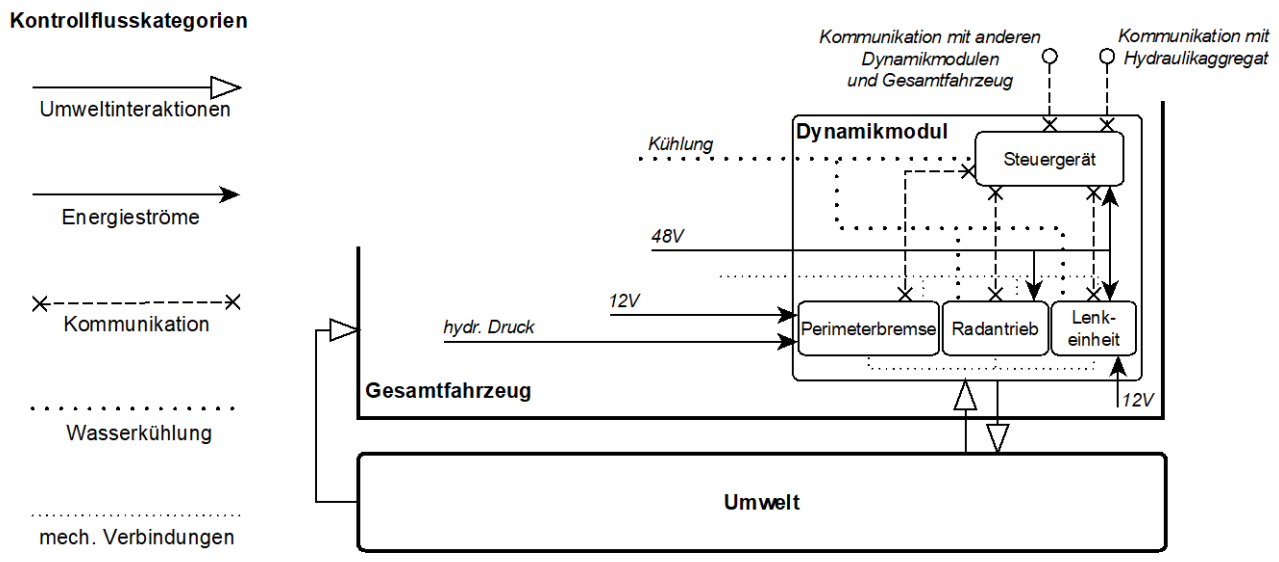

Abb. 5-3: reduziertes Kontrollflussdiagramm des Dynamikmoduls

Letzter Bestandteil in der Informationsgrundlage sind grobe Sicherheitsziele. Für das Gesamtfahrzeug wurden von Stolte und Graubohm im Rahmen einer HARA bereits Sicherheitsziele ermittelt, wobei hier ein besonderer Schwerpunkt auf die automatisierte Fahrfunktion gelegt wurde.[158] Ausgehend davon wurden hier allgemein formulierte Sicherheitsziele für das Dynamikmodul abgeleitet. Sie fließen nicht nur in die ergänzende FTA ein, sondern dienen auch als Leitlinien bei der Ermittlung von Fehlermöglichkeiten und Gefährdungen. Der genauere Hintergrund ihrer Ableitung und die Verknüpfung mit Sicherheitszielen des Gesamtfahrzeugs ist mit Abb. 7-3 im Anhang dargestellt.

In kompakter Form gelten demnach für das Dynamikmodul die folgenden Sicherheitsziele:

SG1-DM: Das Dynamikmodul darf selbst keine Personen direkt gefährden.

SG2-DM: Das Dynamikmodul muss Informationen über den eigenen Zustand, vorhandene Kapazitäten und erreichte Ist-Werte korrekt an das *Stammhirn* kommunizieren.

SG3-DM: Das Dynamikmodul muss mit zügigen Reaktionen arbeiten & kommunizieren.

SG4-DM: Das Dynamikmodul muss seinen Vorgaben sicher folgen.

Zu schützende Personen sind prinzipiell Insassen, Passanten und andere Verkehrsteilnehmer.[159] In einem herkömmlichen Fahrzeug werden Fehler durch den Fahrer überwacht. Diese Aufgaben übernehmen in einem autonomen Fahrzeug Sensoren und entsprechend integrierte Funktionen. Defekte und Fehler gilt es damit nach wie vor zu erkennen und zusätzlich daraus die vorhandene und zukünftige Leistungsfähigkeit abzuschätzen.[160] Für eine grundlegend sichere Teilnahme im Verkehrsgeschehen sind die beiden nächsten Ziele zu erfüllen. Zügiges Reaktionsverhalten ist vor allem für eine sichere Interaktion zwischen planenden Fahrzeugsystemen und der Umwelt von Bedeutung. Kommt

[158] Stolte, T.; Graubohm, R.: UNICARagil Gesamtfahrzeug HARA auf Szenarienbasis (2018), S. 8.

[159] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 181.

[160] Reschka, A.: Sicherheitskonzept für autonome Fahrzeuge (2015), S. 506.

es hier zu Verzögerungen, ist das Fahrzeugverhalten möglicherweise nicht mehr der aktuellen Fahrsituation angemessen. Das letzte Sicherheitsziel verlangt eine wertebezogene Einhaltung der empfangenen Vorgaben und gilt damit vor allem den internen Regelsystemen des Dynamikmoduls.

5.3 Analytische Betrachtungen

Ein funktionsorientiertes Vorgehen hat Auswirkungen bis hin zur Testauswertung. Wie bereits erwähnt schafft eine Kategorisierung nach Fahrzeugfunktionen Übersichtlichkeit. Das erleichtert beispielsweise auch die Beurteilung der erreichten Testabdeckung zum Testende.[161] Bereits zuvor lässt sich der jeweils betrachtete Parameterraum durch funktionale Dekomposition verkleinern. Die gewonnene Übersicht und Kontrollierbarkeit unterstützen so auch das Auffinden von möglichen Fehlerursachen.[162] Bevor die Strukturen und Zusammenhänge innerhalb des Dynamikmoduls genauer betrachtet werden, erfolgt daher eine Kategorisierung der Modulfunktionen. Funktionen mit einem Schwerpunkt in der Informationsverarbeitung und Kommunikation werden hier vereinfachend unter „Informationsfunktionen“ zusammengefasst. Alle Funktionen des Dynamikmoduls, die informationsintensive Aufgaben erfüllen, sind darunter eingeschlossen. Im Detail lassen sich diese Aufgabenbereiche der Erfassung, Kommunikation oder auch der Regelung zuordnen. Das Dynamikmodul beinhaltet selbst keine Funktionen, die ein Situationsverständnis erfordern oder Verhaltensentscheidungen treffen. Diese sind außerhalb des Dynamikmoduls integriert und bauen unter anderem auf den Informationsfunktionen des Dynamikmoduls auf. Damit kommt diesen Informationsfunktionen eine besonders wichtige Bedeutung zu. Die Hauptfunktionen des Dynamikmoduls fallen dennoch unter die Kategorie der Ausführung. In den nachfolgend interaktionsfokussierten Betrachtungen, sind die aktiven Funktionen für Fahrzeugbeschleunigung, Verzögerung und Lenkung von hauptsächlicher Bedeutung. Darüber hinaus erfüllt das Dynamikmodul jedoch auch passive Funktionen bei der Übertragung von Kräften und Momenten. Die hier aufgabenorientiert vollzogene Dekomposition wird angehend in Abb. 5-4 gezeigt.

Auch wenn bei reiner Betrachtung des Dynamikmoduls das hydraulische System der Fahrzeuge, die Batterie und auch das Kühlsystem unberücksichtigt bleiben, haben diese Systeme einen Einfluss auf die Anforderungen des Moduls. Über das Kühlsystem des Fahrzeugs sei an der Stelle ergänzend erwähnt, dass dafür mehrere Kreisläufe mit einer einzigen mehrstufigen Pumpe betrieben werden. Einer dieser Kreisläufe kühlt die Rechensysteme, ein anderer die Radnabenantriebe und der letzte die Temperatur der Fahrkabine. Als Wärmepumpe ist die Anlage damit auch in der Lage, Abwärme aus Motoren und Rechnern für die Heizung des Innenraums nutzen.[163] Auch das Batteriesystem hat Einflüsse auf die Dynamikmodule. Verknüpfte Gefährdungen sind beispielsweise Vergiftung, Explosion, Brand, Feuer, Verbrennung, Überspannung und Überströme.[164]

[161] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), S. 18.

[162] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 9.

[163] Woopen, T. et al.: UNICARagil - Where We Are (2020), S. 296.

[164] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 189.

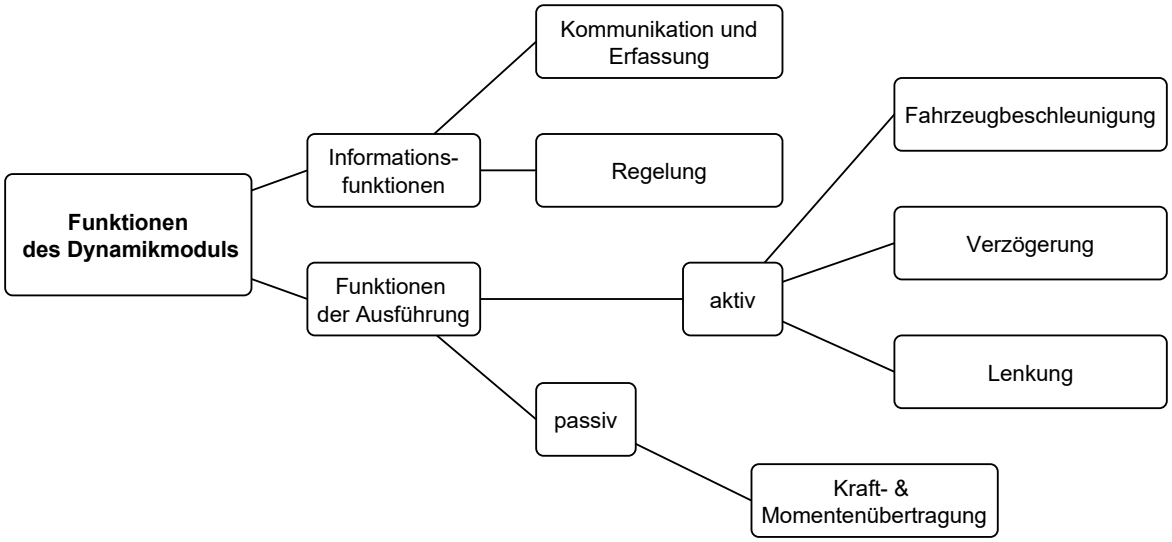

Abb. 5-4: funktionale Dekomposition des Dynamikmoduls

Als weitere Grundlage für FMEA-ähnliche Funktions- und Strukturanalysen kommen die in Abschnitt 3.2 erwähnten Fähigkeitsgraphen zum Einsatz. Sie veranschaulichen die Abhängigkeiten und Interaktionen der einzelnen Systemkomponenten.[165] Mit einer abgewandelten Form dieser strukturbaumartigen Darstellung lassen sich auch Funktionen und Subfunktionen untersuchen. Zusammenhänge zwischen Funktionen und Komponenten lassen sich so gezielt betrachten. Die ausführlichen Fähigkeitsgraphen zu den Funktionen und Modulkomponenten finden sich im Anhang von Abb. 7-4 bis Abb. 7-13. Ihre allgemeine Grundstruktur wird hier jedoch durch Abb. 5-5 beschrieben. Wie im Kapitel der theoretischen Grundlagen mit *Fähigkeiten* erklärt, werden Funktionen und Komponenten untergeordneten Funktionen und verbundenen Zusammenhängen zugeordnet.

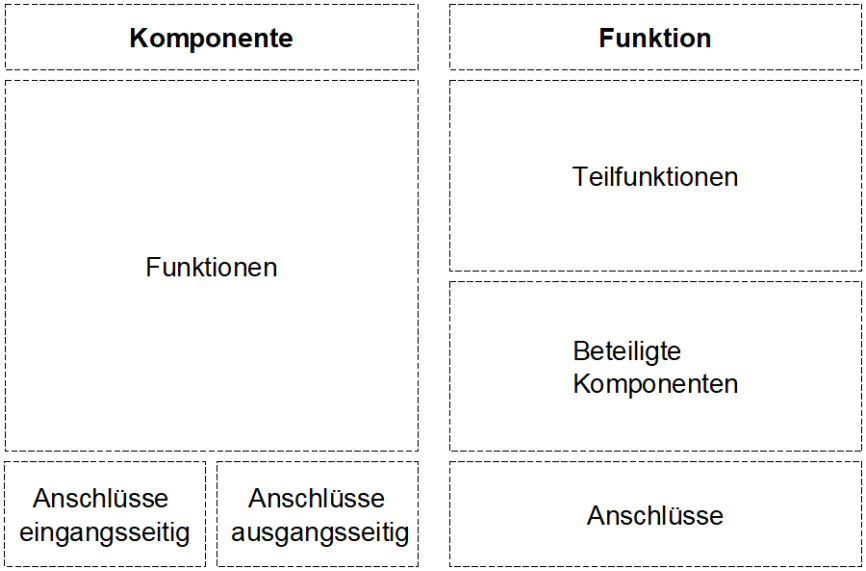

Abb. 5-5: Schemata der konstruierten Fähigkeitengraphen

[165] Reschka, A. et al.: Ability and Skill Graphs (2015), S. 935.

Dafür werden in den dargestellten Bereichen Knoten gebildet, die Komponenten, Funktionen, Teilfunktionen oder Anschlüsse repräsentieren. Innerhalb der einzelnen Bereiche lassen sich diese Knoten durch verschiedene Anordnungen auch in Hierarchien ordnen. Vor allem für die Darstellung von Interaktionen zwischen Subsystemen und Systemkomponenten eignet sich die so entstehende Darstellungsstruktur.[166]

Linien zwischen den Knoten stellen sowohl technische Verbindungen als auch funktionale Verknüpfungen dar. Auch wenn die Linien bei starker Vernetzung kreuz und quer verlaufen, bleiben Zusammenhänge immer noch vergleichsweise schnell und kompakt nachvollziehbar indem man die geraden Linien nachverfolgt. Die Ergebnisse stellen eine Art Funktions- und Strukturanalyse dar. Deswegen unterstützen sie die anschließende Erstellung einer FMEA Tabelle, in der die Auswirkungen und Folgen einzelner Komponentenausfälle gesammelt werden. Auch bei der Ableitung von Kausalfaktoren für Gefährdungen für eine STPA, liefern diese Graphen Informationen über funktionalen Kontext. Gleiches gilt für die ergänzende Durchführung der FTA und sicherlich auch weitere Aktivitäten im Testvorgehen. Die Komponenten aus dem Kontrollflussdiagramm und auch die zerlegten Elementarfunktionen des Dynamikmoduls sind im Anhang in dieser Form dargestellt.

Die Ergebnisse der durchgeführten FMEA finden sich in tabellarischer Form ebenfalls im Anhang mit den Tabelle 7-1 bis Tabelle 7-11. Bei der Durchführung dienten die zuvor erklärten Struktur- und Funktionsanalysen mit *Fähigkeitsgraphen* als strukturgebende Informationsgrundlage. Auch die verfolgte Einteilung nach Aktorsystemen wurde durchgehend beibehalten, wobei abschließende Tabelleneinträge teilweise auch allen Subsystemen gelten. Anstelle der für eine FMEA üblichen Risikobewertung mit einer Risikoprioritätsziffer, erfolgt hier eine Bewertung nach den *Automotive Safety Integrity Levels.* Damit ist eine gewisse Vergleichbarkeit der Ergebnisse gegenüber anderen Modulen oder Analysen im Forschungsprojekt vorhanden.

Im nächsten Schritt werden ausgehend von den Kontrollflüssen des Kontrollflussdiagramms Anforderungen und entsprechende Versagenskriterien nach dem Vorschlag von Lippert et al. abgeleitet.[167] Das schemenhafte Vorgehen unterscheidet an erster Stelle immer, ob jeweils ein fehlender Kontrollfluss oder ein stattfindender Kontrollfluss gefährdungsverursachend wirkt. Mit dieser Aufteilung werden alle vier grundlegenden Varianten eines Steuerungsfehlers wiedergegeben.

Eine Steuerungsanweiseung, die nicht gestellt oder nicht ausgeführt wird, fällt das unter die erste Kategorie. Eine unsichere und ausgeführte Steuerungsanweisung fällt unter die zweite Kategorie. Zusätzlich besteht die Möglichkeit, dass eine möglicherweise sichere Steuerungsanweisung zu früh, zu spät, zu falscher Zeit oder in falschem Zusammenhang gegeben wird. Ebenfalls ist es denkbar, dass eine sicherheitsrelevante Steuerungsanweisung zu früh gestoppt oder zu lange gegeben wird.[168] Alle drei der letzteren Steuerungsanweisungen werden in der hier angewendeten Schablone als stattfindende, gefährdungsverursachende Kontrollflüssen zusammengefasst berücksichtigt.

[166] Ertas, A.: Systemic Thinking & Problem Solving (2018), S. 22–23.

[167] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 8.

[168] Stolte, T. et al.: Functional Safety of Vehicle Actuation (2016), S. 579.

Untergeordnet werden mögliche Ursachen für diese Steuerungsfehler durch Knoten dargestellt. Pfeilverbindungen zeigen auf, in welcher Reihenfolge diese zu einem gefährdenden Kontrollfluss führen. Eine andere Pfeilform leitet aus diesen Ursachen allgemein formulierte Kausalfaktoren ab, aus denen sich ebenfalls allgemeingültige Testkriterien für den jeweilige Kontrollfluss ergeben. Bei dem Erstellen einer zusammengefassten Anforderungsliste für die Testerstellung lassen sich mit diesem Schema für jeden einzelnen Kontrollfluss zwischen den Komponenten spezifische Anforderungen ableiten.

Im letzten Schritt der Analysen liefern die abgeleiteten Sicherheitsziele initiale Fehlerereignisse für eine FTA. Sucht man mit Fehlerbäumen nach ihren möglichen Ursachen werden Ausfallkombinationen ermittelt. Bei der Erstellung und Betrachtung dieser Fehlerbäume ist es hilfreich mit kategorisierten Fehlerfunktionen zu denken. Im einfachsten Fall ist die Funktion völlig eingeschränkt und findet nicht statt. Aber auch eine unerwartete Funktion, zum Beispiel durch unerwünschte gegenseitige Beeinflussung von Systemen, oder auch eine systematisch verfälschte Funktion, stellt einen Fehler dar. Vergleichbar sind auch sporadisch oder unerwartet falsche Funktionen möglich. Resultierend kommt es unter Umständen zu ausbleibender Ausführung, oder vernachlässigter Kommunikation. Grundsätzlich liegt ein Fehler immer vor, wenn eine Funktion nicht kontinuierlich wie gewünscht arbeitet oder auch ein unangemessenes Zeitverhalten aufweist.[169]

Gemeinsam umfassen Ergebnisse dieser Untersuchungen Gefährdungen durch Komponentenausfälle, Gefährdungen durch kombinierte Komponentenausfälle und Gefährdungen durch unpassende Kontrollflüsse. Zusammen liefern sie damit ein umfangreiches Fundament von Anforderungen, aus denen sich Testfälle für alle Schritte des vorgesehenen Testkonzepts spezifizieren lassen. Auch darüber hinaus zeigen sie umfangreiche Bedingungen für den sicheren Betrieb des Dynamikmoduls.

5.4 Aufstellung einer Anforderungsliste

Zusammen mit Anforderungen aus zu Beginn des Kapitels erwähnten Dokumenten, werden die Ergebnisse der durchgeführten Analysen in einer semi-formalen Anforderungsliste gesammelt. Allein aufgrund ihres Umfangs ist diese Tabelle für einen Druck auf Papier ungeeignet und liegt daher ausschließlich in digitaler Form vor. Die gewählte Struktur der tabellarischen Anforderungseinträge lehnt sich grob an die vorgestellten Ansätze des Innovationsprojekts "MASTER" an. Mit konkreten Schablonen und Vorlagen liefert darin die Beratungsgesellschaft der „SOPHISTen“ umfangreiche Ideen für eine verbesserte Dokumentation von Anforderungen in natürlicher Sprache.[170]

[169] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 382.

[170] Die SOPHISTen: MASTeR (2019), S. 6.

In der erstellten Liste wird jeder Anforderungseintrag entweder dem Dynamikmodul oder einem darin enthaltenen Subsystem zugeordnet und erhält eine eigene Identifikationsnummer. Eine Priorisierung erfolgt nach der in Abschnitt 4.5 vorgestellten Weise in drei Kategorien von A bis C, mit einer ergänzenden Angabe zur verknüpften Komplexität. In der Bewertung wurden neben zuvor geschilderten Betriebssituationen des Dynamikmoduls auch erwünschte Redundanzen für autonome Fahrzeuge in die Überlegung einbezogen. Allgemein sind diese für die Längs- und Querführung eines automatisierten Fahrzeugs für eine Gewährleistung der Sicherheit angebracht. Das gilt insbesondere für die Basis-Aktuatoren, die Kommunikation der relevanten Steuergeräte, die Spannungsversorgung dieser Steuergeräte und auch die allgemein dafür nötige Energieversorgung.[171] Darüber hinaus sind aber auch Aufgaben der Kommunikation und Informationserfassung, wie in Abschnitt 2.3 erklärt, von großer Bedeutung für die Sicherheit.

Jede Anforderung hat eine Quellenangabe, wodurch offensichtlich wird, dass unterschiedliche Quellen teilweise von unterschiedlichen Werten ausgehen. Martens weist an der Stelle in seinem Konferenzbeitrag über das Dynamikmodul darauf hin, dass einige Anforderungen und Parameter vorerst als Richtwerte in der Entwicklung angenommen werden. In seinem Beitrag fallen darunter beispielsweise die Fahrzeugmasse, Rollwiderstandskoeffizient, Luftwiderstandskoeffizient, Fahrzeugstirnfläche, Höchstgeschwindigkeit und maximale Beschleunigung.[172] Anhand dieser Quellenangaben lassen sich im weiteren Testvorgehen Unklarheiten klären indem die jeweils verantwortlichen Personen zu den jeweils konkreten oder aktuellen Werten befragt werden.

Der Kerninhalt einer Anforderung wird in natürlicher Sprache nach dem in Abb. 5-6 veranschaulichten Schema beschrieben.

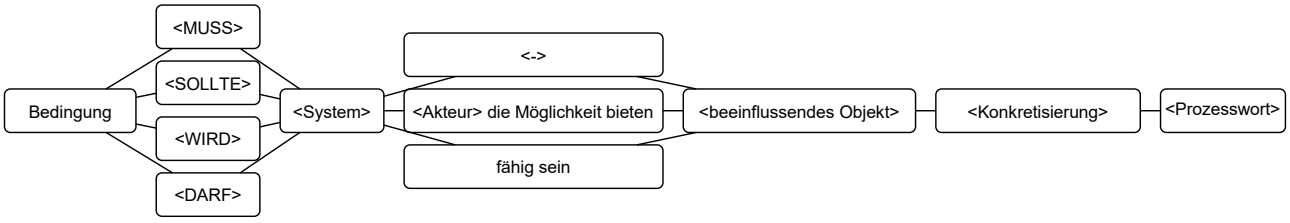

Abb. 5-6: Schablone der Anforderungsliste

Die darin enthaltenen Elemente lassen sich zu einem Satz in natürlicher Sprache verbinden, der den Inhalt einer Anforderung wiedergibt. Unter Bedingungen stehen dabei beispielsweise Situationen oder Bereiche auf die sich die Anforderung beschränkt. Anschließend wird angegeben welche Bedeutung die Anforderung hat, und wie die Erwartung zu erfüllen ist. Das System auf das sich eine Anforderung bezieht wird im nächsten Block eingetragen. So lassen sich Anforderungen mit den Funktionen üblicher Tabellenkalkulationsprogramme gefiltert nach ihren jeweils spezifizierten Systemen anzeigen. Mit dem nächsten Block besteht die Möglichkeit anzugeben, ob die Anforderung dem Modul selbst gilt, oder ob das Dynamikmodul bei der Erfüllung einer Anforderung an ein anderes System beteiligt ist. Unter dem Eintrag „beeinflussendes Objekt“ steht immer ein Bezugsgegenstand, der für

[171] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), S. 132.

[172] Martens, T. e.: UNICARagil Dynamics Module (2020), S. 865.

die Erfüllung der Anforderung eine Rolle spielt. Auch hier lassen sich Anforderungen durch Filterfunktionen selektiv anzeigen. Abschließend steht eine Konkretisierung, mit der beispielsweise quantitative Angaben die Anforderung spezifizieren, und ein Prozesswort. Dadurch wird klar in welcher Art das Dynamikmodul für die Erfüllung der jeweiligen Anforderung sorgt. Eine beispielhafte Anforderung nach diesem Schema lautet folglich:

„Im automatisierten Betriebsmodus | muss | das Dynamikmodul | fähig sein | das Fahrzeug | in Vorzugsrichtung mit einer Höchstgeschwindigkeit von 70 km/h | anzutreiben.“

Zusätzlich wird ein Tabelleneintrag mit zugeordneten Testumgebungen, einer Zuordnung zu Anforderungskategorien und einer „Verknüpfungs-ID“ versehen. Mit dieser Verknüpfungs-ID lassen sich Anforderungen auch im Testvorgehen sortieren und gruppieren. Dabei werden Funktionsbereiche und Sicherheitsziele einbezogen. Die Kennung besteht aus 3 Lettern bzw. Zahlen, die die Anforderungen kategorisieren, wie es Tabelle 5-2 erklärt.

Funktionsbereich	Betroffene Komponenten	Relevanz für Sicherheit
0: keine Zuordnung	D: Dynamikmodul	0: keine Zuordnung
I: Informationsfunktion	S: Steuergerät	1: betrifft SG1 - DM
A: Aktive Funktion	B: Perimeterbremse	2: betrifft SG2 - DM
P: Passive Funktion	R: Radantrieb	3: betrifft SG3 - DM
	L: Lenkeinheit	4: betrifft SG4 - DM

Tabelle 5-2: Aufschlüsselung der Verknüpfungs-ID

Alle Anforderungen mit der Verknüpfungs-ID „IS1“ würden demnach in einem Zusammenhang mit der Bereitstellung von Informationsfunktionen stehen, sich auf das Steuergerät beziehen und für die Erfüllung des ersten Sicherheitsziels des Dynamikmoduls notwendig sein.

Die dabei eingesetzte Einteilung bezieht sich neben den Sicherheitszielen aus Abschnitt 5.2 auf die vollzogene Dekomposition in 5.3 und ermöglicht eine zusätzliche Kategorisierbarkeit der Anforderungen nach funktionalen Bereichen, beteiligten Komponenten und ihrer Rolle für die Sicherheit.

Beispielhaft wird anschließend die Spezifikation von drei Anforderungen beschrieben, deren Ursprung in jeweils unterschiedlichen Methoden liegt.

Ableitung einer Anforderung aus Ergebnissen der FMEA

Bei der Ermittlung von Risiken durch ausgefallene Komponenten lieferten vor allem die Black Box Beschreibung mit Abb. 7-1 und die abgewandelten *Fähigkeitengraphen* (Abb. 7-4 und folgende) strukturgebende und inhaltliche Informationen. Ausgehend von dem Überblick der Black-Box Beschreibung wurden zunächst die darin beschriebenen Funktionen wie in Abb. 5-4 dargestellt kategorisiert. Davon ausgehend wurden die gebildeten Funktionskategorien Kommunikation und Erfassung,

Regelung, Fahrzeugbeschleunigung, Verzögerung, Lenkung und abschließend Kraft & Momentenübertragung durch Fähigkeitengraphen systematisch zerlegt. Jeder Funktionsbereich wurde darin mit untergeordneten Funktionen verknüpft und dafür beteiligten Subsystemen des Dynamikmoduls zugeordnet. Bei der anschließenden Erstellung von Fähigkeitengraphen der Subsysteme ließen sich die so strukturierten Einzelfunktionen systematisch auf Modulkomponenten zuordnen.

Mit diesen Darstellungen lassen sich Ausfälle einzelner Komponenten mit ihren Folgen strukturiert untersuchen. So ermittelte Gefährdungen finden sich gesammelt in Tabelle 7-1 bis Tabelle 7-11.

Um darin enthaltene Einträge nachvollziehen zu können, wird die Ableitung von Eintrag 1001 beispielhaft beschrieben. Für die in der Blackbox-Beschreibung definierte funktionale Einheit des Steuergeräts wird hier eine mögliche Gefährdung ermittelt. Ausgehend von der Darstellung Abb. 7-10 werden dafür zunächst Ausfälle in der Regelung in Betracht gezogen. Noch konkreter werden Folgen eines Ausfalls der verknüpften Unterfunktion „Regelung der Rekuperation“ untersucht. Damit wird deutlich, dass ein Ausfall der regelnden Funktionen des Steuergeräts ineffiziente Regelung der Rekuperation und damit eine verringerte Fahrzeugreichweite zur Folge haben könnte.

Generell wurde in den Analysen auf quantitative Angaben verzichtet. Diese lassen sich später für eine Testentwicklung ergänzen, wodurch erzielte Ergebnisse auch nach technischen Systemveränderungen ihre Gültigkeit behalten. Demzufolge wird für das Steuergerät mit Eintrag 1001 die Anforderung definiert: „Rekuperation muss möglichst effizient stattfinden.“ In der Anforderungsliste entsteht daraus mit dem vereinheitlichenden Schema die Anforderung #0125:

„In keiner Situation | sollte | das Steuergerät | < - > | den Rekuperationsstrom | ineffizient | regeln.“

Ableitung einer Anforderung aus den Ergebnissen der FTA

In gleicher Weise sind auch die Anforderungen aus Fehlerbaumanalysen allgemein gehalten. Ausgehend von der Verletzung der in 5.2 beschriebenen Sicherheitsziele wurden mögliche Ausfallkombinationen des Dynamikmoduls mit Fehlerbäumen untersucht. Die grafischen Ergebnisse finden sich im Anhang von Abb. 7-14 bis Abb. 7-17. Die dabei verwendete Darstellung orientiert sich an der Formalie aus Abb. 4-2. Ausgehend von verletzten Sicherheitszielen ließen sich zusammenhängende Fehlerketten ermitteln. Jeder dadurch ermittelte Standardeingang liefert abschließend die Möglichkeit, aus ihm mindestens eine Anforderung abzuleiten.

Aus dem Standardeingang „Gehäuse unter Strom“, der eine Verletzung des Sicherheitsziels SG1-DM zur Folge hat, geht daher eine Anforderung hervor. Sie hat einen Bezug auf das gesamte Dynamikmodul und ist bedeutend an der Vermeidung von Gefährdungen für Personen beteiligt. So wird daraus letztlich die Anforderung #0063:

„In keiner Situation | darf | das Gehäuse des Dynamikmoduls | < - > | Personen | durch anliegende Stromspannung gefährden.“

Ableitung einer Anforderung aus den Ergebnissen der STPA

Wie in 5.2 beschrieben, unterscheidet das erstellte Kontrollflussdiagramm auch in seiner detaillierten Variante (Abb. 7-2) Energieströme, Kommunikationsverbindungen, Leitungen der Wasserkühlung, mechanische Verbindungen und Umweltinteraktionen. Für jede dieser Kategorien wurde in Anlehnung an den Vorschlag von Lippert et al. schablonenartige Muster zur Ableitung von Anforderungen und testbaren Kriterien erstellt.[173] Diese suchen allgemeingültig, wie es zu einem unsicheren Kontrollfluss der jeweils untersuchten Kategorie kommen kann und sind im Anhang unter Abb. 7-18 bis Abb. 7-22 enthalten. Eine Betrachtung der Umweltinteraktionen liefert die Erkenntnis, dass ungeeignete Vorgabewerte an das Dynamikmodul keine Gefährdungen verursachen dürfen. Im gleichen Zusammenhang muss das Dynamikmodul seinen aktuellen Zustand, seine Leistungskapazitäten und erreichten Ist-Werte für die Planung geeigneter Vorgaben kommunizieren. Eine Verletzung dieser Anforderungen erfolgt ganz allgemein dann, wenn ein gefährdender Kommunikationsaustausch zwischen Dynamikmodul und Stammhirn stattfindet. So steht in der Anforderungsliste unter ID #0194:

„In keiner Situation | darf | das Dynamikmodul | < - > | durch wahrgenommene Kommunikation | eine Gefährdung verursachen.“

Auch wenn diese Anforderung zunächst unspezifisch ist, wurden daraus weitere Anforderungen für das Steuergerät und die Sensorik des Dynamikmoduls abgeleitet.[174]

5.5 Aufstellung von Testfällen

Ausgehend von der damit erweiterten Anforderungsliste lassen sich Testfälle ableiten. Die Spezifikation von Testfällen beinhaltet jeweils typischerweise die Beschreibung einer testbaren Situation, die zugrunde liegende Anforderung und das erwartete Ergebnis.[175a] Nicht jede einzelne Testhandlung wird dafür genauestens beschrieben. Jedoch wird hinreichend beschrieben was zu tun ist, um das gewünschte Ergebnis zu erzielen.[175b] In der gesamten Testentwicklung wird auf eine allgemeingültige Formulierung geachtet, sodass die Tests für alle vier Module eines Fahrzeugs gleichermaßen Gültigkeit besitzen. An anderer Stelle wurde darauf hingewiesen, dass im Rahmen des Projekts keine Prototypen für Fahrzeugaufprallversuche existieren. Notwendige Sicherheitsnachweise seien rein simulativ geplant.[176] Insofern zielen auch die hier entwickelten Testfälle nicht darauf ab, die Komponenten realer Systeme schadenverursachend an ihre Leistungsgrenzen zu bringen.

Für die Dokumentation der der entworfenen Testfälle wurde eine tabellarische Form gewählt. Einzelnen Testumgebungen des Testkonzepts aus 5.1 wurden dabei jeweils eigene Tabellen zugeordnet. Jeder Testfall wird darin mit jeweils fünf Informationsbereichen beschrieben.

[173] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 8.

[174] in der beigefügten Excel Tabelle zu finden unter: #0195 und #0196

[175] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), a: S. 149; b: S. 149.

[176] Woopen, T. et al.: UNICARagil - Where We Are (2020), S. 289.

Strukturliefernde Angaben über das jeweils untersuchte System, eine Test-ID, die zugrundeliegende Anforderungs-ID und eine priorisierende Angabe liefern formelle Voraussetzungen für strukturierte Testdurchführung.

An nächster Stelle werden die Startbedingungen und Konfigurationen für jeden Testfall beschrieben. Einleitend wird in knapper Form der jeweils geprüfte Sachverhalt erklärt und der geplante Vorgang in natürlicher Sprache beschrieben. So lassen sich die formalisierten Angaben über beteiligte Schnittstellen, Startkonfiguration und quantitative Startbedingungen leichter erfassen.

Es folgen ebenfalls formalisierte Angaben über neue Bedingungen, die eine Systemreaktion erzeugen sollen. Quantitative Angaben werden dabei mit einer Angabe über ihren zeitlichen Verlauf vervollständigt.

Unter dem Abschnitt der Erwartungen sind Rahmenbedingungen, das erwartete Verhalten, eine tolerierte Abweichung und eine Auswertungsgrundlage gegeben. Dafür wird nach jedem Test eine Frage mit „Ja“ oder „Nein“ beantwortet, was für jeden Fall ein eindeutiges Ergebnis in Form von Bestehen oder Nicht-Bestehen liefert.

Ergänzend nutzt die Tabelle ein Kommentarfeld, das ergänzende Anmerkungen in der Bearbeitung zulässt. Zuletzt wird die Sicherheitsrelevanz des jeweiligen Testfalls in knapper Form erklärt.

5.6 Diskussion

Wie zu erwarten liefert der kombinierte Methodeneinsatz umfangreiche Anforderungen. Ein strukturierter Umgang mit ihren Informationen wird damit erforderlich. Möglichkeiten für eine Zuordnung der Einträge liefern verschiedene Kategorisierungen. An erster Stelle lassen sich Funktionale Anforderungen, die quantitative Werte für die Testfalldefinition liefern, von Sicherheitsanforderungen unterscheiden. Letztere stellen die Mehrheit der erstellten Anforderungsliste dar und zeigen sicherheitsrelevante Zusammenhänge auf. Die gewählte Priorisierung ermöglicht es, bei einer Testfalldefinition die aufwendigsten und relevantesten Anforderungen zuerst zu testen. Damit lässt sich eine ökonomische Reigenfolge für die Testdurchführung festlegen. Zuordnung von Anforderungen auf das jeweils spezifizierte Subsystem ermöglicht es, die einzelnen Anforderungen geordnet an jeweils vorgesehenen Testumgebungen zu verweisen. Hierbei unterstützt auch die eingeführte „Verknüpfungs-ID“. Sie kategorisiert Anforderungen nach betroffenen Komponenten, der verknüpften Funktion und ihrer Bedeutung für die Sicherheit. Sie unterstützt außerdem ähnliche Anforderungen aufzufinden um diese in der Testentwicklung möglicherweise zusammengefasst zu untersuchen.

Die Menge der Einträge stellt dennoch eine Herausforderung dar. Die Überblickbarkeit für qualitätsverbessernde Überarbeitung ließe sich mit einer stärker formalisierten Darstellung denkbar verbessern. Dann allerdings wären mögliche Einbußen in der Verständlichkeit abzuwägen. Softwaretools mit weniger allgemeiner Ausrichtung als Tabellenkalkulationsprogramme stellen hier verbesserte Handhabung in Aussicht. Durch den Einsatz einer formalisierten Datenbank oder spezieller Programme für Anforderungsmanagement und Testprozesse ließe sich gute Verständlichkeit bei gleichzeitig strukturierter Dokumentation gewährleisten.

Bei einer Untersuchung des Gesamtfahrzeugs wäre der Umgang mit einer Vielzahl an Anforderungen allerdings noch anspruchsvoller. Hier wären noch mehr Anforderungen auf Testumgebungen zuzuordnen. Insofern lässt sich feststellen, dass modulare Absicherung mit einfacheren technischen Möglichkeiten durchführbar ist, als dies bei der Absicherung eines Gesamtfahrzeugs der Fall wäre.

Ein möglicher Engpass für effiziente modulare Testentwicklung besteht dennoch in der geschickten Definition der jeweiligen Betrachtungsgrenzen. Bei der Untersuchung des Dynamikmoduls, ließen sich vor allem für Gefährdungen mit informationstechnischem Bezug nicht immer klare technische Verantwortlichkeiten erkennen. Das liegt zum einen an der Komplexität beteiligter Softwareprogramme aber auch an der funktionalen Vernetzung in der Fahrzeugarchitektur. Das Systemverhalten hängt hier oft von Prozessen außerhalb des Moduls ab. Diese wiederum beziehen sich auf Informationen, die das Modul durch erfassende Systeme zu Verfügung stellt. Diese wechselseitige Beziehung durch getrennte Testprozesse abzusichern, erfordert eine deutliche Spezifikation ihrer funktionalen Verknüpfung. Black-Box Ansätze reichen hier nicht aus um softwareintensive Zusammenhänge zu untersuchen.

Auch wenn die funktionale Einteilung des Forschungsprojekts getrennte Untersuchung der jeweiligen Systeme erlaubt, wäre es durch eine zusätzlich eingeführte Unterscheidungsebene zwischen ausführenden und kognitiven Systemen möglicherweise einfacher, stark vernetzten Funktionen zu überprüfen. Ohne Berücksichtigung der mechanischen und physikalischen Zusammenhänge, ließe sich somit das gesamte „kognitive System“ effizienter testen. Damit ließe sich der Schwerpunkt der Absicherung für eine Freigabe auf das Zusammenspiel in der Fahrzeugarchitektur legen. Sicherheitsnachweise für mechatronische Subsysteme, ließen sich dann wie im Fall der im Dynamikmodul eingesetzten Lenkeinheit[177] von jeweiligen Zulieferern verlangen oder getrennt erbringen. Eine abgesicherte „kognitive Architektur“ ließe sich dann auch mit austauschbaren Modulen betreiben, die allein für die Erfüllung einfacher Funktionen verantwortlich sind.

[177] Pouansi, B.: Leistungsbeschreibung der Aktoreinheiten des Dynamikmoduls (2020)

6 Ergänzungen und Schlussfolgerungen

Abschließend folgen Bemerkungen über den Umgang mit erzielbaren Testergebnissen. Zusätzlich werden Herausforderungen für eine modulare Absicherung, aber auch Chancen knapp aufgeführt.

Testauswertung

Zum Abschluss eines Testprojekts wird das Projekt üblicherweise selbst untersucht. Dabei werden Leistungsparameter betrachtet um Gründe für gute oder schlechte Leistungen zu entdecken.[178a] Vor allem mit der Entscheidung, ob das Ziel der Tests erreicht wurde, kommt dem Testende eine große Bedeutung zu. Wurden die zuvor definierten Testendekriterien erfüllt, ist das Testende erreicht. Beispiel für ein solches Testendekriterium ist eine zuvor bestimmt geforderte Testabdeckung. Auch die mittlere Anzahl aufgedeckter Fehler pro Teststunde ist ein möglicher Indikator. Als eigene Aktivität, schafft die Testauswertung Klarheit über erreichte Ziele und den Testfortschritt.[178b] Die Testabdeckung beschreibt dabei das Verhältnis der durchgeführten Tests eines jeweiligen Testkriteriums. Vollständige Testabdeckung ließe sich durch vollständiges Testen mit White-Box Testmethoden erreichen. Eine aufwandsärmere Vorgehensweise nach Black-Box Methoden liefert grundsätzlich eine geringere Testabdeckung. Werden außerdem kontinuierliche Wertebereiche vereinfachend diskretisiert, verringert sich die erreichbare Testabdeckung zusätzlich.[179] Vor allem wegen der Absicht die Absicherung des Forschungsprojekts modular durchzuführen, ist die Auswertung des Testvorgehens besonders relevant. Die Eignung dabei eingesetzter Vorgehensweisen gilt es anhand in Abschnitt 3.4 erwähnter Maßstäbe zu bewerten. Auch eine Validierung der Methoden ist notwendig.

Die Norm ISO 26262 sieht auch in der Auswertung von Testergebnissen formelle Angaben vor. Sie verlangt allgemein eine eindeutige Identifikation des untersuchten Gegenstands mit Referenzen zu einem Testplan und der verwendeten Testspezifikation. Auch die Konfiguration der Testumgebung, die eingesetzten Werkzeuge und Kalibrierungsdaten werden beschrieben. Dokumentiert wird die Übereinstimmung der Testergebnisse mit den erwarteten Werten und eindeutigen Angaben ob der Test bestanden wurde oder nicht. Im Falle eines Nichtbestehens sind auch mögliche Ursachen und Vorschläge für daraus resultierende Maßnahmen beschrieben. Werden nicht alle Testfälle durchgeführt, sind die Gründe für nicht ausgeführte Testfälle genannt.[180] Es bietet sich an, durch Tests erkannte Fehler in Kategorien zu ordnen. Im Fall kritischer Fehler würde eine Nichtbehebung im Betrieb zu Funktionsversagen führen. Schwere Fehler würden im Betrieb erhebliche Beeinträchtigungen der Funktionen verursachen. Unrelevante Fehler bilden die letzte Kategorie. Ihre Nichtbehebung würde auch im späteren Betrieb keine erheblichen Beeinträchtigungen hervorrufen.[181]

[178] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), a: S. 16; b: S. 16.

[179] Schuldt, F.: Dissertation, Test automatisierter Fahrfunktionen (2016), S. 22–23.

[180] Ross, H.-L.: Functional Safety for Road Vehicles (2016), S. 227.

[181] Droste, O.; Merz, C.: Testmanagement in der Praxis (2019), S. 169.

Herausforderungen

Ganz allgemein ist für das autonome Fahren eine Testdurchführung nach herkömmlichen Methoden aus ökonomischen und technischen Gründen nicht angebracht.[182] Einfache Ansätze für eine Absicherung schlagen vor, Äquivalenzklassen für einzelne Dimensionen wie Straßenbeschaffenheit, Dynamische Objekte und Umweltbedingungen zu bilden. Jedoch entstehen damit trotzdem große Mengen praktisch nicht umsetzbarer Tests. Methoden aus Normen wie der ISO 26262 oder Standards wie ISO PAS 21448 weisen diesbezüglich Unzulänglichkeiten auf, ohne mögliche Lösungshinweise zu enthalten.[183] Als Schwachstelle der daraus oft eingesetzten FMEA ist auch die Risikobewertung zu erwähnen. Abhängig von persönlichem Erfahrungshorizont und anderen subjektiven Einflüssen fällt eine Risikobewertung unterschiedlich aus, was ihre Aussagekraft grundsätzlich einschränkt.[184] Ohnehin reichen Anforderungen der ISO 26262 nicht für eine Zulassung von Fahrzeugen im Straßenverkehr. Länderabhängig gelten verschiedenste Zulassungsverfahren, wohingegen die Norm weltweit anwendbar ist.[185] Vor einer umfangreichen Produktion gilt es zusätzlich die Zuverlässigkeit eines Systems unter erschwerten Bedingungen zu untersuchen. Dabei stellt der mittlerer Ausfallabstand MTBF (*Mean Time Between Failures*) eine wichtige Kenngröße dar. Schwachpunkte gilt es zu beheben, bis dieser unter einem geforderten Wert liegt.[186a] Dessen Definition stellt einen möglichen Anknüpfungspunkt für weitere Arbeiten dar. Im Übrigen bietet es sich für nicht reparierbare Komponenten auch an einen Zielwert der zu erreichenden mittleren Erstfehlereintrittswahrscheinlichkeitszeit (MTTF, *Mean Time To Failure*) zu ermitteln.[186b]

Auch der modulare Ansatz von UNICAR*agil* bringt neue Herausforderungen hervor.[187] Das beabsichtigte partikuläre Testen sieht eine Aufteilung in Subsysteme vor, die einzeln an Stelle des Gesamtsystems untersucht werden. Im Vergleich mit dem Ermitteln der Testkriterien für gesamte Fahrzeuge, ist eine Konkretisierung auf partikulärer Ebene oft schwieriger.[188] Tests von fortgeschrittenen Fahrassistenzsystemen sind meistens Black-Box-Tests. Interne Strukturen und Systemzustände sind deswegen zusätzlich überwiegend unbekannt.[189] In allen Fällen stehen neuen Methoden und Vorgehensweisen Kosten-Nutzen-Abwägungen gegenüber. Auch ist grundsätzlich zu bedenken, dass neue Ansätze nicht die beabsichtigte Wirkung erzielen könnten. Kontinuierliche Prozesserweiterungen in der Praxis sind dennoch allein aufgrund veränderter Haftungsgrundlagen erforderlich.[190]

---

[182] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 454.

[183] Stellet, J. E. et al.: Validation of automated driving (2020), S. 64–65.

[184] Tietjen, T.; Decker, A.: FMEA-Praxis (2020), S. 81.

[185] Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010), S. 147.

[186] Ross, H.-L.: Funktionale Sicherheit im Automobil (2019), a: S. 122; b: S. 123.

[187] Woopen, T. et al.: UNICARagil - Disruptive Modular Architectures (2018), S. 22.

[188] Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019), S. 5.

[189] Schuldt, F. et al.: Test Case Generation for DAS (2018), S. 151.

[190] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), S. 96.

Chancen

Es existieren mehrere Vorschläge für neue und alternative Vorgehensweisen für die Testentwicklung automatisierter Fahrzeugsysteme. Einer sieht eine Testentwicklung mit testbaren Szenarien aus Äquivalenzklassen und Grenzwertanalysen vor. Gezieltes Testen durch Experten ist ein weiterer Ansatz. Personen mit umfangreichem Fachwissen wären möglicherweise in der Lage, auch ohne explizit erklärbare Methoden angemessene Tests zu definieren und Fehler zu finden.[191a] Eine weitere Idee sieht eine Zusammenfassung von Testergebnissen durch eine modellhafte "Fitness-Funktion" vor. Mit Testwiederholungen ließe sich das Minimum dieser Testfunktion bestimmen. Das globale Minimum der dabei ermittelten Funktion stünde dann für den kritischsten Testfall. Vorteil dieser Vorgehensweise wäre der Verzicht einer Zusammenfassung von Parameterbereichen. Im Gegenzug wird jedoch die Definition der "Fitness-Funktion" zur grundlegenden Herausforderung.[191b] Diese Ansätze ließen sich alle ebenfalls mit einer modularen Vorgehensweise kombinieren.

In jeder Entwicklung zweiter Ordnung, der Entwicklung von Entwicklungsprozessen, beschäftigen sich Kernfragen unter anderem mit Denkprozessen. Ganz konkret spielt die Bedeutung von Beurteilungen, Entscheidungen, Auswahlergebnissen, Entwürfen und Darstellungen auch in einer modularen Testentwicklung eine Rolle.[192] Nachvollziehbarkeit ist daher in allen Überlegungen von Bedeutung. Die von Noack in seiner Dissertation vorgeschlagene Vorgehensweise weist hier darauf hin, Informationselemente eines Testvorgehens systematisch zu verknüpfen. Treten trotz im Rahmen der Freigabe durchgeführter Testprozesse Fehler beim Verbraucher auf, ist so eine schnelle Rückverfolgung der verletzten Anforderungen auf zugeordnete Testfälle möglich.[193] Schon zuvor unterstützt eine solche Verknüpfung bei der Zuordnung von Testfällen auf einzelne Module.

Der Einsatz von Simulationsumgebungen liefert allgemeine Chancen, die sich auch für modulare Absicherung wahrnehmen lassen. Je nach Anwendungsfall reduzieren simulierte Umgebungen den Testaufwand, vereinfachen die Umsetzbarkeit oder reduzieren begleitende Gefährdungen. Schon bevor das reale System existiert besteht mit ihnen die Möglichkeit frühzeitige Untersuchungen durchzuführen. Ist das reale System unverstanden oder sehr komplex, lassen sich Interaktionen mit dem Umfeld manchmal auch leichter simulieren. Darüber hinaus sind Simulationstests unter anderem aufgrund vereinfachter Parametermodifikation besser reproduzierbar.[194] Möglicherweise ließe sich für solche Tests mit Sensordaten von Fahrzeugen aus dem Straßenverkehr ein realer Bezug herstellen.[195] Generell wäre mit maschinenlesbaren Spezifikationen eine Testautomatisierung denkbar. Auch die Dokumentation der Testaktivitäten könnte somit maschinell erfolgen. Wären Testziele und Testfälle automatisch durch Software ableitbar, wäre es möglich Prüfgegenstände ohne menschliche Eingriffe zu testen.[196]

---

[191] Schuldt, F. et al.: Test Case Generation for DAS (2018), a: S. 149–150; b: S. 150.

[192] Norbert Bolz: Bausteine zu einer Designwissenschaft (2016), S. 315.

[193] Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015), S. 96.

[194] Jipp, M.; Schneider, L.: Fahrtests unter Realbedingungen (2020), S. 34.

[195] Stellet, J. E. et al.: Validation of automated driving (2020), S. 67.

[196] Baumann, G.: Was verstehen wir unter Tests? (2006), S. 14–15.

7 Allgemeine Zukunftsperspektive

Bis vollständig automatisierte Fahrzeuge den Straßenverkehr verändern können, gilt es weiterhin auftretende Problemstellungen zu bewältigen. Elementare Herausforderung des Projekts UNICAR*agil* liegt im Umgang mit der Komplexität des entwickelten Systems. Allein durch die Automation des Fahrzeugs entstehen zwischen einzelnen Blickwinkeln in der Fahrzeugarchitektur stärkere Verflechtungen.[197a] Unabhängig davon, ob das Projekt ein marktreifes Fahrzeug hervorbringt, wird es daher neue Herangehensweisen für den Umgang mit Komplexität liefern. Nicht nur die beabsichtigte modulare Zusammensetzung aus unabhängigen Komponenten wird neue Erkenntnisse hervorbringen. Sicherheitsaspekte werden bereits während der Auslegungen berücksichtigt. Ohne Verschwiegenheitserklärungen findet dabei ein offener Austausch verschiedener Sicherheitsansätze statt.[197b]

Modulare Vorgehensweisen bieten hier die Möglichkeit auch herausfordernde Aufgaben intensiv zu bearbeiten. Der offene Austausch des Projekts liefert hier auch die nötigen Voraussetzungen um aus einzelnen Resultaten durch Ergänzen und Verknüpfen ein einheitliches Arbeitsergebnis zu schaffen.

Bei allem bleibt dennoch die bedeutende Frage: "Wie sicher, ist sicher genug?"[198] Unter allen autonom intelligenten Systemen, die sich derzeit in Entwicklung befinden, gelten den selbstfahrenden Autos besonders hohe Erwartungen. Möglicherweise sind die größten entstehenden Herausforderungen autonomer Systeme nicht technischer, sondern menschlicher Natur. Digital verbundene Technik wird größere Mengen von Daten produzieren, als angemessen menschlich interpretierbar. Auch mit zunehmender Zusammenarbeit in virtuellen Umgebungen sind neue Fähigkeiten gefragt.[199] Zunehmende Komplexität der zu entwickelnden Systeme verlangt nach einem formalisierten Umgang mit dem Wissen einzelner Entwicklungsbereiche. Grundsätzlich wichtig ist hier an erster Stelle die Akzeptanz für neue Konzepte und Ansätze.[200] Neben technologischen Hürden in Forschung und Entwicklung, sind für eine fortschreitende Fahrzeugautomatisierung jedoch auch juristische und gesellschaftliche Herausforderungen zu lösen.[201] Eine vollständige Sicherheit im Straßenverkehr wird es durch autonomes Fahren vermutlich nicht geben. Unfälle bereits freigegebener Fahrzeuge werden methodische Zweifel an einzusetzenden Freigabeverfahren erhalten. Daher stellt eine transparente öffentliche Diskussion eine notwendige Grundlage für alle Freigabeverfahren dar.[202]

Unser Erfolg bei der Gestaltung von Lösungen für komplexe Probleme, wird weiterhin von der Fähigkeit abhängen die damit einhergehende Komplexität zu bewältigen.[203]

---

[197] Stolte, T. et al.: Safety Concepts for Automated Vehicles (2020), a: S. 1562; b: S. 1562-1563.

[198] Amersbach, C. T.: Dissertation, Decomposition Approach - Reducing Validation Effort (2020), S. 101.

[199] Briffaut, J.-P.: Complexity and Systems Thinking (2019), S. 44.

[200] Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011), S. 362.

[201] Reschka, A.: Sicherheitskonzept für autonome Fahrzeuge (2015), S. 510.

[202] Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015), S. 463.

[203] Ertas, A.: Systemic Thinking & Problem Solving (2018), S. 6.

Anhang

Black Box Betrachtung des Dynamikmoduls mit inneren Zusammenhängen

Subsystem	Eingangsgrößen		Funktionen	Ausgangsgrößen
Steuergerät	**Vorgaben** Signale **Energie** **Umwelt**	**Soll-Radgeschwindigkeit** **Soll-Lenkwinkel** Temperatur Lenkung Ist-Raddrehzahl Ist-Antriebsmoment Ist-Lenkwinkel Ist-Lenkmoment **48V DC Bordstrom** **Einflüsse und Störgrößen**	**Wertevorgaben empfangen**, **erreichte Leistungswerte,** **Zustand und Leistungskapazitäten** **an Stammhirn kommunizieren,** statische und dynamische Geschwindigkeits- und Lenkvorgaben umsetzen, Energieverwaltung für Rekuperation & Leistungsabgabe	**Umwelt: Wärmeabgabe** **Signal: Hydrauliksteuerung** **Signal: Temperatur Lenkung** **Signal: Ist-Raddrehzahl** **Signal: Ist-Antriebsmoment** **Signal: Ist-Lenkwinkel** **Signal: Ist-Lenkmoment**
Perimeter-bremse	Vorgaben Signal **Energie** **Umwelt**	Parkbremssignal, Rückenmark hydraulischer Druck Raddrehzahl für ABS **hydraulischer Druck** **12V DC Bordstromnetz** **Einflüsse und Störgrößen**	**mechanisches Bremsen** **Notbremsfunktion mit Bremspedal** **in der Fahrgastzelle** **Parkbremsfunktion,** **Positionssicherung im Stillstand** ABS-Funktion	**Moment: Bremse** Signal: Drehzahl
Radantrieb	Vorgaben **Energie** **Umwelt**	Sollmoment Drehzahlgrenzen **48V DC Bordstromnetz** **Einflüsse und Störgrößen**	**Radgeschwindigkeit halten** **Radgeschwindigkeit erhöhen** **Radgeschwindigkeit rekuperativ verzögern** Sensorerfassung: Raddrehzahl Leistungselektronik: Strom transformieren (DC & AC)	**Moment: Antrieb / Bremse** **Leistung: Strom rekuperiert** **Umwelt: Wärmeabgabe** Signal: Ist-Raddrehzahl Signal: Ist-Antriebsmoment
Lenkeinheit	Vorgaben **Energie** **Umwelt**	Lenkwinkel **48V DC** **12V DC für Fail Silent Bremse** **Einflüsse und Störgrößen** **auch: Widerstandsmomente**	**statische & dynamische Lenkwinkelvorgaben** **einhalten,** **Feststellbremse für Ausfallsituationen,** Spannungswellengetriebe: Übersetzung, Zustandsüberwachung durch Temperatursensoren, Sensorerfassung: Lenkmoment, Sensorerfassung: Lenkwinkel, Leistungselektronik: Strom transformieren (DC zu AC)	**Moment: Lenkmoment** **Moment: FS Bremse** **Umwelt: Wärmeabgabe** Signal: Ist-Lenkwinkel Signal: Ist-Lenkmoment Signale: Temperaturwerte

Fett gedruckte Angaben sind auch dann von Bedeutung, wenn innere Zusammenhänge unberücksichtigt bleiben.

Abb. 7-1: Detaillierte Tabellarische Black Box Betrachtung des Dynamikmoduls

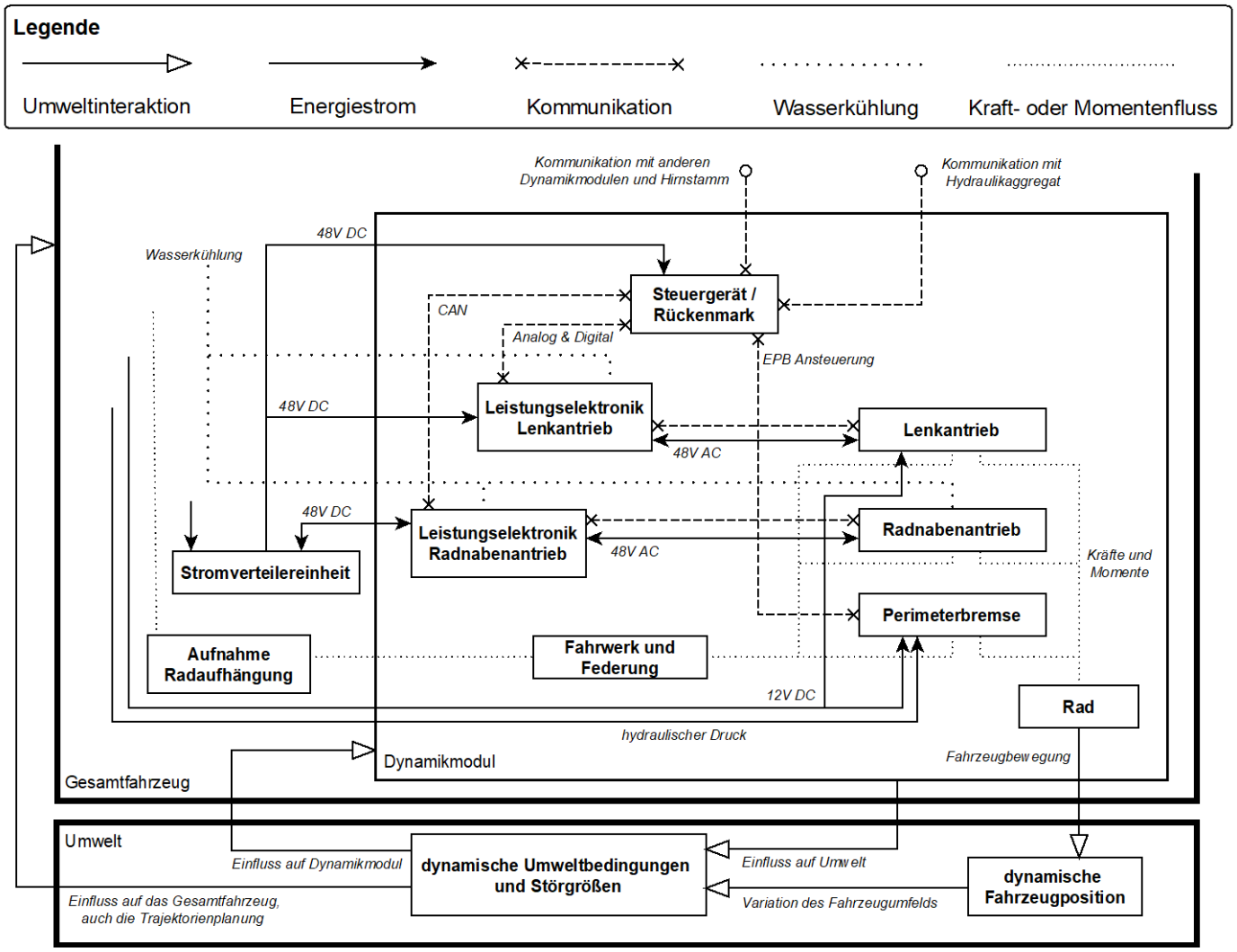

Abb. 7-2: Umfangreiches Kontrollflussdiagramm des Dynamikmoduls

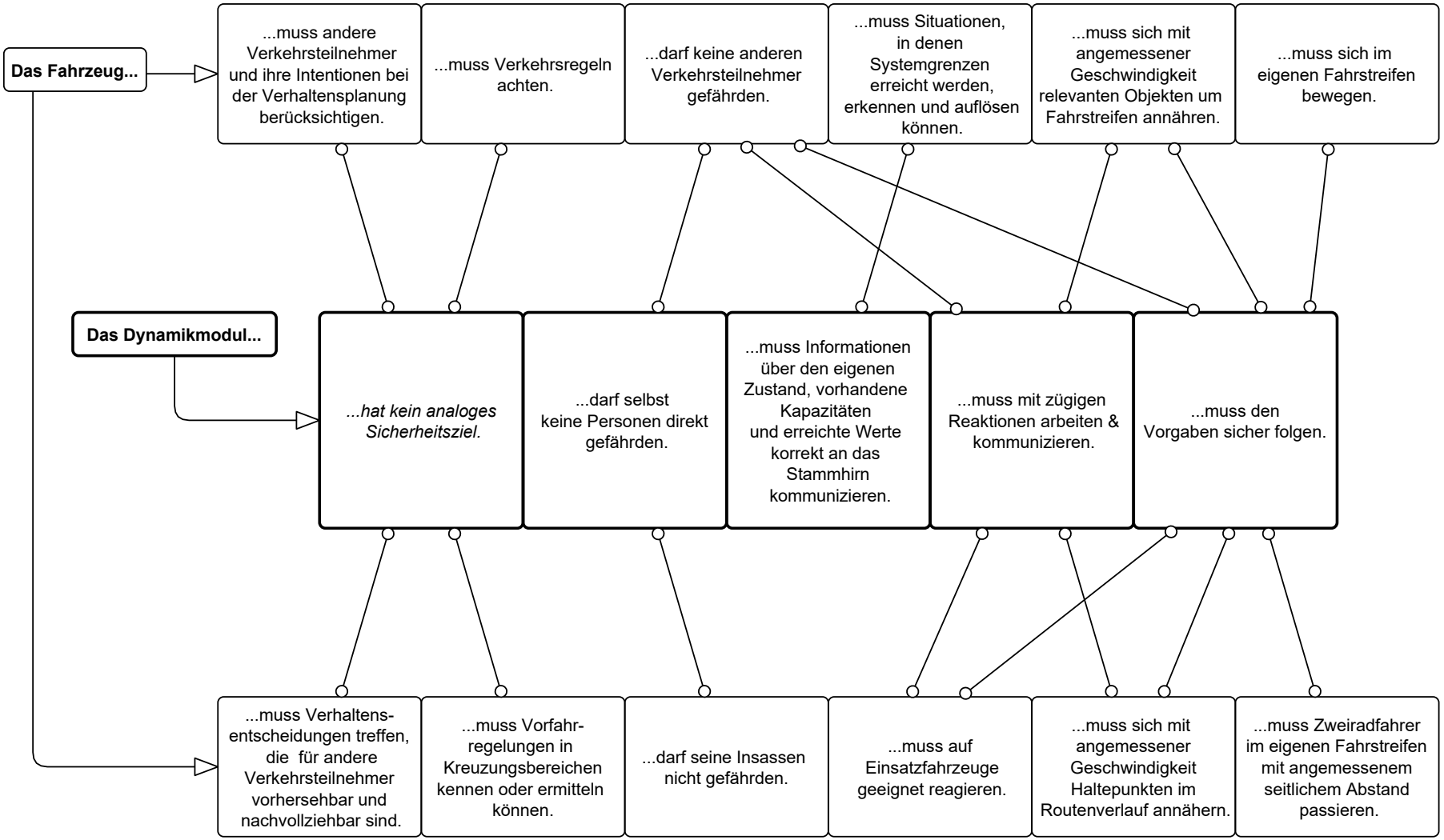

Abb. 7-3: Ableitung von Sicherheitszielen für das Dynamikmodul

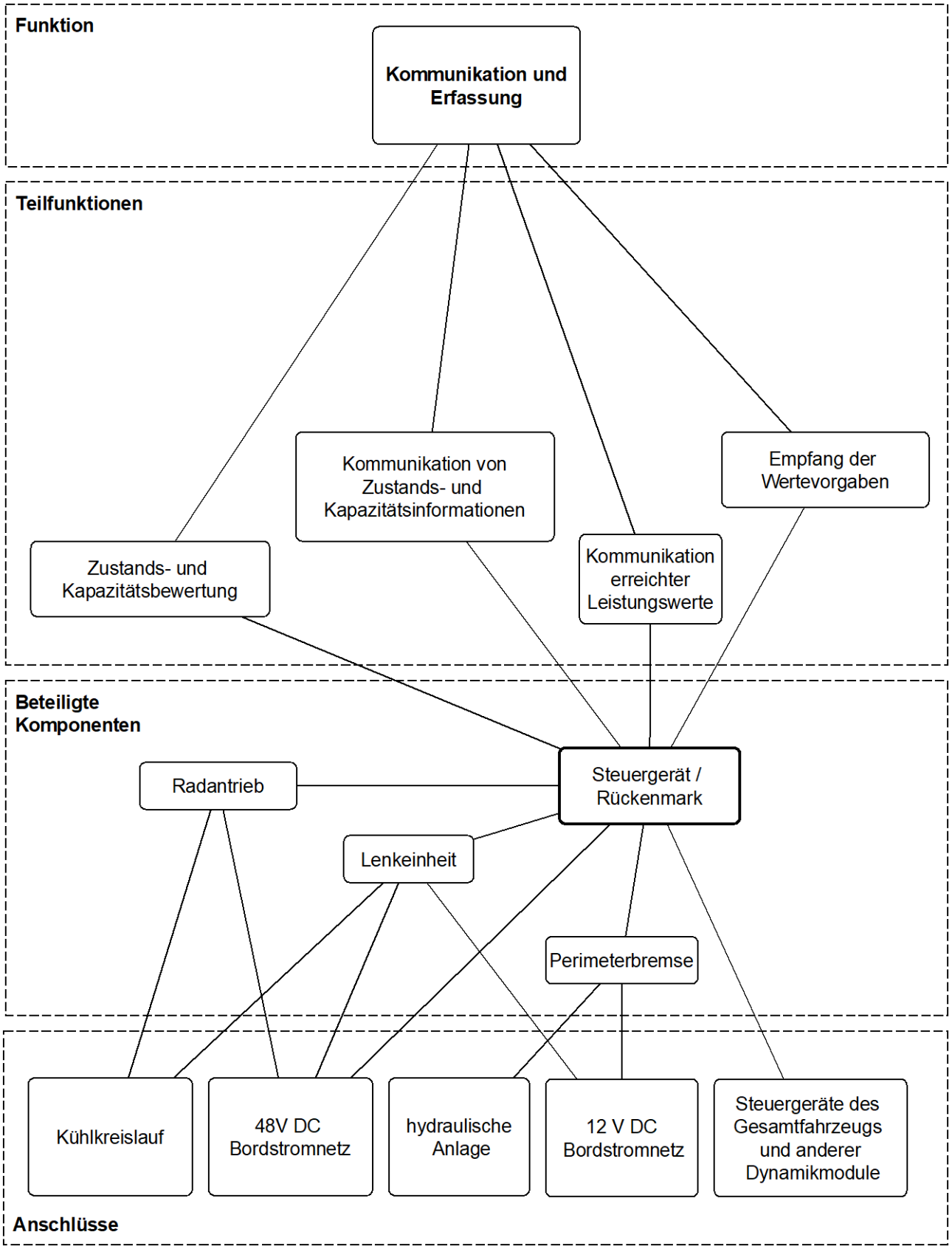

Abb. 7-4: Funktionsanalyse: Kommunikation und Erfassung

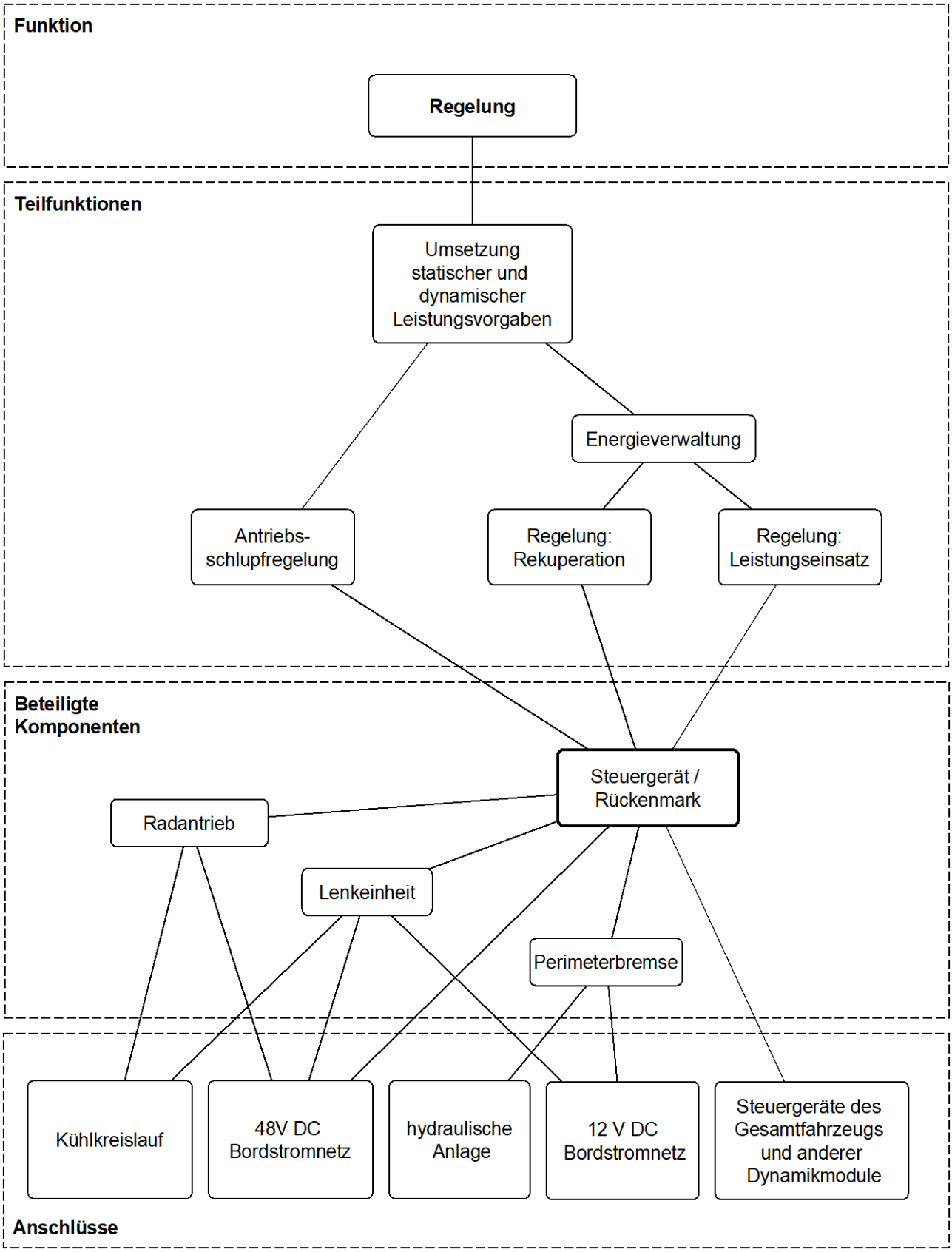

Abb. 7-5: Funktionsanalyse: Regelung

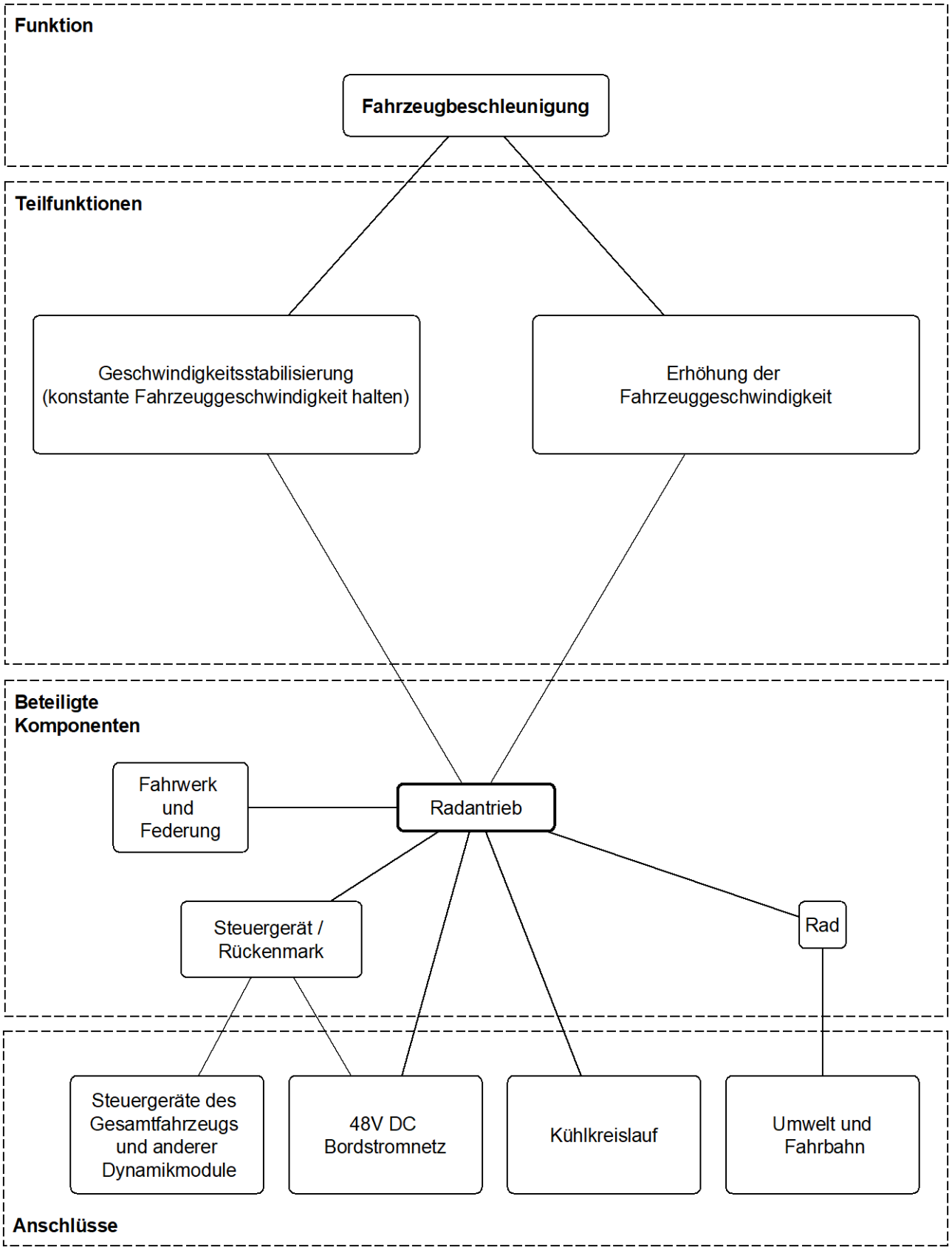

Abb. 7-6: Funktionsanalyse: Fahrzeugbeschleunigung

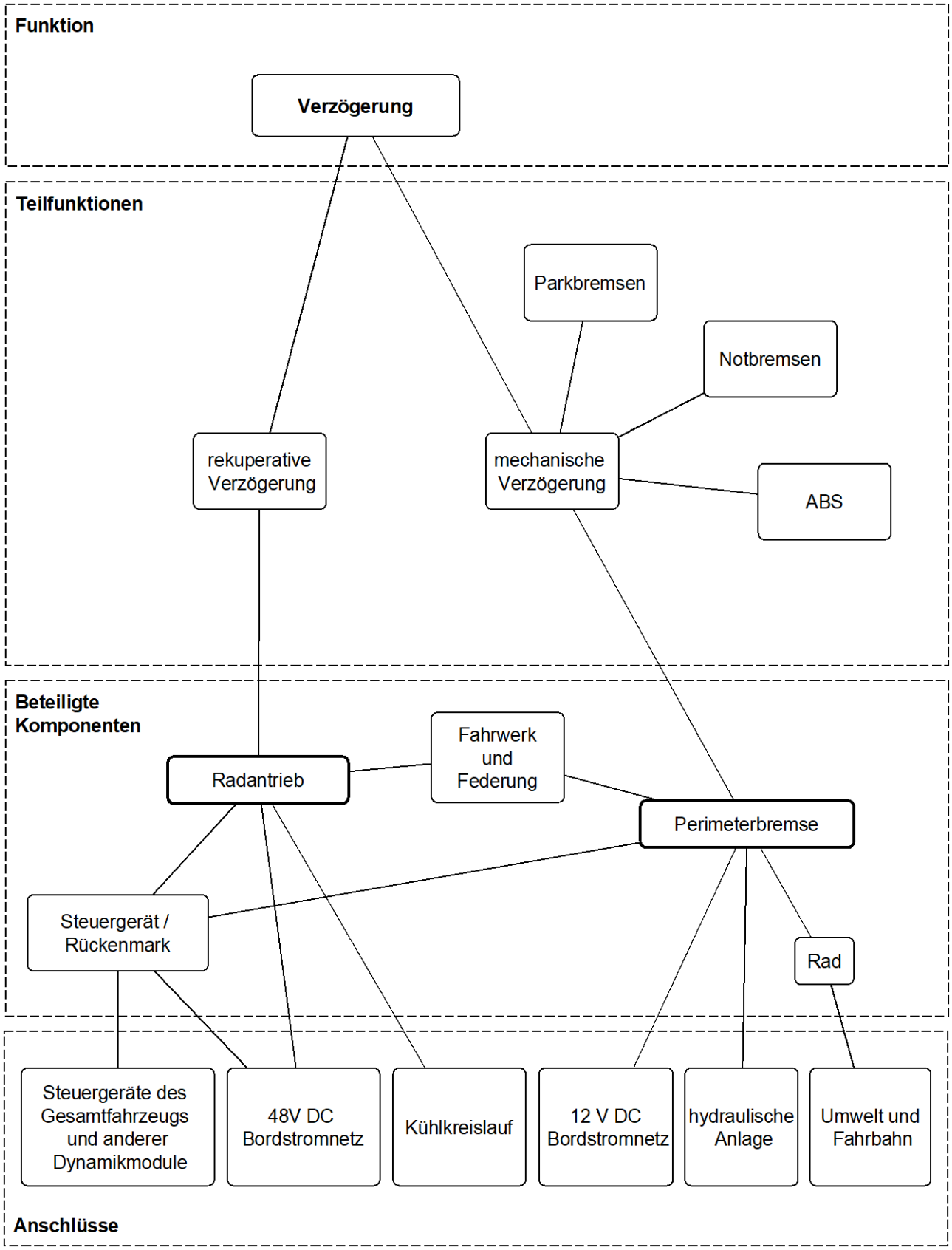

Abb. 7-7: Funktionsanalyse: Verzögerung

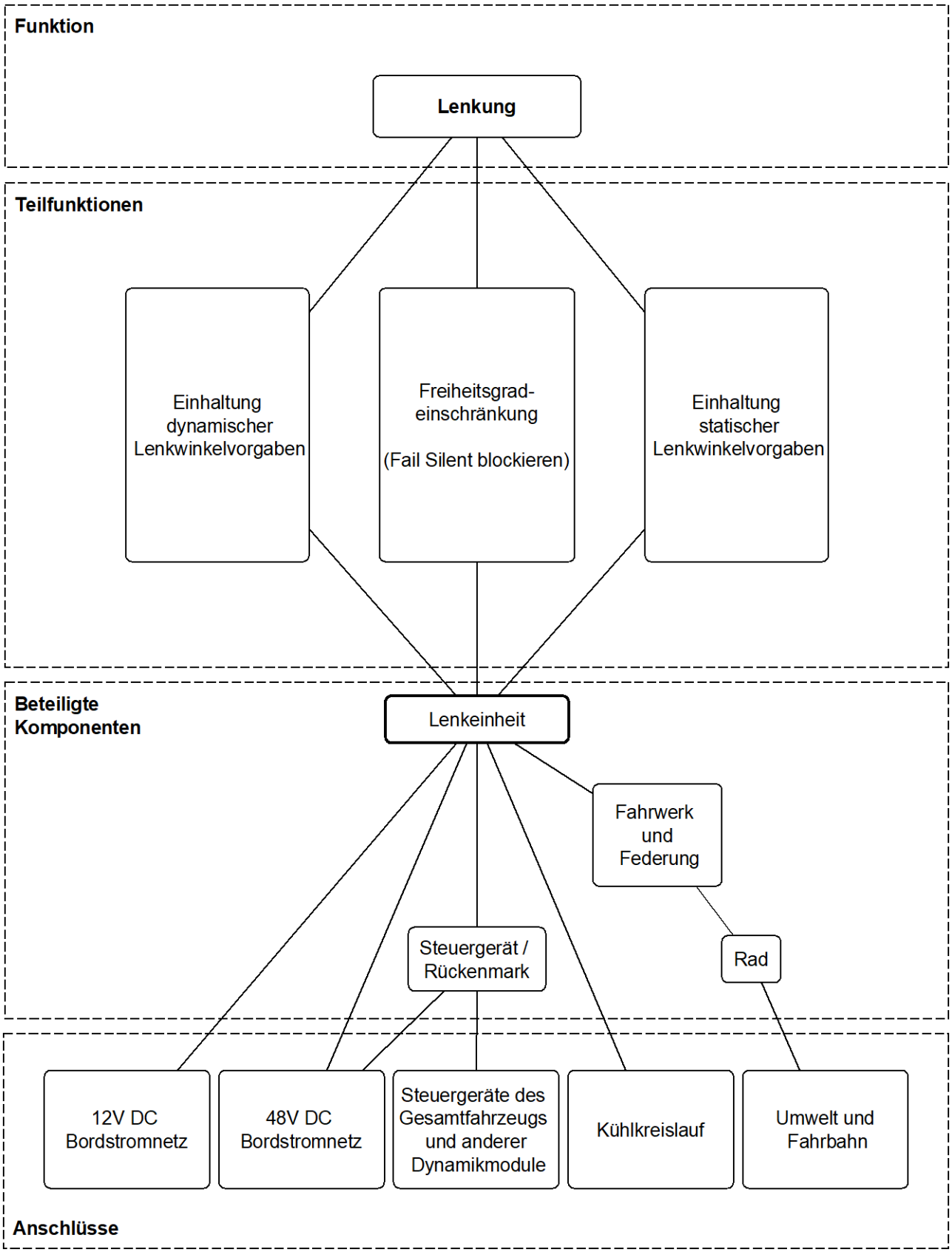

Abb. 7-8: Funktionsanalyse: Lenkung

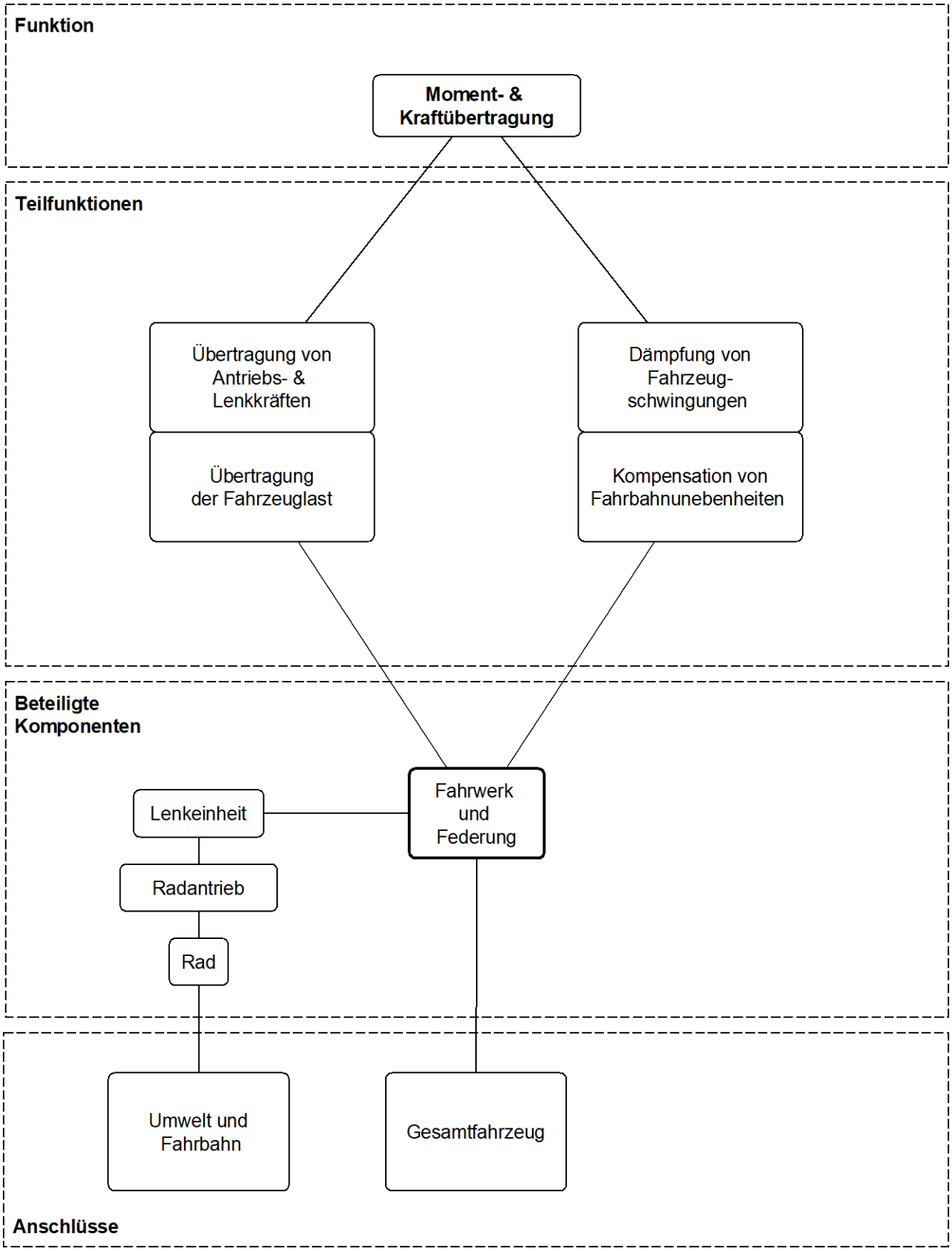

Abb. 7-9: Funktionsanalyse: Moment- & Kraftübertragung

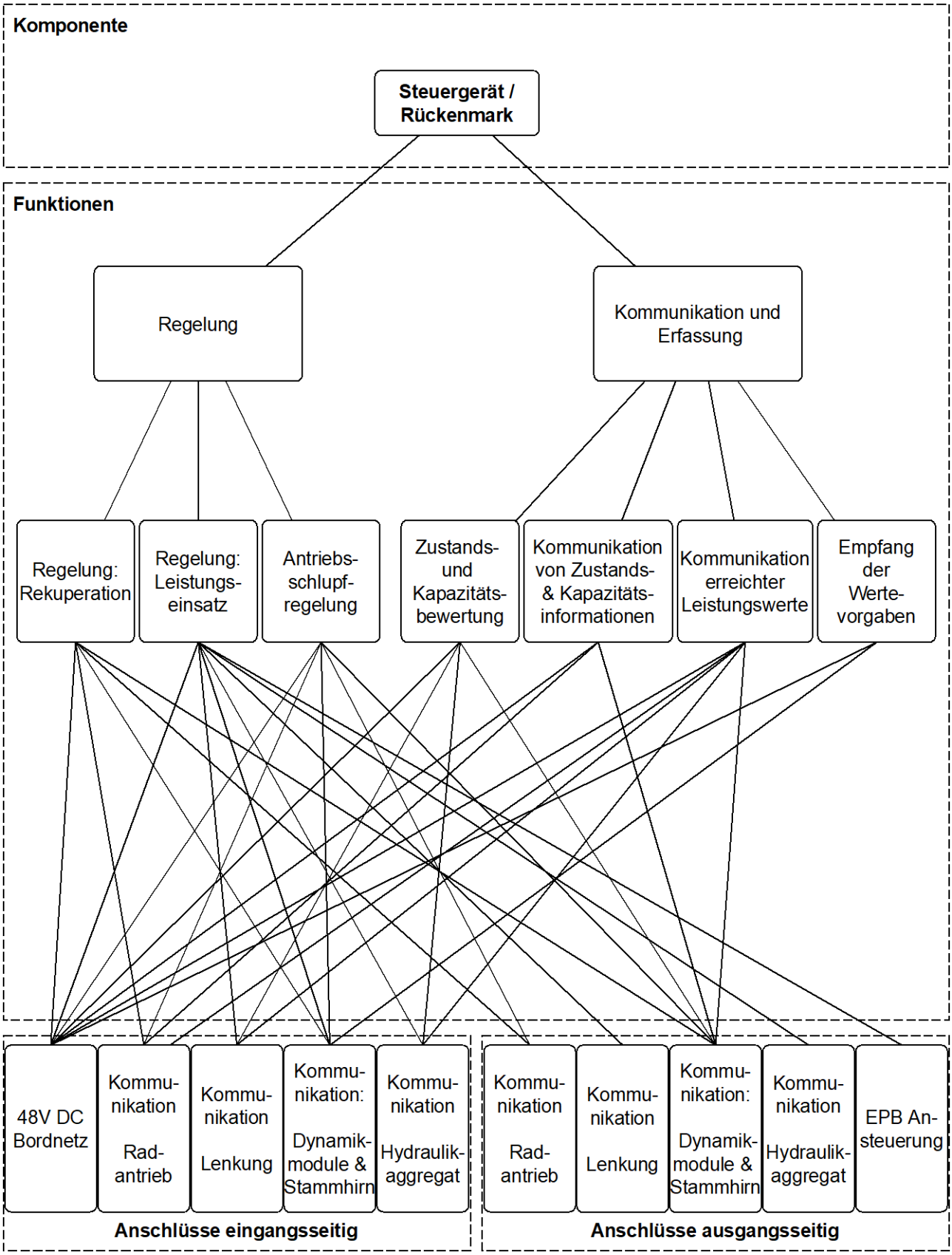

Abb. 7-10: Strukturanalyse: Steuergerät

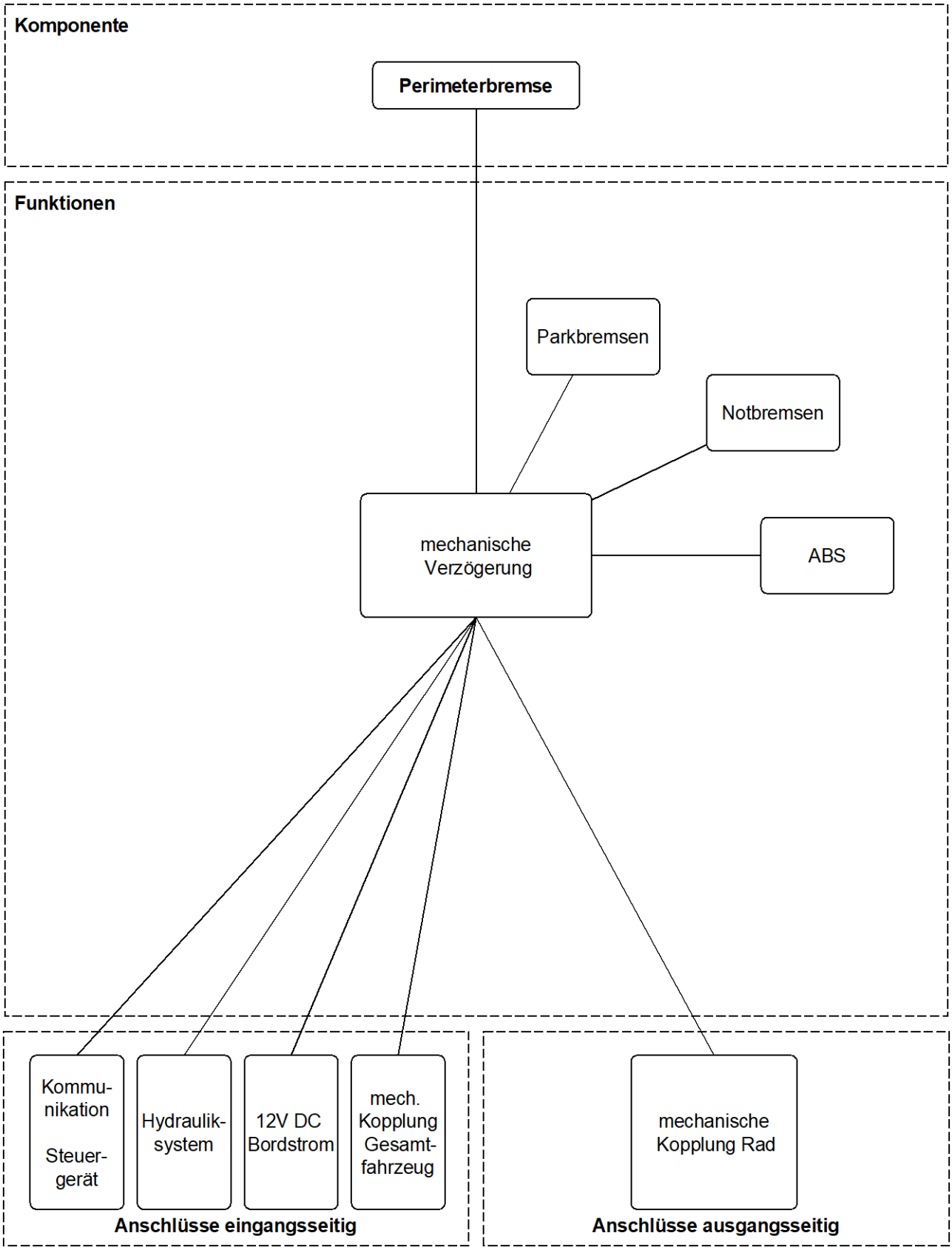

Abb. 7-11: Strukturanalyse: Perimeterbremse

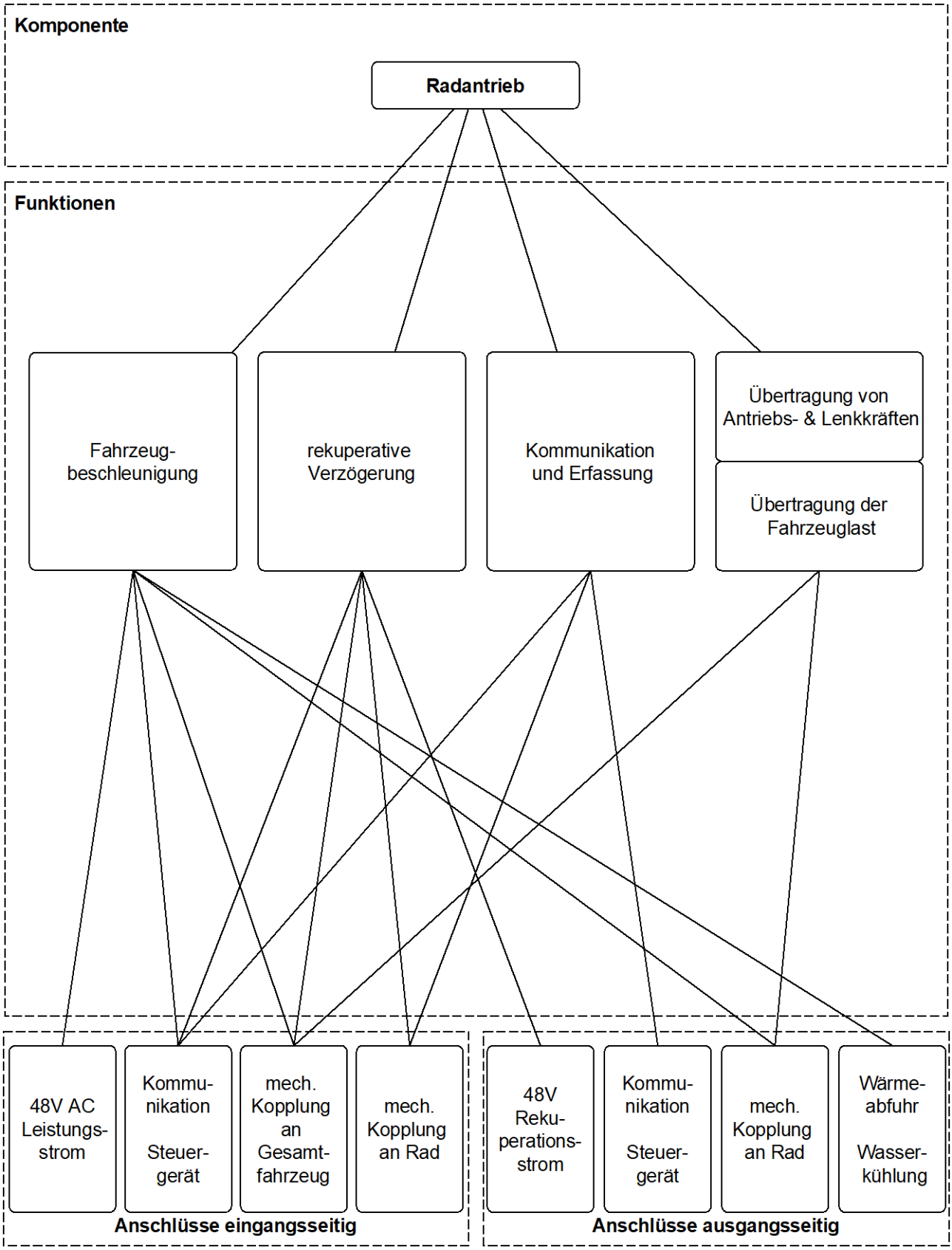

Abb. 7-12: Strukturanalyse: Radantrieb

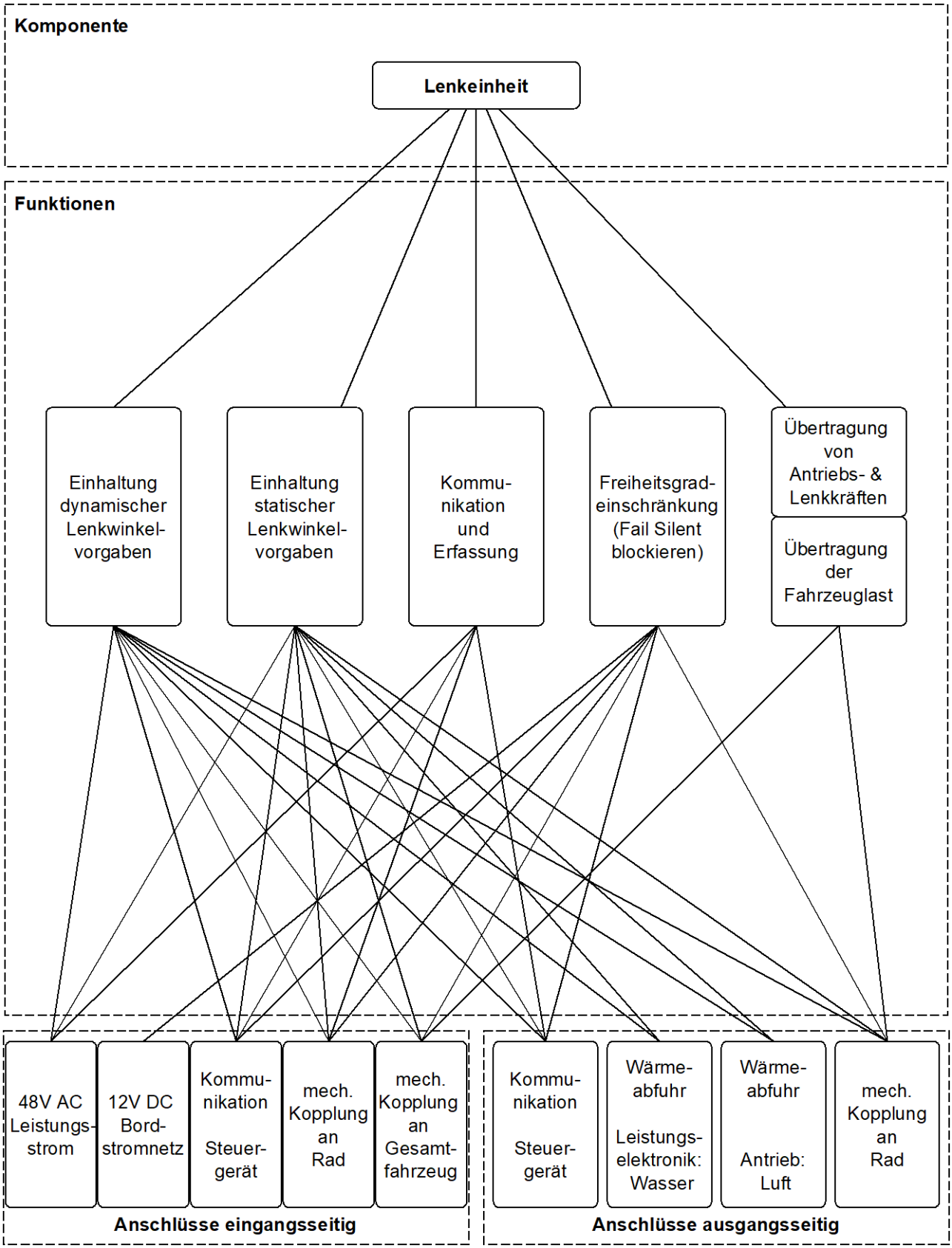

Abb. 7-13: Strukturanalyse: Lenkeinheit

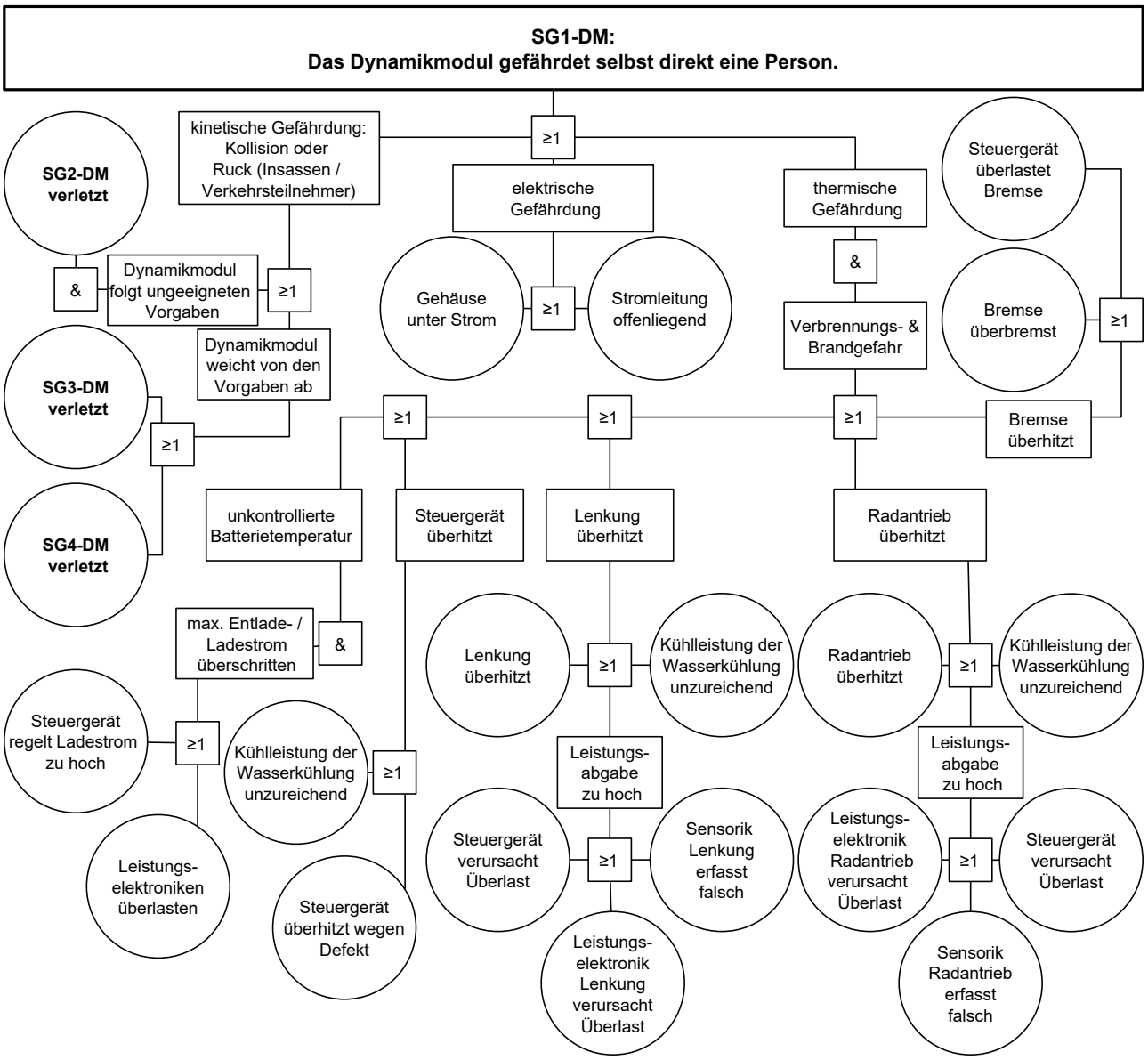

Abb. 7-14: Fehlerbaumanalyse: Verletzungen von SG1-DM

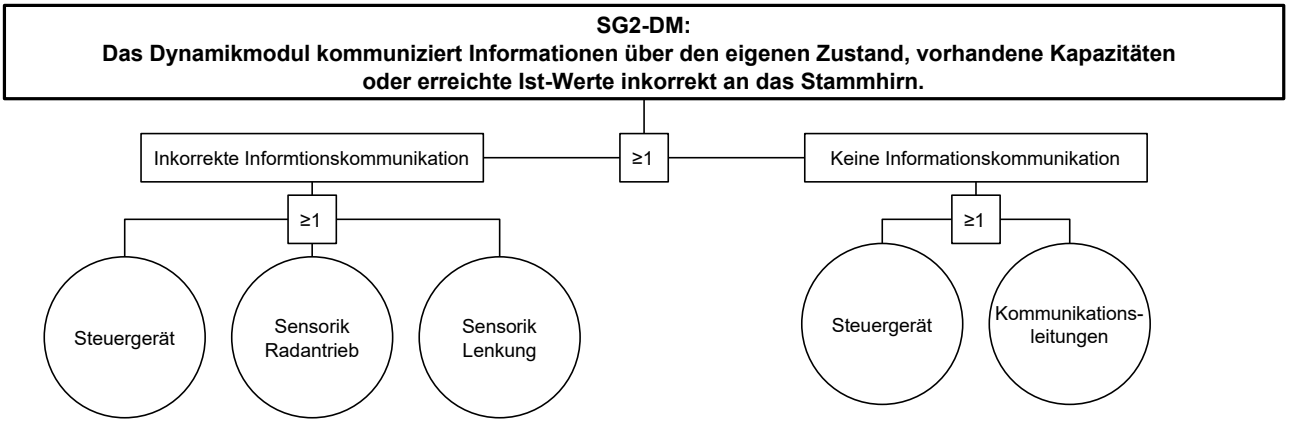

Abb. 7-15: Fehlerbaumanalyse: Verletzungen von SG2-DM

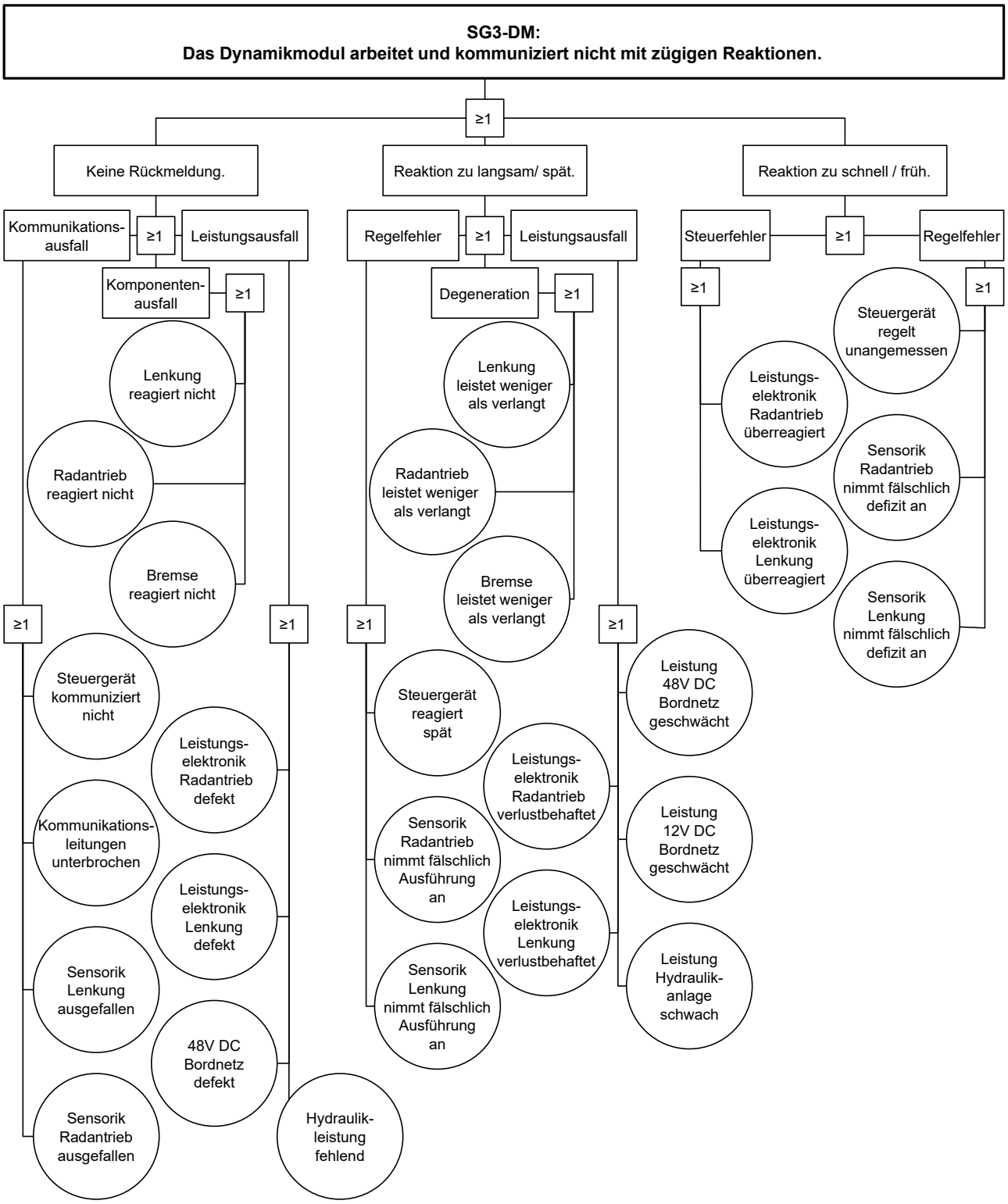

Abb. 7-16: Fehlerbaumanalyse: Verletzungen von SG3-DM

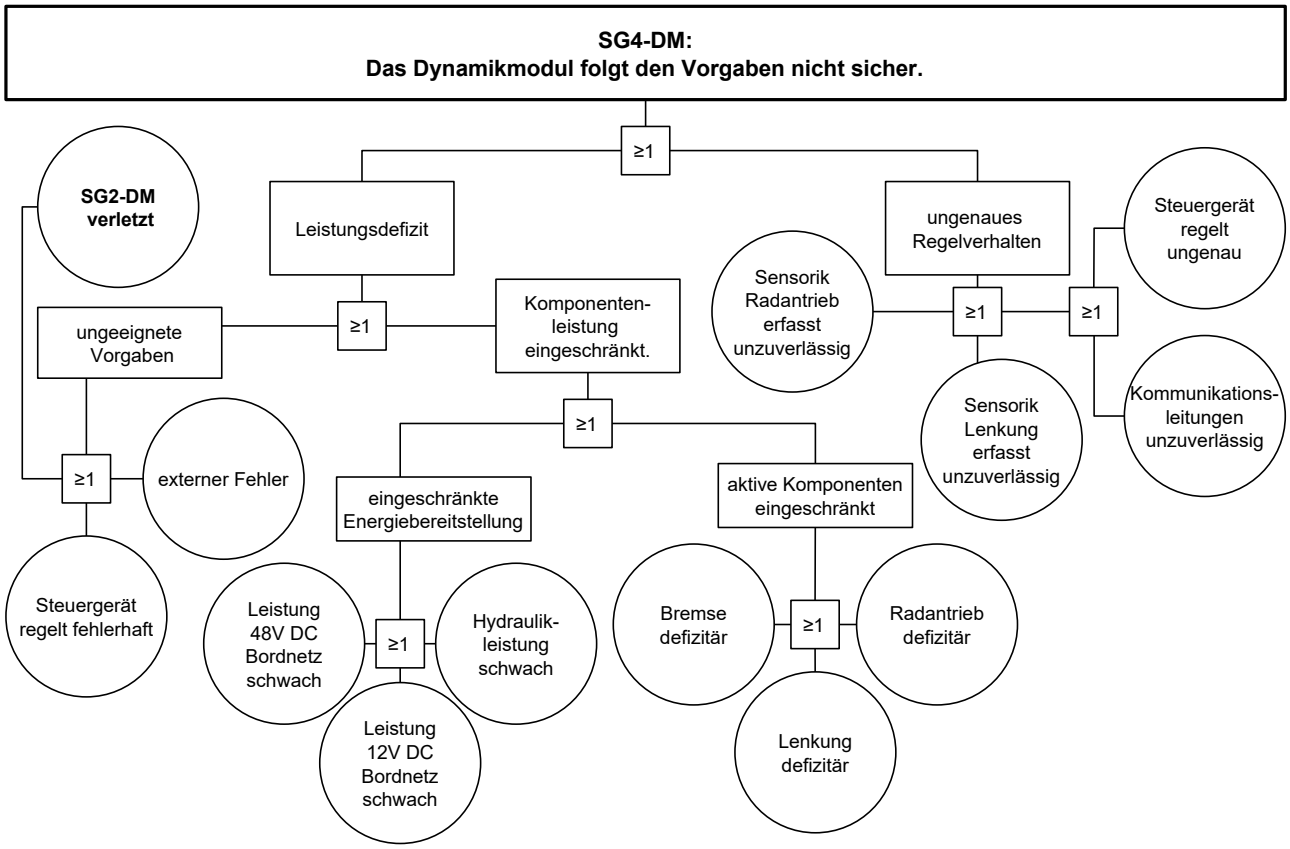

Abb. 7-17: Fehlerbaumanalyse: Verletzungen von SG4-DM

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
1001	Steuergerät	Regelung	Regelung: Rekuperation	Verringerte Reichweite	Ineffiziente Rekuperation	Rekuperation muss möglichst effizient stattfinden.	S0	E2	C1	QM	fehlt
1002				Brandgefahr	Zu starke Rekuperation, Batterieüberlastung	Der temporär maximal zulässige Ladestrom darf nicht überschritten werden.	S3	E1	C3	QM	SG1 DM
1003				Unsicheres Ruckhaftes Anhalten	Regelung unsanft	Ruckartige Regelung der Rekuperation darf Beschleunigungsgrenzen nicht überschreiten.	S2	E1	C1	QM	SG1 DM
1004				Bremsen nicht mehr ausfallsicher	Rekuperatives Bremsen unmöglich	Kontrolliertes Anhalten muss jederzeit möglich sein.	S3	E1	C1	QM	SG1 DM
1005	Steuergerät	Regelung	Regelung: Leistungseinsatz	Brandgefahr	zu starke Energieabfrage, Batterieüberlastung	Der temporär maximal zulässige Entladestrom darf nicht überschritten werden.	S3	S1	S3	A	SG1 DM

Tabelle 7-1: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (I)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
1006	Steuergerät	Regelung	Regelung: Leistungseinsatz	Verringerte Reichweite	Ineffiziente Leistungsregelung	Steuerung der Leistungsregelung muss effizient erfolgen	S 0	E 2	C 1	QM	fehlt
1007				Unsicheres Fahrverhalten	Ungeeignete Leistungsregelung	Die empfangenen Vorgaben müssen eingehalten werden.	S 3	E 2	C 3	B	SG4 DM
1008				Unsicheres Fahrverhalten	Reaktionsgeschwindigkeit langsam	Die Reaktionsgeschwindigkeit muss in einem angemessenen Rahmen bleiben.	S 3	E 2	C 3	B	SG3 DM
1009				Thermische Belastung	Komponenten und Stromleiter überhitzen	Zu spezifizierende Temperaturgrenzen müssen eingehalten werden.	S 1	E 3	C 1	QM	SG1 DM
1010	Steuergerät	Regelung	ASR	Unsicheres Fahrverhalten	Traktionsverlust	Die ASR muss bestmögliche Traktion sichern.	S 2	E 2	C 2	QM	SG4 DM
1011				Unsicheres Fahrverhalten	Verlangsamtes Beschleunigen	Die ASR muss bestmögliche Beschleunigung sichern.	S 1	E 3	C 2	QM	SG4 DM

Tabelle 7-2: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (II)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
1012	Steuergerät	Regelung	ASR	Unsicheres Fahrverhalten	Schlechtes Kurvenverhalten *(Differential)*	Die ASR darf sicheres Kurvenverhalten nicht einschränken	S 2	E 2	C 2	QM	SG1 DM
1013	Steuergerät	Kommunikation	Empfang der Wertevorgaben	Unsicheres Fahrverhalten	Leistungsvorgaben werden nicht umgesetzt	Vorgabewerte müssen immer sicher empfangen werden.	S 3	E 2	C 3	B	SG4 DM
1014				Unsicheres Fahrverhalten	Umsetzung unangemessener Leistungsvorgaben	Unangemessene Vorgabewerte dürfen nicht umgesetzt werden.	S 3	E 2	C 3	B	SG1 DM
1015				Komponentenschaden	Umsetzung von Kapazitätsüberschreitenden Vorgaben	Kapazitätsübergreifende Vorgaben dürfen nicht umgesetzt werden.	S 3	E 3	C 1	A	SG1 DM
1016	Steuergerät	Kommunikation	Zustands- und Kapazitätsbewertung	Komponentenschaden	Zustand und Kapazitäten ungenau erfasst	Zustand und Kapazität müssen korrekt erfasst werden.	S 3	E 2	C 2	A	SG2 DM

Tabelle 7-3: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (III)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
1017	Steuergerät	Kommunikation	Zustands- und Kapazitätsbewertung	Unsicheres Fahrverhalten	Zustand und Kapazitäten ungenau erfasst	Zustand und Kapazität müssen korrekt erfasst werden	S 3	E 2	C 3	B	SG2 DM
1018	Steuergerät	Kommunikation	Kommunikation über Zustand & Kapazität	Verringerte Leistungsabgabe	Fälschlich als schlecht erfasste Kapazität	Zustände und Kapazitäten müssen korrekt kommuniziert werden.	S 0	E 1	C 2	QM	SG2 DM
1019			Kommunikation über Zustand & Kapazität	Vorgaben nicht umsetzbar	Fälschlich gut erfasste Kapazität	Zustände und Kapazitäten müssen korrekt kommuniziert werden.	S 2	E 1	C 3	QM	SG2 DM
1020	Steuergerät	Kommunikation	Kommunikation erreichter Werte	Planung der Vorgaben erfolgt unsicher.	Voraussehen der Planung falsch	Erreichte Werte müssen korrekt erfasst und kommuniziert werden.	S 2	E 2	C 2	QM	SG2 DM
2001	Perimeterbremse	mech. Verzögerung	Schlechte Steuerung	Anfahrruck	Bremse löst beim Anfahren ruckartig	Die Bremse muss komfortables Anfahren ermöglichen.	S 0	E 4	C 2	QM	SG1 DM

Tabelle 7-4: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (IV)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
2002	Perimeter-bremse	mech. Verzöge-rung	Ungewünsch-tes Lösen	Fahrzeug rollt unkontrolliert aus Parkposition	Stromenergie / hydr. Druck fal-len ab	Die Perimeterbremse muss auch langfristig sicheres Par-ken ermöglichen.	S 2	E 1	C 3	QM	SG1 DM
2003			schwache Bremskraft	Kollision	geringer hydrau-lische Druck	Die gesetzlich geforderte Bremsleistung muss jederzeit leistbar sein.	S 2	E 2	C 3	QM	SG4 DM
3001	Radantrieb	Fahrzeug-beschleu-nigung	Leistungsstrom stellen	Unangemessener Leistungsstrom	Falsche Regelung durch Steuergerät	Leistungsstrom des Antriebs muss korrekt geregelt wer-den.	S 3	E 1	C 2	A	SG4 DM
3002		Rekupera-tive Ver-zögerung	Rekuperations-strom übermit-teln	Unangemessener Rekuperations-strom	Falsche Regelung durch Steuergerät	Rekuperationsstrom des An-triebs muss korrekt geregelt werden.	S 3	E 1	C 2	QM	SG4 DM
3003		Fahrzeug-beschleu-nigung & Rekupera-tion	Vorgabenab-weichung	Reaktionsge-schwindigkeit weicht ab	Verschlissene Komponenten	Komponentenverschleiß des Motors darf Einhaltung von Vorgaben nicht stören.	S 1	E 1	C 2	QM	SG3 DM

Tabelle 7-5: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (V)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
3004	Radantrieb	Fahrzeug-beschleu-nigung & Rekupera-tion	Vorgabenab-weichung	Reaktionsge-schwindigkeit weicht ab	Sensorik arbeitet mangelhaft.	Die Antriebssensorik muss genaue Informationen über das erreichte Verhalten lie-fern.	S 3	E 2	C 2	A	SG3 DM
3005				Reaktionsge-schwindigkeit weicht ab	Umwelteinflüsse (Schmutz / Eis)	Umwelteinflüsse dürfen den Motor nicht bei der Einhal-tung von Vorgaben stören.	S 3	E 2	C 2	A	SG3 DM
3006				Reaktionsgenau-igkeit weicht ab	Sensorik mangel-haft	Mangelhafte Sensorik darf die Genauigkeit des Radan-triebs nicht einschränken.	S 1	E 3	C 3	A	SG4 DM
3007				Vorgabenüber-schreitung	Sensorik arbeitet mangelhaft	Die Antriebssensorik muss genaue Informationen über das erreichte Verhalten lie-fern.	S 1	E 3	C 3	A	SG4 DM
3008				Vorgabenunter-schreitung	Leistungskapazi-tät überschritten	Antriebsvorgaben dürfen nicht außerhalb der Kapazitä-ten.	S 3	E 2	C 3	A	SG2 DM

Tabelle 7-6: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (VI)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
3009	Radantrieb	Fahrzeug-beschleu-nigung & Rekupera-tion	Vorgabenab-weichung	Vorgabenunter-schreitung	Sensorik arbeitet mangelhaft	Die Antriebssensorik muss genaue Informationen über das erreichte Verhalten lie-fern.	S 2	E 3	C 3	B	SG2 DM
4001	Lenkeinheit	Vorgaben-einhaltung	Regelung	Unangemessener Leistungsstrom	Falsche Regelung durch Steuergerät	Leistungsstrom der Lenkung muss korrekt geregelt wer-den.	S 3	E 1	C 2	Q M	SG4 DM
4002			Vorgaben ver-letzt	Reaktionsge-schwindigkeit schlecht	Verschlissene Komponenten	Komponentenverschleiß darf Einhaltung der Vorgaben nicht stören.	S 3	E 2	C 2	A	SG3 DM
4003					Umwelteinflüsse (Schmutz / Eis)	Umwelteinflüsse dürfen nicht bei der Einhaltung von Lenk-vorgaben stören.	S 3	E 3	C 2	B	SG3 DM
4004				Reaktionsgenau-igkeit schlecht	Sensorik mangel-haft	Mangelhafte Sensorik darf die Genauigkeit des Lenkan-triebs nicht beeinträchtigen.	S 3	E 3	C 2	B	SG4 DM

Tabelle 7-7: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (VII)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
4005	Lenkeinheit	Vorgaben-einhaltung	Vorgaben ver-letzt	Lenkvorgaben übertroffen	Sensorik arbeitet mangelhaft	Die Lenksensorik muss ge-naue Informationen über das Ist-Verhalten liefern.	S 3	E 2	C 2	A	SG4 DM
4006				Lenkvorgaben unterschritten	Leistungskapazi-tät überschritten.	Der vorgesehene Einsatzbe-reich darf nicht überschritten werden.	S 3	E 1	C 3	A	SG4 DM
4007					Sensorik arbeitet mangelhaft.	Die Lenksensorik muss ge-naue Informationen über er-reichte Werte liefern.	S 3	E 2	C 2	A	SG4 DM
4008			Falsche Vorga-ben umgesetzt	Zulässiger Lenk-winkelbereich wird überschrit-ten	Anschlag überschritten	Ein Anschlag muss den Lenk-winkelbereich begrenzen.	S 2	E 3	C 1	Q M	SG4 DM
4009		Freiheits-grad Ein-schrän-kung	Feststellbremse funktioniert nicht.	Unkontrollierba-res Fahrzeugver-halten.	Bremse festge-setzt.	Ein Kontrollmechanismus muss die Freigängigkeit der Bremse erfassen.	S 3	E 1	C 1	Q M	SG1 DM

Tabelle 7-8: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (VIII)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
4010	Lenkeinheit	Lenkung blockieren	Feststellbremse funktioniert nicht.	Unkontrollierbares Fahrzeugverhalten.	fehlende Stromversorgung	Die Stromversorgung der Feststellbremse muss sichergestellt sein.	S 3	E 1	C 2	QM	SG1 DM
4011					Signal wird nicht ausgelöst	Die Feststellbremse muss ausgelöst werden sobald die Lenkung unkontrollierbar wird.	S 3	E 1	C 3	A	SG1 DM
8001	Radantrieb & Lenkeinheit	Erfassung	Einschränkung wird nicht erfasst.	Unvorhersehbares Verhalten	Lagerschaden verursacht Schwingungen, Harmonic Drive lokal defekt	Vorgesehene Kontrollmechanismen müssen alle gefährdenden Defekte entdecken.	S 3	E 2	C 2	A	SG1 DM
8002				Spätes Erkennen von Defekten	Unvorhergesehener Temperaturanstieg meldet Schaden zu spät.	Kritische Schäden müssen temperaturunabhängig erkannt werden.	S 2	E 2	C 1	QM	SG1 DM

Tabelle 7-9: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (IX)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
8003	Radantrieb & Lenkeinheit	Erfassung	Einschränkung fälschlich erfasst.	Ineffizientes Verhalten	Wirkende Momente werden falsch gemessen.	Die Sensorik darf Einschränkungen nicht fälschlich wahrnehmen.	S 1	E 2	C 2	QM	SG2 DM
8004		Erfassung	Einschränkung mangelhaft erfasst.	Unangemessenes Fahrzeugverhalten	Reales Schadensausmaß weicht vom erfassten ab.	Mangelhafte Erfassung darf kein unsicheres Fahrzeugverhalten hervorrufen.	S 3	E 2	C 2	A	SG1 DM
8005		Kräfte und Momente übertragen	Lose Verbindung	Unkontrollierbares Fahrzeugverhalten.	Gelöste Schraube	Verbindungen müssen in allen Betriebssituationen halten.	S 3	E 1	C 1	QM	SG1 DM
8006			Deformation / Bruch	Unkontrollierbares Fahrzeugverhalten.	Vorgesehener Einsatzbereich überschritten.	Der Einsatz des Moduls darf den vorgesehen Bereich nicht überschreiten.	S 3	E 1	C 2	QM	SG1 DM
9001	alle	alle	Lokales Überhitzen	Funktionale Einschränkung	Transformationsverluste resultieren in Wärmestau	Stromdurchflossene Komponenten dürfen nicht überhitzen.	S 1	E 2	C 2	QM	SG1 DM

Tabelle 7-10: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (X)

ID	Subsystem	Funktion	Potentieller Ausfall	Potentielle Folgen	Potentielle Ursachen	Anforderung	*Severity (S)*	*Exp. Probability (E)*	*Controllability (C)*	ASIL	Sicherheitsziel
9002	alle	alle	Lokales Überhitzen	Brandgefahr	Hitze sorgt für entflammen	Hitzeentwicklung darf keine Brandgefahr verursachen	S 3	E 1	C 2	QM	SG1 DM
9003	alle	Kommunikation	Ausfall der Kommunikation	Unsicheres Fahrverhalten & Unangemessene Wertvorgaben	Unterbrochene Verbindung	Unterbrochene Kommunikation darf die Fahrsicherheit nicht gefährden.	S 3	E 2	C 2	A	SG1 DM
9004					Kommunikationsverbindungen unstabil	Instabile Kommunikation darf keine zusätzlichen Gefährdungen erzeugen.	S 3	E 2	C 2	A	SG2 DM
9005					Stromausfall	Lokaler Stromausfall darf die Kommunikation nicht gefährden.	S 3	E 2	C 3	B	SG2 DM
9006					Elektromagnetische Interferenz	Elektromagnetische Interferenz darf die Kommunikation nicht gefährden.	S 3	E 1	C 1	QM	SG2 DM

Tabelle 7-11: Fehlermöglichkeiten und Fehlereinflüsse des Dynamikmoduls (XI)

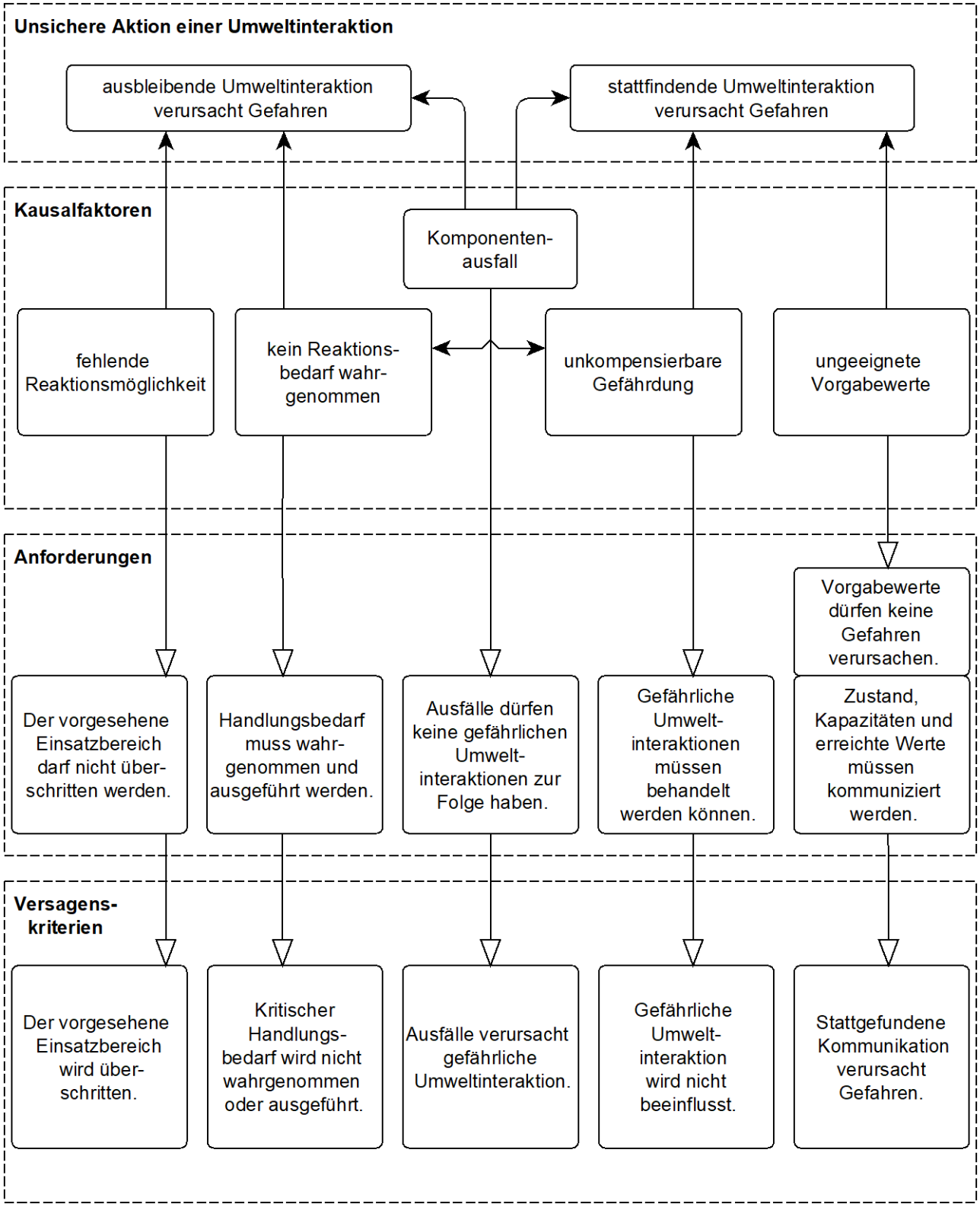

Abb. 7-18: Kontrollflussanalyse: Umweltinteraktionen

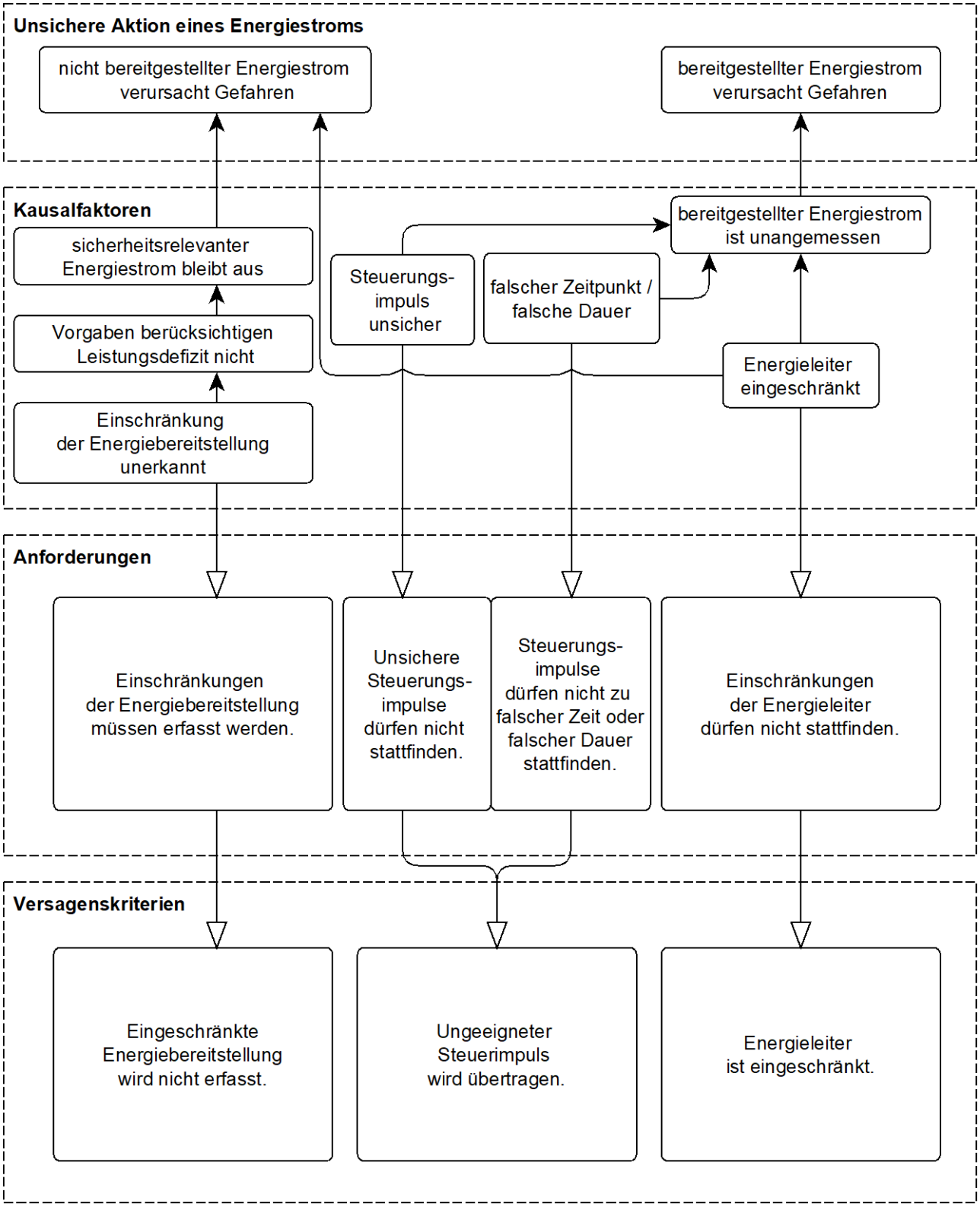

Abb. 7-19: Kontrollflussanalyse: Energieströme

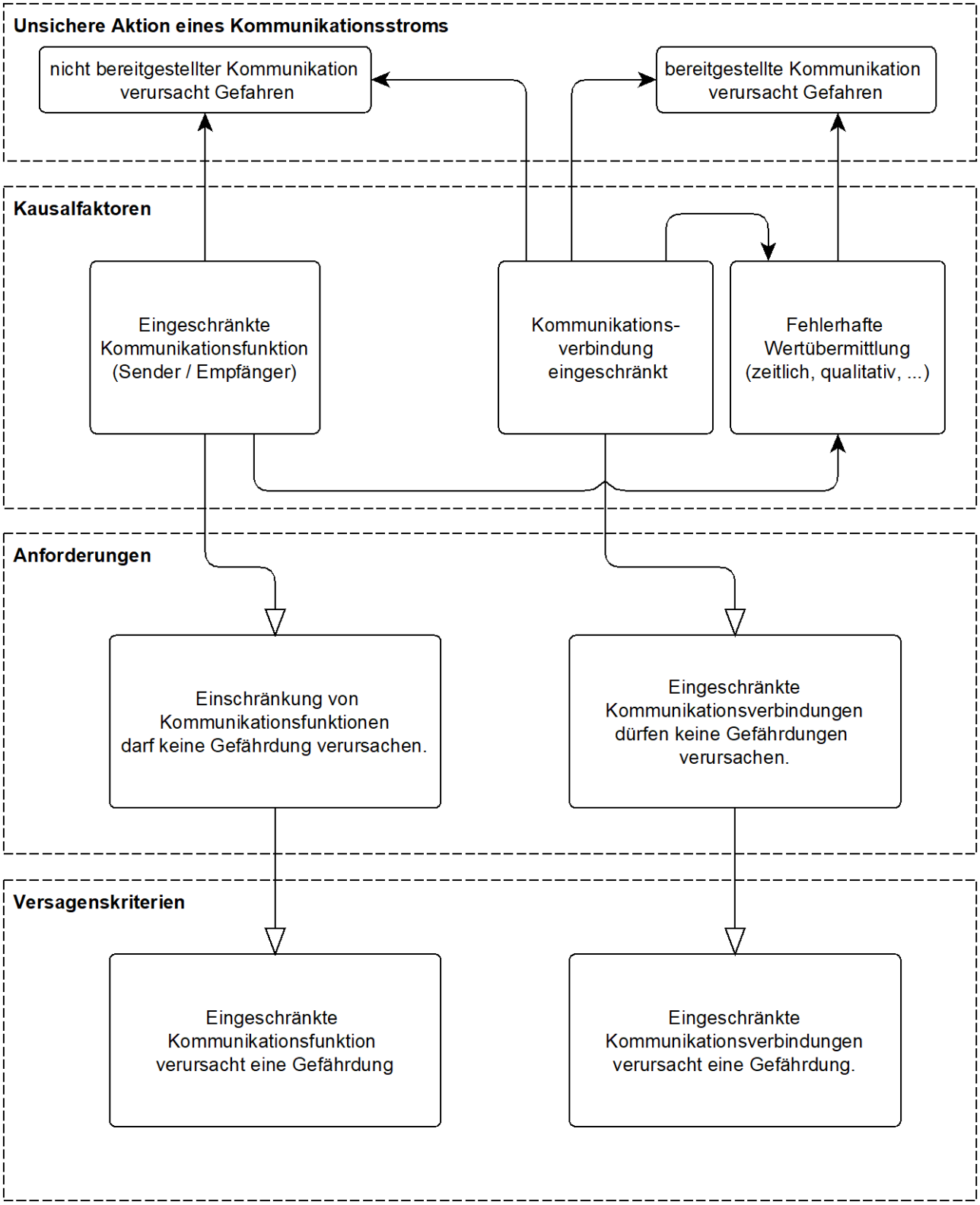

Abb. 7-20: Kontrollflussanalyse: Kommunikation

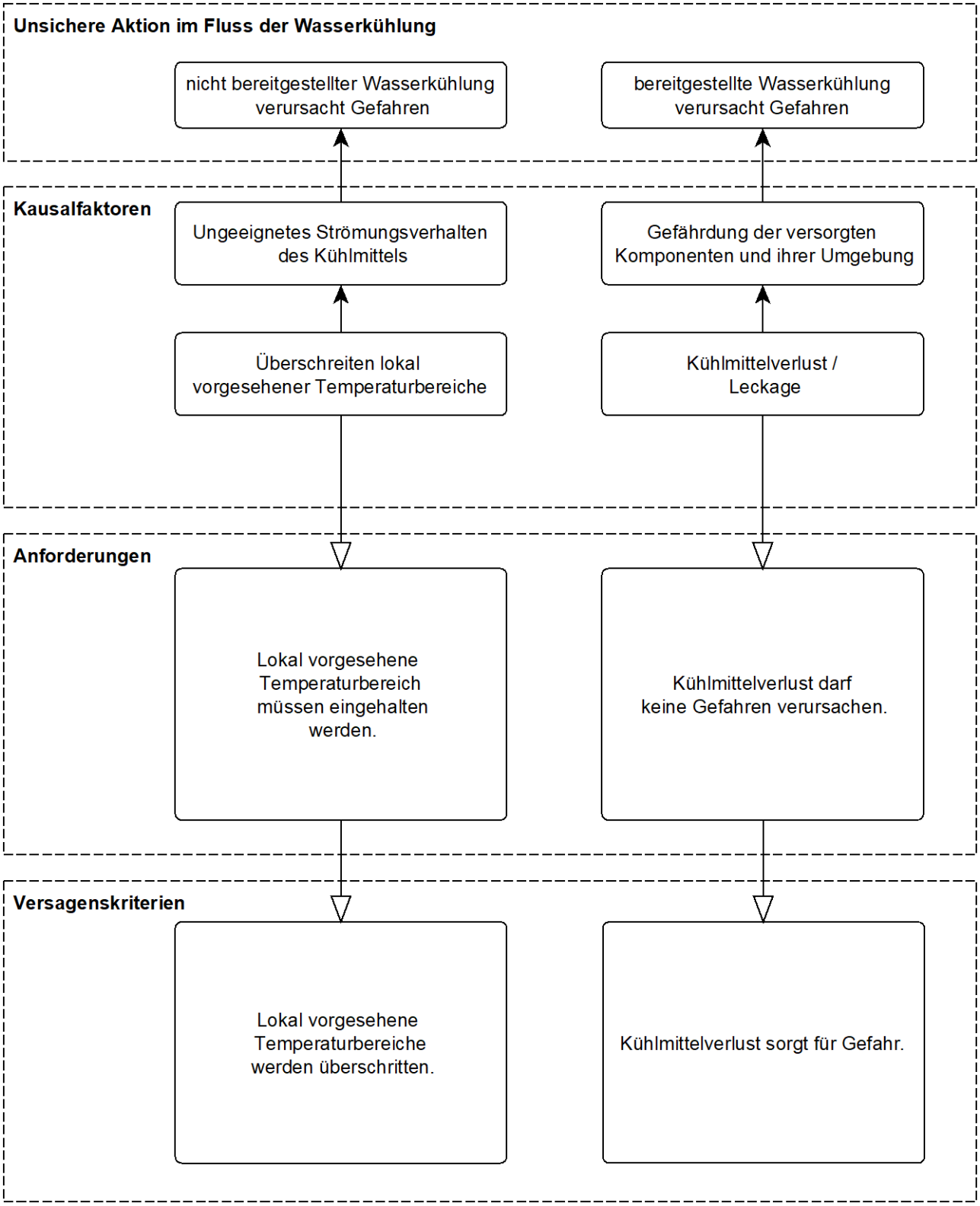

Abb. 7-21: Kontrollflussanalyse: Wasserkühlung

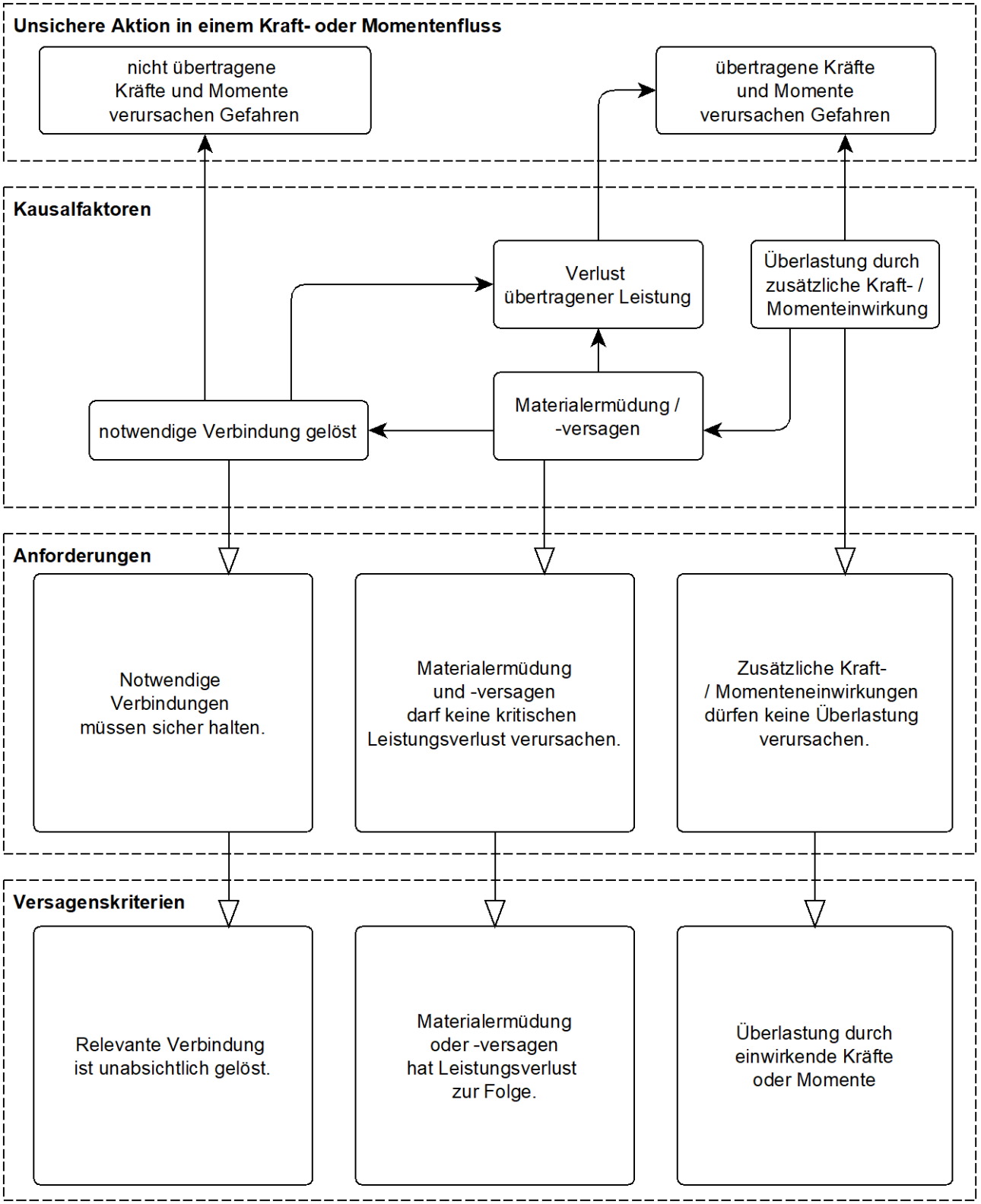

Abb. 7-22: Kontrollflussanalyse: Kraft- und Momentübertragung

Literaturverzeichnis

Abdulkhaleq, A. et al.: STPA Compliance with ISO 26262 (2017)
Abdulkhaleq, Asim; Wagner, Stefan; Lammering, Daniel; Boehmert, Hagen; Blueher, Pierre: Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles, in: In: Dencker, S. 11–24, 2017

Ackermann, S.; Winner, H.: Sicheres Anhalten Modularer Automatisierter Fahrzeuge (2020)
Ackermann, Stefan; Winner, Herrmann: Systemarchitektur und Fahrmanöver zum sicheren Anhalten modularer automatisierter Fahrzeuge, in: Eckstein, Lutz (Hrsg.): 13. Workshop Fahrerassistenz und automatisiertes Fahren, Walting im Altmühltal, Uni-DAS e.V., Darmstadt, 2020

Amersbach, C. T.: Dissertation, Decomposition Approach - Reducing Validation Effort (2020)
Amersbach, Christian T.: Functional Decomposition Approach - Reducing the Safety Validation Effort for Highly Automated Driving, Dissertation
Technische Universität Darmstadt, Darmstadt, 2020

Baumann, G.: Was verstehen wir unter Tests? (2006)
Baumann, Gerd: Was verstehen wir unter Test?, in: 1. AutoTest; Fachkonferenz zum Thema Test und Diagnose in der Automobilentwicklung. Stuttgart, 26./26.10.2006.

Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau (2004)
Bertsche, Bernd; Lechner, Gisbert: Zuverlässigkeit im Fahrzeug- und Maschinenbau, 3. Auflage, Springer-Verlag, Berlin/Heidelberg, 2004

Braess, H.-H.; Seiffert, U.: Vieweg Handbuch Kraftfahrzeugtechnik (2013)
Braess, Hans-Hermann; Seiffert, Ulrich: Vieweg Handbuch Kraftfahrzeugtechnik, Springer Fachmedien Wiesbaden, Wiesbaden, 2013

Briffaut, J.-P.: Complexity and Systems Thinking (2019)
Briffaut, Jean-Pierre: Complexity and Systems Thinking, in: Briffaut, Jean-Pierre (Hrsg.): From complexity in the natural sciences to complexity in operation management systems, Systems of systems complexity set, Wiley-ISTE, London, 2019

Buchholz, M. et al.: Automation of the UNICARagil Vehicles (2020)
Buchholz, Michael; Gies, Fabian; Danzer, Andreas; Henning, Matti; Hermann, Charlotte; Herzog, Manuel; Horn, Markus; Schön, Markus; Rexin, Nils; Dietmayer, Klaus; Fernandez, Carlos; Janosovits, Johannes; Kamran, Danial; Kinzig, Christian; Lauer, Martin; Molinos, Eduardo; Stiller, Christoph; Wang, Linguan; Ackermann, Stefan; Homolla, Tobias; Winner, Hermann; Gottschalg, Grischa; Leinen, Stefan; Becker, Mathias; Feiler, Johannes; Hoffmann Simon; Diermeyer, Frank; Lampe, Bastian; Beemelmanns, Till; van Kempen, Raphael; Woopen, Timo; Eckstein, Lutz; Voget, Nicolai; Moormann, Dieter; Jatzkowski, Inga; Stolte, Torben; Maurer, Markus; Graf, Jürgen; V. Hinüber, Edgar; Siepenkötter, Norbert: Automation of the UNICARagil Vehicles, in: 29th Aachen Colloquium Sustainable Mobility 2020

Chen, L. et al.: HARA through STPA with FMEA (2020)
Chen, Lei; Jiao, Jian; Zhao, Tingdi: A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA, in: Applied Sciences (21), Jahrgang 10, 2020

Die SOPHISTen: MASTeR (2019)
Die SOPHISTen: MASTeR; https://www.sophist.de/fileadmin/user_upload/Bilder_zu_Seiten/Publikationen/Wissen_for_free/MASTeR_Broschuere_5-Auflage_Komplett_Lesezeichen_Update_web.pdf, 2019, Zugriff 18.11.2020

Dittes, F.-M.: Komplexität reduzieren (2012)
Dittes, Frank-Michael: Bitte zurücktreten! – 5 Wege, Komplexität zu reduzieren, in: Dittes, Frank-Michael (Hrsg.): Komplexität, Technik im Fokus, Springer Vieweg, Berlin, 2012

Droste, O.; Merz, C.: Testmanagement in der Praxis (2019)
Droste, Oliver; Merz, Christina: Testmanagement in der Praxis, Springer Berlin Heidelberg, Berlin, Heidelberg, 2019

Eckstein, L.: 13. Workshop Fahrerassistenz und automatisiertes Fahren (2020)
Eckstein, Lutz (Hrsg.) 13. Workshop Fahrerassistenz und automatisiertes Fahren, Uni-DAS e.V., Darmstadt, 2020

Elster, L.: Master Thesis, Simulationsmodelle für elektrische Radnabenantriebe (2020)
Elster, Lukas: Entwicklung eines Simulationsmodells für elektrische Radnabenantriebe, Master Thesis, TU Darmstadt, Darmstadt, 2020

Ertas, A.: Systemic Thinking & Problem Solving (2018)
Ertas, Atila: Systemic Thinking and Complex Problem Solving, in: Ertas, Atila (Hrsg.): Transdisciplinary engineering design process, John Wiley & Sons, Hoboken, NJ, 2018

G. Bagschik et al.: Entwicklung, Absicherung & Test automatisierter Fahrzeuge (2017)
G. Bagschik; T. Menzel; A. Reschka; M. Maurer: Szenarien fur Entwicklung, Absicherung und Test von automatisierten Fahrzeugen, in: Bengler, Klaus (Hrsg.): 11. Workshop Fahrerassistenzsysteme und automatisiertes Fahren, Walting im Altmühltal, Uni-DAS e.V., Darmstadt, 2017

Hillenbrand, M.: Dissertation, Funktionale Sicherheit nach ISO 26262 (2011)
Hillenbrand, Martin: Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen, Dissertation
Karlsruher Institut für Technologie, Hannover, Karlsruhe, 2011

Jipp, M.; Schneider, L.: Fahrtests unter Realbedingungen (2020)
Jipp, Meike; Schneider, Lars: Fahrtests unter Realbedingungen, Springer Vieweg, Wiesbaden, 2020

Junietz, P. et al.: Macroscopic Requirements for Automated Driving (2019)
Junietz, Philipp; Steininger, Udo; Winner, Hermann: Macroscopic Safety Requirements for Highly Automated Driving, in: Transportation Research Record (3), Jahrgang 2673, S. 1–10, 2019

Klamann, B.: Aktuelle Möglichkeiten in Aachen (2021)
Klamann, Bjorn: Aktuelle Möglichkeiten in Aachen, Darmstadt, 2021

Lalli, M.: Autonomes Fahren und die Zukunft (2020)
Lalli, Marco: Autonomes Fahren und die Zukunft der Mobilität, 1. Auflage, 2020

Lippert, M. et al.: Bestehens- & Versagenskriterien für Tests (2019)
Lippert, Moritz; Klamann, Björn; Amersbach, Christian; Winner, Hermann: Definition von Bestehens-/Versagenskriterien für das partikuläre Testen von automatisierten Fahrfunktionen, in: 9. Tagung Automatisiertes Fahren

Löw, P. et al.: Funktionale Sicherheit in der Praxis (2010)
Löw, Peter; Pabst, Roland; Petry, Erwin: Funktionale Sicherheit in der Praxis, 1. Auflage, dpunkt.verlag, s.l., 2010

Martens, T.; Pouansi, B.: Testmöglichkeiten und Hintergründe (2020)
Martens, Timm; Pouansi, Brice: Testmöglichkeiten und Hintergründe, Aachen, Darmstadt, 2020

Martens, T. e.: UNICARagil Dynamics Module (2020)
Martens, Timm e. a.: UNICARagil Dynamics Module, in: 29th Aachen Colloquium Sustainable Mobility 2020

Martin Glinz: Spezifikation von Anforderungen
Martin Glinz: Spezifikation von Anforderungen; https://files.ifi.uzh.ch/rerg/amadeus/teaching/courses/software_engineering_hs07/skript/Kapitel_07.pdf, Zugriff 03.12.2020

Noack, T.: Dissertation, Automatische Verlinkung von Testfällen & Anforderungen (2015)
Noack, Thomas: Automatische Verlinkung von Testfällen und Anforderungen, Dissertation Technische Universität Berlin, Berlin, 2015

Norbert Bolz: Bausteine zu einer Designwissenschaft (2016)
Norbert Bolz: Bausteine zu einer Designwissenschaft, in: Baecker, Dirk (Hrsg.): Schlüsselwerke der Systemtheorie, 2. Auflage, Springer VS, Wiesbaden, 2016

Philipp, R. et al.: Decomposition of Automated Driving Systems (2020)
Philipp, Robin; Schuldt, Fabian; Howar, Falk: Functional Decomposition of Automated Driving Systems for the Classification and Evaluation of Perceptual Threats, in: Eckstein, Lutz (Hrsg.): 13. Uni-DAS e.V. Workshop Fahrerassistenz und automatisiertes Fahren, digital, 2020

Pouansi, B.: Leistungsbeschreibung der Aktoreinheiten des Dynamikmoduls (2020)
Pouansi, Brice: Leistungsbeschreibung der Aktoreinheiten für das Institut für Kraftfahrzeuge der RWTH Aachen University, Aachen

Reschka, A. et al.: Ability and skill graphs (2015)
Reschka, Andreas; Bagschik, Gerrit; Ulbrich, Simon; Nolte, Marcus; Maurer, Markus: Ability and skill graphs for system modeling, online monitoring, and decision support for vehicle guidance systems, in: 2015 IEEE Intelligent Vehicles Symposium (IV), Seoul, 2015

Reschka, A.: Sicherheitskonzept für autonome Fahrzeuge (2015)
Reschka, Andreas: Sicherheitskonzept für autonome Fahrzeuge, in: Maurer, Markus et al. (Hrsg.): Autonomes Fahren, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015

Reschka, A.: Dissertation, Fertigkeiten- und Fähigkeitengraphen (2016)
Reschka, Andreas: Fertigkeiten- und Fähigkeitengraphen als Grundlage des sicheren Betriebs von automatisierten Fahrzeugen im öffentlichen Straßenverkehr in städtischer Umgebung, Dissertation Technische Universität Carolo-Wilhelmina zu Braunschweig, Braunschweig, 2016

Reschka, A. et al.: System-Wide Functional Safety (2018)
Reschka, Andreas; Bagschik, Gerrit; Maurer, Markus: Towards a System-Wide Functional Safety Concept for Automated Road Vehicles, in: Winner, Hermann; Prokop, Günther; Maurer, Markus (Hrsg.): Automotive Systems Engineering II, Springer International Publishing, Cham, 2018

Ross, H.-L.: Functional Safety for Road Vehicles (2016)
Ross, Hans-Leo: Functional Safety for Road Vehicles, Springer International Publishing, Cham, s.l., 2016

Ross, H.-L.: Funktionale Sicherheit im Automobil (2019)
Ross, Hans-Leo: Funktionale Sicherheit im Automobil, 2. Auflage, 2019

Scheffel, T.: Masterthesis, Entwicklung und Implementierung von Ausfallmodellen für elektrische Radnaben- antriebe (2020)
Scheffel, Timo: Entwicklung und Implementierung von Ausfallmodellen für elektrische Radnaben-antriebe, Masterthesis
Technische Universität Darmstadt, Darmstadt, 2020

Schuldt, F.: Dissertation, Test automatisierter Fahrfunktionen (2016)
Schuldt, Fabian: Ein Beitrag für den methodischen Test von automatisierten Fahrfunktionen mit Hilfe von virtuellen Umgebungen, Dissertation
Braunschweig, Technische Universität Braunschweig, 2016

Schuldt, F. et al.: Test Case Generation for DAS (2018)
Schuldt, Fabian; Reschka, Andreas; Maurer, Markus: A Method for an Efficient, Systematic Test Case Generation for Advanced Driver Assistance Systems in Virtual Environments, in: Winner, Hermann; Prokop, Günther; Maurer, Markus (Hrsg.): Automotive Systems Engineering II, Springer International Publishing, Cham, 2018

Stellet, J. E. et al.: Validation of automated driving (2020)
Stellet, Jan E.; Woehrle, Matthias; Brade, Tino; Poddey, Alexander; Branz, Wolfgang: Validation of automated driving - a structured analysis and survey of approaches, in: Eckstein, Lutz (Hrsg.): 13. Workshop Fahrerassistenz und automatisiertes Fahren, Walting im Altmühltal, Uni-DAS e.V., Darmstadt, 2020

Stolte, T. et al.: Safety goals and functional Safety (2016)
Stolte, Torben; Bagschik, Gerrit; Maurer, Markus: Safety goals and functional safety requirements for actuation systems of automated vehicles, in: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, IEEE, 01.11.16 - 04.11.16

Stolte, T. et al.: Safety Concepts for Automated Vehicles (2020)
Stolte, Torben; Graubohm, Robert; Jatzkowski, Inga; Maurer, Markus; Ackermann, Stefan; Klamann, Björn; Lippert, Moritz; Winner, Herrmann: Towards Safety Concepts for Automated Vehicles by the Example of the Project UNICARagil, in: 29th Aachen Colloquium Sustainable Mobility 2020

Stolte, T. et al.: Functional Safety of Vehicle Actuation (2016)
Stolte, Torben; Hosse, René S.; Becker, Uwe; Maurer, Markus: On Functional Safety of Vehicle Actuation Systems in the Context of Automated Driving, in: IFAC-PapersOnLine (11), Jahrgang 49, S. 576–581, 2016

Stolte, T. et al.: HARA for Automated Unmanned Vehicle (2017)
Stolte, Torben; Bagschik, Gerrit; Reschka, Andreas; Maurer, Markus: Hazard Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle, in: 2017 IEEE Intelligent Vehicles Symposium (IV), 2017

Stolte, T.; Graubohm, R.: UNICARagil Gesamtfahrzeug HARA auf Szenarienbasis (2018)
Stolte, Torben; Graubohm, Robert: UNICARagil – AP 1.4.2, HARA Fahrzeug-Items V 0.3, Braunschweig, 2018

Struth, M. et al.: Dynamikmodul (2020)
Struth, Michael; Martens, Timm; Wielgos, Sebastian; Brandt, Sven; Schlupek, Martin: Dynamikmodul; https://www.unicaragil.de/images/events/2020_Events/HZE/Geometrie/Poster_2_-_Dynamikmodul_web_klein.png, 2020, Zugriff 29.02.2021

Sulaman, S. M. et al.: Comparison of FMEA and STPA (2019)
Sulaman, Sardar M.; Beer, Armin; Felderer, Michael; Höst, Martin: Comparison of the FMEA and STPA safety analysis methods–a case study, in: Software Quality Journal (1), Jahrgang 27, S. 349–387, 2019

Thomas, J. et al.: Requirements Development and Hazard Analysis (2019)
Thomas, John; Sgueglia, John; Suo, Dajiang; Leveson, Nancy; Vernacchia, Mark; Sundaram, Padma: An Integrated Approach to Requirements Development and Hazard Analysis, in: Pimentel, Juan R. (Hrsg.): The Role of ISO 26262, Automated Vehicle Safety Series Book 4, SAE International, Warrendale, Pa, 2019

Tietjen, T.; Decker, A.: FMEA-Praxis (2020)
Tietjen, Thorsten; Decker, André: FMEA-Praxis, 4. Auflage, 2020

Unbekannte Autoren: Homepage des Projekts UNICARagil (2021)
Unbekannte Autoren: Homepage des Projekts UNICARagil; www.unicaragil.de, 2021, Zugriff 03.03.2021

Wachenfeld, W.; Winner, H.: Die Freigabe des autonomen Fahrens (2015)
Wachenfeld, Walther; Winner, Hermann: Die Freigabe des autonomen Fahrens, in: Maurer, Markus et al. (Hrsg.): Autonomes Fahren, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015

Winner, H. et al.: Automotive Systems Engineering II (2018)
Winner, Hermann; Prokop, Günther; Maurer, Markus (Hrsg.) Automotive Systems Engineering II, Springer International Publishing, Cham, 2018

Wolf, C.: Dynamikmodul: Boundary Diagramm mit Kontakten
Wolf, Christian: Dynamikmodul: Boundary Diagramm mit Kontakten

Woopen, T. et al.: UNICARagil - Disruptive Modular Architectures (2018)
Woopen, Timo; Eckstein, Lutz; Kowalewski, Stefan; Moormann, Dieter; Maurer, Markus; Ernst, Rolf; Winner, Hermann; Katzenbeisser, Stefan; Becker, Matthias; Stiller, Christoph; Furmans, Kai; Bengler, Klaus; Lienkamp, Markus; Reuss, Hans-Christian; Dietmayer, Klaus; Lategahn, Henning; Siepenkötter, Norbert; Elbs, Martin; V. Hinüber, Edgar; Dupuis, Marius; Hecker, Christian: UNICARagil - Disruptive Modular Architectures for Agile, Automated Vehicle Concepts, in: 27th Aachen Colloquium Automobile 2018

Woopen, T. et al.: UNICARagil - Where We Are (2020)
Woopen, Timo; van Kempen, Raphael; Bödekker, Torben; Eckstein, Lutz: UNICARagil - Where we are and where we are going, in: 29th Aachen Colloquium Sustainable Mobility 2020