Verkehrssicherheit im systemischen Kontext

Von der Fakultät für Maschinenbau
der Technischen Universität Carolo-Wilhelmina zu Braunschweig

zur Erlangung der Würde

eines Doktor-Ingenieurs (Dr.-Ing.)

genehmigte Dissertation

von:	Dipl.-Ing. Jörn Drewes
aus (Geburtsort):	Stade

eingereicht am:	08. Mai 2009
mündliche Prüfung am:	03. September 2009
Referenten:	Prof. Dr.-Ing. Dr. h.c. Eckehard Schnieder Prof. Dr.-Ing. Alexander Fay

2009

Vorwort

Die vorliegende Arbeit enstand auf Basis meiner Tätigkeiten am Institut für Verkehrssicherheit und Automatisierungstechnik der Technischen Universität Braunschweig in den Jahren 2002 bis 2008.

Dem Leiter des Instituts, Herrn Prof. Dr.-Ing. Dr. h.c. Eckehard Schnieder, danke ich gleichermaßen für seine langjährige Unterstützung bei sowohl fachlichen, beruflichen als auch freundschaftlichen Fragestellungen, wie auch für die Möglichkeit die gewährten Freiräume sowohl fachlich als auch thematisch nutzen zu können und die Ergebnisse national und international diskutieren zu dürfen.

Desweiteren danke ich Herrn Prof. Dr.-Ing. Alexander Fay, Leiter des Instituts für Automatisierungstechnik der Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg, für die Übernahme des Koreferats und die gemeinsame konstruktive Vertiefung und Diskussion methodischer Ideen im Rahmen einer gemeinsam betreuten Studienarbeit. Ebenfalls danke ich Herrn Prof. Dr.-Ing. Karsten Lemmer für den Vorsitz der Prüfungskommission.

Auch bedanke ich mich bei allen Mitarbeitern des Instituts, die das Entstehen dieser Arbeit begleitet haben und mich bei der thematischen Ausrichtung der Arbeit stets mit interessanten Fragestellungen und Hinweisen unterstützt haben. Herrn Dipl.-Ing. Jörg May, der mir die Welt des Schienenverkehrs geöffnet hat und mir über die gesamte Zeit am Institut ein vorbildlicher Projekt-, Diskussionspartner und Freund war, gilt mein besonderer Dank. Frau Regine Stegemann und das gesamte Team des Geschäftszimmers haben mir über die vielen Jahre mit Rat und Tat beiseite gestanden und mich beim Korrekturlesen nicht nur bei diesen Zeilen unterstützt.

Meinen Eltern danke ich für ihre ideelle und materielle Förderung in Schul- und Studienzeit, aus der heraus letztendlich diese Arbeit entstanden ist.

Bei meinen beiden Kindern Tom und Max sowie meiner Frau Astrid möchte ich mich für die Liebe, das Verständnis und die Ruhe bedanken, die mir Wochenende für Wochenende und Abend für Abend im letzten Jahr gewährt wurden und so der ein oder andere gemeinsame Zoobesuch schweren Herzens verschoben wurde.

Braunschweig, im Mai 2009

„Sicher ist, dass nichts sicher ist. Selbst das nicht.“

(Joachim Ringelnatz 07.08.1883 - 17.11.1934)

Ich widme diese Arbeit den Menschen, die sich Tag für Tag auf die Sicherheit unterschiedlicher Systeme im Verkehr verlassen und damit ihr Leben vertrauensvoll in die Hand von uns Ingenieuren legen.

„...Design to Safety“

Inhaltsverzeichnis

Kurzfassung

Die Verkehrssicherheit, im ingenieurswissenschaftlichen Fokus, lässt sich aus vielen verschiedenen Blickwinkeln betrachten. Je nach Zugehörigkeit einer Domäne (z.B. Schienenverkehr, Straßenverkehr bzw. Luftverkehr oder Schifffahrt), dem Systemblickwinkel oder unterschiedlichen Detaillierungstiefen ergeben sich verschiedene Interpretationen und Ansätze die Sicherheit zu beeinflussen. Mit dem Ziel die Verkehrssicherheit zu verbessern, werden zum Teil komplexe technische Lösungen aufwendig entwickelt, ohne eine direkte oder indirekte sicherheitsfördernde Auswirkung zu prognostizieren. Auf Basis lokaler akuter Probleme werden häufig lokale Lösungen erstellt, deren erhoffte Wirkung jedoch teilweise ausbleibt. Mögliche Ursachen für die Entwicklung vorwiegend schneller lokaler Lösungen sind zum einen der akute Handlungsbedarf, der sich zum Teil durch die hohe Erwartungshaltung der Gesellschaft bei Unglücksfällen begründet, und zum anderen auch die hohe Komplexität des jeweils betroffenen Verkehrssystems selber, sowie die eher abstrakte und nicht unmittelbar messbare Größe der Verkehrssicherheit und dem damit verbundenen Problem, diese nicht direkt beeinflussen zu können. Die Kausalität zwischen Einflussnahme auf Systemkonstituenten und der möglichen Auswirkung auf die Verkehrssicherheit wird dabei häufig nicht vollständig berücksichtigt und zum Teil der nächstliegende Angriffspunkt irrtümlich als am erfolgversprechendsten wahrgenommen.

Die vorliegende Arbeit konzentriert sich auf eine systemische, auf systemtheoretischen Grundlagen aufbauende Analyse der Systemsicherheit. Ein wesentlicher Bestandteil dieser Analyse ist die Verwendung von Begriffsmodellen zur Identifikation einer konsistenten Begriffswelt und somit zur Vermittlung eines umfassenden Systemwissens, um darauf aufbauend Theorien der Systemsicherheit in Verbindung mit generischen Sicherheitsimplementierungskonzepten formalisieren zu können. Anhand dieser systemunspezifischen jedoch konsistenten Betrachtungen gelingt die Portierung der Erkenntnisse auf das System Verkehr und die Formalisierung der Verkehrssicherheit mit einfachen verkehrssystemunabhängigen Modellen. Systematische Implementierungskonzepte zur gezielten Beeinflussung der Verkehrssicherheit unter Berücksichtigung der Effizienz werden anhand ausgewählter Anwendungsbeispiele und entwickelter Methoden ausführlich beschrieben und deren Einordnung in einen zuvor geschaffenen Gesamtsystemkontext erläutert.

1 Einleitung

Der Begriff der Verkehrssicherheit lässt je nach Domänenzugehörigkeit des Betrachters unterschiedliche Assoziationen zu. Zerlegt man zunächst den Begriff Verkehrssicherheit in seine Wortbestandteile *Verkehr* und *Sicherheit* ergeben sich bereits jeweils eigenständige Interpretationen.

Das allgemeine Verständnis des Begriffs Verkehr (V) im ingenieurswissenschaftlichen Kontext beschränkt sich zweifelsfrei auf die realisierte Ortsveränderung von Personen, Gütern, Energien oder Nachrichten (V_1) auf entsprechenden Verkehrswegen. Gesellschaftlich ergibt sich jedoch eine weitere Bedeutung dieses Begriffs. So wird der gesellschaftliche Umgang mit anderen Personen, die Pflege sozialer Kontakte sowie der damit verbundene soziale oder verbale Austausch (V_2) ebenfalls unter dem Begriff Verkehr verstanden und beschreibt somit die Interaktion verschiedener sozialer Akteure. Zusätzlich existieren weitere verschiedene Inhalte und Interpretationen des Begriffs Verkehr bezogen auf die jeweilige Domäne. Definitionen des Begriffs Verkehr in der Biologie, der Geschäftswelt und dem Rechtswesen zeigen nur einige weitere Möglichkeiten.

Diese Homonymie eines Begriffs setzt sich auch bei der Betrachtung des Begriffs Sicherheit (S) fort. Wird die Sicherheit im Kontext von Maschinen, Anlagen oder technischen bzw. biologischen Systemen als exogene Gefahrlosigkeit (S_1) der betrachteten Systeme verstanden, wird aus individueller menschlicher Sicht die Sicherheit primär im Sinne der eigenen Unversehrtheit (S_2) interpretiert. Aber auch im menschlich-psychologischen Kontext hat sich der Begriff der Sicherheit im Sinne der Gewissheit (S_3), bezogen auf natürliche oder moralische Sachverhalte, etabliert.

Eine Permutation der angesprochenen Begriffskontextkombinationen zu dem Begriff der Verkehrssicherheit (VS) ergibt folgende Relation

$$VS_{ij} = V_i \times S_j$$

und verdeutlicht die mögliche Komplexität und Tragweite des Begriffs „Verkehrssicherheit“, sofern dieser nicht durch einen konkreten Kontextbezug begrenzt betrachtet wird.

1.1 Stand der Wissenschaft

Es existieren eine Vielzahl von Literaturquellen, die die Worte „Verkehr“ und „Sicherheit“ einzeln oder in Kombination im Titel führen bzw. den Begriff der „Verkehrssicherheit“ explizit thematisieren. Viele dieser Literaturquellen fokussieren dabei jedoch

ein konkretes Verkehrssystem, wie z.B. Straßen-, Schienen- oder Luftverkehr und stellen spezifische Verbesserungsmaßnahmen vor. Eine verkehrssystemübergreifende und implementierungsfreie Sichtweise, d.h. die Sicherheit als allgemeine Eigenschaft des generischen Systems „Verkehr“ zu betrachten, exisitert derzeit nicht. Im weiteren Umfeld sind in der Literatur Ansätze der Systemsicherheit, auch System Safety genannt, zu finden, dessen Ursprung oft im Bereich der Luftfahrt zitiert wird. Diese Systemsicherheit verfolgt jedoch einen vollständig systemunabhängigen Ansatz, ohne die Anwendung für das generische System „Verkehr“ zu thematisieren. Eine aussagekräftige, dokumentierte Verschmelzung dieser Ansätze konnte auch nach längerer Recherche nicht gefunden werden.

1.2 Motivation, Ziel und Ansatz

Neben der Permutation der Begriffsbestandteile „Verkehr“ und „Sicherheit“ führt zusätzlich die unbegrenzte Ausdehnung des möglichen Begriffsumfelds zu einer nahezu endlosen Kette von Assoziationen, kausalen Abhängigkeiten, Allokationen und Theorien, die jenseits der Trivialitätsgrenze liegen. Eine gewisse Analogie lässt sich dabei im Bereich der komplexen Automatisierungssysteme finden, der aufgrund der immer komplexer werdenden technischen Systeme vor einer ähnlichen Herausforderung stand. Auch dort musste die Aufgabe, eine nichttriviale Komplexität in einer dem Betrachter verständlichen und eindeutigen Beschreibung vollständig präsentieren zu können, gelöst werden.

Viele Grundlagen für Methoden und Beschreibungsmittel der Automatisierungtechnik lassen sich auf die Systemtheorie zurückführen. Die Erkenntnisse aus der Automatisierungstechnik, von der Systembeschreibung bis zur implementierten Steuerungs- und Sicherungstechnik, in die Domäne der Verkehrssicherheit zu transferieren, bietet eine lohnenswerte Chance um zu einer tiefergehenden Durchdringung und Nutzung zu gelangen und stellt gleichzeitig eine große Herausforderung dar. Die gezielte und wirksame Reduzierung von verkehrsbedingten Unfällen und somit die Vermeidung der damit verbundenen Schäden auf der Basis von systematischen Modellierungen, strukturierten Analysen und daraus konsequent abgeleiteten Konzepten zur Implementierung von Sicherheitsmaßnahmen dient als Motivation für die Erstellung dieser Arbeit.

Das Ziel dieser Arbeit ist die Identifikation und Beschreibung von systematischen Zusammenhängen und wirksamen Implementierungskonzepten zur Erhöhung der Verkehrssicherheit, sowie eine exemplarische Anwendung entwickelter Methoden, die auf den erarbeiteten Grundsätzen aufbauen. Die Motivation Maßnahmen und Methoden zu entwickeln, um dieses Ziel zu erreichen, ist mit verschiedenen Teilzielen verbunden. Zum einen muss die Verkehrssicherheit dafür in einem systemtheoretischen Kontext betrachtet werden, ein gemeinsames Begriffsverständnis aufgebaut und anhand dieser Teilziele sollen generische Maßnahmen zur Implementierung der Sicherheit im Verkehr identifiziert und analysiert werden. Erst darauf aufbauend lassen sich wirksame Methoden zur Erhöhung der Verkehrssicherheit ableiten und anwenden.

Zur Erreichung der geplanten Ziele verfolgt diese Arbeit den Ansatz einer systema-

tischen und systemorientierten (systemischen) Analyse. Zu Beginn werden terminologische, auf den Grundlagen der Systemtheorie aufbauende, Begriffsanalysen durchgeführt. Diese beschränken sich zunächst auf eine allgemeine systemunspezifische Sicherheit und ermöglichen dadurch die Ableitung generischer Sicherheitsimplementierungskonzepte. Dabei verfolgt diese Arbeit ausschließlich die Sichtweise der Ingenieurwissenschaften und berücksichtigt verschiedene in der Fachwelt etablierte Definitionen, die in einen Systembezug gestellt werden.

Die Übertragung dieser Erkenntnisse auf das Zielsystem *Verkehr* und somit die Beschreibung der systemspezifischen *Verkehrssicherheit* ermöglicht eine Konkretisierung der Sicherheitsimplementierungskonzepte für den *Verkehr* und stellt die Basis für exemplarische Beispiele.

Im Rahmen der Forschungstätigkeit entwickelte Methoden aus der Verkehrssicherheitsdomäne werden basierend auf den Erkenntnissen verknüpft und verifiziert.

1.3 Struktur der Arbeit

Die Arbeit kann in vier inhaltliche Hauptbereiche unterteilt werden, wie in Abbildung 1.1 farblich dargestellt ist. Während die Einleitung und die Zusammenfassung den äußeren Rahmen aufspannen, bilden Kapitel 2 bis 7 den inhaltlichen Kern der Arbeit.

In Kapitel 2 werden die in der Arbeit verwendeten Beschreibungsmittel und allgemeine systemtheoretische Grundlagen für den Leser vorgestellt. Des Weiteren wird die Thematik der Begriffsbildung und -systematik erläutert, die in den nachfolgenden Kapiteln sukzessiv zum Einsatz kommt.

Das Kapitel 3 beschreibt die Sicherheit domänenunabhängig mit Blickrichtung auf die ingenieurswissenschaftliche Anwendung. Dabei werden das zuvor erläuterte Vorgehen zur Begriffsbestimmung und die Grundlagen der Systemtheorie angewendet, um den Begriff *Sicherheit* ausführlich und systematisch darzustellen. Verschiedene generische Sicherheitsimplementierungskonzepte werden darauf in Anlehnung an die Automatisierungstechnik erarbeitet und mögliche allgemeine Maße zur Quantifizierung der Sicherheit vorgestellt.

Kapitel 4 konkretisiert die Sicherheit in Bezug auf die Anwendungsdomäne Verkehr, indem das System Verkehr sowohl begrifflich als auch systemisch analysiert und formalisiert wird. Die aus Kapitel 3 gewonnenen Konzepte zur Implementierung werden hier konsequent angewendet. Konventionelle und neue Maße der Verkehrssicherheit runden das Kapitel ab.

Kapitel 5 bis 7 beinhalten den vierten thematischen Bereich der Arbeit und zeigen verschiedene Methoden, Ansätze und Modelle, welche auf die zuvor erarbeiten Erkenntnisse aufbauen. Sowohl eine Methode zur Identifikation generischer Gefahren am Beispiel einer Stellwerksapplikation, als auch eine Methode zu sicherheitsgerichteten Anforderungsanalyse für Fahrerassistenzsysteme zeigen die exemplarische Anwendbarkeit der zuvor gewonnenen Erkenntnisse. Ein vernetztes Modell eines durchgängigen sicherheitsgerichteten Entwicklungsprozesses in Kapitel 7 zeigt Schnittstellen zwischen allgemeinen und

sicherheitsgerichteten Aktivitäten sowie die Quellen und Senken der Sicherheitsnachweisführung am Beispiel der Europäischen Normen für Bahnanwendungen EN 5012x. Dieses Vorgehensmodell liefert den Managementrahmen für eine erfolgreiche Umsetzung der theoretischen und methodischen Erkenntnisse zur Verbesserung der Verkehrssicherheit bevor die Zusammenfassung die essenziellen Inhalte der Arbeit komprimiert darstellt und der Ausblick Anreiz für weitere Forschungs- und Entwicklungstätigkeiten bietet.

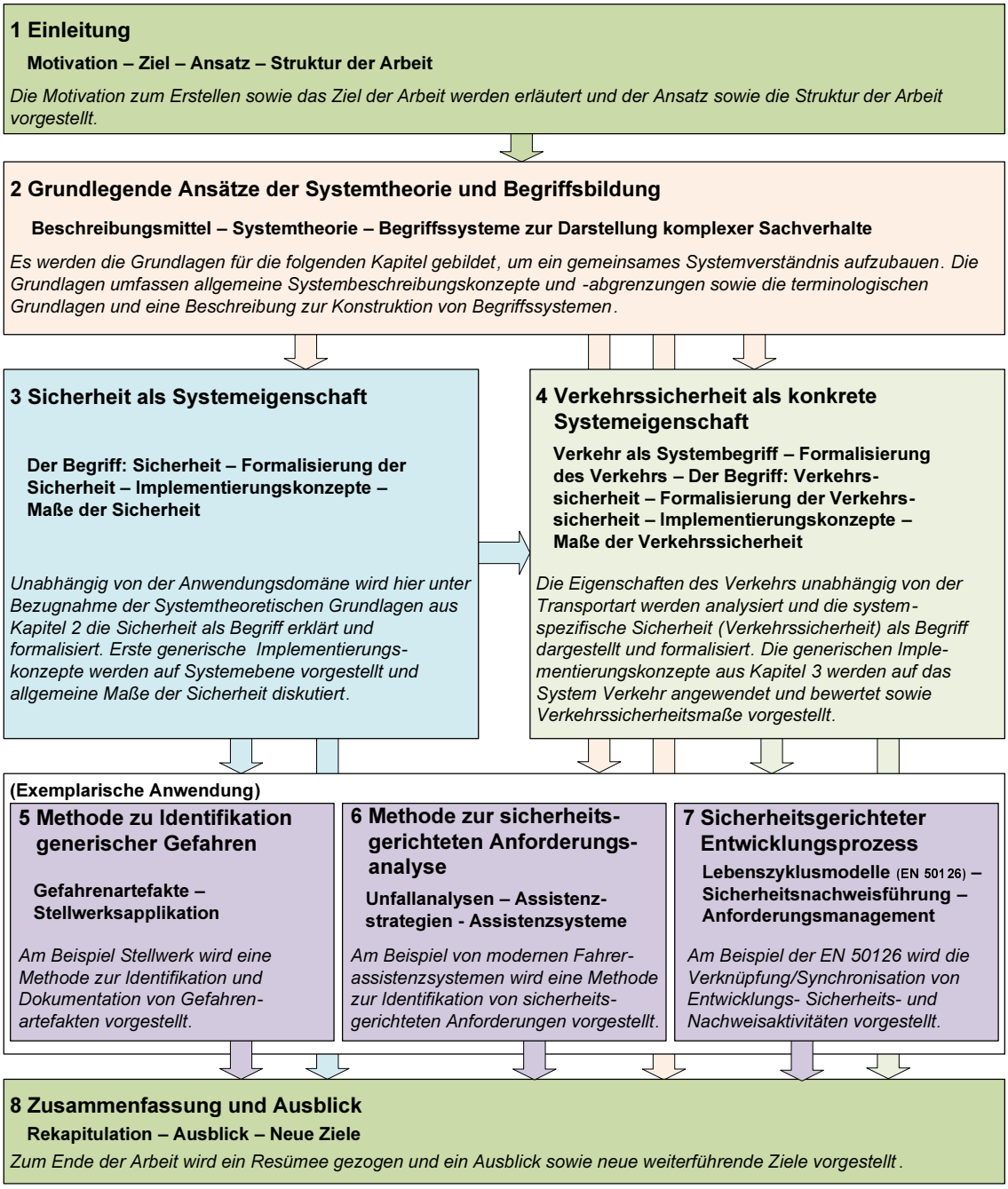


Abbildung 1.1: Darstellung der Kapitelstruktur

2 Grundlegende Ansätze der Systemtheorie und Begriffsbildung

Die in diesem Kapitel aufgeführten Grundlagen bilden die Basis der systematischen Analyse der Verkehrssicherheit und zeigen sowohl Konzepte zur Beschreibung von Systemeneigenschaften als auch methodische Vorgehensweisen der Modellierung und Analyse. Die Unterscheidung des statischen Aufbaus und des dynamischen Verhaltens von generischen Systemen bietet hier eine fundamentale Möglichkeit einer strukturierten Systembeschreibung, welche durch eine geeigenete formalisierte Modellierung nach [Sch99] einen allgemeingültigen Charakter erlangt. Diese Erkenntnisse fördern eine systemische Betrachtungsweise und ermöglichen das Verständnis von abstrakten und vor allem komplexen teilweise nicht materiellen Begriffssystemen, z.B. *Verkehrssicherheit*. Weitere Ansätze zur begrifflichen (terminologischen) Analyse nach [Sch02b] schließen sich dem an und ergänzen die Theorien der strukturierten Modellierung in einer geeigneten Form.

2.1 Grundlagen der konzeptuellen Modellierung

Ein Modell ist ein abstrahiertes Abbild eines realen oder fiktiven (d.h. zukünftigen) Realitätsausschnitts [Sei03]. Das Objekt der Abbildung kann dabei sowohl materiell als auch immateriell sein. Der Gegenstandsbereich der Modellbildung wird häufig als Diskurswelt bezeichnet und meint damit den abzubildenden Ausschnitt der realen oder fiktiven Realität.

In den unterschiedlichen Domänen und Disziplinen werden verschiedene Arten von Modellen verwendet. Während in der Ingenieursdomäne neben grafischen Modellen (z.B. technische Zeichnungen) zusätzlich auf physische Modelle zurückgegriffen wird, die primär als ein maßstabsreduzierter aber funktionsidentischer Nachbau des zu konstruierenden Gegenstands zu verstehen sind, sind in anderen Branchen eher abstraktere Abbildungen etabliert, um Modelle einer materiellen Welt zu erschaffen. Architekten beispielsweise verwenden neben abstrahierten maßstabsgerechten Grundrissen konkrete plastische Modelle zur Veranschaulichung bzw. auch Ausführung des Bauobjekts. In der Musik, die eine vorwiegend immaterielle Welt verkörpert, werden Partituren zur reproduzierbaren Aufbewahrung von Kompositionen erstellt. Eine physische oder physikalische Modellierung steht hier der grafischen Modellierung nach.

Grafische Modelle repräsentieren im Gegensatz zum natürlichsprachlichen Text den Gegenstandsbereich anschaulich und fördern die Kommunikation, da die Konzentration

der verschiedenen Betrachter nicht von möglichen Mehrdeutigkeiten des Textes abgelenkt wird. In der Softwareentwicklung, ebenfalls eine Disziplin der immateriellen Welt, werden aufgrund des hohen Abstraktionsgrades bei gleichzeitig hoher Realitätskomplexität häufig grafische Modelle verwendet, um bei geringerer Modellkomplexität spezifische Aspekte des Gegenstandsbereichs anschaulich zu visualisieren. Diese werden dort häufig als konzeptuelle Modelle bezeichnet.

Modelle können dabei grundlegend deskriptiv, d.h. die aktuelle Realität bzw. präskriptiv, d.h. eine zukünftige Realität beschreiben. Beide zeitlich differenzierten Modelle können die jeweilige Realität dabei zusätzlich entweder verkürzend oder erweiternd darstellen. Eine Verkürzung der Realität beruht auf der Abstraktionsfähigkeit eines Modells, die es ermöglicht eine komplexe Realität vereinfacht darzustellen, indem beispielweise eine Reduzierung von Details verfolgt wird. Beispiele dafür sind elektische Schaltpläne, die die Realität lediglich in seiner elektrischen Struktur darstellen und Bauteilgrößen, Kabelformen, Lagen und Gehäuseformen ausblenden. Aber auch einfache Straßennetzkarten sind vereinfachende Modelle, die in der Realität existente optische Charakteristiken von Straßen ausblenden. Gleiches gilt für die bereits erwähnten abstrakten Modelle eines Architekten.

Modelle können die Realität zusätzlich erweitern, indem Informationen künstlich hinzugefügt werden, die in der Realität nur implizit vorhanden sind. Dieser Zusatz an artifiziellen Informationen dient im jeweiligen Verwendungszweck einem besseren Verständnis bzw. einer besseren Handhabbarkeit des Modells. Eine Straßenkarte, die eine farbliche Differenzierung von Straßen vorsieht, die beispielsweise die Unfallzahlen oder die Verkehrsdichte widerspiegelt, erweitert im Modell die Realität ähnlich wie die künstliche Erweiterung um Längen- und Breitengrad bei geografischen Karten die korrekte Zuordnung der Kartenkoordinaten zur Realität erleichtert.

Je nach Domäne haben sich verschiedene Beschreibungsmittel und Methoden entwickelt, um Modelle mit einer der Anwendung spezifizischen Notation, bzw. Semiotik beschreiben und interpretieren zu können [OR74], [Sch99]. Verschiedene Werkzeuge ermöglichen den Anwendern die Umsetzung der Methoden über verschiedene Beschreibungsmittel, die zum Teil in ganzen Arbeitsumgebungen zusammengefasst werden. Das s.g. „BMW-Konzept“ zur Beschreibung der Zusammenhänge zwischen Beschreibungsmittel (B), Methoden (M) und Werkzeugen (W) kann ergänzend berücksichtigt werden [Sch99]. Im folgenden Unterabschnitt wird eine kleine Auswahl aus der Vielzahl von vorhandenen Beschreibungsmitteln getroffen, die im weiteren Verlauf der Arbeit eingesetzt werden. Die Modellierungsmethode anhand der Beschreibungsmittel wird zudem kurz erläutert.

2.1.1 Beschreibungsmittelauswahl

Der Begriff Beschreibungsmittel stammt aus der Domäne der Automatisierungstechnik und wird heute übergreifend verwendet. Als Beschreibungsmittel werden dort textuelle, mathematische oder grafische Mittel zur Darstellung von Sachverhalten im gesamten Lebenszyklus einer automatisierungstechnischen Einrichtung verstanden. Das behandel-

te Spektrum reicht von einfachen Anforderungsformulierungen über Spezifikationen von Strukturen und Verhalten, Implementierungssprachen bis hin zur Anlagen- bzw. Produktdokumentation sowie Wartungshandbüchern [Sch99], [VDI05].

Beschreibungsmittel dienen somit der Formalisierung von Sachverhalten mit verschiedenen Zielstellungen. Es lassen sich mit Hilfe von Beschreibungsmitteln, unabhängig von der Domäne, zum einen Aufgaben und Probleme einer existenten Realität deskriptiv dargestellen, zum anderen aber auch Lösungen einer fiktiven Realität präskriptiv beschreiben, die sich auf verschiedene Eigenschaften von Systemen konzentrieren, mit dem Ziel, dem Betrachter ein klares und eindeutiges Verständnis zu vermitteln. Für ein besseres Verständnis und eine eindeutige Darstellung werden im weiteren Verlauf vorwiegend grafische Beschreibungsmittel mit festgelegten Notationen verwendet. Eine Notation kann dabei sowohl aus vereinbarten textuellen Zeichen, als auch aus definierten Zeichen bzw. Symbolen bestehen. Eine umfangreiche Auswahl und Bewertung von Beschreibungsmitteln der Automatisierungstechnik ist in [Sch99] durchgeführt worden. Die hier verwendeten Beschreibungsmittel werden in den folgenden Unterabschnitten kurz vorgestellt.

UML - Diagramme

Die vereinheitlichte Modellierungssprache - UML („Unified Modelling Language“) ist in der ISO/IEC 19501 in der Version 1.4.2 standardisiert worden, aus der sich die aktuelle UML 2.0 Notation entwickelt hat.

- UML 2.0 Diagramme
  - Strukturdiagramme
    - Klassendiagramm
    - Objektdiagramm
    - Verteilungsdiagramm
    - Komposistionsstrukturdiagramm
    - Paketdiagramm
    - Komponentendiagramm
  - Verhaltensdiagramme
    - Use-Case Diagramm
    - Aktivitätsdiagramm
    - Zustandsautomat
      - Interaktions-Übersichtsdiagramm
      - Timingdiagramm
      - Kommunikationsdiagramm
      - Sequenzdiagramm

Stark durch die objektorientierte Softwareentwicklung geprägt, beinhaltet die UML weit verbreitete Diagrammarten. Die Diagramme werden in Struktur- und Verhaltensdiagramme unterschieden. Dazu zählen u.a. strukturelle Beschreibungen wie z.B. Klassendiagramme, Kompositionsstrukturdiagramme, Objektdiagramme und Paketdiagramme. Die wichtigsten verhaltensbeschreibenden Diagramme sind Anwendungsfalldiagramme („Use-Case Diagramme“), Zustandsautomaten, Aktivitätsdiagramme und Sequenzdiagramme.

Die UML ist derzeit, nicht zuletzt aufgrund der leichten Verständlichkeit, eine der dominierenden Sprachen in der Modellierung von Softwaresystemen, in der sie ihren Ursprung hat. Aber auch über die Grenzen von Softwaresystemen hinaus hat sich die UML bereits vielfach bewährt und findet eine immer größer werdende Beliebtheit bei Systemingenieuren und in der Spezifikation von Anforderungen.

Im Sinne einer Sprache definiert die UML Bezeichner für die meisten Begriffe, die für eine Modellierung wichtig sind, und legt mögliche Beziehungen zwischen diesen Begriffen fest. Die UML definiert grafische Notationen für diese Begriffe und für Modelle von statischen Strukturen und von dynamischen Abläufen, die man mit diesen Begriffen formulieren kann.

Für die Modellierung von statischen Strukturen eignet sich eine Beschreibung mittels Klassendiagrammen. Ein Menge von Objekten mit identischen Eigenschaften wird dort als Klasse definiert und namentlich bezeichnet. Klassen werden in ihren statischen Eigenschaften und Beziehungen durch typische Merkmale, die ein Element einer Klasse genauer beschreiben (Attribute), spezifiziert.

Der Aufbau von Partonomien kann durch die Ganzes-Relation (*ist-Teil-von-Relation*) sowie die Gattungsrelation (*ist-ein-Relation*) mittels s.g. Assoziationen und Vererbungen dargestellt werden. Bei der Spezialisierung bzw. Generalisierung von Klassen erhalten die individuellen (Unterklassen) die Eigenschaften (Attribute, Operationen, Methoden) der übergeordneten (Oberklassen) im Sinne der Vererbung.

Eine Assoziation, die eine Teile-Ganzes-Beziehung beschreibt, wird als Aggregation bezeichnet, sofern die Teile unabhängig vom Ganzen existieren können. Teil-Ganzes-Beziehungen dagegen, bei denen die Existenz der Teile abhängig vom Ganzen ist, werden als Komposition bezeichnet (ein Raum als Teil eines Gebäudes existiert nicht ohne dieses). Ein erklärendes Beispiel ist in Abbildung 2.1 dargestellt.

Für die Darstellung und Erläuterung struktureller Zusammenhänge im Kontext der Verkehrssicherheit eignen sich Klassendiagramme aufgrund ihrer einfachen aber doch eindeutigen Notation hervorragend. Die einfache Modellierung und die Möglichkeit, auch komplexe Strukturen verständlich darstellen zu können, tragen zur Auswahl dieses Beschreibungsmittels für die Abbildung statischer Zusammenhänge und Eigenschaften in dieser Arbeit bei.

Für die Beschreibung dynamischer Verhalten wird in dieser Arbeit auf die Verwendung der UML Verhaltensdiagramme allerdings verzichtet. Wenngleich die UML mit der Einführung der Aktivitätsdiagramme über eine den Petrinetzen ähnliche Diagrammart verfügt, werden Dynamiken hier vorzugsweise mit einfachen Petrinetzen beschrieben. Die Darstellung von Prozessen bzw. von allgmeien dynamischen Zusammenhängen muss für eine eindeutige Interpretation formaler Natur und zugleich für den Leser leicht verständ-

lich sein. Die Verwendung von Petrinetzen wird in dieser Arbeit nicht zuletzt aufgrund ihrer einfachen Notation (lediglich drei verschiedene Elemente) sondern auch aufgrund ihrer sonstigen Eigenschaften, die ausführlich in [Jan97] sowie in [VDI05] mit anderen Beschreibungsmitteln verglichen werden, bevorzugt.

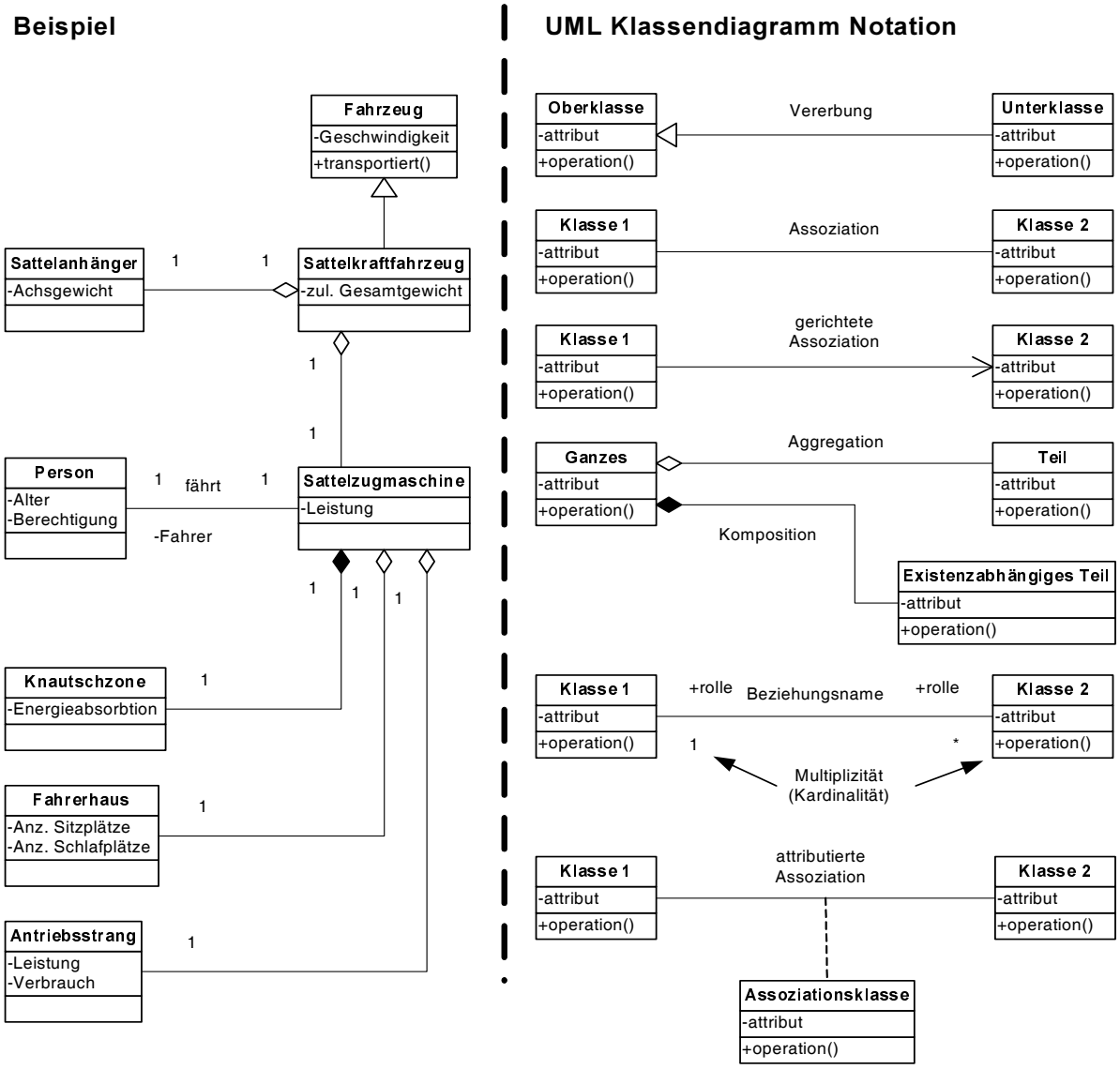


Abbildung 2.1: Notation der UML Klassendiagramme

Petri-Netze

Petrinetze sind nach ihrem Erfinder, Carl Adam Petri, benannt und sind ebenso wie Zustandsübergangsdiagramme Modelle, mit denen Zustände eines Systems sowie die Übergänge zwischen diesen aufgrund von Ereignissen modelliert werden können. Petrinetze eignen sich insbesondere für die Modellierung paralleler bzw. verteilter Systeme, die aus Komponenten bestehen, deren Zustand sich unabhängig weiterentwickelt. Petrinetze lassen sich wie folgt unterscheiden.

- Petrinetze
  - Low-Level Netze
    - Kanal-/Instanzen-Netz (K/I-Netz)
    - Bedingungs-/Ereignis-Netz (B/E-Netz)
    - Stellen-/Transitions-Netz (S/T-Netz)
  - High-Level Netze
    - Gefärbtes Netz (CPN)
    - Hierarchisches Petrinetz
    - Attributiertes Petrinetz
    - Zeitbewertete Petrinetze
      - Stochastisches Petrinetz (SPN)
      - Generalisiertes Stochastisches Petrinetz (GSPN)
      - Deterministisches Stochastisches Petrinetz (DSPN)
    - ...

Ein Petrinetz ist ein bipartiter und gerichteter Graph. Er besteht aus Stellen und Übergängen bzw. Transitionen, welche durch gerichtete Kanten verbunden sind. Es existieren keine direkten Verbindungen zwischen zwei Stellen oder zwei Transitionen. Stellen werden als Kreise, Transitionen als Rechtecke und Kanten als Pfeile dargestellt (vgl. Abbildung 2.2). Die Belegung der Stellen mittels Token, Marken oder Zeichen wird als Markierung bezeichnet und beschreibt den Zustand des Petri-Netzes. Jede Stelle besitzt eine definierte Kapazität und kann entsprechend viele Token, Marken bzw. Zeichen enthalten. Ist keine explizite Kapazität angegeben, so wird von einer unbegrenzten bzw. von einer Kapazität von eins ausgegangen. Jeder Kante ist ebenfalls ein Gewicht (s.g. Kantengewicht) zugeordnet, das die „Kosten“ dieser Kante festlegt. Ist einer Kante kein explizites Gewicht zugeordnet, wird hier der Wert eins verwendet. Sind alle Kapazitäten der Stellen und Kanten eines Petri-Netzes gleich eins, so wird dieses abweichend zu den Stellen-/Transitions-Netzen (S/T-Netz) auch als Bedingungs-/Ereignis-Netz (B/E-Netz) bezeichnet. Wird vollständig auf Markierungen und Kapazitäten verzichtet, wird sogar von einem Kanal-/Instanzen-Netz (K/I-Netz) gesprochen. Neben den einfachen low-level Netzen sind eine Reihe von erweiterten Petrinetztypen entstanden, die in in der Lage

sind, verhaltensorientierte Modelle möglichst nah an der Realität zu beschreiben und darüber hinaus durch komplexe mathematische Verfahren zu analysieren. Die Notation der einfachen Petrinetze ist in Abbildung 2.2 anhand eines Beipiels dargestellt.

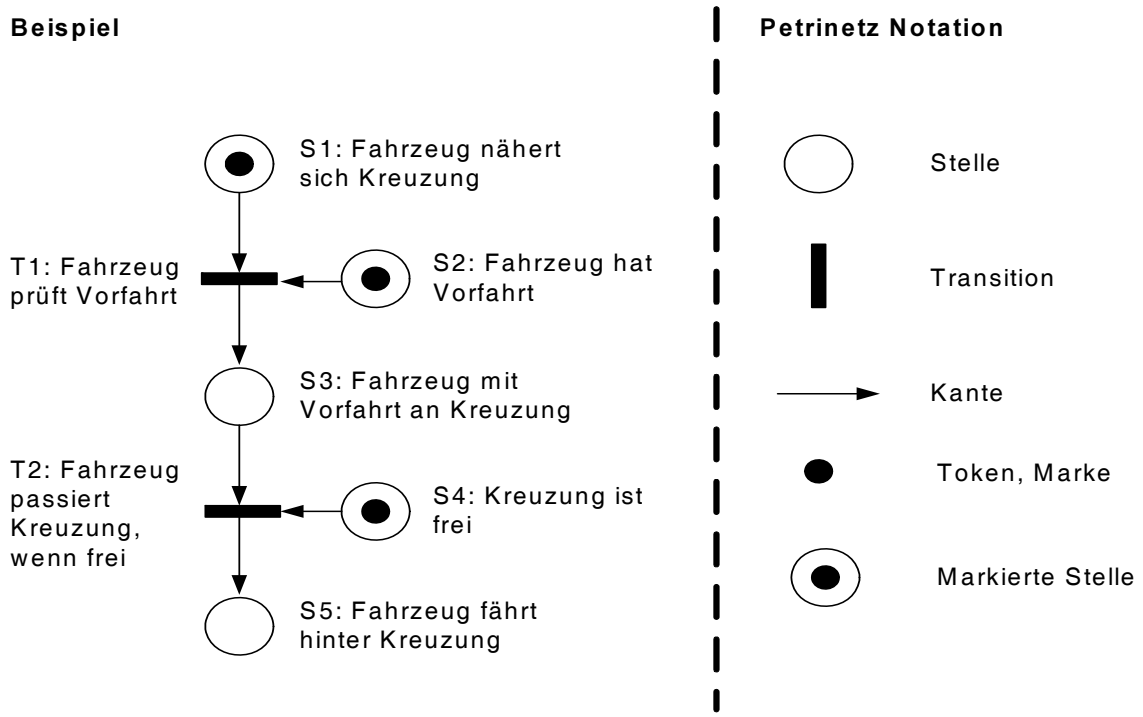


Abbildung 2.2: Notation einfacher (low-level) Petrinetze

Im Folgenden werden vorerst einfache S/T-Netze für die Beschreibung der dynamischen Systemeigenschaften verwendet, bevor in einem späteren Beispiel kurz auf zeitbewertete Petrinetze eingegangen wird. Das Verhalten eines Systems wird durch die Schaltbarkeit der Transitionen bzw. durch die davor existierenden Schaltbedingungen bestimmt. Transitionen sind aktiviert bzw. schaltbereit, falls sich in allen Eingangsstellen mindestens so viele Marken befinden, wie die Transitionen „Kosten“ verursacht und alle Ausgangsstellen noch genug Kapazität haben, um die neuen Marken aufnehmen zu können. Schaltbereite Transitionen können zu einem beliebigen Zeitpunkt schalten. Beim Schalten einer Transition werden aus deren Eingangsstellen entsprechend den Kantengewichten Marken entnommen und bei den Ausgangsstellen entsprechend den Kantengewichten Marken hinzugefügt. Die Marken eines Petri-Netzes sind in ihrer einfachsten Form voneinander nicht unterscheidbar. Für komplexere, aussagekräftigere Petri-Netze sind über die erweiterten Netze Markeneinfärbungen, Aktivierungszeiten und Hierarchien definiert worden.

2.2 Systemtheorie

Auf Grundlage unterschiedlicher Methoden und Ideen setzt sich die Systemtheorie zum Ziel einen wesentlichen Aspekt der realen Welt zu erkennen und zu beschreiben. Mit einer axiomatisch deduktiven Denkweise versucht sie, einen schwer übersehbaren Gesamtkomplex von Erscheinungen in möglichst einfache und zueinander in Wechselwirkung stehende Teilkomplexe aufzulösen, zu analysieren und ggf. mathematisch zu beschreiben [Wun85].

Die Systemtheorie befasst sich dabei mit der interdisziplinären modellhaften Darstellung von Systemen zur Beschreibung und Erklärung unterschiedlich komplexer Phänomene und Prozesse und wurde auch unter der Bezeichnung der "Systemlehre" durch Ludwig van Bertalanffy bereits 1949 [Ber69] als wissenschaftliches Paradigma eingeführt, da sie im Widerspruch zur klassischen Physik stand. Die Systemtheorie gilt allgemein als domänenunspezifisch und lässt sich auf verschiedene zu analysierende (Fach-)Gebiete anwenden und verfügt dementsprechend über vielfältig ausgeführte Ansätze und Theorien. Als wichtigste Vertreter der am ehesten bekannten soziologischen Systemtheorie gelten Niklas Luhmann (kommunikationstheoretische Systemtheorie) und Talcott Parsons (handlungstheoretische Systemtherorie). Niklas Luhmann ordnet die Wirklichkeit auf der Grundlage der Unterscheidung bzw. Abgrenzung zwischen System und Umwelt. Er versteht die Umwelt als eine Handlungsverlängerung des Systems nach außen [Wil01]. Diese Denkweise ließe vermuten, dass die Grenze zwischen dem System und seiner Umwelt als eine scharfe Systemgrenze verstanden wird. Luhmann allerdings beschreibt Systemgrenzen als diffus und nicht klar und eindeutig zu bestimmen. Die Luhmannschen Systeme definieren sich allein durch sogenannte Zuschreibungen von Eigenschaften und Teilsystemen. Die erste Annahme für ein System auf Basis einer rein deterministischen Systemstruktur und rein deterministischem Verhalten wäre demnach ein rein theoretischer Ansatz und nur in einem ersten Ansatz praktikabel. Talcot Parsons, einer der Nachfolger von Max Weber, hat durch die Entwicklung des AGIL-Schemas einen Vorsprung im Bereich des sogenannten Strukturfunktionalismus erreicht. Das Grundkonzept beruht auf einem Vier-Quadranten-System zur Beschreibung der erforderlichen Funktionen zur Selbsterhaltung von Systemen. Die grundlegenden Funktionen eines Systems werden dort wie folgt beschrieben [BJK07]:

- Anpassung: die Fähigkeit eines Systems, auf die sich verändernden äußeren Bedingungen zu reagieren, sich anzupassen.
- Zielverfolgung: die Fähigkeit eines Systems, Ziele zu definieren und zu verfolgen.
- Eingliederung: die Fähigkeit eines Systems, Kohäsion (Zusammenhalt) und Inklusion (Einschluss) herzustellen und abzusichern.
- Aufrechterhaltung: die Fähigkeit eines Systems, grundlegende Strukturen und Wertmuster aufrechtzuerhalten.

Für das Verständnis und die strukturierte Analyse der (Verkehrs-)sicherheit ist sowohl die Kenntnis der involvierten Systeme, Teilsysteme, Komponenten in einer definierten Systemstruktur, als auch die Berücksichtigung der Funktionsstruktur im Sinne von Funktion und Verhalten der Systeme bzw. Teilsysteme von gleicher Bedeutung, so dass hier für ein systematisches Konzept auf unterschiedliche Systemgrenzen aus unterschiedlichen Sichten zurückgegriffen wird. Unterschieden wird im weiteren Verlauf zwischen funktionalen und konstruktiven Systemgrenzen. Während sich einerseits ein System aufgrund seiner technisch funktionalen Zugehörigkeit definiert (z.B. Unterscheidung zwischen Querführung und Längsführung bei der Fahrzeugbewegung), kann ein System sich andererseits anhand seiner konstruktiv physikalischen Zugehörigkeit definieren (z.B. Unterscheidung zwischen (Lenk-)Achse und Antriebsstrang). Beide Sichtweisen ergeben verschiedene Systemgrenzen und Schnittstellen innerhalb eines übergeordneten Systems (hier: Fahrzeug). Diese Sichtweisen spiegeln sich zum einen durch den klassischen Begriff der System-Umwelt-Relation nach Luhmann, der strukturell-funktionalen Systemtheroie nach Parsons als auch zum anderen mit den Ansätzen der ingenieurwissenschaftlichen Systemtheorie, die insbesondere in der Regelungstechnik und der Elektrotechnik ihre Anwendung findet.

2.2.1 Identifikation von Systemen durch Systemgrenzen

In der Konzeption eines geschlossenen Systems wird die Existenz einer Beziehung zur Systemaußenwelt ausgeschlossen bzw. das Systemmodell wird nicht im Bezug zu seiner dennoch existierenden Systemumwelt betrachtet. Geschlossene Systeme verfügen demnach über keinerlei Schnittstellen über ihre eigenen Systemgrenzen hinweg, da die Systemumwelt explizit außer Betracht liegt. In der Praxis sind solche Systeme kaum vorstellbar. Sie existieren fast ausschließlich auf Modellebene, da eine vollständige Isolation eines realen Systems in der Praxis nur schwer erreichbar ist. Häufig werden sie jedoch zur Vereinfachung bei komplexen Rechenmodellen oder zur vereinfachten (freigeschnittenen) Veranschaulichung verwendet. Offenen Systemen hingegen, die nicht wie geschlossene Systeme isoliert betrachtet werden, ermöglicht die Definition der Schnittstellen zur Überwindung der Systemgrenzen zu anderen Systemen und zu der Systemumwelt eine definierte Dynamik.

Ein System mit definierten Systemgrenzen (vgl. Abbildung 2.3) wird als eine Menge von Elementen (bzw. Teilsystemen) verstanden, die in einem abgegrenzten oder abgrenzbaren Bereich so zusammenwirken, dass dabei ein vollständiges, sinnvolles, zweck- und zielgerichtetes Zusammenwirken in einem funktionellen Sinne erzielbar wird. Erreicht werden kann dieses funktionale Zusammenwirken (die Funktion) durch das Verhalten und die Struktur des Systems in dessen Umwelt. Das in seiner Umwelt eingebettete System steht somit in einer definierten Beziehung zu eben dieser bzw. zu anderen Systemen; d.h. es existieren definierte Wechselwirkungen über die Systemgrenzen hinweg, die u.a. zu einem positiven Nutzen oder zu einer negativen Beeinflussung des Systems führen. Eingaben (Einflüsse oder Stimuli von außen, denen ein System unterliegt) und Ausgaben (Wirkungen des Systems nach außen auf andere Systeme oder auf seine direkte

Systemumwelt) überwinden die Systemgrenzen über die Schnittstelle zur Systemumwelt. Dazu gehören z.B. der Austausch von Stoff, Energie und Information sowie die Einwirkung äußerer Faktoren korrespondierender Systeme wie z.B. Temperatur, Strahlung, bzw. jegliche Art von Zuständen, die die Systemumwelt oder das Nachbarsystem einnehmen können.

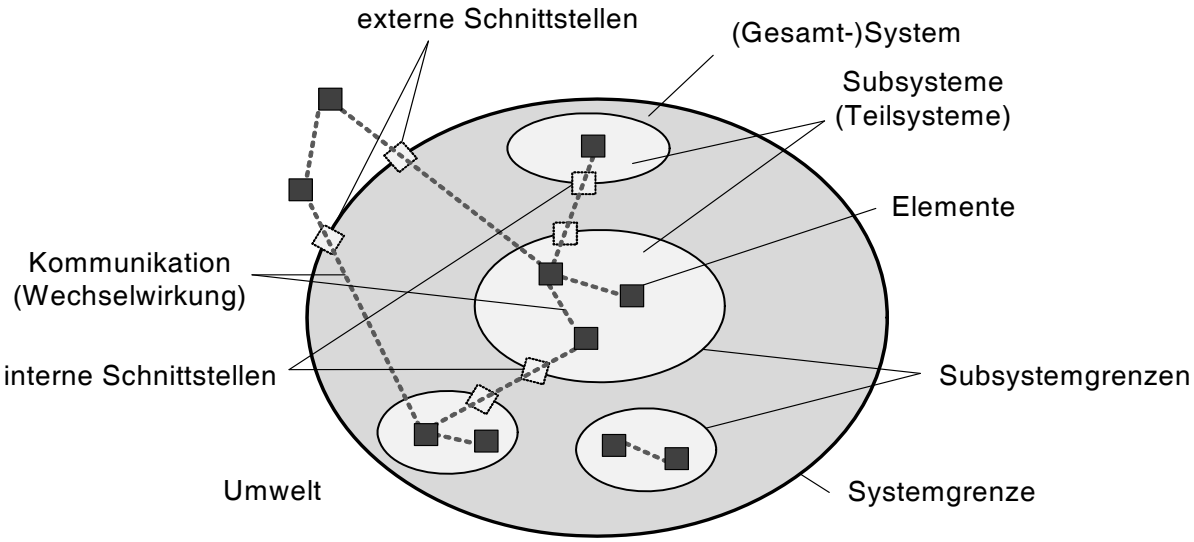


Abbildung 2.3: Grundlegendes Systemverständnis als Basis

Die jeweilige Ausprägung der Einflussnahme bzw. Beeinflussung lässt sich einerseits durch die inhärenten Systemeigenschaften charakterisieren, andererseits sind es die Systemeigenschaften selbst, die beeinflusst werden und dann zu einem veränderten Systemverhalten führen. Die Exposition eines Systems (z.B. Mensch) einer einwirkenden Umgebung (z.B. radioaktiver Strahlung) kann zum einen die eigenen Systemeigenschaften sowohl negativ (z.B. Krebsbildung durch Zellmutation) als auch positiv (z.B. Antitumorwirkung in der Strahlentherapie) beeinflussen. Zum Anderen ist die strahlende Wirkung durch die jeweilige Systemeigenschaft des radioaktiven Systems geprägt. Neben dieser energetischen Beeinflussung von Systemen können viele andere externe Einflüsse unterschiedliche Wirkungen auf die Struktur, das Verhalten, den Zustand und somit ggf. auch auf die Funktion und die daraus resultierende Sicherheit von Systemen auslösen. Eine genauere Betrachtung der Systemeigenschaften und -merkmale in einem systematischen Zusammenhang folgt im nächsten Abschnitt.

2.2.2 Systemeigenschaften und -merkmale

Die Art und Weise in der sich Systeme ihrer Umwelt oder anderen Systemen darstellen, sich verändern oder andere beeinflussen, wird durch die Charakteristik eines Systems bestimmt. Die Charakteristik eines Systems wird durch seine Eigenschaften und Merkmale geprägt.

Die Unterscheidung zwischen Eigenschaft und Merkmal ist in der Terminologie und in der Fachwelt uneinheitlich. Es existieren dabei gleichermaßen Ansätze, die einer objektorientierten Sichtweise entweder im Sinne einer Klassenbildung gleichkommen, oder eher einer reinen hierarchischen Struktur folgen.

Objektorientierte Interpretation

Die Definition von Eigenschaft und Merkmal kann auf die Unterscheidung von Gegenstand und Begriff zurückgeführt werden [Deu93], wobei Gegenstände als konkrete Instanziierung eines Begriffs lediglich über Eigenschaften verfügen, während ein Begriff als Klasse eigenschaftsähnlicher Gegenstände zusätzlich über Merkmale verfügt [Fre02]. Diese Interpretation folgt einer Sichtweise im Sinne der Klassenbildung und Instanziierung.

Als erklärendes Beispiel bietet sich die Betrachtung von *Personen* als instanziierte Objekte einer übergeordneten Klasse *Mensch* an. Während *blonde Haare* für die Person X als Eigenschaft eines Gegenstands definiert werden kann, verfügt Person Y als weiterer Gegenstand über die Eigenschaft *schwarze Haare*. Entsprechend dem vorliegenden Ansatz verbindet beide Gegenstände (Personen X und Y) als Klasse Mensch das Merkmal *Haarfarbe*. Diese Interpretation stützt sich dabei auf die Prinzipien der Instanziierung innerhalb der Objektorientierung und stellt den „Begriff“ im objektorientierten Sinn als „Klasse“ dar, während der „Gegenstand“ den instanziierten Begriff (hier: instanziierte Klasse) bzw. das Objekt repräsentiert.

Das Beispiel in Abbildung 2.4 zeigt diesen Ansatz zusätzlich auf Basis sicherheitsbezogener Eigenschaften von Objekten und Merkmalen von Klassen. Das Beispiel zeigt neben einem allgemeinen Beispiel zu Fahrzeugen zwei unterschiedlich aufgebaute Steuerungskomponenten als implementierte Gegenstände einer Klasse Speicher-Programmierbarer-Steuerung (SPS). Es wird deutlich, dass bei diesem Ansatz die Sicherheitsintegrität als Merkmal eines Systems betrachtet werden kann, während die konkret erreichte Sicherheitsintegritätsstufe der Implementierung dessen konkrete Eigenschaft charakterisiert und z.B. über die späteren Einsatzmöglichkeiten entscheiden kann.

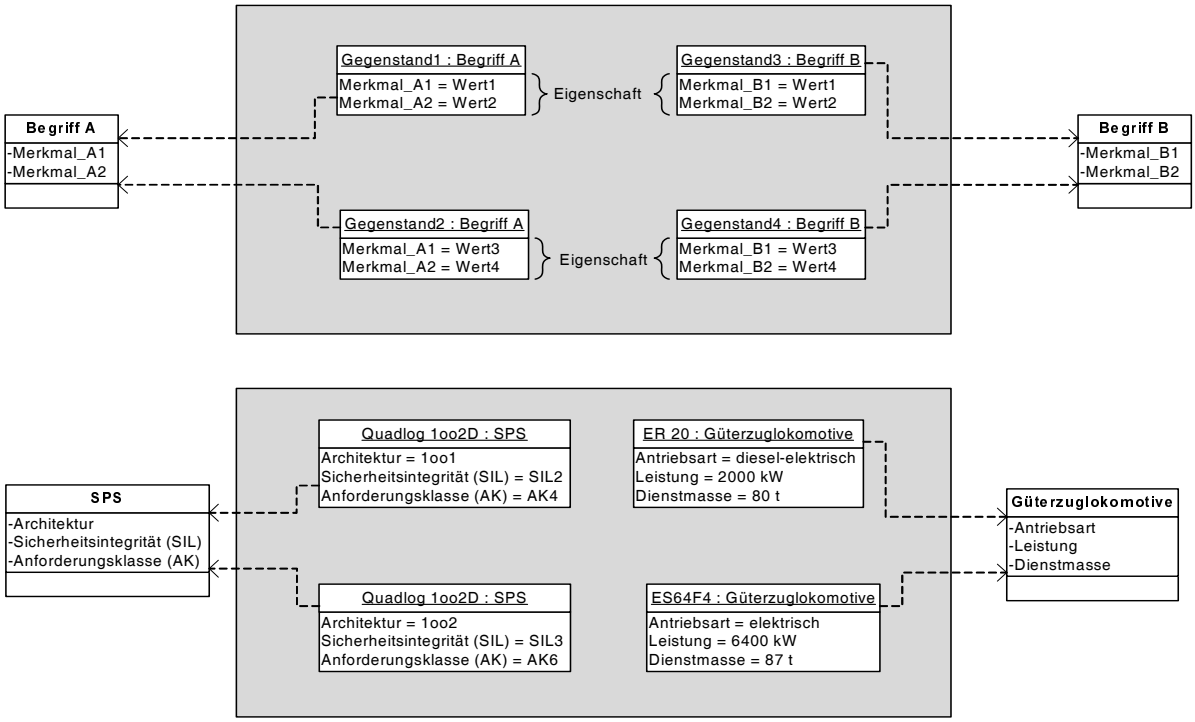


Abbildung 2.4: Objektorientierte Sichtweise der Systemeigenschaftswelt

Dieser Ansatz ermöglicht zwar eine Unterscheidung zwischen konkreten und abstrakten Systemen, der Mehrwert und die Handhabbarkeit bezüglich der systematischen Analyse der Verkehrssicherheit ist jedoch nicht klar ersichtlich und kann eher zu Missverständnissen führen als Wissen fördern. Aus diesem Grund wird ein anschaulicheres und ebenso fundiertes Konzept nach [SS07] verfolgt, das sich bis zu den Erkenntnistheorien von Carnap zurückführen lässt [Car34].

In diesem hierarchisch partitiven Konzept wird eine Eigenschaft allgemein als Beschaffenheit eines Objektes beschrieben, die durch verschiedene Mermale weiter charakterisiert werden kann. Die Merkmale selber werden zudem durch Größen und die damit verbundenen Werte konkretisiert. Das Merkmal ist dort als systematischer Oberbegriff der Größe definiert. Der Ansatz ermöglicht es auf Basis von Hierarchisierungen die Komplexität von Systemen und insbesondere auf Merkmalsebene zu reduzieren und somit leichter zu veranschaulichen.

In Abbildung 2.5 wird die hierarchische Struktur von Eigenschaft, Merkmal, Größe und Wert anhand eines Beispiels verdeutlicht. Verkehr, dort als System definiert, weist u.a. die Verkehrsverlässlichkeit als Eigenschaft auf. Daneben könnten Eigenschaften mit abweichenden Merkmalen existieren, z.B. Verkehrswirtschaftlichkeit o.ä., die hier nicht weiter vertieft werden. Als Merkmale der Verkehrsverlässlichkeit werden die Verkehrssicherheit, Verkehrsverfügbarkeit, Verkehrszuverlässigkeit und Verkehrswartbarkeit definiert, die jeweils über verschiedene Größen und damit verbundene Werte verfügen. Die Verkehrssicherheit lässt sich beispielsweise durch die beiden Größen Unfallhäufigkeit und Schadensausmaß konkretisieren, die durch entsprechende Werte, z.B. die konkrete Un-

fallopferhäufigkeit von 4949 Straßenverkehrstoten in Deutschland im Jahr 2008, belegt werden. Die Gesamtheit der untergeordneten Merkmale prägen die jeweils überlagerte Eigenschaft des Systems.

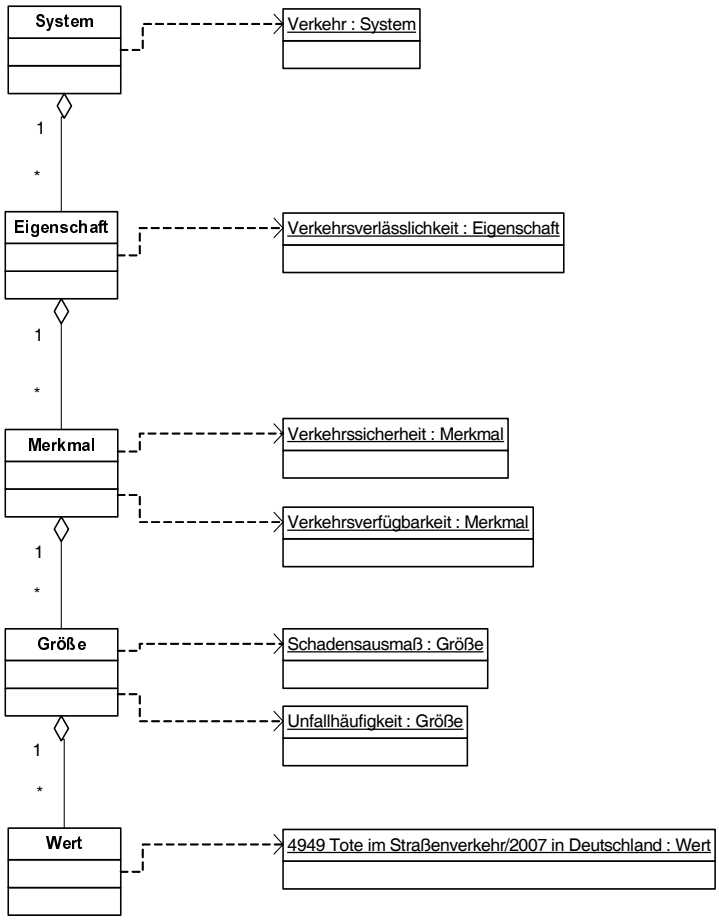


Abbildung 2.5: Hierarchischer Strukturansatz zu den Systemeigenschaften

Die Unterscheidung zwischen Eigenschaft, Merkmal und Größe ermöglicht somit die einfache hierarchische Interpretation von Systemeigenschaften anhand einfacher Dekompositionsprinzipien und trägt damit erheblich zum Gesamtverständnis von Systemen bei. Für weitere Beschreibungen wird aus diesem Grund dieser zweite Ansatz verfolgt.

Konkrete Systemeigenschaften

Nach [Sch99] lässt sich ein jedes System grundsätzlich systematisch durch statische und dynamische Grundeigenschaften beschreiben. Jedes System, gleich ob natürlicher oder künstlicher Herkunft, besitzt eine spezifische *Struktur*, ist für die Ausführung einer oder mehrerer *Funktionen* zuständig und ändert durch sein *Verhalten* seine lokalen und globalen *Zustände*. Die Ausprägung dieser in Abbildung 2.6 gezeigten Systemeigenschaften:

Struktur, Zustand, Verhalten und Funktion charakterisiert somit ein System grundlegend.

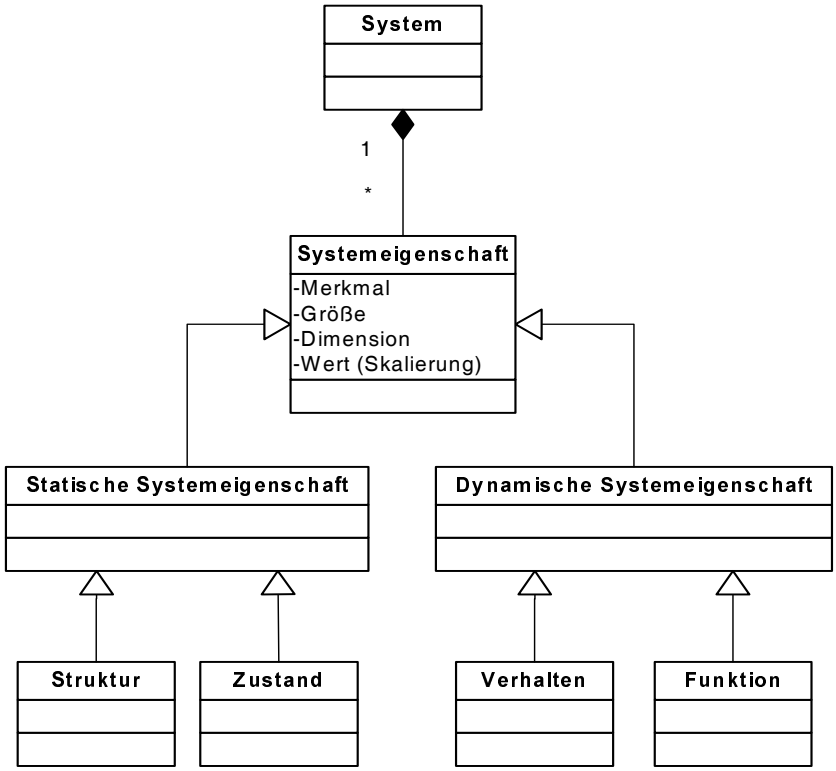


Abbildung 2.6: Grundeigenschaften eines Systems

Die vier Systemeigenschaften werden in den folgenden Unterabschnitten anhand von Beispielen erläutert.

Struktur

Als Struktur wird der (innere) Aufbau eines Systems verstanden und damit die Art und Weise wie Teile eines Ganzen untereinander und zu diesem Ganzen verbunden sind.

Eine Struktur kann sowohl den funktionalen, logischen als auch physischen Aufbau eines Systems beschreiben. Die logische Struktur zeigt die Hierarchisierung von Informationen bzw. von logischen Zuständen, während die physische Struktur die Zusammensetzung eines technischen Systems, wie z.B. die Zerlegung einer Lenkung (vgl. Abbildung 2.7) in seine Komponenten, darstellt. Neben der logischen und physischen Struktur können auch Funktionen strukturiert werden. Dazu zählen vor allem funktionale Architekturen mit dem Ziel ein verändertes Systemverhalten zu erwirken. Redundante oder sogar diversitäte Strukturen, die eine definierte Funktion durch Verdoppelung der Ressource bzw. bei gleichzeitiger Verschiedenheit der Ressource parallel ausführt und somit das Ausfallverhalten des Systems bzw. die Ausfallsicherheit des Systems verbessert, sind Beispiele dafür.

Die *Struktur* eines Systems beeinflusst somit sein *Verhalten* und charakterisiert dadurch die beabsichtigte vorgesehene *Funktion*. Werden zudem bestimmte logische Strukturen z.B. in einem Gelenkgetriebe realisiert, entstehen zusätzliche oder reduzierte Freiheitsgrade, die den Funktionsumfang entweder erweitern oder reduzieren. Erst das definierte *Verhalten* eines Getriebes ermöglicht dessen *Funktion*, die sich auf die Übertragung und Wandlung von Bewegungen konzentriert. Das spezifische *Verhalten* von Systemen hingegen wird in der Änderung seiner *Zustände* bedingt. Instabile Systeme neigen beispielsweise aufgrund ihres instabilen *Verhaltens* eher dazu einen gestörten oder defekten *Zustand* einzunehmen als stabile Systeme.

Über die Realisierung verschiedener in einer definierten *Struktur* angeordneten *Funktionen* wird das beabsichtigte *Verhalten* eines Systems ermöglicht und beeinflusst. Umgekehrt kann ein bestimmtes kausales und zeitliches Verhalten durch eine definierte Funktion oder Teilfunktion umgesetzt werden, wie es in den meisten Fertigungsanlagen erfolgreich demonstriert wird. Diese systematische und eng vermaschte Betrachtung der gezeigten Systemeigenschaften kann einen großen Beitrag bei der Analyse und der gezielten Implementierung von Sicherheit in Systemen leisten.

Zustand

Unter einem Zustand versteht man die Gesamtheit aller Eigenschaften oder Attribute, die zur Abgrenzung und Unterscheidung des jeweils betrachteten Objekts von anderen Objekten nötig sind.

Zustände können dabei sowohl in Form von physikalischen als auch in Form von logischen Zuständen vorliegen [Sch99]. Physikalische und informationelle (logische) Eigenschaften eines Systems werden als abstrakter Zustandsbegriff, bestehend aus einem Attribut-Wertemengen-Paar, beschrieben. Das Attribut charakterisiert über die Art der Zustandsgröße (z.B. physikalische Ausprägung) die Systemeigenschaft, während die Wertemenge als Wert der Zustandsmenge die Größe beschreibt. Ein eindeutiger Wert einer Zustandsgröße wird als Elementarzustand bezeichnet. Die konkrete Temperatur von 37°C beschreibt einen Elementarzustand des menschlichen Körpers, während sich der abstrakte logische Zustand „sicher“ aus einer Menge von einzelnen Elementarzuständen eines Systems zusammensetzt.

Grundsätzlich wird auf diese Weise zwischen lokalen und globalen Zuständen unterschieden. Der zu einem definierten Zeitpunkt existente Globalzustand (z.B. Systemzustand) besteht aus der Menge aller zum gleichen Zeitpunkt existierenden (Elementar-) bzw. Lokalzustände.

Ungeachtet dieser Differenzierung lassen sich Zustände unterschiedlich skalieren. Diese Skalierung wirkt sich auf die Auflösungseigenschaften der Zustandsgrößen aus. Lässt sich ein Zustand nur durch diskrete Werte z.B. „intakt“ oder „defekt“ oder durch eine abzählbare Zustandsmenge beschreiben, so wird dieser Zustand als diskreter Zustand bezeichnet. Lässt sich die Zustandsmenge hingegen sehr fein auflösen (z.B. durch eine Wertedarstellung mit rationalen oder reellen Zahlen), wird dies als kontinuierliche Auflösung bezeichnet.

Diese Charakterisierung von Zustandsgrößen und die Unterscheidung von möglichen

Zustandsübergängen (diskret oder kontinuierlich) bedingt das jeweilige Verhalten bzw. die realisierte Funktion des betrachteten Systems.

Verhalten

Technische Systeme sind künstliche Gebilde, die von Menschen in der Regel nur dann erschaffen werden, wenn diese ein gewünschtes Verhalten erfüllen können, das mittels definierter Funktionen realisiert wird. Aber auch natürliche Systeme können wichtige Funktionen erfüllen. Als Beispiel dafür kann die biologische Schutzfunktion, durch s.g. Antikörper, innerhalb des menschlichen Immunsystems dienen. Über einen wirksamen Mechanismus (über die DNA vorbestimmtes Verhalten der einzelnen Zellen) wird beispielsweise die Bekämpfung gefährlicher Infektionen ermöglicht. Das Verhalten (Veränderung bzw. Folge von Zuständen) der Systeme, unabhängig von natürlicher oder künstlicher Herkunft, kann dabei grundlegend durch folgende ursächliche Einflüsse begründet sein:

- selbsttätig ohne externe Einflüsse (autonom)
- zusammenhängend mit einem externen Einfluss (konsistent)
- widerstandsfähig gegen externe Einflüsse (resistent)

Wie bereits in Unterabschnitt 2.2.1 beschrieben, kann das Verhalten im Sinne von Einfluss und Wirkung in Stoff- bzw. Materie-, Energie- sowie Informationsflüsse differenziert werden. Dabei sind sämtliche Kombinationen zwischen Einfluss und Wirkung möglich. Die kausalen Zusammenhänge zwischen Einfluss und Wirkung können dabei sowohl qualitativ als auch quantitativ betrachtet werden (vgl. Tabelle 2.1). Anders als bei quantitativen Reizen, die zu quantitativen Wirkungen führen können, lassen sich durch qualitative Reize nicht direkt quantifizierbare Wirkungen ableiten. Bei quantifizierbaren Reiz/Wirkungsbeziehungen bestimmt beispielsweise die Stärke oder auch die Richtung des Reizes wiederum die Stärke bzw. Richtung der Wirkung und wird geprägt durch die spezifische Funktion des Systems.

Tabelle 2.1: Einfluss- und Wirkungsrelationen im Vergleich

Art	**Einfluss**	**Wirkung**
Qualitativ	qualitativer Reiz z.B. Hitze	qualitative Reaktion z.B. Ausdehnung
Quantitativ	quantitativer Reiz z.B. def. Stoßvektor z.B. def. el. Spannung	quantitative Reaktion z.B. def. Beschleunigungsvektor z.B. def. Drehzahl

Die Ursache-Wirkung Beziehung ist dabei nicht auf eine intersystemische Relation beschränkt und kann zusätzlich in einer intrasystemischen Beziehung wirken. Die Funktion eines Systems und damit sein Verhalten kann dabei zusätzlich wie folgt auf den eigenen Zustand zurückwirken:

- direkt: der mechanische Stoß erwirkt die direkte Verformung
- indirekt: die Einwirkung durch Hitze löst über eine Ausdehnung eine Schutzreaktion des Systems aus und führt zu dessen Stillstand

Aus der Automatisierungstechnik ergibt sich die Definition des Prozesses, der einen speziellen Verlauf der Zustände als Ausdruck des Systemverhaltens bezeichnet [Sch99]. Wird weiter zwischen Objekt- und Steuerungsprozess unterschieden, können Systemfunktion und Automatisierungsfunktion differenziert werden, wobei der Objektprozess das Verhalten des zu steuernden Objektes und der Steuerungsprozess das eingreifende, steuernde oder regelnde Verhalten der Automatisierungsfunktion beschreibt.

Funktion

Die definierte Kombination aus einzelnen Teilfunktionen und somit das kombinierte Verhalten von Systembestandteilen kann die gezielte übergeordnete Funktion und somit das Systemverhalten ermöglichen.

Die gezielten strukturellen Kombinationen von Einfluss-Wirkungsbeziehungen (siehe Struktur) verschiedener Funktionselemente können somit ausgenutzt werden, die Systemfunktionen eines Systems zu ermöglichen und das Systemverhalten zu bestimmen.

Die primäre Funktion eines Kraftfahzeugs, die Umsetzung von fossilem Kraftstoff bzw. erneuerbaren Energien in kontrollierbare Bewegungsenergie und der damit verbundene kontrollierte Transport von Objekten, wird durch eine Vielzahl von Teilfunktionen, die auf unterschiedlichste Verhalten von Teilsystemen und Komponenten basieren, realisiert. Das vollständige Systemverhalten drückt sich in einer Vielzahl von gewünschten wie auch in einer Vielzahl von unerwünschten, bzw. auch unbekannten Teilsystemverhalten aus. Die Änderung der Trajektorie eines Fahrzeugs nach Änderung des Lenkwinkels kann als gewünschtes, das Ausbrechen des Hecks beim Übersteuern des Fahrzeugs hingegen als ungewüschtes Verhalten bei der Umsetzung der Lenkfunktion interpretiert werden.

Diese Beziehung zwischen Funktion und Verhalten kann sowohl auf Systemebene als auch auf Subsystem- und Komponentenebene beobachtet werden. Auf Subsystem-/Komponentenebene erfüllt beispielsweise ein Wälzlager die Funktion der Abstützung von radialen und axialen Kräften an Achsen und Wellen. Das Verhalten hängt zwar stark von der Bauweise des Wälzlagers ab, kann aber grundsätzlich ebenfalls durch Einfluss-Wirkungsbeziehungen beschrieben werden. Als Einflussgröße kann die Rotation der Welle oder Achse verstanden werden, während die Wirkung als eine resultierende möglichst geringe Reibungsenergie und der damit verbundenen Wärmeentwicklung neben der Unveränderlichkeit der geometrischen Lage der Welle definiert werden kann. In Abhängigkeit von der Einflussgröße werden die Wirkungsgrößen definiert. Bei unzulässig großer Drehzahl beispielsweise könnte die Reibungsenergie einen zulässigen Wert überschreiten

und die daraus resultierende Wärme die Lage der Welle entsprechend verändern. Das Resultat dieses ungewollten Verhaltens könnte sogar die gewünschte Funktion eliminieren und zu einem Funktionsausfall führen, der sich auf die eigene Systemfunktionalität oder das Verhalten anderer auswirken könnte.

Funktionen werden, wie durch das Wälzlagerbeispiel gezeigt, durch Ressourcen (Funktionsträger), die ein spezifisches Verhalten aufweisen, implementiert und erfüllt. In [Sch99] sind die Merkmale und Strukturierung von Funktionsträgern ausführlich behandelt worden.

Die Trennung von Funktion und Ressource spielt bei einer systemischen Betrachtung eine große Rolle, da hierdurch eine Modularität des Systems insbesondere beim Systemdesign erhalten bleibt. Eine Funktion kann durchaus in unterschiedlicher Weise implementiert und realisiert werden. Das schließt sowohl unterschiedliche Ressourcen (Komponenten und Subsysteme) als auch die damit verbundenen verschiedenen Verhalten ein.

In Abbildung 2.7 ist die Funktion „Lenken“ (Überführung von Lenkwinkeländerungen in Trajektorienänderungen von Fahrzeugen) mit verschiedenen Ressourcen belegt worden. Beispiele für implementierte Lenkungen sind Knicklenkungen, Achsschenkellenkungen aber auch Gabellenkungen oder andere. Sie lassen sich, wie in der Abbildung dargestellt, in Komponenten zerteilen. Gleichzeitig ließe sich die Funktion „Lenken“ in generische Teilfunktionen wie z.B. Lenkwunschaufnahme, Lenkinformationsverarbeitung, Lenkinformationsübertragung usw. dekomponieren und einzeln mit technischen Ressourcen belegen.

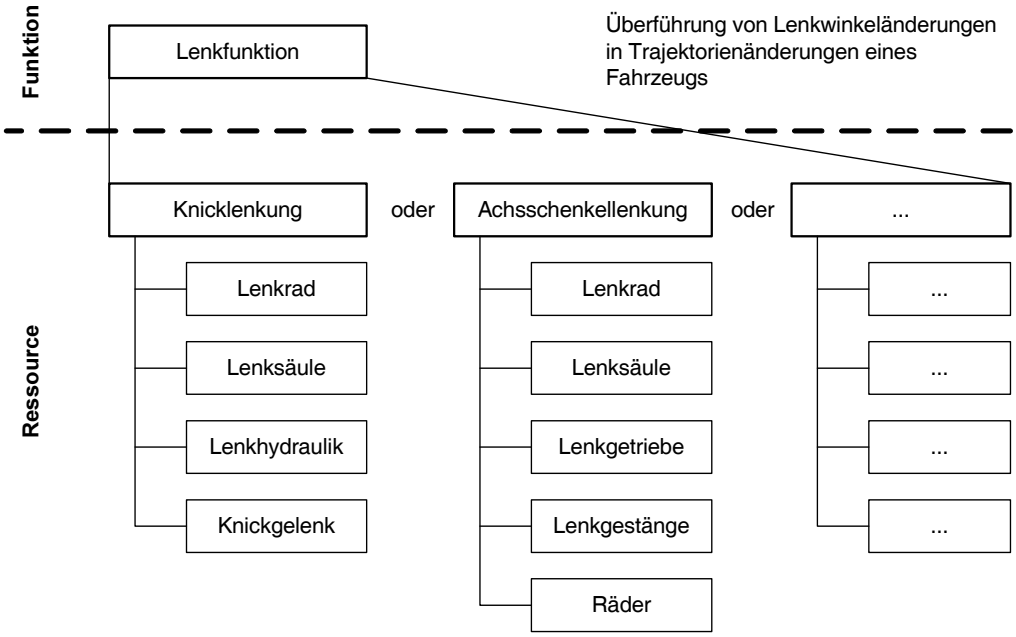


Abbildung 2.7: Trennung von Funktionen und Ressourcen

Die Allokation von Funktionen auf Ressourcen kann zusätzlich bei der generischen

Bezeichnung von technischen Systemen unterstützen. In der Verfahrenstechnik existieren dazu beispielsweise bereits Ansätze zu einer genormten Bezeichnung technischer Systeme auf Basis der ausgeführten Funktion sowie deren zu Grunde liegenden Funktions- bzw. Zustandsmerkmale [Hir99]:

- Informationsumsatz – Gerät
- Stoffumsatz – Apparat
- Energieumsatz – Maschine

Das System „Fahrzeug“ beispielsweise überführt in seiner Hauptfunktion die Eingangsgröße (Energie) in die Ausgangsgröße (mechanische Arbeit – Bewegung) und realisiert die Funktion *Fahren*. Die Teilsysteme weisen dabei unterschiedliche Funktionen auf z.B. Energiespeicherung, Energiewandlung, Antriebsenergie erzeugen, Vortrieb erzeugen, Abgasemission usw. Bei Anwendung der verfahrenstechnischen Bezeichnungsstruktur würde das Fahrzeug aufgrund des erfolgenden Energieumsatzes als Maschine bezeichnet.

Die Sicherungstechnik (logische Ebene) als Teilsystem eines technischen Gesamtsystems Stellwerk überführt Eingabeinformationen (aktuelle Weichenlagen, Gleisabschnittsbelegung, Fahrstraßenauswahl des Fahrdienstleiters etc.) in sichere Ausgabeinformationen (Stellbefehle an Weichen, Signale etc.). Dadurch erfüllt sie die Funktion der *Fahrwegsicherung*. Dabei setzen Teilsysteme sensierte Informationen (z.B. Weichenlagen) in andere Informationen (z.B. die Anzeigen der korrekten Weichenlage über Meldungen, Status etc.) um. Aufgrund des reinen Informationsumsatzes stellt dieses Teilsystem demnach ein Gerät dar. Wird allerdings der ausführende (stellende) Teil des Stellwerks betrachet (Stellebene), der aus Informationen entsprechende Energien zum Stellen der Fahrwegelemente erzeugt, ist eine Einordnung in das vorgeschlagene Schema nicht eindeutig, sofern man von einer Information als z.B. gepulste Energie absieht. Hilfreich kann dabei die Darstellung der Systemstruktur sein, um die Zugehörigkeit einzelner Teilsysteme und den damit verbundenen Funktionen zu verdeutlichen.

Systemaxiome nach [Sch99]

Die dargestellten Systemeigenschaften werden von den vier Systemaxiomen [Sch99] zur Struktur, Dekomposition, Kausalität sowie zur Temporalität umschlossen. Basierend auf diesen Axiomen können die vier grundsätzlichen Eigenschaften eines Systems mit diesen Prinzipien in Verbindung gebracht werden.

Das **Strukturprinzip** bzw. die Struktur eines Systems beschreibt dessen Teile, die untereinander und mit ihrer Umwelt in wechselseitiger Beziehung stehen, und deren Aufbau. Die Werte der Größen, die die Teile des Systems beschreiben, können den Zustand des Systems kennzeichnen. Des Weiteren lässt sich die Menge von Teilen nach dem **Dekompositionsprinzip** (vgl. Abbildung 2.8) in Unterteile zerlegen, die ihrerseits in einer wechselseitigen Beziehung stehen. Im Detail betrachtet, weisen die Unterteile wiederum die Komplexität, d.h. sämtliche allgemeine Systemmerkmale eines Systems auf und kennzeichnen ebenfalls durch die konrekten Eigenschaften den Systemzustand.

Das **Kausalitätsprinzip** und das **Temporalitätsprinzip** (vgl. Abbildung 2.8) weisen auf die zwischen den Systemelementen bestehenden dynamischen Relationen hin, bei denen im Sinne eines kausalen bzw. temporalen Wirkzusammenhangs spätere Zustände von ihren vorangegangenen Zuständen abhängig sind und somit das Verhalten bzw. auf Systemebene die Funktion realisieren. Kausalität wird dabei als Logik von Abläufen verstanden, während die Temporalität die zeitliche Folge von Abläufen und Veränderungen beschreibt. Abläufe können beispielsweise nebenläufig oder sequentiell sowie kontinuierlich oder diskret bzw. deterministisch oder stochastisch ablaufen.

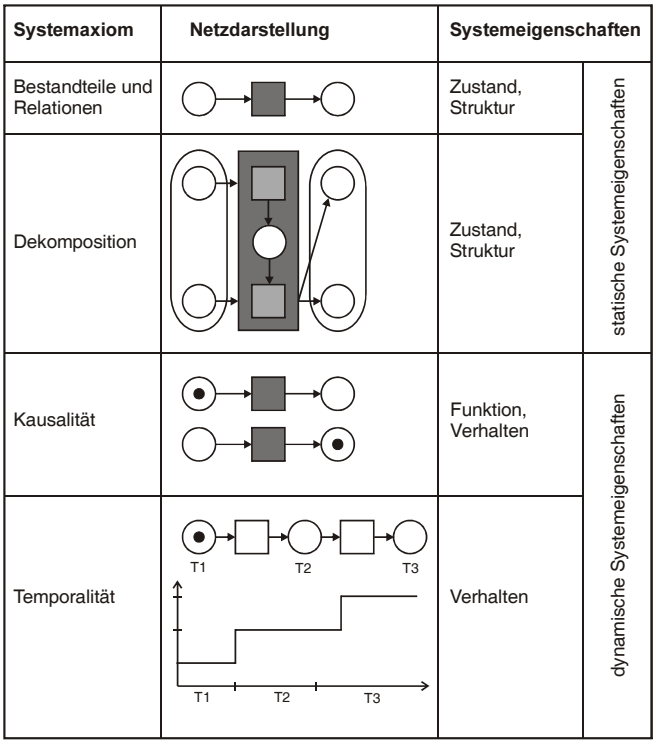


Abbildung 2.8: Systemaxiome und deren Netzdarstellung nach [Sch99]

Neben den unmittelbaren Eigenschaften eines Systems bzw. eines Teilsystems existieren Eigenschaften eines Systems (als Ganzes), die sich nur aus dem Zusammenwirken der einzelnen Eigenschaften der beteiligten Teilsysteme ergeben. Diese neuen Eigenschaften werden als emergente Eigenschaften bezeichnet. Emergenz[1] ist die Eigenschaft eines Systems, die sich erst durch das Zusammenwirken von Funktionen der einzelnen Subsysteme einstellt. Systemtheoretisch betrachtet steht der Begriff Emergenz im ingenieurwissenschaftlichen Kontext für das "Erscheinen" von Phänomenen bzw. neuen Merkmalen auf der Makroebene eines Systems, die erst durch die Kombination der Teilfunktionen bzw. Eigenschaften der Teilsysteme zustande kommen. Dadurch ergeben sich für bestimmte Systeme neue emergente Merkmale oder Eigenschaften, die sich auf das Systemverhalten auswirken können.

[1]Emergenz: "Das Ganze ist mehr als die Summe seiner Teile" (Aristoteles) [Rat98]

Sicherheit, als emergente Eigenschaft eines Systems, kann somit neben der direkten Implementierung mittels Sicherheitfunktionen indirekt durch das Zusammenwirken von Teilfunktionen entstehen, die nicht explizit eine Sicherheitsverantwortung tragen. Eine (sicherheitsgerichtete) Systemfunktion und insbesondere das dazu erforderliche Systemverhalten kann systemtheoretisch als Veränderung eines globalen Zustands bzw. der Zustandsgrößen auf Systemebene (als Ganzes) betrachtet werden.

Die sicherheitsgerichtete Funktion eines Systems kann als gezielte Überführung von Eingangsgrößen in umgewandelte sichere Ausgangsgrößen verstanden werden. Ihre Funktion ist die Entscheidung zwischen sicher und unsicher. Das Verhalten eines Systems zur Ausführung einer sicherheitsgerichteten Funktion beschreibt dabei die internen bzw. auch zum Teil externen Zustandsänderungen (und damit unter Umständen auch die Veränderungen der eigenen oder fremden Systemeigenschaften) innerhalb oder auch außerhalb der Systemgrenzen.

Abbildung 2.9 zeigt schematisch die Abgrenzung von Funktion, Verhalten, Zustand und Struktur eines Systems. Während das Gesamtsystem mit seinem, durch eine definierte Struktur von Teilfunktionen realisierten, Verhalten (ggf. auf mehrere Teilsysteme verteilt) ausschließlich die Funktion der Umwandlung von Eingangsgrößen zu Ausgangsgrößen verfolgt, kann das Verhalten der einzelnen Teilsysteme Auswirkungen auf den Zustand sowohl der Teilsysteme selbst als auch auf den Zustand des Gesamtsystems zeigen.

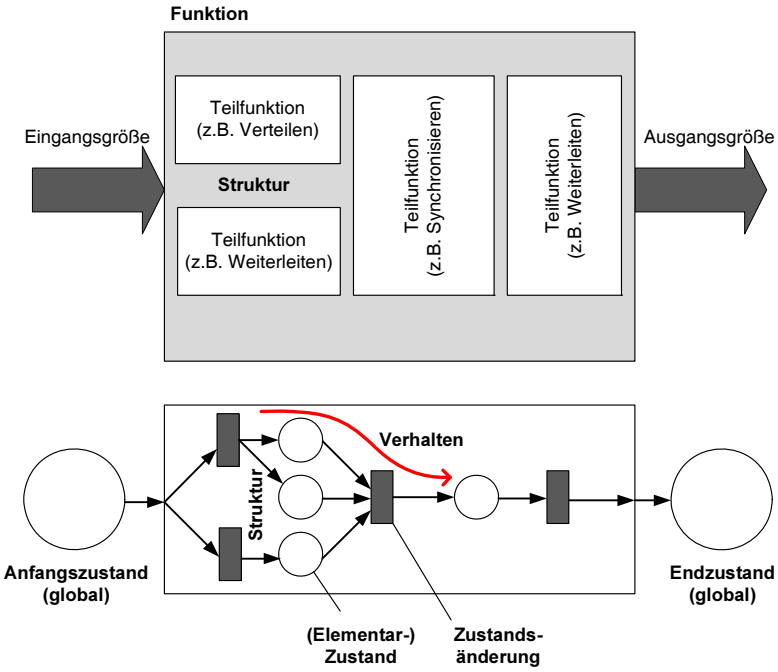


Abbildung 2.9: Dynamische Eigenschaften eines Systems

2.3 Begriffssysteme zur Darstellung komplexer Sachverhalte

"Unter einem Begriff wird eine Denkeinheit verstanden, die einem abstrakten Gegenstand zugeordnet ist und diesen im Denken vertritt." [Bro06]

Ein *Begriff* selbst wird dabei durch Worte oder Laute benannt, die beispielweise durch Symbole bezeichnet werden. Der Inhalt eines Begriffs wird dabei von dem Betrachter mit der Begriffsbenennung/-bezeichung assoziiert und erzeugt ein mentales Modell des Begriffs der zusätzlich den möglichen Umfang impliziert. Begriffe beinhalten somit mehr als die reine Benennung/Bezeichnung eines Gegenstands durch ein oder mehrere Worte oder Bilder.

Die in Unterabschnitt 2.2.2 gezeigten Ansätze zur genormten Bezeichnung technischer Systeme dienen einem besseren Verständnis der Sachverhalte aufgrund von Bezeichnungen und der klaren Abgrenzung von Begriffen (hier: Systemen) zueinander. Eine grundsätzliche Zuordnung von Funktionen zu technologischen Ressourcen lässt sich aber wie gezeigt nicht immer konsistent einhalten. Eine relationelle Einordnung verschiedener Begriffe sowie deren Bezeichnungen in einem ggf. formal modellierten Begriffssystem kann diese Absicht unterstützen und ermöglicht die vereinfachte konsolidierte Darstellung komplexer Sachverhalte auf begrifflich inhaltlicher Ebene.

Insbesondere im Zusammenhang mit sicherheitsverantwortlichen Systemen ist die Darstellung der Sachverhalte (Strukturen, Verhalten, Funktionen bzw. Funktionalität sowie der sicheren und/oder gefährlichen Zustände) in einer eindeutigen Form essentiell. Diese Eindeutigkeit dient einer korrekten und unverfälschten Kommunikation zwischen den verschiedenen Beteiligten wie sie z.B. bei der Anforderungsspezifikation während des Entwicklungsprozesses, einer Systemzulassung/-abnahme und insbesondere bei der Anwendung des Systems durch den Kunden oder bei einem ggf. notwendigen oder gewünschten Re-Design erforderlich ist. Beispiele für mögliche Ursachen, die zu Problemen während der Kommunikation zwischen beteiligten Personen führen, können wie folgt aufgeführt werden:

- Unterschiedliche fachliche Wissensstände der Kommunikationspartner (z.B. Anfänger vs. Routinier)
- Unterschiedliche domänenspezifische Interpretationen (z.B. Luftfahrt vs. Schienenverkehr)
- Unterschiedliche sprachliche Wissensstände der Kommunikationspartner (z.B. verschiedene Muttersprachen)
- Verwechselungen von Bedeutungen bei möglichen Mehrdeutigkeiten der Bezeichnungen

Ein konsistentes Begriffssystem zur Beschreibung von Sachverhalten kann helfen, diese Probleme zu vermeiden oder zu entschärfen. Um die komplexen Sachverhalte bzgl.

der Verkehrssicherheit in dieser Arbeit zu kommunizieren, werden aus diesem Grund zunächst begriffliche Analysen durchgeführt und vereinfachte Begriffssysteme erstellt und dadurch das Ziel, unterschiedlichen Kommunikationspartnern aus unterschiedlichen Disziplinen und Domänen einen einheitlichen Zugang zu der Materie zu ermöglichen, verfolgt.

Als Basis ist zunächst ein umfangreiches Verständnis der Begriffe der Terminologielehre notwendig. In den folgenden Abschnitten werden diese Aspekte näher beleuchtet und ein Zusammenhang zur Systemtheorie geschaffen.

2.3.1 Terminologische / Linguistische Grundlagen

Einen genaueren Einblick in die Domäne der Sprachwissenschaften liefern zunächst die Normen zur Terminologie DIN 2342 [Deu04] und DIN 2330 [Deu93]. Eine Terminologie beschreibt demnach das einfachste Konstrukt zur Darstellung von Begriffen und deren Benennungen. Eine referenzielle Strukturierung zwischen einzelnen Begriffen oder Benennungen findet in der reinen Terminologie jedoch nicht statt. Für das reine Verständnis eines Begriffsmodells ist dies jedoch von größerer Bedeutung, da erst der konkrete Zusammenhang einzelner Informationen zu Wissen verarbeitet werden kann und dadurch ein emergentes Verständnis entsteht. Dies trifft insbesondere auf die Vernetzung von Begriffen zu.

Aus diesem Grund werden in diesem Abschnitt zunächst die verwendeten Gesichtspunkte für eine begriffsorientierte Modellierung erklärt und anschließend mögliche Beziehungen zwischen den Teilbegriffen dargestellt.

Die verwendeten Begriffsgesichtspunkte umfassen die Begriffsbezeichnung, den Begriffsinhalt, den Begriffsumfang sowie Begriffsbeziehungen, die in einem Begriffssystem zusammenhängend gebildet, festgelegt und geordnet werden [Sch02b]. Diese Gesichtspunkte sind nachfolgend zusammenfassend aufgeführt:

Begriffsbezeichnung: Repräsentation eines Begriffs mit sprachlichen oder anderen Mitteln. Begriffe werden sprachlich vertreten durch verschiedene Bezeichnungen. Die hauptsächliche Bezeichnungsart ist die Benennung.

Begriffsinhalt: Gesamtheit der Eigenschaften und Merkmale eines Begriffs den Begriff inhaltlich zu beschreiben. Dabei charakterisieren die Merkmale die Eigenschaften der Teilbegriffe.

Begriffsumfang: Gesamtheit aller Unterbegriffe, die unter einen Begriff fallen. Diese Unterbegriffe weisen die Eigenschaften auf, die den Begriffsinhalt in Form einer identischen Merkmalmenge ausmachen und den Begriffsumfang bestimmen.

Begriffsbeziehung: Beziehung zwischen Begriffen, die aufgrund von Eigenschaften und/oder Merkmalen besteht oder festgelegt wird. Begriffsbeziehungen sind die Grundlage zur Ordnung von Begriffsmengen und zum Aufbau von Begriffssystemen.

Begriffssystem: Geordnete Menge von Begriffen, die aufgrund ihrer Begriffsbeziehungen verbunden sind.

Die Modellierung einer Begriffsstruktur, d. h. von Begriffen/Teil- und Unterbegriffen und ihren Beziehungen, kann ausgezeichnet mit Klassendiagrammen der UML-Notation dargestellt werden (siehe Unterabschnitt 2.1.1), da, wie bereits in Unterabschnitt 2.2.2 erwähnt, eine gewisse Ähnlichkeit zwischen der Begriffssystemwelt und der Objektorientierung, insbesondere der Hierarchisierung, existiert.

Die Begriffe selbst werden dabei als Klasse (Menge von Objekten mit identischen oder ähnlichen Eigenschaften) definiert und namentlich bezeichnet. Sie werden sowohl in ihren statischen Eigenschaften und Beziehungen durch typische Merkmale, die ein Element einer Klasse genauer beschreiben (Attribute), spezifiziert und können in ihren dynamischen Verhaltensweisen (Operationen bzw. Methoden) zusätzlich beschrieben werden. Auf eine Modellierung der dynamischen Eigenschaften über Operationen bzw. Methoden wird aus Gründen der Übersichtlichkeit hier verzichtet. Eine Modellierung der dynamischen Eigenschaften wird zu einem späteren Zeitpunkt durch geeignete Beschreibungsmittel weiter vertieft, um eine anschauliche Darstellung zu ermöglichen.

Abbildung 2.10 zeigt die Charakteristik und die terminologischen Beziehungen aus der DIN 2342 zwischen Begriffen in einem vereinfachten Klassendiagramm, welches hier ein metaisiertes Begriffssystemmodell darstellt. Eine ähnliche Darstellung ist auch in [SS07] und [SS08] vorgeschlagen. Ausgehend von Begiff *A*, der sowohl für die Teilbegriffe *A-A* und *A-B* den Verbandsbegriff, als auch den Oberbegriff für die Unterbegriffe *A1* und *A2* darstellt, existieren weitere Begriffe, die in einer bidirektionalen (Begriffs-)Beziehung stehen (hier zu Begriff *B*). Begriffe auf einer gleichen hierarchischen Ebene gelten als nebengeordnete Begriffe und stellen in ihrer Gesamtheit den Begriffsumfang (Extension) dar, während die Gesamtheit der charakterisierenden Teilbegriffe als Begriffsinhalt (Intension) verstanden wird. Eine Bezeichnung ist in der Semiotik ein Code aus Zeichen und Symbolen, der auf einen Gegenstand oder Sachverhalt (bzw. den Begriff davon) verweist. So besitzt jeder Begriff eine oder mehrere Bezeichnungen, die entweder durch natürlichsprachliche Mittel (Wörter) zu einer Benennung oder in Form von Symbolen oder Formeln ausgedrückt werden (vgl. Abbildung 2.11. Zwischen den Bezeichnungen existieren Bezeichnungsbeziehungen.

Im Folgenden werden verschiedene bekannte Begriffssystemausprägungen kurz vorgestellt und deren Abgrenzung bzw. der erweiterte Umfang erläutert.

2.3.2 Terminologien

Als Terminologie wird nach [Deu92] der Gesamtbestand der Begriffe und ihrer Bezeichnungen in einem Fachgebiet verstanden. Als synonyme Benennung kann auch Fachwortschatz verwendet werden. Eine Terminologie kann ein-, zwei-, oder mehrsprachig sein. Terminologien werden üblicherweise bei der Erstellung von Wörterbüchern oder Glossaren verwendet und können somit ein nutzbares Vokabular für ein Fachgebiet zur Verfügung stellen.

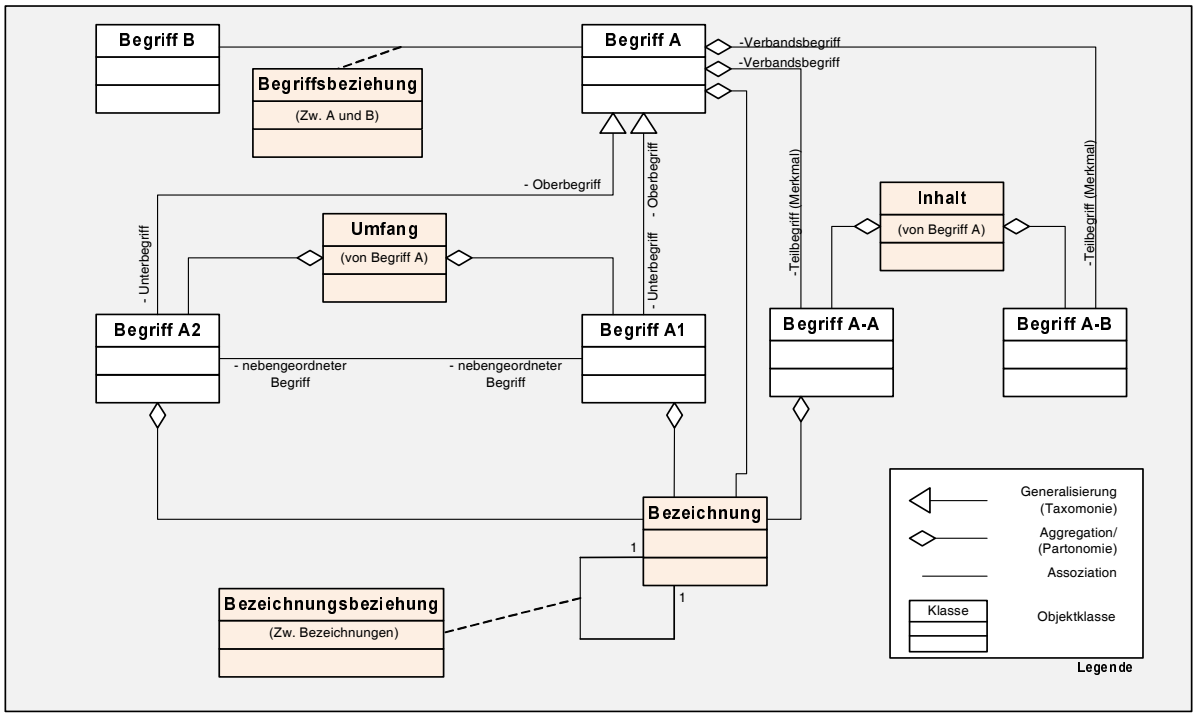


Abbildung 2.10: Begriffssystematik dargestellt als vereinfachtes Klassendiagramm

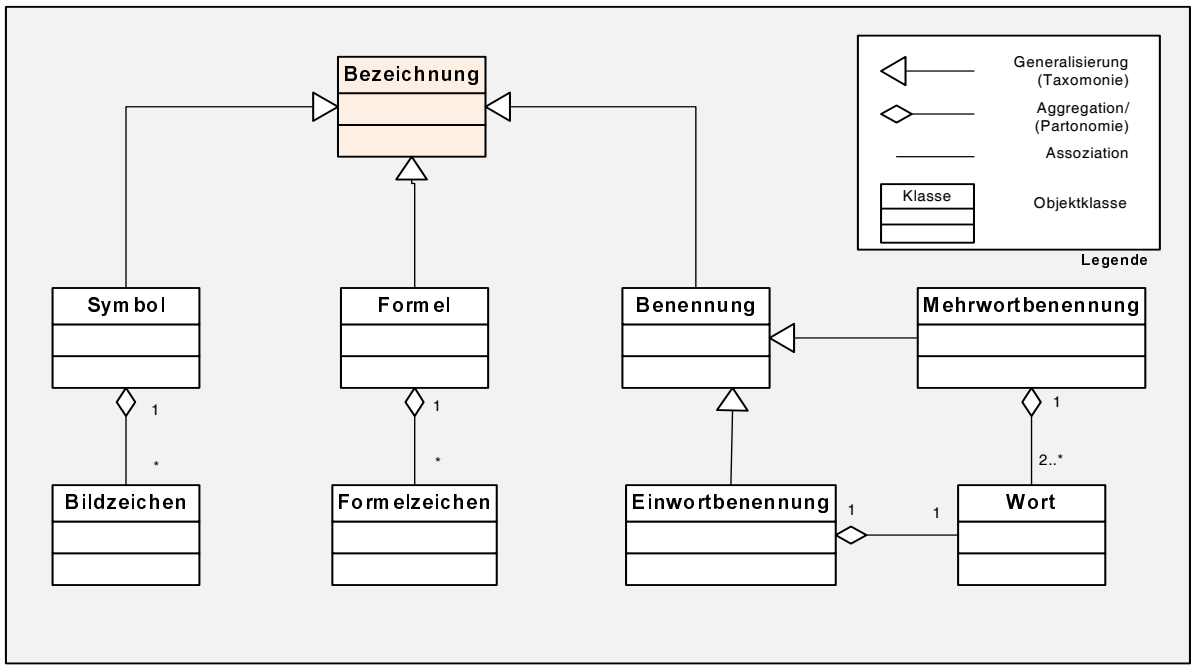


Abbildung 2.11: Unterscheidung von Bezeichnungen als vereinfachtes Klassendiagramm

Terminologien berücksichtigen weder Strukturen wie beispielsweise eine Unterscheidung von Begriffsinhalt oder -umfang auf der Basis von Unter- und Teilbegriffen noch Beziehungen zu anderen Begriffen. Terminologien werden in der Regel alphabetisch dokumentiert.

2.3.3 Nomenklatur

Eine Nomenklatur beschreibt eine systematisch strukturierte Terminologie, der ein methodisch stringentes Benennungsprinzip zugrunde liegt [Deu92]. Dabei wird das in der Terminologie verfügbare Vokabular durch eine verbindliche Sammlung von Benennungen kontrolliert und eingegrenzt. Eine inhalts- oder unfangsorientierte Struktur sowie dokumentierte Beziehungen zu anderen Begriffen sind jedoch auch bei Nomenklaturen nicht vorzufinden. Eine andere Bennenung für eine Nomenklatur ist das Namensverzeichnis.

2.3.4 Taxonomien

Im Gegensatz zu einer Terminologie bzw. Nomenklatur, die auf eine strukturierte Darstellung der Begriffsbenennungen abzielt, stellt eine Taxonomie einfache, hierarchische Begriffsrelationen zur Abstraktion her. Eine Taxonomie beinhaltet somit ein einfaches Begriffssystem mit einfachen Relationen in Form von Generalisierungs- und Spezialisierungsbeziehungen. Die bekannteste Taxonomie reicht bis in das Jahr 1740 zurück und wurde durch Linné für die Einteilung von Lebewesen verwendet [Lar68]. Bezugnehmend auf Abbildung 2.10 beschränkt sich eine Taxonomie auf die systematische Darstellung der Begriffe A, A1 und A2. Mögliche Beziehung zu dem Begriff B, sowie der Begriff B selbst werden in einer Taxonomie nicht berücksichtigt.

2.3.5 Ontologien

Eine Erweiterung der Taxonomien stellt die Ontologie dar, die neben der Berücksichtigung von hierarchischen Relationen einen besonderen Fokus auf die Modellierung der nicht-hierarchischen Relationen zwischen unterschiedlichen Begriffen gelegt hat. Zurückzuführen sind Ontologien aus philosophischer Sicht bis auf Aristoteles, der bereits in seiner Kategorienlehre [Rat98] zehn Kategorien unterscheidet: Substanz, Quantität, Qualität, Relation, Wo, Wann, Lage, Haben, Tun und Leiden, die zur Klärung der philosophischen Grundfrage: “Was ist das Wesen selbst?” dienen.

In der Informatik allerdings wird eine Ontologie primär zur Darstellung von Wissen und dem damit verbundenen Wissensmanagement verwendet [SS04]. Dabei hat sich insbesondere die Domäne der künstlichen Intelligenz auf die Darstellung von abstrakten und vereinfachten Sichten auf die Welt befasst und versucht, diese mathematisch in Form von geschlossenen oder offenen Systemmodellen zu definieren (siehe Kapitel 2).

Das semantische Netzwerk (Semantic Web)[BLHL01], als Erweiterung des World Wide Web verstanden, verwendet Sammlungen von Begriffen (allerding meistens nur deren

Benennungen) zusammen mit deren Relationen und stellt diese als ontologischen Zusammenhang dar mit dem Ziel, vernetzte Informationen potenziellen Nutzern intuitiv zugänglich zu gestalten um Wissen zu generieren.

Aus den unterschiedlichen Anwendungsdomänen der Ontologie und deren Interpretation wird deutlich, dass die Analyse und Definition der Relationen zwischen den Begriffen ein wichtiges Kriterium für die Begriffssystematik darstellt. In den folgenden Abschnitten werden aus diesem Grund die grundlegenden Relationen zwischen Objekten bzw. Begriffen erläutert.

2.3.6 Relationen zwischen Begriffen

Wie bereits in Unterabschnitt 2.3.1 beschrieben, stehen Begriffe in Beziehungen zu anderen Begriffen, um sich und somit den eigenen Inhalt und Umfang zu definieren. Die Gesamtheit der Begriffsrelationen zwischen den Begriffen strukturiert das Begriffssystem. Die Begriffsrelationen enthalten zudem den eigentlichen semantischen Inhalt eines Begriffssystems.

Unter dem Begriff der *Relation* ist grundsätzlich eine Beziehung zwischen mindestens zwei Elementen einer Menge zu verstehen. Oftmals werden *Beziehung* oder *Begriffsbeziehung* im Bereich der Begriffssysteme synonym zur Benennung Relation verwendet.

Relationen selbst sind nach [Deu93] und [Deu92] abstrakte Gegenstände bzw. Eigenschaften, die Beziehungen zu anderen Objekten (Begriffen) herstellen und für die Ordnung des jeweilig betrachteten Weltausschnittes von großer Bedeutung sind. Die Festlegung von Beziehungen zwischen Gegenständen oder Begriffen setzt deren Vergleichbarkeit voraus.

Umfang und Art der Relationen machen die wesentlichen Unterschiede zwischen den verschiedenen Arten von Begriffssystemen aus. In den meisten Systemen sind die möglichen Relationen sehr beschränkt (vgl. Taxonomien Unterabschnitt 2.3.4). Für die Terminologiearbeit wird lediglich in hierarchische und nicht-hierarchische Relationen unterschieden, welche nicht weiter differenziert werden. Ein einfacher Thesaurus nach DIN 1463 [Deu87], [Wer85] verwendet beispielsweise nur Bezeichnungs-/Äquivalenz-, Hierarchische- und Assoziationsrelationen. In einer Enzyklopädie gibt es zudem, abgesehen von den vielfältigen in natürlicher Sprache dargelegten inhaltlichen Beziehungen, nur Relationen in Form von direkten assoziativen Verweisen auf andere inhaltlich oder sprachlich verwandte Begriffe.

Die Eigenschaften dieser Relationen können vielfältiger Art sein. Als generelle Unterteilung eignet sich eine Klassifikation nach einem Schichtenansatz [Hän08]. Hierbei kann nach mathematischen und begrifflich/semiotischen (genauer: taxonomischen / syntaktischen, semantischen und pragmatischen) Eigenschaften differenziert werden. [Hän08] unterscheidet primär in Bezeichnungs- und Begriffsrelationen und setzt diese mit mathematischen Relationen in Verbindung.

Mathematische Grundrelationen

Eine binäre Relation kann nach [BSMM95] folgende neun grundlegende Eigenschaften haben:

Reflexivität: Eine binäre mathematische Relation R über einer Menge A wird als *reflexiv* bezeichnet, wenn jedes Element bezüglich R mit sich selbst in Relation steht, wenn also gilt:

$$\forall a \in A : (aRa)$$

Irreflexivität: Eine binäre mathematische Relation R über einer Menge A wird als *irreflexiv* bezeichnet, wenn *kein* Element zu sich selbst bezüglich R in Relation steht, wenn also gilt:

$$\forall a \in A : \neg(aRa)$$

Symmetrie: Eine binäre mathematische Relation R über einer Menge A wird als *symmetrisch* bezeichnet, wenn gilt:

$$\forall a, b \in A : (aRb) \Rightarrow (bRa)$$

Steht ein Element a mit einem Element b bezüglich R in Relation, so muss bei einer symmetrischen Relation notwendigerweise auch das Element b mit dem Element a bezüglich R in Relation. "*Gut* ist das Gegenteil von *Schlecht*, daher ist *Schlecht* auch das Gegenteil von *Gut*"

Antisymmetrie: Eine binäre mathematische Relation R über einer Menge A wird als *antisymmetrisch* bezeichnet, wenn gilt:

$$\forall a, b \in A : (aRb \wedge bRa) \Rightarrow (a = b)$$

Für kein Paar *verschiedener* Elemente a und b steht sowohl a mit b bezüglich R in Relation als auch b mit a.

Transitivität: Eine binäre Relation R über einer Menge A wird als *transitiv* bezeichnet, wenn gilt:

$$\forall a, b, c \in A : (aRb \wedge bRc) \Rightarrow aRc$$

Die Elemente a, b und c bilden bezüglich der Relation R eine Art „Dreiecksbeziehung". "Wenn eine Relation zwischen A und B existiert und B in einer Relation zu C steht, dann stehen A und C ebenfalls in Relation"

Linearität: Eine binäre Relation R über einer Menge A wird als *linear* bezeichnet, wenn von zwei Elementen a und b immer mindestens eines mit dem anderen bezüglich R in Relation steht, wenn also gilt:

$$\forall a, b \in A : (aRb \vee bRa)$$

Inverse Relation: Eine binäre Relation R über den Mengen A und B wird als *inverse Relation* zu einer Relation R' über den Mengen B und A bezeichnet, wenn gilt:

$$\forall a \in A, b \in B : (aRb) \Leftrightarrow (bR'a)$$

Die Relation R stellt also die Umkehrung oder das Gegenteil zur Relation R' dar. "*Gut* ist das Gegenteil von *Schlecht*"

Funktion: Eine binäre Relation R über den Mengen A und B wird als *funktional* oder *Funktion* bezeichnet, wenn jeder Wert des Definitionsbereichs (englisch: Domain) mit genau einem Element im Wertebereich (englisch: Range) in Relation steht, wenn also gilt:

$$\forall a \in A : \exists b \in B : aRb$$

und

$$\forall a \in A\ b, c \in B : (aRb \wedge aRc) \Rightarrow (b = c)$$

Synonym mit der Bezeichnung *Funktion* ist die Bezeichnung *Abbildung*.

Ordnung: Eine binäre Relation R in einer Menge A wird als *Ordnungsrelation* bezeichnet, wenn R reflexiv, antisymmetrisch und transitiv ist. Ist R zusätzlich linear, so heißt R *vollständige Ordnung(-srelation)* oder *Kette*.

$$\forall a \in A : (aRa)$$

und

$$\forall a, b \in A : (aRb \wedge bRa) \Rightarrow (a = b)$$

und

$$\forall a, b, c \in A : (aRb \wedge bRc) \Rightarrow aRc$$

für die vollständige Ordnung gilt zusätzlich

$$\forall a, b \in A : (aRb \vee bRa)$$

Begriffliche/semiotische Relationen

Begriffsrelationen setzen Begriffe zueinander in Relation. Die mathematischen Grundrelationen können auf die Begriffsrelationen angewendet werden, um diese zu charakterisieren. Die Zuordnung der mathematischen Relationstypen auf die Begriffsrelationen gewinnt stark an Bedeutung sobald die Relationen zwischen Begriffen formalisiert werden müssen. Diese Formalisierung kann für die elektronische Informationsumsetzung z.B. für das semantische Web [Bir06] bzw. [BP06] oder in anderen elektronischen Anwendungen erforderlich sein, um die Bedeutung und Richtung einer Relation z.B. bei nicht bestehender Reflexivität nicht zu verfälschen. Die Unkenntnis einer z.B. nicht vorhandenen Reflexivität kann zu fehlerhaften Interpretationen und damit zu fehlerhaft dargestelltem Wissen führen. Begriffsrelationen sind den mathematischen Relationen übergeordnet und repräsentieren sowohl die inhaltlichen Verbindungen zwischen Begriffen als auch die Beziehungen zwischen Begriffen auf Bezeichnungsebene.

Ein Auszug möglicher Begriffsrelationen in Verbindung mit der Zuordnung der mathematischen Relationen wird im Folgenden aufgezeigt und anhand von Beispielen kurz erläutert (Tabelle 2.2).

Die gezeigten Relationen vernetzen unterschiedliche Begriffe miteinander auf unterschiedlichen semiotischen Ebenen. Die Grundbegriffe der Semiotik: Sigmatik, Syntaktik, Semantik und Pragmatik dienen dabei als Basis zur Unterscheidung. Die Sigmatik in Verbindung mit der Syntax, die den Begriff erweckt und über seine Systemgrenzen hinweg mittels Bezeichnungen repräsentiert, steht dabei für den konkreten Gegenstand auf den sich der Begriff bezieht [Nöt99]. Die Semantik stellt die inhaltliche Bedeutung und den Umfang des Begriffs dar, während die Pragmatik dessen Interpretation bzw. auch die Nutzung ermöglicht.

In Tabelle 2.3 werden die bereits in Tabelle 2.2 dargestellten Beziehungen zum einen mit der Semiotik und zum anderen mit den in Unterabschnitt 2.3.6 beschriebenen mathematischen Relationen verknüpft.

Die sigmatisch/syntaktischen Eigenschaften beschreiben dort die rein formale Verknüpfung der sprachlichen Zeichen – auf Begriffssystemebene die sprachliche „Systemgrenze“ des einzelnen Begriffs – und werden durch s.g. Bezeichnungsrelationen repräsentiert. Die semantischen und pragmatischen Eigenschaften der Begriffrelationen zielen auf inhaltliche Interpretationen und Charakteristiken der Begriffe ab.

Bei einer strukturbasierten Unterscheidung der inhaltlichen Relationen in hierarchische und nicht-hierarchische Relationen können die hierarchischen Relationen als semantische Eigenschaften interpretiert werden. Die nicht-hierarchischen Relationen gehen über den reinen Bedeutungs- bzw. Sinnbezug hinaus und nehmen eine pragmatische Rolle ein, die z.B. den Verwendungskontext bzw. die Interpretation der Nutzung beschreibt.

Desweiteren beinhaltet die Tabelle 2.3 aus Gründen der Vollständigkeit die zusätzlichen Bezeichnungsrelationen *Monosemie*, *Polysemie*, *Homonymie*, *Homographie* und *Homophonie*, die jedoch hier eher eine untergeordnete Rolle spielen und daher nicht weiter betrachtet werden. Eine detaillierte Betrachtung dieser Bezeichnungsrelationen ist in [Hän08] durchgeführt worden.

Bezugnehmend auf Abbildung 2.10 kann das dort gezeigte Klassendiagramm zur metaisierten Darstellung der Begriffe der Terminologielehre um die semiotische Klassifizierung der Relationen aus Tabelle 2.3 erweitert werden. Dazu werden zwei unterschiedliche Begriffe sowohl auf Bezeichnungsebene als auch auf inhaltlicher Ebene in Relation gesetzt. Zusätzlich können bestimmte Systemstrukturmerkmale, wie z.B. die Systemgrenze, aus Unterabschnitt 2.2.2 berücksichtigt werden. Das Ergebnis ist in Abbildung 2.12 dargestellt.

Der Begriff „A“ als Oberbegriff von den Unterbegriffen „A1“ und „A2“ (Umfang) mit den Merkmalen, die durch seine inhaltlichen Teilbegriffe „A-A2“ und „A-B“ repräsentiert werden (Inhalt), steht auf inhaltlicher Ebene im Gegensatz zu dem Begriff B. Die inhaltliche systemgrenzenübergreifende Relation zwischen den beiden Begriffen ist demnach eine oppositionelle pragmatische Relation, während die systeminterne Relation zwischen Begriff, Begriffsumfang und -inhalt eine semantische Relation darstellt. Auf Bezeichnungsebene drückt sich die Gegensätzlichkeit der Begriffe in Form einer Antonymie zwischen den Bezeichnungen „a“ und „b“ aus. Diese Relation wird als syntaktische

Tabelle 2.2: Beschreibung der wichtigsten begrifflichen Relationen

	Relationsbenennung	**Relationsdefinition**
Bezeichnungsrelationen	Synonymie	Ähnlichkeit der begrifflichen Bedeutung bei verschiedener Bezeichnung z.B. „Pkw“ - „Auto“
	Quasisynonymie	Ähnlichkeit der begrifflichen Bedeutung bei verschiedener Bezeichnung nur in einer Domäne z.B. „Keyboard“ = „Tastatur“ für PC „Keyboard“ ≠ „Tastatur“ für Musikintrumente
	Antonymie	gegensätzliche Bezeichnungen zur komplementären Abgrenzung auf Bezeichnungsebene z.B. „Sicherheit“ - „Gefahr“, „heiß“ - „kalt“
	Äquivalenz	sprachübergreifende Ähnlichkeit der begrifflichen Bedeutung auf Bezeichnungsebene z.B. „safety“ - „Sicherheit“
Begriffsrelationen	Abstraktionsrelation (Konkretisierung)	Generische Relation: Vererbung auf Begriffsebene z.B. Fahrzeug - Personenkraftwagen
	Meronymie (Partitive Relation)	Zugehörigkeitsrelation: Aggregation/Komposition Teil-Ganzes-Relation (Dekomposition) z.B. Fahrzeug - Motor, Weiche - Weichenantrieb
	Importanz	Priorisierungsbeziehung zwischen Begriffen z.B. Gesetz „vor“ Richtlinie
	Temporalität	zeitlicher Zusammenhang zwischen Begriffen z.B. Ende „nach“ Anfang
	Kausalität	kausaler Zusammenhang zwischen Begriffen z.B. Ursache-Wirkung: Unfall - Schaden
	Genetizität	Erzeugungsrelation, Ressource - Produkt z.B. Komponenten - System, Energie - Bewegung
	Intentionalität	Mittel-Ziel-Beziehung z.B. Redundanz - Verfügbarkeitserhöhung
	Assoziativität	Thematischer (pragmatischer)Zusammenhang z.B. Nutzungsrelation PKW - Fahrer
	Oppositionalität	inhaltlich gegensätzliche Relation z.B. Haltbegriff (Hp0) - Fahrtbegriff (Hp1)

Tabelle 2.3: Darstellung der unterschiedlichen Relationen nach [Hän08]

		Relation	Reflexivität	Irreflexivität	Symmetrie	Antisymmetrie	Transitivität	Linearität	Funktion	Ordnung
Bezeichnungsrelationen	sigmatisch/syntaktisch	Synonymie	X	-	X	-	X	-	-	-
		Quasisynonymie	-	X	X	-	-	-	-	-
		Antonymie	-	X	X	-	-	-	-	-
		Äquivalenz	-	X	X	-	X	X	-	-
		Monosemie				einstellig				
		Polysemie				einstellig				
		Homonymie				einstellig				
		Homographie	-	X	X	-	X	-	-	-
		Homophonie	-	X	X	-	X	-	-	-
Begriffsrelationen	semantisch	Abstraktion	-	X	-	X	X	X	-	-
		Konkretisierung	-	X	-	X	X	X	-	-
		Meronymie	X	-	-	X	X	X	-	-
		Importanz	-	X	-	X	X	-	-	-
	pragmatisch	Temporalität	-	X	-	X	X	-	-	-
		Kausalität	-	X	-	X	X	-	-	-
		Genetizität	-	-	-	-	X	-	-	-
		Intentionalität	-	X	-	X	X	-	-	-
		Assoziativität	-	-	-	-	-	-	-	-
		Oppositionalität	-	X	X	-	-	-	-	-

Relation verstanden. Die Bezeichnung eines Begriffs kann, ähnlich wie eine Hülle, als sichtbare Repräsentation der Schnittstelle des Begriffs auf der System- (Begriffs-)grenze verstanden werden. Besitzt ein Begriff mehrere Bezeichnungen, stehen diese ebenfalls in einer syntaktischen Relation (Synonymie) zueinander.

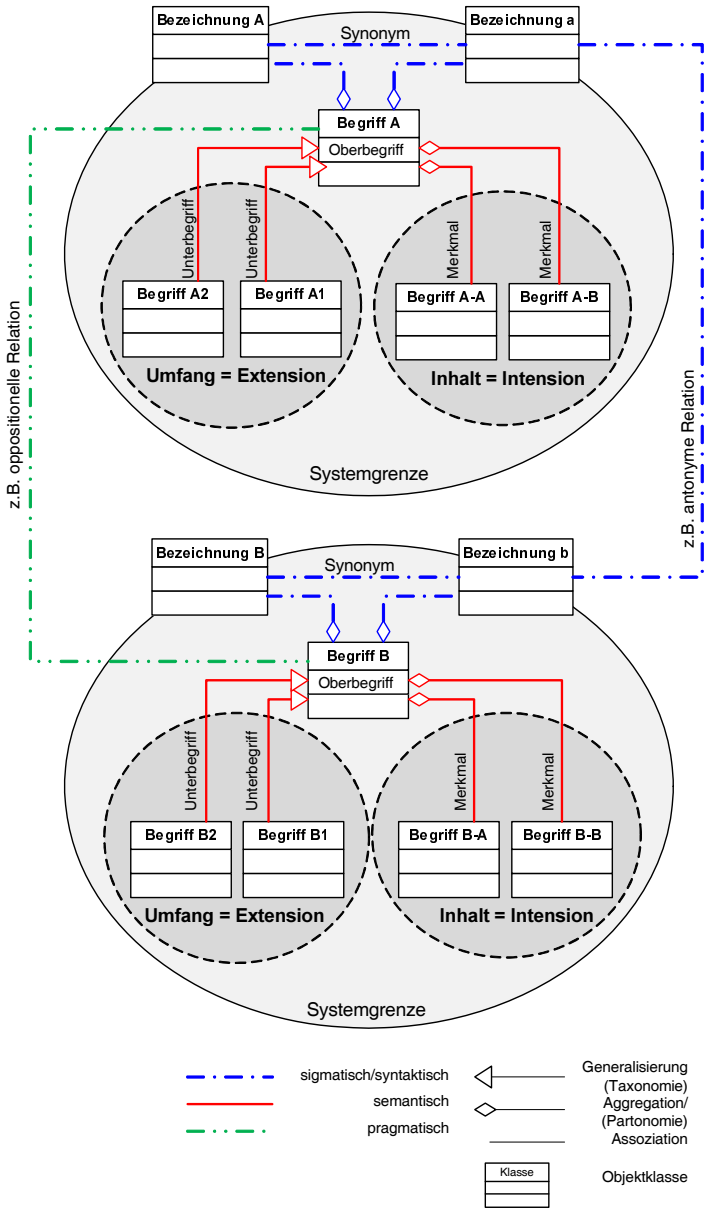


Abbildung 2.12: Semiotische Grundrelationen auf Begriffsebene in der Darstellung als Klassendiagramm

Wird diese Systematik abstrahiert, ergibt sich ein einfaches systemorientiertes Modell zur Darstellung von Relationen im Systembezug, das in Abbildung 2.13 schematisch dargestellt wird. Die Abbildung zeigt das systemorientierte Modell eines semiotischen

Begriffssystems. Die Systemaxiome aus Abbildung 2.8 lassen sich hierauf anwenden. Das Struktur- und Dekompositionsprinzip ermöglicht die strukturierte Unterteilung eines Begriffs in seine Unterbegriffe und Teilbegriffe (Merkmale), während das Kausalitäts- und Temporalitätsprinzip die pragmatischen Relationen und somit die Wechselwirkung von Begriffen zu anderen Begriffen betrifft.

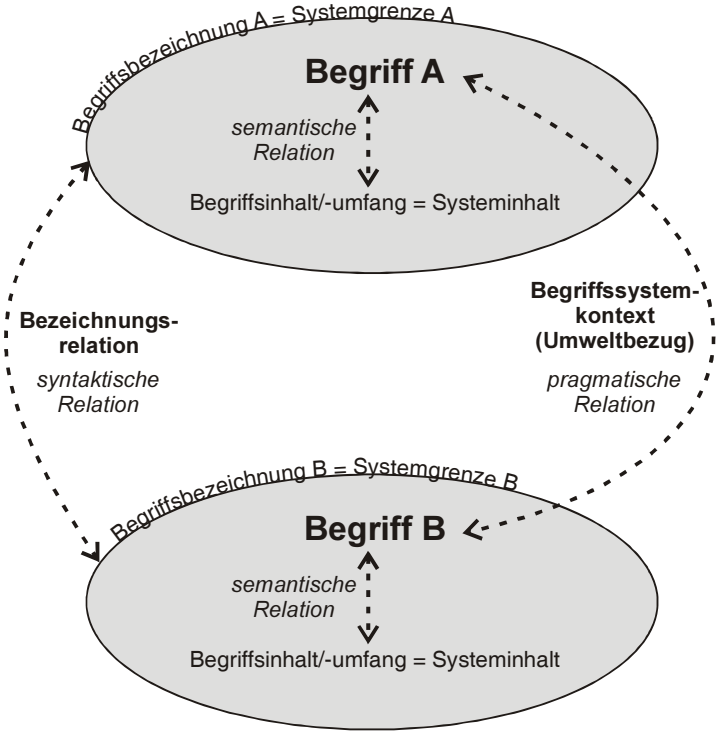


Abbildung 2.13: Semiotische Relationen auf Begriffsebene in systemtheoretischer Darstellung

Eine weiterführende Unterscheidung und detailliertere Analyse der verschiedenen Relationen ist in [Hän08] aufgeführt und würde in der Form den inhaltlichen Rahmen dieser Arbeit überschreiten, so dass hier nicht weiter darauf eingegangen wird. Insbesondere die Darstellung von dynamischen Prozessen über eine ontologische Modellierung auf Basis eines neues Ansatzes, der sowohl die Ontologie der Anwendungsdomäne als auch die Ontologie des Beschreibungsmittels über ein Prozessmodell verknüpft, wird dort ausführlich anhand von Beispielen beschrieben. Da die begriffliche Analyse hier ausschließlich dem besseren Verständnis der interessierenden Begriffswelt und zur Herstellung des systematischen Bezugs zur Erschließung des Begriffskontextes verwendet wird, werden Begriffsysteme hier vorwiegend zur Darstellung von statischen Eigenschaften konstruiert. Dynamische Zusammenhänge zwischen einzelnen oder mehreren Begriffen werden aufgrund der Übersichtlichkeit und des einfacheren Verständnisses darauf aufbauend mit Petrinetzen modelliert (vgl. Unterabschnitt 2.1.1).

2.4 Konstruktionsmethode zur Erstellung von ontologischen Begriffssystemen

Als Begriffssystem lassen sich, wie in Unterabschnitt 2.3.1 beschrieben, verschiedene Arten von Systemen aus klar voneinander abgrenzbaren Begriffen und ihren Bezeichnungen zusammenfassen, die durch verschiedene Relationen (vgl. Unterabschnitt 2.3.6) miteinander verbunden sind.

Die hier verwendete Konstruktionsmethode nach [Sch02b], die auch in [Hor05] angewendet wurde, beruht auf den Tätigkeiten Bestandsaufnahme, Bestandsuntersuchung und Bestandsfestlegung. Sie dient einer strukturierten Vorgehensweise zur Gestaltung eines Begriffssystems.

Bestandsaufnahme: Hierzu gehört die Sammlung relevanter Begriffe sowie deren Quellen. Die Bestandsaufnahme bildet die Grundlage für die aspektabhängige Ordnung einer interessierenden Begriffsmenge. Das Ergebnis dieses ersten Schritts ist eine umfassende, ungeordnete (oder teilgeordnete) Zusammenstellung der Begriffe.

Bestandsuntersuchung: Der zweite Schritt beinhaltet die Untersuchung von Beziehungen zwischen Begriffen sowie deren Abgrenzung. Als Mittel dieser Phase dient eine begriffsbezogene Textanalyse.

Bestandsfestlegung: Durch Partitionierung und andere Strukturierungen erfolgt die Abgrenzung von Begriffen, die Beibehaltung einiger bestehender sowie das Vereinbaren neuer Beziehungen zwischen Begriffen.

Erweiternd zu diesem Vorgehen wird hier die Bestandsuntersuchung und -festlegung durch eine systematische, terminologische Einordnung der Begriffe und deren Merkmale sowie Relationen durchgeführt. Über die Merkmalsanalyse wird der Begriffsinhalt begrifflich geklärt und führt somit zu einer terminologisch eindeutigen Begriffsdefinition in einem eindeutigen Begriffssystemkontext. Das Vorgehen und die systematische Unterteilung wird in Abbildung 2.14 skizziert und zeigt die unterschiedlichen Kontexte eines Begriffs und greift somit die in Unterabschnitt 2.3.1 aufgeführte terminologische Systematik auf.

Ein Begriff kann aus dreierlei Sicht kontextuell betrachtet werden. Während erstens der sprachliche Kontext sich auf die rein textuelle Beschreibung des Begriffs konzentriert und damit die Bezeichnung und Definition des Begriffs instanziiert, ermöglicht zweitens der nicht-sprachliche Kontext eine inhaltliche Konkretisierung des Begriffs über die Formulierung der charakterisierenden Merkmale und des geltenden Umfangs (vgl. Intension und Extension in Unterabschnitt 2.3.1). Systemtheoretisch betrachtet beschreibt der rein sprachliche Kontext somit die Betrachtung der umhüllenden „Systemgrenze“ (Repräsentation des Begriffs zur Umwelt), während die nichtsprachlichen inhaltlichen Kontexte die systeminternen Merkmale und Eigenschaften darstellen. Zusätzlich sind Relationen, die

das eigentliche System (hier: den jeweiligen Begriff) und damit die Systemgrenzen überschreiten notwendig, um ein vollständiges System- (hier: Begriffs-) verständnis zu erhalten. Diese Relationen werden durch den ausgewiesenen Begriffssystemkontext beschrieben, der die Bindung des fokussierten Begriffs zu anderen Begriffen (Verbindung zur angrenzenden Umwelt des fokussierten Begriffs) charakterisiert (vgl. Unterabschnitt 2.3.6. Die unterschiedlichen Ausprägungen der möglichen Relationen, sowohl begrifflich als auch mathematisch, sind bereits in Unterabschnitt 2.3.6 ausführlich betrachtet worden und werden hier konsequent umgesetzt.

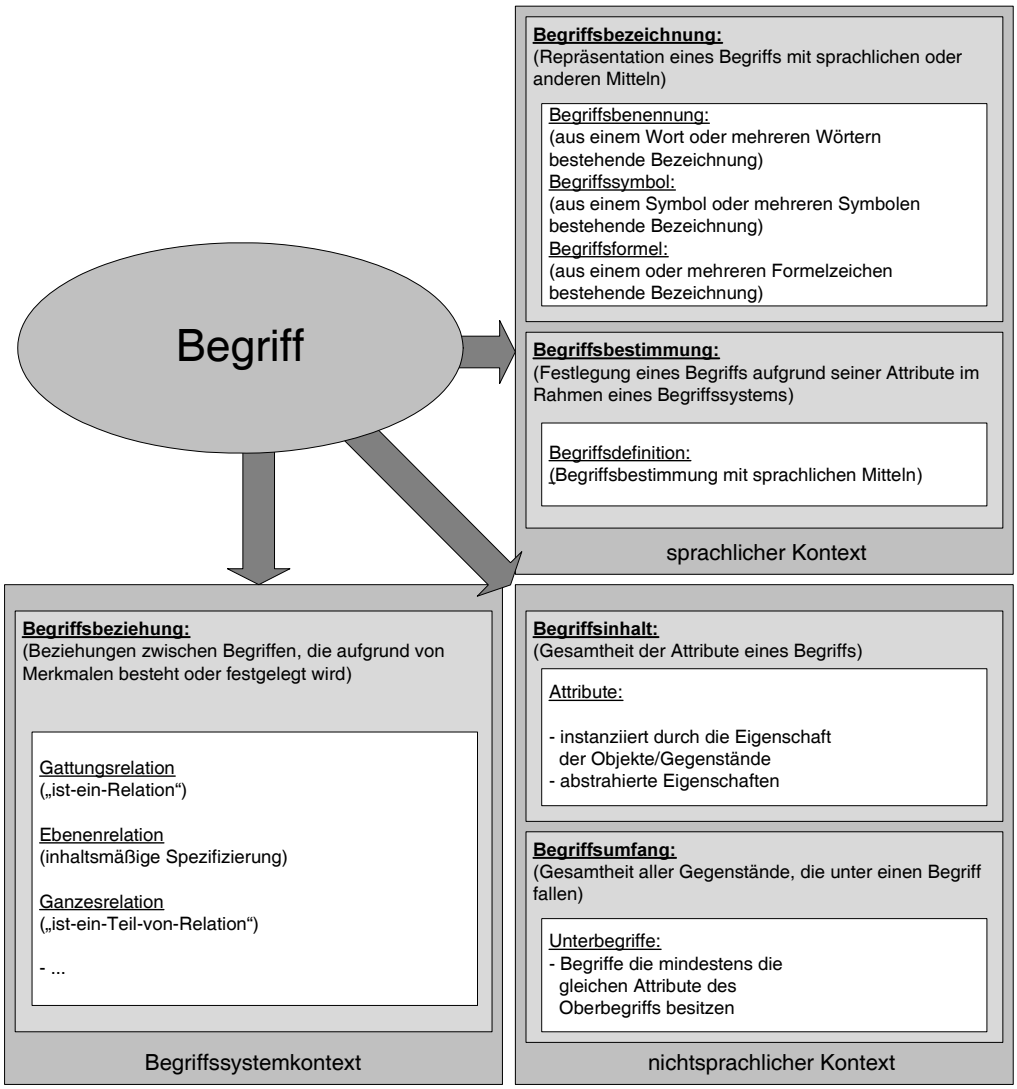


Abbildung 2.14: Sprachliche und nicht-sprachliche Kontexte von Begriffen

Das Vorgehen zur Konstruktion eines Begriffssystems vereint die Phasen der Bestandsuntersuchung und -festlegung und ermöglicht durch die Analyse der begrifflichen Relationen die Konsolidierung eines aussagekräftigen Begriffssystems.

3 Sicherheit als Systemeigenschaft

In diesem Kapitel werden die systemtheoretischen und begrifflichen Grundlagen aus Kapitel 2 auf den Begriff "Sicherheit" angewendet, um ein eindeutiges Verständnis von Sicherheit zu vermitteln. Analog zu Unterabschnitt 2.2.2 wird hier die Sicherheit als abstrakte ggf. emergente Eigenschaft eines Systems betrachtet. Das Kapitel enthält neben der erweiterten Begriffsanalyse Beispiele zur Formalisierung der Systemsicherheit und zeigt abschließend unterschiedliche Implementierungskonzepte und Maßnahmen zu dessen Realisierung. Begleitet wird das Kapitel mit der Betrachtung und Vorstellung verschiedener allgemeiner Sicherheitsmaße.

3.1 Begriffsanalyse des Begriffs Sicherheit

Die begriffliche Betrachtung der Sicherheit erscheint im ersten Ansatz ein triviales Vorhaben zu sein, da sich der Begriff allein durch die assoziative Beschreibung *Gefahrlosigkeit* (vgl. Kapitel 1) zu erklären scheint. Erst bei genauerer Betrachtung zeigt sich der zum Teil undurchsichtige und sehr weitreichende Inhalt und Umfang des Begriffs. Die Ermittlung des quantitativen Risikos und dessen Relation zur Sicherheit, der kausale Zusammenhang zu Unfällen und den damit verbundenen Schäden sowie unterschiedliche Methoden der Sicherheitsimplementierung durch Sicherungstechnik sind nur Beispiele für Fragestellungen, die nicht rein assoziativ beantwortet werden können bzw. bei einer intuitiven Herangehensweise ggf. zu widersprüchlichen Sachverhalten führen können.

In den folgenden Abschnitten wird der Begriff *Sicherheit* terminologisch analysiert und die erweiterte Konstruktionsmethode aus Abschnitt 2.4 unterstützend angewendet. Es wird dabei vorrangig auf die wichtigsten Begriffe eingegangen, um somit ein grundlegendes Verständnis für die Sicherheit sowie eine beispielhafte Anwendung der Methodik zur Begriffssystemkonstruktion zu vermitteln. Das Vorgehen der Analyse gliedert sich in Bestandsaufnahme, Bestandsanalyse und Bestandsfestlegung.

3.1.1 Bestandsaufnahme: Sicherheit

Bezugnehmend auf Abschnitt 2.4 wird in diesem Abschnitt eine Bestandsaufnahme bzgl. des Begriffs Sicherheit durchgeführt. Die Sammlung der relevanten Begriffe und deren thematischen Quellen kann unterschiedlich erfolgen. Das Ziel dieser Bestandsaufnahme ist die Zusammenstellung einer interessierenden Begriffsmenge, deren Zentrum durch den Kernbegriff *Sicherheit* definiert ist. Die Bestandsaufnahme erfolgt assoziativ durch Re-

cherchen, Fachgespräche sowie systematische Überlegungen. Eine assoziative Bestandsaufnahme kann zum einen rein sprachlich durch Volltextsuchen in Lexika, Wörterbüchern oder z.B. dem Internet erfolgen (z.B. Sicherheit - Fahrzeug*sicherheit*) und zum anderen systematisch-inhaltlich durch die Betrachtung von thematisch benachbarten Begriffen unter der Verwendung von existierenden Taxonomien oder Ontologien (z.B. Sicherheit - Gefahr, Schutzeinrichtungen etc.).

Für den Begriff *Sicherheit*, insbesondere mit der Bezeichnung: Sicherheit, ergeben sich folgende sprachliche und inhaltliche Assoziationen, die den ersten Umfang und Inhalt des Begriffs *Sicherheit* repräsentieren. Bei der Auswahl der Begriffe und der entsprechenden Definitionen wurden vorzugsweise Normen, Richtlinien und Fachliteratur verwendet. Eine Auswahl relevanter Begriffe und Definitionen zeigt nachfolgende Liste:

Sicherheit: Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.
Quelle: Wikipedia

Zustand, in dem das Risiko eines Personen- oder Sachschadens auf einen annehmbaren Wert begrenzt ist.
Quelle: EN ISO 9000

Das Nichtvorhandensein eines unzulässigen Schadensrisikos.
Quelle: DIN EN 50126 [Deu00]

Freiheit von nicht-akzeptablen Risiken.
Quelle: DIN EN 50128 [Deu01]

Freisein von nicht akzeptierbaren Risiken eines Schadens.
Quelle: DIN EN 50129 [Deu03b]

Abwesenheit von Gefahr. Wird durch die Erfüllung sicherheitsbezogener Korrektheits- und Zuverlässigkeitsanforderungen angestrebt bzw. erreicht.
Quelle: VDI 3542-4 [35400]

Sachlage, bei der das Risiko kleiner ist als das Grenzrisiko.
Quelle: VDI 4003-2 [VDI07b]

Wahrscheinlichkeit, mit der von einer Betrachtungseinheit während einer bestimmten Zeit keine Gefahr ausgeht. **Quelle:** Meyna [MP02]

Risiko: Die kalkulierte Prognose eines möglichen Schadens bzw. Verlustes im negativen Fall (Gefahr).
Quelle: Wikipedia

Eine Kombination der Wahrscheinlichkeit und des Schweregrades der möglichen Verletzung oder Gesundheitsschädigung in einer Gefährdungssituation.
Quelle: VDI 3542-3 [35400]

Wahrscheinlichkeitsaussage, die quantitativ die zu erwartende Häufigkeit H des Eintritts eines zum Schadens führenden Ereignisses und das bei Ereigniseintritt zu erwartende Schadensausmaß S zusammenfasst.
Quelle: VDI 3542-2 [35400]

Die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, sowie der Schweregrad eines Schadens.
Quelle: DIN EN 50126 [Deu00]

Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses.
Quelle: DIN EN 50129 [Deu03b]

Gefahr: Gefahr kann von der Nutzung eines technischen Systems ausgehen und bedeutet die - vielfach zeitlich begrenzte - Möglichkeit einer Schädigung von Mensch oder Sachgut.
Quelle: Kuhlmann [Kuh81]

Gefahr ist ein Zustand bzw. eine Anzahl von Bedingungen eines Systems, die zusammen mit anderen Bedingungen außerhalb des Systems unvermeidlich zu einem Schaden führen. **Quelle:** Rakowski [Rak02]

Sachlage, bei der das Risiko größer als das Grenzrisiko ist, wobei unter Grenzrisiko das größte noch vertretbare Risiko verstanden wird. Komplementär zur Sicherheit.
Quelle: VDI 3542-4 [35400]

Die mögliche Schadwirkung der Gefahrenquelle oder der Zustand einer Bedrohung durch eine Gefahrenquelle.
Quelle: ISO/IEC Guide 51 [ISO99]

Gefahr ist eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist.
Quelle: VDE 31000 /VDE1987/

Zustand, aus dem ein Unfall entstehen kann.
Quelle: VDI 4003-4 [VDI07b]

Eine physikalische Situation, die potentiell einen Schaden für den Menschen beinhaltet.
Quelle: DIN EN 50126 [Deu00]

Gefahrenquelle: Ein technisches System, von dem Gefahr ausgeht und sich ausbreiten kann auf Güter, die geschädigt werden können. Ist eine Gefahrenquelle örtlich bestimmbar, so definiert die ortsabhängige Gefährdung ein Gefahrenfeld, das bei Festlegung eines Maßes für die Gefährdung durch Linien gleicher Gefährdung beschrieben werden kann. Einer Gefahrenquelle werden mehrere Gefahrenfelder zugeordnet, wenn es mehrere Schadensarten gibt mit unterschiedlicher Gefahrenausbreitung.
Quelle: Kuhlmann [Kuh81]

Gefährdung: Eine Gefährdung stellt eine potentiell existente Gefahrenquelle (Schadensquelle) dar. Die negative Auswirkung einer Gefährdung kann Personen, Sachen, Sachverhalte, Umwelt oder Tiere treffen.
Quelle: Wikipedia

Gefährdung kann sich für Mensch und Sachgut ergeben, wenn ein technisches System genutzt wird und sich Mensch und Sachgut in seinem Wirkungsbereich befinden.
Quelle: Kuhlmann [Kuh81]

Eine Quelle einer möglichen Verletzung oder Gesundheitsschädigung.
Quelle: DIN EN 292-1

Ereignis, das einen Schaden hervorrufen kann.
Quelle: DIN EN ISO 14121 [Int07]

Verhalten, das zu einer Gefahr führen kann, wenn es nicht beherrscht wird.
Quelle: VDI 4003-4 [VDI07b]

Eine potentielle Schadensquelle.
Quelle: ISO/IEC Guide 51 [ISO99], DIN EN ISO 14121 [Int07], EN 61508-4 [Deu02]

Bedingung, die zu einem Unfall führen kann.
Quelle: DIN EN 50129 [Deu03b]

Schaden: Die konkrete schädigende Auswirkung der Gefahrenquelle, als Möglichkeit, oder wahrgeworden.
Quelle:ISO/IEC Guide 51 [ISO99]

Physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden von Gütern oder der Umwelt.
Quelle:EN 61508-4 [Deu02]

Sicherungstechnik: Technischen Vorrichtungen, die der Sicherheit dienen.
Quelle: Meyna [MP02], VDI 4004-1 [40086]

Sicherungsfunktion: Funktion, die von einem E/E/PE-sicherheitsbezogenen System, einem sicherheitsbezogenen System anderer Technologie oder externen Einrichtungen zur Risikominderung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC (Equipment under control) zu erreichen oder aufrechtzuerhalten.
Quelle: EN 61508-4 [Deu02]

Sicherheit/Gewissheit: Die subjektive Sicherheit bezüglich bestimmter, für gut gerechtfertigt gehaltener Überzeugungen, die sich z. B. auf natürliche oder moralische Sachverhalte beziehen können.
Quelle: Wikipedia

3.1.2 Bestandsuntersuchung: Sicherheit

Die Bestandsaufnahme aus Unterabschnitt 3.1.1 zeigt einen Ausschnitt einer Sammlung von Begriffen, die thematisch bzw. assoziativ mit dem Begriff Sicherheit in Relation stehen. Eine Vollständigkeit sämtlicher Assoziationen kann aufgrund der Komplexität und

des ausgedehnten Umfangs hier nicht erreicht werden. Die Begriffe der Bestandsaufnahme werden somit als interessierende Begriffsmenge festgelegt, die bei Bedarf jederzeit erweitert oder reduziert werden kann.

Neben der rein assoziativen Bestandsaufnahme kann das systematisch-strukturierte Vorgehen hilfreich sein, die Qualität des Inhalts und Umfangs der Begriffsmenge zu verbessern. Dabei kann auf die grundlegenden Eigenschaften und Merkmale des jeweiligen Begriffs zurückgegriffen werden und anhand dieser der Inhalt und der Umfang systematisch ermittelt werden. Dazu können unterstützend die vier Systemaxiome zur Struktur, Dekomposition, Kausalität und Temporalität aus Abbildung 2.8 angewendet werden, da die Sicherheit als Eigenschaft eines Systems betrachtet wird.

Im Rahmen der Bestandsuntersuchung werden die einzelnen Begriffe der interessierenden Menge voneinander abgegrenzt und die jeweiligen Inhalte und Umfänge (nicht-sprachlicher Kontext) analysiert. Die Bezeichnungen und Definitionen (der sprachliche Kontext) wurden bereits während der Bestandsaufnahme ausreichend betrachtet und werden an dieser Stelle nicht weiter vertieft.

Die Relationen zwischen den Begriffen (Begriffssystemkontext) werden im Anschluss an die Analyse der nicht-sprachlichen Kontexte durchgeführt. Dabei werden insbesondere die vier Systemeigenschaften (Zustand, Verhalten, Funktion und Struktur) herangezogen, um die einzelnen Begriffe in eine kausale, temporale oder partitive Relation setzen zu können.

Nachfolgend werden die nicht-sprachlichen und Begriffssystemkontexte der interessierenden Begriffsmenge beschrieben.

Analyse der nicht-sprachlichen Kontexte

Die nicht-sprachlichen Kontexte werden entsprechend der erweiterten Kontruktionsmethode aus Abschnitt 2.4 analysiert. während die sprachlichen Kontexte durch die Beschreibungen der Bestandsaufnahme und der dortigen Benennung ausreichend belegt wurden. Die nicht-sprachlichen Kontexte werden hier primär durch die Beschreibung der Unterbegriffe zur Bestimmung des Umfangs sowie der Teilbegriffe (Merkmale) zur Bestimmung des Inhalts aus den Definitionen der Bestandsaufnahme abgeleitet. Auf eine Erweiterung des sprachlichen Kontextes z.B. durch Mehrsprachigkeit oder Symbole wird an dieser Stelle verzichtet.

Die einzelnen Inhalte und Umfänge der jeweiligen Begriffe werden in den nachfolgenden Tabellen für jeden Begriff der interessierenden Begriffsmenge einzeln aufgeführt.

Analyse der begrifflichen Relationen

Werden die in der Bestandsaufnahme ermittelten sprachlichen Kontexte und die im vorangegangenen Unterabschnitt ermittelten nicht-sprachlichen Kontexte der Begriffe betrachtet, ergibt sich zwar schon der ein oder andere Bezug zwischen einzelnen Begriffen, lässt aber weitere Relationen offen, die in diesem Abschnitt analysiert werden.

Wird der gesamte Kontext des Begriffs „Gefahr“ betrachtet, kann festgestellt werden, dass eine „Gefahr“ in mehreren Definitionen als Zustand beschrieben wird, während eine

Tabelle 3.1: Nicht-sprachliche Begriffskontexte der Sicherheit

Sicherheit	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrssicherheit	Sicherheitsmaß
Personensicherheit	Gefährdungsrate
	Gefahrenvermeidungspotenzial
Risiko	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrsrisiko	Schadensausmaß
Grenzrisiko	Schadenseintrittswahrscheinlichkeit
Verletzungsrisiko	Risikoakzeptanz
Gefahr	
Unterbegriffe	Teilbegriffe (Merkmale)
Personengefahr	Gefahrenart
Umweltgefahr	Schadenspotenzial
Verkehrsgefahr	Vermeidungspotenzial
Gefahrenquelle	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrsgefahrenquelle	Gefährdungsgrad
	Gefahren(feld)ausdehnung
	Wirkungsbereichausdehnung
Gefährdung	
Unterbegriffe	Teilbegriffe (Merkmale)
Personengefährdung	Gefährdungsrate
Verkehrsgefährdung	Vermeidbarkeitsgrad
	Gefährdungszeitpunkt
Schaden	
Unterbegriffe	Teilbegriffe (Merkmale)
Sachschaden	Schadensausmaß
Personenschaden	Schadensart
Umweltschaden	Schadensakzeptanz
	Schadenseintritt

Tabelle 3.2: Nicht-sprachliche Begriffskontexte der Sicherheit (Fortsetzung)

Sicherungsfunktion	
Unterbegriffe	Teilbegriffe (Merkmale)
Abschaltfunktion	Wirksamkeit
Abstützfunktion	Sicherheitintegrität
Reserve	Verfügbarkeit
	Struktur
Sicherungstechnik	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrssicherungstechnik	Zuverlässigkeit
Anlagensicherungstechnik	Instandhaltbarkeit
Brandsicherungstechnik	Aufbau
Sicherungsanlagen	
Sicherheit/Gewissheit	
Unterbegriffe	Teilbegriffe (Merkmale)
Wissen	Grad der Gewissheit
	Dauer der Gewissheit
Sicherheit/Schutz	
Unterbegriffe	Teilbegriffe (Merkmale)
Datensicherheit	Grad des Schutzes
Staatssicherheit	Verlässlichkeit
Personenschutz	Sichtbarkeit
Schadenseintritt	
Unterbegriffe	Teilbegriffe (Merkmale)
Sachschadenseintritt	Schadenseintrittshäufigkeit
Personenschadenseintritt	Zeitpunkt

„Gefährdung“ vereinzelt entweder vage umschrieben oder konkret als Ereignis, Bedingung oder Verhalten verstanden wird. Kuhlmann [Kuh81] umschreibt beispielseise eine Gefährdung als etwas, das sich ergeben kann, wenn potenzielle Objekte in den Wirkungskreis des gefährlichen Systems treten und widerspricht somit der Interpretation der Gefährdung als Verhalten bzw. Zustandsübergang nicht.

Die „Gefahr“ als Zustand wird als komplementär zur „Sicherheit“ beschrieben, die ebenfalls als Zustand definiert ist. Die Relation (r_1[1]) zwischen „Sicherheit“ und „Gefahr“ kann somit gleichermaßen als Oppositionalität auf Begriffssystemebene, als auch Antonymie auf Bezeichnungsebene interpretiert werden. Die beiden Zustände „Gefahr“ und „Sicherheit“ sind zusätzlich über eine Zustandsfolge (Kausalität (r_2)) voneinander abgrenzbar. Aus dem Zustand „Sicherheit - kurz: sicher“ kann der Zustand „Gefahr“ werden und aus dem Zustand „Gefahr“ wiederum der Zustand „Sicherheit“.

Der als Verhalten verstandene Zustandsübergang zwischen diesen beiden globalen Zuständen wird als „Gefährdung“ interpretiert, die an verschiedene Bedingungen geknüpft werden kann, wie z.B. die Anwesenheit von verletzbaren Systemen (Menschen oder Sachgüter) im Wirkungskreis des gefährlichen Systems, oder die Benutzung des Systems an sich. Je nach Quelle unterscheidet sich der Umfang der verletzbaren Systeme und schließt Sachgüter nicht immer in die Betrachtung mit ein. Hier wird jedoch eine allgemeine Beschreibung bevorzugt und somit eine Ausgrenzung von Sachgütern vermieden. Die Relation zwischen dem Begriff „Gefährdung“ und dem Begriff „Sicherheit“ (r_3) kann analog zur Relation zur „Gefahr“ (r_8) im Sinne eines zeitlichen Ablaufs als Temporalitäten interpretiert werden.

Sowohl die aufgeführten Normen als auch Kuhlmann interpretieren den Zustand einer „Gefahr“ inhaltlich als Bedrohung, die von einem System (z.B. technischen) ausgeht und auf ein sekundäres verletzbares System (z.B. Mensch oder Sachgüter) wirkt und dort im weiteren Verlauf zu einem „Schaden“ führen kann. Der „Schaden“ beschreibt demnach einen weiteren Zustand der in einer kausalen Relation (r_{12}) zu dem Zustand „Gefahr“ und implizit auch zu dem Begriff „Sicherheit“ steht. Aus einer „Gefahr“ kann sich folglich der Zustand „Schaden“ ergeben. Dieser Zustandsübergang kann als „Schadenseintritt“ oder auch „Schädigung“ bezeichnet werden. Der durch eine „Gefahr“ ermöglichte „Schadenseintritt“ (kausale Relation (r_{15})) aktiviert bzw. realisiert (Kausalität (r_{13})) den „Schaden“ als globalen Zustand und definiert dessen Merkmale (u.a. das Schadensausmaß). Gleichzeitig wird durch den „Schadenseintritt“ dessen Merkmal der Schadenseintrittshäufigkeit mit Werten belegt. Beide Merkmale sind gleichzeitig auch Merkmale des Begriffs: „Risiko“.

Zwischen dem Begriff „Risiko“ und den Begriffen „Schaden“ sowie „Schadenseintritt“ kann aus der Analyse der nicht-sprachlichen Kontexte eine Relation auf Merkmalsebene festgestellt werden. Das „Risiko“ quantifiziert sowohl das Merkmal „Schadensausmaß“ des Begriffs „Schaden“ als auch das Merkmal der „Häufigkeit (Rate)“ des Begriffs „Schadenseintritt“. Diese Relationen stellen jedoch keine direkten Relationen zwischen den in der interessierenden Begriffsmenge aufgeführten Begriffen dar.

Als „Gefahrenquelle“ wird in der Bestandsaufnahme ein z.B. technisches System be-

[1] sämtliche Relationsindizes beziehen sich auf Tabelle 3.3, Tabelle 3.4 und Abbildung 3.1

zeichnet, von dem eine Gefahrensituation ausgeht, wobei eine entsprechende „Gefährdung“ von verletzbaren Systemen (Menschen oder Sachgüter) vorausgesetzt wird. Setzt man die „Gefahrenquelle“ in Relation zur „Gefährdung“, kann eine kausale Abhängigkeit (r_{10}) identifiziert werden. Die Gefahrenquelle löst demnach als Ursache eine Gefährdung aus. Die Ausprägung der „Gefahr“ wird durch die Art der „Gefahrenquelle“ im Sinne eines Produktes definiert, so dass diese Relation (r_7) als Genetizität bezeichnet werden kann.

Die Begriffe „Sicherungsfunktion“ und „Sicherungstechnik“ sind über eine direkte pragmatische Relation (Assoziation (r_{14}))im Sinne einer Bereitstellung der Funktionalität durch die jeweilige Technik miteinander verbunden. Die „Sicherungsfunktion“ mit seinen Merkmalen kann „Gefährdungen“ vermeiden (r_{11}) bzw. Situationen, in der es zu einer „Gefährdung“ kommen könnte, durch die Beherrschung von „Gefahrenquellen“ kontrollieren (Assoziation r_9). „Sicherungsfunktionen“ bestimmen demnach über die Vermeidung von Gefahren und die dadurch resultierende Reduktion der Schadenseintrittshäufigkeit und des Schadensausmaßes das „Risiko“ im Sinne einer Genetizität (r_6) und fördert die „Sicherheit“ (r_5).

Der Begriff „Sicherheit/Schutz“ übernimmt, anders als die „Sicherungsfunktion“, die Aufgabe, verletzbare Systeme (Mensch oder Sachgüter) vor den Auswirkungen von Gefahren zu schützen, ohne direkten Einfluss auf die Gefahrenquelle auszuüben. Analog zur „Sicherungsfunktion“ fördert der Begriff „Sicherheit/Schutz“ die „Sicherheit“ ebenfalls im Sinne einer Genetizität (r_4) durch die Reduktion des Schadensausmaßes am Gefahrenobjekt.

Zwischen dem Begriff „Sicherheit/Gewissheit“ und den bereits aufgeführten Begriffen der interessierenden Begriffsmenge kann keine relevante Relation erkannt werden, die zu einem besseren Verständnis der Thematik beitragen kann. Aus diesem Grund wird dieser Begriff aus der Menge der interessierenden Begriffe entfernt.

Tabelle 3.3 zeigt zusammenfassend die analysierten direkten Relationen zwischen den Begriffen der interessierenden Begriffsmenge.

Tabelle 3.3: Darstellung direkter Relationen der sicherheitsrelevanten Begriffsmenge

		Senke										
		Sicherheit	Risiko	Gefahr	Gefahrenquelle	Gefährdung	Schaden	Sicherungsfunktion	Sicherungstechnik	Sicherheit/Gewissheit	Sicherheit/Schutz	Schadenseintritt
Quelle	Sicherheit	X	-	$r_{1;2}$	-	r_3	-	-	-	-	-	-
	Risiko	-	X	-	-	-	-	-	-	-	-	-
	Gefahr	$r_{1;2}$	-	X	-	-	r_{12}	-	-	-	-	r_{15}
	Gefahrenquelle	-	-	r_7	X	r_{10}	-	-	-	-	-	-
	Gefährdung	r_3	-	r_8	-	X	-	-	-	-	-	-
	Schaden	-	-	-	-	-	X	-	-	-	-	-
	Sicherungsfunktion	r_5	r_6	-	r_9	r_{11}	-	X	-	-	-	-
	Sicherungstechnik	-	-	-	-	-	-	r_{14}	X	-	-	-
	Sicherheit/Gewissheit	-	-	-	-	-	-	-	-	X	-	-
	Sicherheit/Schutz	r_4	-	-	-	-	-	-	-	-	X	-
	Schadenseintritt	-	-	-	-	-	r_{13}	-	-	-	-	X

3.1.3 Bestandsfestlegung: Sicherheit

Anhand der begrifflichen Relationen aus Unterabschnitt 3.1.2 und der interessierenden Begriffsmenge selbst kann das Begriffssystem für den Begriff Sicherheit modelliert werden. Die Relationen können durch Zuweisung von Benennungen ebenfalls attributiert werden und somit das Begriffssystem erweitern. Die direkten Relationen werden nachfolgend in Tabelle 3.4 mit Benennungen, der Relationsart sowie den mathematischen Relationen dargestellt.

Neben den bereits analysierten und dargestellten direkten Relationen zwischen den Begriffen der interessierenden Begriffsmenge existieren weitere „Zwischen-"Begriffe, über die indirekte Relationen hergestellt werden können. Aus der inhaltlichen Analyse (Bestandsuntersuchung) sind vorwiegend Merkmale (Teilbegriffe), die wiederum als eigenständige Begriffe zu verstehen sind, als bindende Elemente nutzbar. In Abbildung 3.1 sind diese Merkmalsbegriffe im Gegensatz zu den Begriffen der interessierenden Begriffsmenge als nicht ausgefüllte Elemente dargestellt worden. Die „Sicherheitsintegrität", die „Risikoakzeptanz" und „Schadenshäufigkeit" sowie das „Schadensausmaß" sind Beispiele für merkmalsbezogene Teilbegriffe, über die indirekte Relationen zwischen den interessierenden Begriffen hergestellt werden können. Das „verletzbare System" als Oberbegriff für „Mensch" und „Sachgut" ermöglicht eine weitere Eingrenzung der Interpretation auf Begriffssystemebene.

In Abbildung 3.1 werden sowohl die Begriffe der interessierenden Begriffsmenge als auch die erweiterten und merkmalsbezogenen Teilbegriffe aufgeführt und die analysierten Relationen dargestellt.

Der Vorteil einer solchen Modellierung ist die Eindeutigkeit der Abgrenzung zwischen den einzelnen Begriffen. Durch die fest definierten Begriffsrelationen, die den mathematischen Relationseigenschaften aus Unterabschnitt 2.3.6 unterliegen, lässt sich das Modell des Begriffssystems mit geeigneten Werkzeugen elektronisch auslesen, analysieren und implizites Wissen daraus ableiten. Sind beispielsweise Begriffe über transitive Relationen miteinander verbunden, ergeben sich indirekt modellierte Assoziationen, die dem Betrachter als zusätzliche Informationen zur Verfügung stehen können.

Auffällig in Abbildung 3.1 ist die zentrale Rolle des Begriffs „Gefahr". Als Zustandsbegriff steht dieser in einer direkten oppositionellen Relation zum Begriff Sicherheit und es existieren zusätzlich kausale bzw. assoziative Relationen zwischen der Gefahr und den Begriffen Gefahrenquelle, Schaden bzw. Schadeneintritt. Diese inhaltlichen zum Teil pragmatischen Relationen dienen der Interpretation des Ursprungsbegriffs und ermöglichen einen im Vergleich zum Begriff Sicherheit leichteren inhaltlichen Zugang. Über die oppositionelle Relation zwischen Sicherheit und Gefahr kann somit ein inhaltlicher Zusammenhang zum Schaden und Risiko als Begriff implizit hergestellt werden.

Die statischen und dynamischen Zusammenhänge im Kontext des allgemeinen Sicherheitsbegriffs können aus der Begriffsanalyse abgeleitet werden. Dabei fällt auf, dass die Relationen zwischen den Begriffen aus Tabelle 3.4 vorwiegend dynamische Eigenschaften beschreiben, die es zu formalisieren gilt. Die statische, also strukturelle, Auffälligkeit liegt dabei wie eingangs beschrieben in der zentralen Rolle der Gefahr.

Tabelle 3.4: Relationen der sicherheitsrelevanten Begriffsmenge im Detail

Relation	Relationsbenennung	Relationsart	math. Relation
r_1	ist komplementär zu	Oppositionalität, Antonymie	irreflexiv, symmetrisch
r_2	wird zu	Kausalität	irreflexiv, antisymmetrisch, transitiv
r_3	beeinflusst	Temporalität	reflexiv, antisymmetrisch, transitiv
r_4	fördert	Genetizität	transitiv
r_5	fördert	Genetizität	transitiv
r_6	definiert	Genetizität	transitiv
r_7	definiert	Genetizität	transitiv
r_8	führt zu	Temporalität	irreflexiv, antisymmetrisch, transitiv
r_9	beherrscht	Assoziation	-
r_{10}	löst aus	Kausalität	irreflexiv, antisymmetrisch, transitiv
r_{11}	verhindert	Assoziation	-
r_{12}	wird zu	Kausalität	irreflexiv, antisymmetrisch, transitiv
r_{13}	aktiviert	Kausalität	irreflexiv, antisymmetrisch, transitiv
r_{14}	implementiert	Assoziation	-
r_{15}	ermöglicht	Kausalität	irreflexiv, antisymmetrisch, transitiv

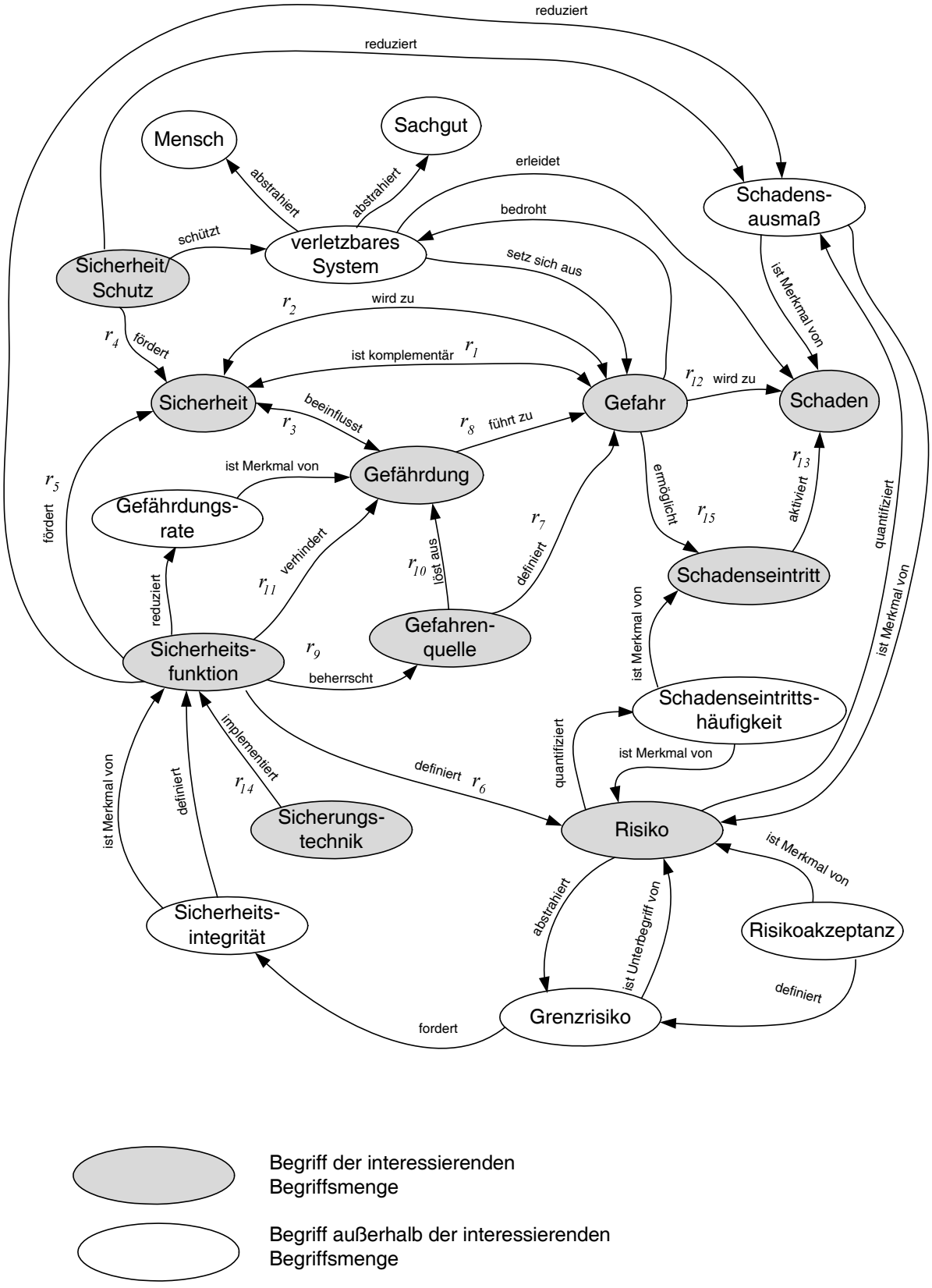


Abbildung 3.1: Sicherheit als Begriffssystem

3.2 Formalisierung der Systemsicherheit

Nach der terminologisch-begrifflichen Analyse der Sicherheit im vorangegangenen Abschnitt folgt in diesem Abschnitt ein Ansatz zur Formalisierung. Ausgehend von dem zur Sicherheit in einer oppositionellen Relation stehenden Begriff *Gefahr* werden unterschiedliche Sicherheitsbedingungen beschrieben und formalisiert. Der Ansatz der Formalisierung konzentriert sich dabei zunächst auf die Darstellung der Gefahr als Systemzustandsbegriff und erweitert diese Sicht um die dynamischen Systemeigenschaften (das globale Verhalten). Unterschiedliche auf die formalisierten Sicherheitsbedingungen aufbauende Sicherheitsimplementierungskonzepte zeigen mögliche systematische Ansätze, um die Sicherheit von Systemen bei deren Umsetzung zu gewährleisten.

3.2.1 Gefahr als globaler Zustandsbegriff

Im normativen Sprachgebrauch und im vorgestellten Begriffssystem wird die Gefahr mit einer Situation, die potenziell zu einer Schädigung eines Menschen oder einer Sache führen kann, gleichgesetzt (vgl. Abschnitt 3.1). Zusätzlich können drohende materielle, ideelle oder finanzielle Verluste ebenfalls allgemein als Gefahr verstanden werden. Im Sinne der in dieser Arbeit verwendeten Definition des Begriffs Sicherheit wird jedoch ausschließlich die Gefahr einer direkten oder indirekten Schädigung des Menschen bzw. seiner Umwelt sowie die in der Bestandsuntersuchung aufgeführten Kontexte verwendet, obwohl eine abstrakte Interpretation eher einer Wahrscheinlichkeit des Eintritts eines negativen oder unerwünschten Zustands entspräche.

Im Bezug auf die Grundlagen aus Kapitel 2 in Verbindung mit den Ausführungen der begrifflichen Analyse aus Abschnitt 3.1 wird diesbezüglich deutlich, dass eine gefährliche Situation „Gefahr“ einen globalen in der Regel unerwünschten bzw. gefährlichen Zustand eines Systems in Verbindung zu seiner Umwelt beschreibt. Der analysierte Gefahrenzustand lässt sich kausal zwischen den globalen Zuständen „Sicherheit“ und „Schaden“ einordnen und wird über das Ereignis „Gefährdung“ initiiert. Die Ausprägung der „Gefahr“ wird durch die jeweilige „Gefahrenquelle“ definiert. Ein globales aus dem Begriffsmodell abgeleitetes dynamisches Gefahrenmodell zeigt Abbildung 3.2 in Petrinetzdarstellung.

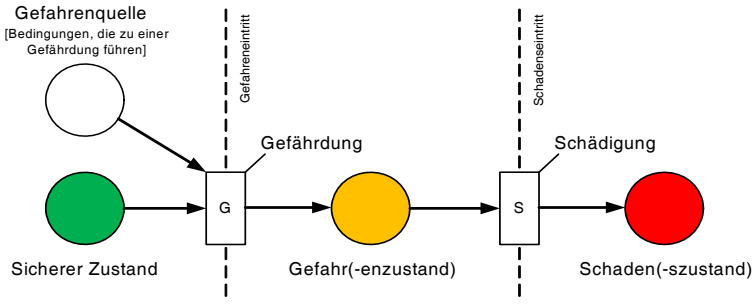


Abbildung 3.2: Globales Gefahrenmodell

Werden die drei Globalzustände eines Systems interpretiert, kann der kategorische Ausschluss der Zustände Gefahr und Schaden als Bedingung für die Sicherheit vorerst angenommen werden.

Abbildung 3.3) zeigt die globalen Systemzustände, bestehend aus einer definierten Menge von lokalen (Teil-) Systemzuständen, die in unterschiedlichen Konstellationen vorliegen können. Der Schadenzustand aus Abbildung 3.3 stellt dabei einen möglichen Schadenzustand innerhalb der betrachteten Systemgrenze dar. Dies bedeutet, dass die Wahl der Systemgrenze bei der Modellierung sorgfältig getroffen werden muss. Nur so lassen sich mögliche Schäden, z.B. am Systemnutzer, berücksichtigen. Dazu müssen diese entweder in modellierten Systemgrenzen eines künstlich (über das Modell) geschlossenen Systems bzw. über eine definierte Schnittstelle eines offenen Systemmodells integriert werden.

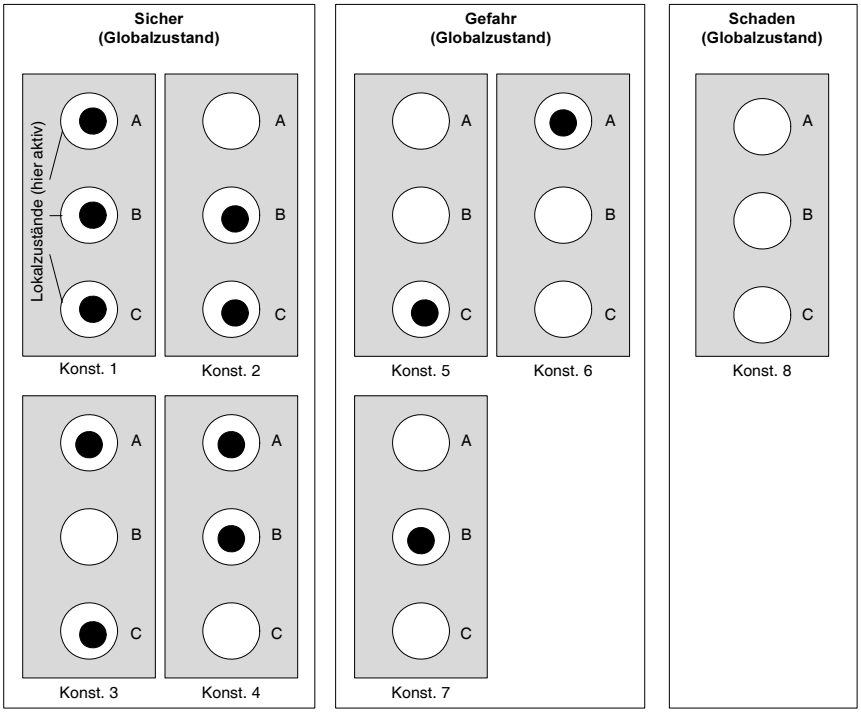


Abbildung 3.3: Zusammenhang zwischen lokalen und globalen Zuständen

3.2.2 Globale Gefährdungen und lokales Systemverhalten

Basierend auf den systemtheoretischen Annahmen aus Unterabschnitt 2.2.2 charakterisiert die Änderung eines Zustands das Systemverhalten. Die Übergänge zwischen den unterschiedlichen Konstellationen der lokalen Zustände und die daraus resultierenden Änderungen der Globalzustände lassen sich durch eine vereinfachte Verhaltensbeschreibung des Systems darstellen. Abbildung 3.4 zeigt die Zusammenhänge zwischen korrekter (Teil-)Systemfunktion, dem unerwünschten (lokalen) Verhalten und als Folge des-

sen den nicht erkannten lokalen Fehlzustand, der die Bedingung für einen globalen Zustandsübergang von einem sicheren Systemzustand zum Gefahrenzustand darstellt. Unterschiedliche lokale Verhalten können somit verschiedene Gefährdungen erzeugen und den globalen Gefahrenzustand auslösen. Zum einen können einzelne Funktionsausfälle bereits zu einer Gefährdung (G1)und somit folglich zu einem Gefahrenzustand führen. Zum anderen kann ein einzelner Ausfall einer einzelnen Systemfunktion zwar die Unverfügbarkeit der Teilfunktion bedeuten aber erst in Kombination mit einem zweiten Funktionsausfall in einer Gefährdung (G2) resultieren.

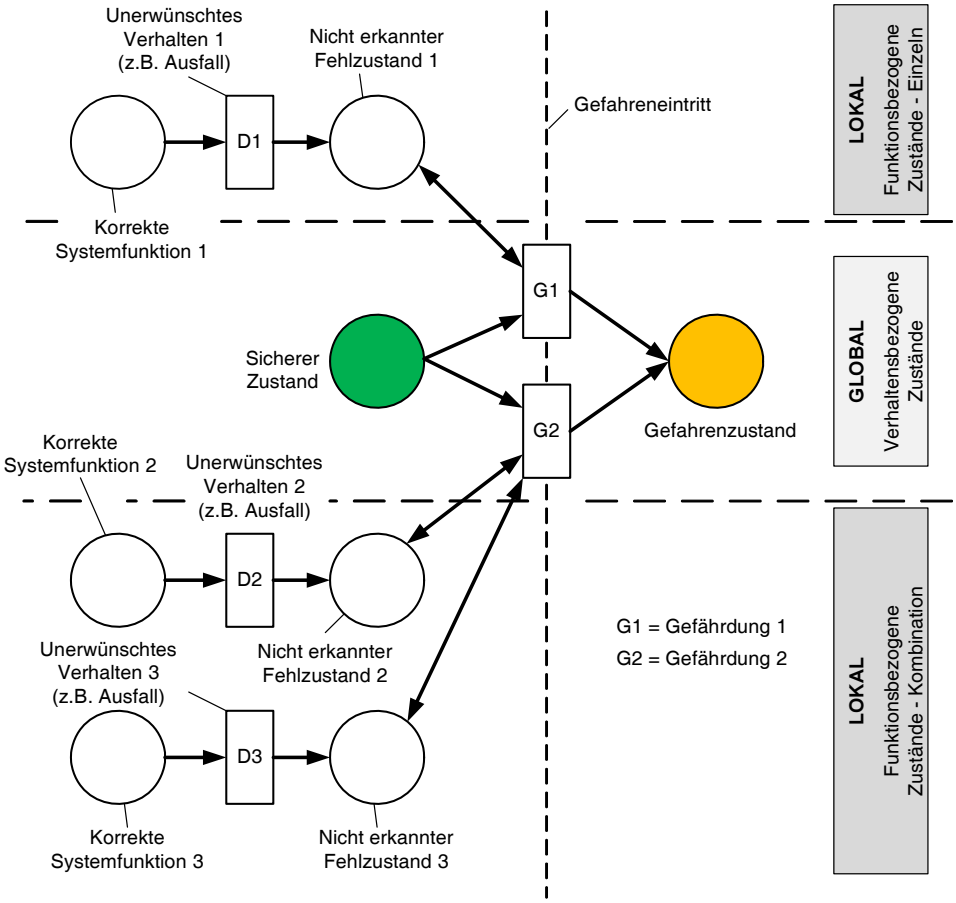


Abbildung 3.4: Fehlfunktion als Ursache einer Gefahr

3.2.3 Schadenseintritt als Auswirkung eines Gefahrenzustands

Die aufgezeigte Definition des Gefahrenzustands als “Situation die potenziell einen Schaden an Menschen oder Gütern ermöglicht” definiert nicht explizit, ob die potenziell gefährliche Situation (z.B. resultierend aus einem nicht erkannten Fehlzustand) mit einer Mindestwahrscheinlichkeit zu einer Schädigung führen muss, um diese als existente

Gefahr zu definieren. Die logischen und quantitativen Bedingungen, die aus einem globalen Zustand „Sicherheit“ den Eintritt einer „Gefährdung“ aktivieren, sind dabei undefiniert. Zwar wird aus den inhaltlichen Definitionen aus Abschnitt 3.1 deutlich, dass das Ereignis „Gefährdung“ als Bedingung die Überschreitung von s.g. Gefahrenfeldern durch die verletzbaren Systeme vorsieht, aber der potenzielle Grad des Schadens (Schadensausmaß) bleibt ebenfalls undefiniert. Es liegt also nahe, dass ein Zusammenhang zwischen dem Übergang vom sicheren zum gefährlichen Zustand (Gefährdung) und dem Übergang vom Gefahrenzustand in den Schadenszustand (Schadenseintritt) mit seinen Merkmalen Schadenseintrittsrate und Schadensausmaß besteht.

Betrachtet man diesen Ansatz weiter, so ergibt sich die durch [Rak02] geprägte Definition der Gefahr: “Eine Gefahr ist ein Zustand bzw. eine Anzahl von Bedingungen eines Systems und seiner Umwelt, die unvermeidlich zu einem Schaden führen.” Allerdings setzt diese Definition durch die angesprochene Unvermeidbarkeit des Schadens die Gefährdungsrate der Schadensrate gleich und schließt somit Beinaheunfälle aufgrund vorausgegangener abgewendeter Gefahren ohne resultierende Schäden implizit kategorisch aus. Dieses Definition deckt sich nicht vollständig mit der systemtheoretischen Denkweise, die in dieser Arbeit verfolgt wird.

Entscheidenden Aufschluss gibt neben der Festlegung der Bedingungen für eine Gefährdung die Festlegung von Bedingungen für den Schadenseintritt. Erst das Zusammentreffen unterschiedlicher ungünstiger Einzelzustände als Bedingung (z.B. Fortsetzen des Betriebs bei bestehender Gefahr), die ohne korrigierende bzw. intervenierende Maßnahmen mit hoher Wahrscheinlichkeit zu einer drohenden Schädigung eines Menschen oder seiner Umwelt führen würde, wird hier als existente Gefahr verstanden.

Der Eintritt eines Schadens ist durch sichernde (z.B. sicherungstechnische oder organisatorische) Maßnahmen vermeidbar und führt bei positivem Ausgang zu einem Beinaheunfall. Aber auch der zufällige Nichteintritt des Schadens verhindert ein Überschreiten dieser Grenze. Beide reduzieren die Wahrscheinlichkeit eines Schadens bei bestehender Gefahr über die Merkmale Schadenseintritt und Schadensausmaß.

Aus der Abbildung 3.5 ergibt sich der Zusammenhang zwischen Schadenseintritt, Gefahrenabwehr und zufälliger Vermeidung eines Schadens. Eine Situation (Zustand) wird dann als existente Gefahr (akuter Gefahrenzustand) eingestuft, wenn die Wahrscheinlichkeit des Schadenseintritts die Summe der Wahrscheinlichkeiten zur Schadensabwehr und -vermeidung übersteigt. Diese Interpretation entspricht der begrifflichen Definition der Gefahr: „Situation, die potenziell eine Schädigung des Menschen oder Sachguts ermöglicht“.

Zusammenfassend können aus den Definitionen und Formalisierungsansätzen Bedingungen für den Erhalt des globalen Zustands „Sicherheit“ abgeleitet werden. Im folgenden Abschnitt werden zwei grundsätzliche Sicherheitsbedingungen beschrieben.

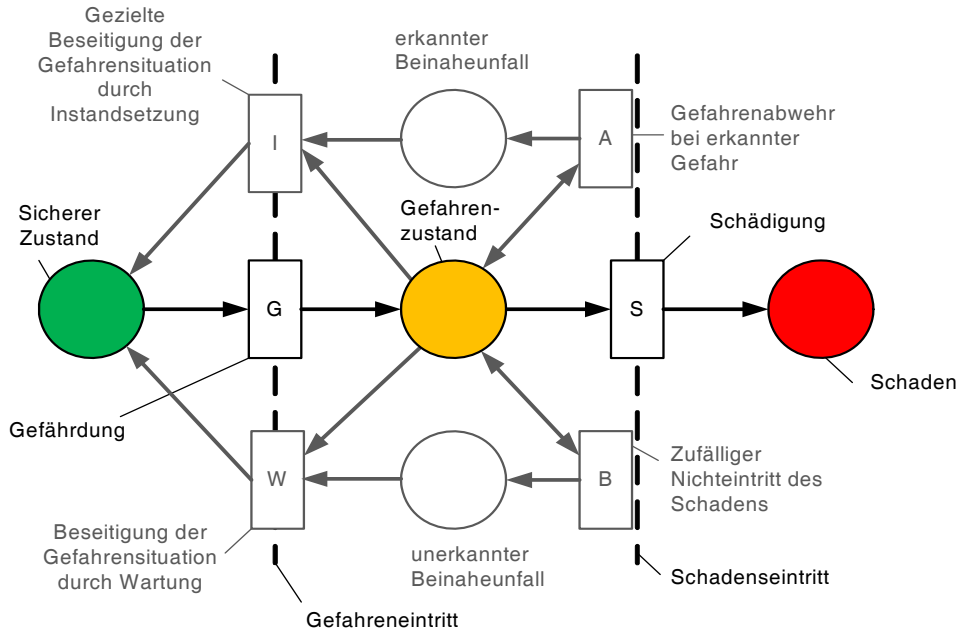


Abbildung 3.5: Modellierung des Schadenseintritts und zufälliger Vermeidung

3.3 Herleitung von Sicherheitsbedingungen

Aus der Verknüpfung des Zustands „Gefahr“, des gefährlichen Verhaltens „Gefährdung“ und der damit verbundenen Möglichkeit eines „Schadenseintritts“ zu einem Schaden ergeben sich zwei grundsätzliche Sicherheitsbedingungen. Eine eher aus der pragmatischen Überlegung heraus resultierende Bedingung stellt die *absolute Sicherheitsbedingung* dar, die eine diskrete Nicht-Überschreitung der Gefahrenschwelle und dadurch einen Ausschluss einer Gefährdung fordert, während die auf Zustandswahrscheinlichkeiten basierende *probalistische Sicherheitsbedingung* ein kontinuierliches Systemverhalten berücksichtigt und primär die akzeptable Wahrscheinlichkeit im sicheren Zustand zu verharren fordert und somit den Anforderungen zur Berücksichtigung einer möglichen Schadensabwehr und -vermeidung bei der Bestimmung der Systemsicherheit eher nachkommt.

3.3.1 Absolute Sicherheitsbedingung

Ein System gilt theoretisch als „absolut sicher“, wenn keine Konfiguration der lokalen Zustände des Systems in Verbindung mit dem Einwirken der lokalen Zustände seiner Umwelt ein Erreichen des gefährlichen globalen Systemzustands ermöglicht. Die Zusammensetzung der lokalen Elementarzustände, die in diesem Fall zu keinem globalen Gefahrenzustand führen können, wird aus der Parametrisierung der Zustandsvariablen, die insgesamt den Zustandsraum definieren, bestimmt.

Die in Abbildung 3.6 gezeigten Grenzen repräsentieren neben der Linie für den Scha-

denseintritt (äußere Grenze) die Schwelle der Gefährdung (innere Grenze), deren Überschreitung per Definition der absoluten Sicherheitsbedingung nicht zulässig ist, um das System als „absolut“ sicher zu bezeichnen.

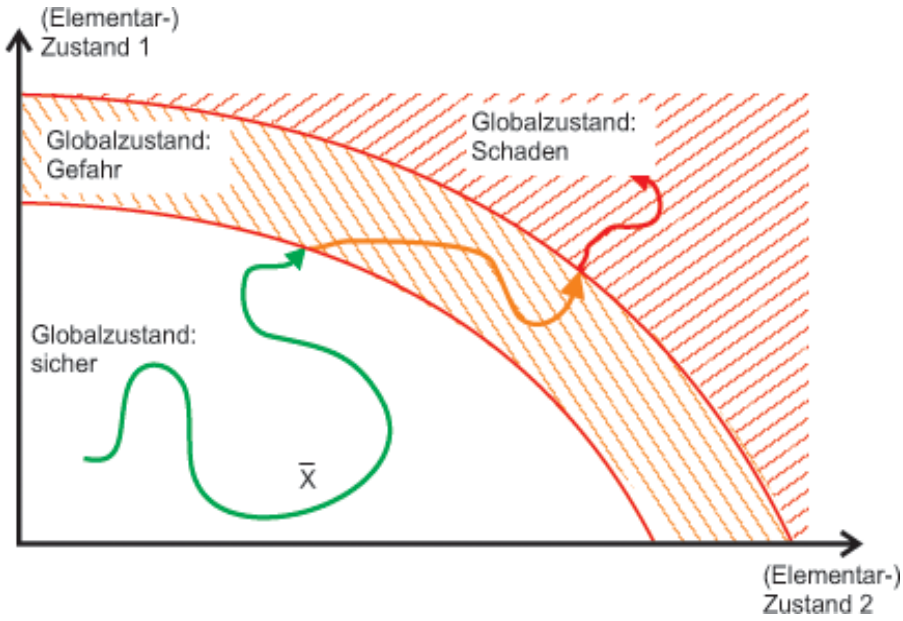


Abbildung 3.6: Zustandsraumdarstellung lokaler und globaler Zuständen

Wird die Trajektorie (Zustandsvektor) in Abbildung 3.6 mit $\bar{X}$ und die Gefährdungsgrenze als $\bar{X}_{zul}$ bezeichnet, ergibt sich folgende absolute Sicherheitsbedingung:

$$\bar{X} = \bar{X}_{safe} \qquad \text{, wenn} \qquad \bar{X} < \bar{X}_{zul} \tag{3.1}$$

Die absolute Sicherheitsbedingung kann somit als kategorischer Ausschluss sowohl des Gefahren- als auch Schadenszustands definiert werden.

Werden exemplarisch drei der unzähligen Zustandsvariablen einer Fahrzeugbewegung im Straßenverkehr: Geschwindigkeit, Griffigkeit des Straßenbelags, und Kurvenradius betrachtet, wird eine starke Abhängigkeit der Grenzgeschwindigkeit von den beiden anderen Größen deutlich. Ein Übertreten der Grenzgeschwindigkeit führt beispielsweise zu einer existenten Gefahr mit der potenziellen Möglichkeit einer Kollision mit einem vorausliegenden Hindernis, sofern keine vermeidenden Maßnahmen angewendet werden. Hervorzuheben ist dabei, dass die einzelnen Größen, isoliert betrachtet, keine eigenständigen Grenzen besitzen. Die Geschwindigkeit allein ist nicht durch sich selbst begrenzt, sondern wird durch andere Parameter, wie z.B. das angesprochene Hindernis, eingeschränkt. Auch die Griffigkeit und der Kurvenradius, isoliert betrachtet, führen zu keiner gefährlichen Situation, sondern lediglich zu einer Verfügbarkeitseinschränkung des Systems, da ein Durchfahren einer zu engen Kurve oder das Beschleunigen aus dem Stillstand bei unzureichender Griffigkeit nahezu unmöglich würden.

3.3.2 Probabilistische Sicherheitsbedingung

Die probabilistische Sicherheitsbedingung erweitert die absolute Sicherheitsbedingung um definierte Zustandswahrscheinlichkeiten und Übergangsraten. Zum besseren Verständnis wird daher ein vereinfachtes Modell zur Veranschaulichung von Zustandswahrscheinlichkeiten und Zustandsübergangsraten vorgestellt. Dafür eigenet sich besonders die Darstellung einer qualitativen Markoff-Kette [Eri05], die sich besonders zur Modellierung und Analyse stochastischer Zustandsänderungen innerhalb eines Systems eignen, um Aussagen über Wahrscheinlichkeiten für das Eintreten zukünftiger Ereignisse treffen zu können.

Die Zustandswahrscheinlichkeiten ($P(X_i)$) aus Abbildung 3.7 stehen dabei in folgendem Zusammenhang:

$$\frac{d}{dt}P(\bar{X}_2) = P(\bar{X}_1) \cdot \lambda_{12}t - P(\bar{X}_2) \cdot \lambda_{21}t \tag{3.2}$$

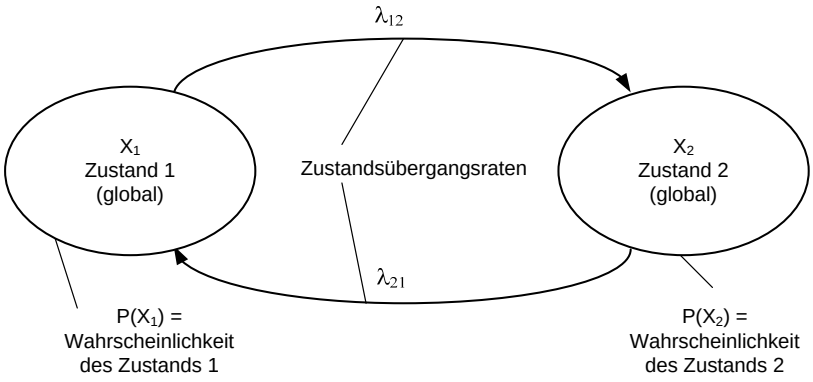


Abbildung 3.7: Einfache Markoff-Kette zur Darstellung probabilistischer Zustandsübergänge

Die Wahrscheinlichkeit eines Zustands errechnet sich somit aus der Summe der Produkte von zulaufenden Zustandswahrscheinlichkeiten und deren Zustandsübergangsraten abzüglich der Summe der Produkte der eigenen Zustandswahrscheinlichkeit und der jeweiligen abfließenden Zustandsübergangsraten. Die Summe der Wahrscheinlichkeiten der gesamten Zustände muss definitionsgemäß gleich eins sein.

$$\sum P(\bar{X}_i) = 1 \tag{3.3}$$

Die Verallgemeinerung dieser Darstellung erlaubt die Berechnung von Änderungen der Zustandswahrscheinlichkeiten über folgenden Ansatz einer Matrix-Differenzialgleichung.

$$\frac{d\bar{P}(\bar{X})}{dt} = \Lambda \cdot \bar{P}(\bar{X}) \tag{3.4}$$

mit Λ als Zustandsübergangsmatrix. Im stationären Zustand ergibt sich daraus

$$\text{wenn} \qquad \frac{dP(\bar{X})}{dt} = 0 \tag{3.5}$$

$$\Lambda \cdot P(\bar{X}) = 0 \tag{3.6}$$

Unter Berücksichtigung von gültigen Anfangsbedingungen kann eine homogene Lösung der Einzelwahrscheinlichkeiten aus den Zustandsübergangsraten abgeleitet werden. Für die probabilistische Sicherheitsbedingung bedeutet dieser Ansatz, dass die Zustandswahrscheinlichkeit des sicheren Systemzustands (X_S) aus Abbildung 3.8 maßgebend ist.

Die probalistische Sicherheitsbedingung fordert, dass die vorhandene Zustandswahrscheinlichkeit des Zustands "sicher" (P(Sicherer Zustand) größer einer minimal akzeptablen (Sicherheits-)Wahrscheinlichkeit ($P_{S_{zul}}$) sein muss, oder anders ausgedrückt, die Wahrscheinlichkeit, nicht in dem sicheren Zustand zu verweilen ($1-P$(Sicherer Zustand)) kleiner einer maximal akzeptablen Gefahrenzustandswahrscheinlichkeit ($P_{G_{zul}}$) ist. Der Wert der Gefahrenzustandswahrscheinlichkeit ergibt sich aus dem damit verbundenen zulässigen Risiko bzw. Schadensschwere, was in dem folgenden Abschnitt erläutert wird.

$$P(\text{Sicherer Zustand} \quad \geq \quad P_{S_{zul}} \tag{3.7}$$

$$1 - P(\text{Sicherer Zustand}) \quad \leq \quad P_{G_{zul}} \tag{3.8}$$

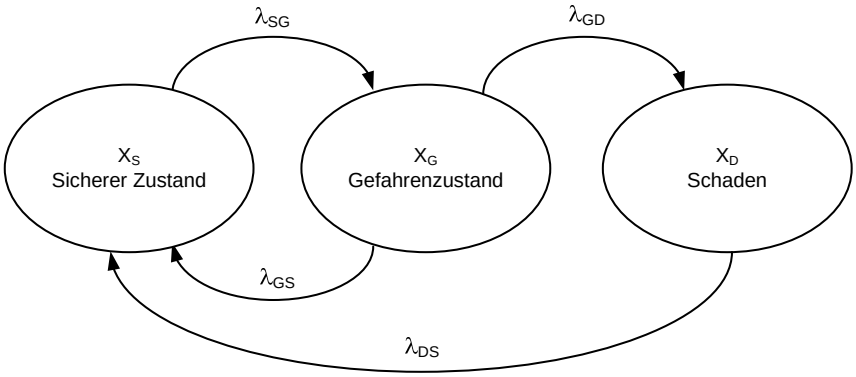


Abbildung 3.8: Markov-Kette zur Darstellung der probabilistischen Sicherheitsbedingung

Zusammenfassend kann nach diesem Abschnitt die Sicherheit als Eigenschaft eines Systems verstanden werden, die gewährleistet, dass in vorgegebenen räumlichen und zeitlichen Grenzen keine existenten Gefahrenzustände erzeugt oder zugelassen werden, aus denen Schäden entstehen können. Diese Anforderung gezielt zu implementieren ist Inhalt der Sicherheitsimplementierungskonzepte, die im Anschluss an die Vorstellung allgemeiner Sicherheitsmaße abgeleitet werden.

3.3.3 Allgemeine Maße der Systemsicherheit

Die Abschätzung der Wirksamkeit unterschiedlicher Implementierungen oder Maßnahmen zur Verbesserung der Sicherheit erfordert eine vergleichbare Bemessung der Sicherheit. Die Einschätzung der Sicherheit findet je nach Domäne und Anwendung in unterschiedlicher Form entweder qualitativ oder quantitativ statt. Aussagen über die Wahrscheinlichkeit eines Systems, einen gefährlichen Zustand einzunehmen bzw. gerade diesen nicht zu erreichen, sind in der Praxis eher selten zu finden, aber dennoch existent. Dieser Abschnitt beschreibt unterschiedliche Maße der Sicherheit, die einer Quantifizierung der probabilistischen Sicherheitsbedingung ähneln, aus unterschiedlichen Domänen.

In der Automatisierungstechnik werden hinsichtlich der Bemessung der funktionalen Sicherheit elektronischer / elektrischer und programmierbarer elektronischer Systeme u. a. die Maße für: Mittlere Ausfallwahrscheinlichkeit bei Anforderung (engl.: Probability of Failure on Demand (PFD)), Mittlere gefahrbringende Ausfallwahrscheinlichkeit pro Stunde (engl.: Probability of Failure per Hour (PFH)), welches bei Gleichsetzung des Fehlers mit einer Gefahr der (tolerierbaren) Gefährdungsrate (engl.: (Tolerable) Hazard Rate ((T)HR)) entspricht, sowie die in Tabelle 3.5 aufgeführten Sicherheitsintegritätsstufen (Safety Integrity Level kurz SIL) verwendet [Deu03b], [Deu02].

Die PFD beschreibt die Wahrscheinlichkeit einer Fehlfunktion einer Sicherungsfunktion im Anforderungsfall, während die PFH, unabhängig vom Anforderungsfall, die Wahrscheinlichkeit eines gefahrbringenden Ausfalls einer Sicherungsfunktion pro Stunde beschreibt. Entscheidend ist hierbei der Zusammenhang zwischen Sicherungsfunktion und Systemfunktion, da wie bereits in Unterabschnitt 3.5.2 gezeigt, ein auftretender Systemfehler bei vorhandenem Sicherheitskonzept, der ggf. Sicherungsfunktionen beinhaltet, einer Gefahr gleichzusetzen ist. D.h. der Ausfall einer Sicherungsfunktion entspricht dem gefährlichen Ausfall einer Systemfunktion. Ein Ausfall einer Sicherungsfunktion, die das Eintreten eines ansonsten wahrscheinlichen Gefahrenzustands verhindern soll, wird somit als reziprokes Sicherheitsmaß angenommen.

Die Sicherheitsintegrität (Safety Integrity) beschreibt die Wahrscheinlichkeit, dass ein System die geforderten Sicherungsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraums anforderungsgemäß erfüllt. Diese ist nach [Deu02] bzw. [Deu03b] in vier Sicherheitsintegritätsstufen (Safety Integrity Level SIL) eingeteilt, die je nach Anwendung entweder in Abhängigkeit der beiden Werte PFD und PFH, bzw. ausschließlich über die PFH/THR ermittelt werden können (vgl. Tabelle 3.5). Keine dieser Maße berücksichtigt allerdings das potenzielle Schadensausmaß, sondern konzentriert sich allein auf Wahrscheinlichkeiten eines gefährlichen Zustands, der zu einem mehr oder weniger undefinierten Schaden führt.

Allgemein domänenunspezifisch kann diesbezüglich das Risiko als Maß der Eintrittswahrscheinlichkeit eines Schadens in Verbindung mit dem potenziellen Schadensausmaß betrachtet werden (vgl. Unterabschnitt 3.1.3). Abbildung 3.9 zeigt diesbezüglich die Zusammenhänge der einzelnen Größen bei der Bestimmung des Risikos in Form eines Klassendiagramms. Ausgehend von erfassten Einzelschäden und der entsprechenden Mittelwertbildung in Zusammenhang mit der Schadensausmaß- und -häufigkeitsverteilung kann durch Produktbildung das Risiko bestimmt werden.

Tabelle 3.5: Sicherheitsintegrität und gefährliche Ausfallraten nach [Deu02]

Sicherheitsintegritätslevel	**Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung** (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Das Risiko, als komplementäres Maß der Sicherheit, wird in unterschiedlichen Domänen verwendet. Dabei wird das Schadensausmaß, entweder in monetärer Form oder in Form von Fatalitäten, berücksichtigt. Einige Ansätze verwenden im Hinblick auf eine angestrebte normierte Skalierung zur Überführbarkeit von Verletzung, Toten und Sachschäden eine volkswirtschaftliche Monetarisierung eines Menschenlebens und unterschiedlicher Verletzungen. Diese Monetarisierung wird allerdings oft aus ethischen Gründen nicht durchgehend akzeptiert.

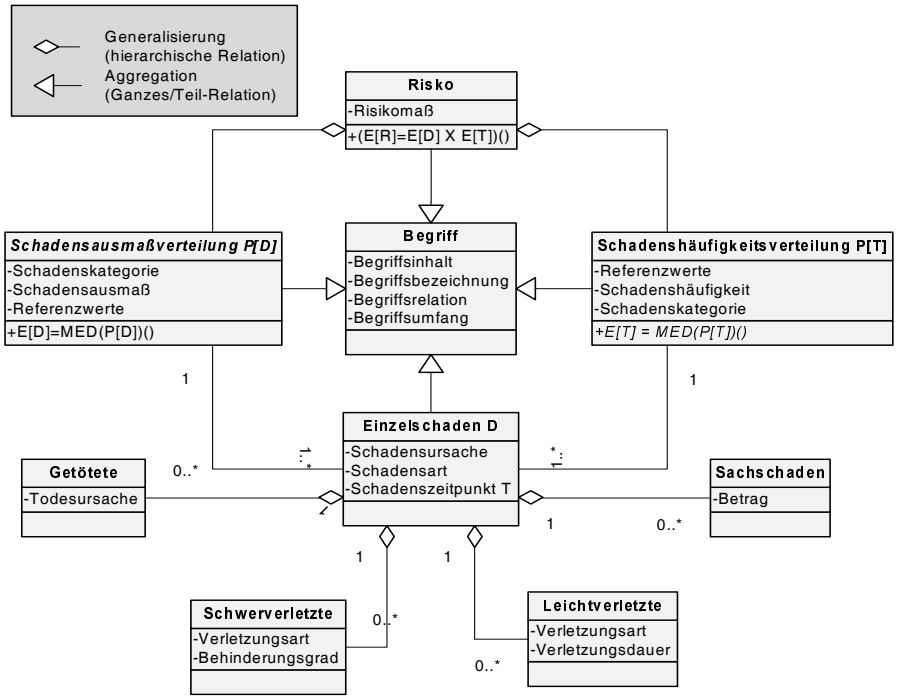


Abbildung 3.9: Formalisierung des Risikobegriffs

Aufgrund der bereits angesprochenen Problematik einer einheitlich skalierbaren Schadensausmaßbestimmung findet die Bestimmung und Bewertung des Risikos in der Regel mit s.g. Risikomatrizen statt, wie sie z.B. in [Int07] und [Deu02] sowie [Deu00] aufgeführt sind. Abbildung 3.10 zeigt nominal skalierte Koordinatenwerte, die in der Kombination die jeweilige Risikostufe bestimmen. Eine je nach Anwendungsdomäne erforderliche Kalibrierung der Skalen ermöglicht zumindest einen Vergleich innerhalb einer Domäne, bei einer domänenübergreifenden Kalibrierung wäre sogar ein unabhängiger Risikovergleich möglich. Eine solche Kalibrierung beinhaltet allerdings die jeweilige Beurteilung der Risikoakzeptanz, so dass eine objektive Vergleichbarkeit eher unwahrschweinlich wäre.

Häufigkeit der Gefahrenfälle	Risikostufen			
häufig	unerwünscht	intolerabel	intolerabel	intolerabel
wahrscheinlich	tolerabel	unerwünscht	intolerabel	intolerabel
gelegentlich	tolerabel	unerwünscht	unerwünscht	intolerabel
selten	vernachlässigb.	tolerabel	unerwünscht	unerwünscht
unwahrscheinlich	vernachlässigb.	vernachlässigb.	tolerabel	tolerabel
unvorstellbar	vernachlässigb.	vernachlässigb.	vernachlässigb.	vernachlässigb.
	unbedeutend	marginal	kritisch	katastrophal
	Gefahrenstufen			

Abbildung 3.10: Risikomatrix zur Bewertung des Risikos nach [Deu00]

3.4 Generische Sicherungsimplementierungskonzepte

Das Ziel oder der Zweck der Sicherungsimplementierung ist die Minimierung der Zustandswahrscheinlichkeit des definierten Schadenszustands durch die Planung und Umsetzung von Sicherungsmaßnahmen. Diese Implementierung kann in unterschiedlicher Weise erfolgen. Die Priorisierung der unterschiedlichen Implementierungsansätze wird in der Regel durch die so genannte Sicherheitsstrategie festgelegt, die der verfolgten Sicherheitspolitik eines Herstellers, Betreibers oder Gemeinwesens entspricht.

Unterschieden werden können unterschiedliche Ausprägungen der Sicherheitsstrategie wie folgt [Bör06]:

- Gefahrenvermeidung
- Gefahrenabwehr
- Auswirkungsminderung

Die drei Ausprägungen beschreiben prinzipiell die Reduzierung der einzelnen Risikobestandteile „Häufigkeit des Gefahreneintritts bzw. Schadenseintritts“ und „Schadensausmaß“. Während eine Sicherheitsimplementierung im Sinne einer Gefahrenvermeidung

den Zustandsübergang („Gefährdung“) von einem sicheren zu einem gefährlichen globalen Systemzustand durch geeignete Funktionen zu vermeiden bestrebt ist, lassen implementierte Funktionen zur Gefahrenabwehr grundsätzlich den Übergang in den Gefahrenzustand zu und versuchen diesen mit geeigneten Mitteln abzuwehren und einen sicheren (Ausfall-)Zustand wieder herzustellen. Die Auswirkungsminderung geht sogar vom Erreichen eines Schadenszustands aus und konzentriert sich darauf durch geeignete Maßnahmen das Schadensausmaß zu minimieren bzw. auf eine akzeptable Höhe zu begrenzen. Zur Auswirkungsminderung zählen auch Konzepte zur Selbstrettung und Fremdrettung im bereits eingetretenen Schadenszustand. Diese sind bestrebt Sekundärfolgen, die das Gesamtschadensausmaß ausdehnen können, zu vermeiden.

Die Sicherungsmaßnahmen lassen sich für alle genannten Konzepte in passive und aktive Maßnahmen unterscheiden. Während passive Funktionen ihre Funktionsfähigkeit grundsätzlich nicht verlieren können (z.B. Haltefunktionen, Abstützungen etc.) und dem entsprechend keine besonderen Handlungen oder Aktivitäten zur Bereitschafterhaltung der Funktion erfordern, sind aktive Sicherheitsmaßnahmen reaktive bzw. auch proaktive Funktionen, die ihre Eigenschaften grundsätzlich verlieren können sofern ein Funktionsausfall dies verursacht. Aktive Sicherungsfunktionen verwenden i.d.R. ein grundsätzliches Sicherheitskonzept.

Ein einfaches Sicherheitskonzept zur Einführung aktiver Sicherheitsmaßnahmen kann sich in einem ersten Ansatz auf folgende Forderung beschränken:

- Jeder Systemfehler muss erkannt werden
- Im erkannten Fehlerfall ist das System in einen sicheren Zustand zu überführen

Das Erkennen des Systemfehlers ist dabei grundsätzlich als Bedingung des aktiven Eingriffs der Sicherungsfunktion zu verstehen. Je nach Ausprägung der Sicherheitsstrategie sind dazu unterschiedliche globale und/oder lokale Systemzustände zu erkennen und unterschiedliche Maßnahmen erforderlich. Das Erkennen eines eingetretenen gefährlichen Zustands („Gefahr“) würde bei angestrebter Gefahrenvermeidung nicht ausreichend sein, da bereits das potenzielle Eintreten der Gefahr („Gefährdung“) zu verhindern ist. Dies impliziert die Einbindung von möglichen Gefährdungsursachen bei der Implementierungsplanung bzw. dem Design der Sicherheit.

3.4.1 Gefährdungsursachen

Die Ursachen für die einzelnen lokalen Zustandsänderungen innerhalb eines Systems können vielfältig sein. Aufgrund chemischer und physikalischer Eigenschaften technischer und biologischer Systeme und dem damit verbundenen Zerfall ist kein System im Laufe der Zeit vollkommen ausfallsicher und eine potenzielle Schädigung von Bauteilen oder Teilsystemen kann somit bei keinem System vollständig ausgeschlossen werden [Int07]. Die völlige Gefahrenfreiheit eines Systems ist somit grundsätzlich ausgeschlossen, da diese Annahme ebenso für steuernde als auch für sichernde Systeme gilt.

Die Reduzierung der Wahrscheinlichkeit des globalen Gefahrenzustands (vgl. gefährliche Konstellation von lokalen Zuzständen) durch entsprechende technische und/oder organisatorische Maßnahmen zur größtmöglichen Vermeidung einer Gefährdung kann einen großen Beitrag zur Sicherheit leisten. Diese Reduzierung der Gefährdungsrate kann z.B. über die Beherrschung von offensichtlichen bzw. systematisch ermittelten Gefahrenquellen erreicht werden. Die Ursachen für den Eintritt einer Gefährdung können entsprechend in

- mechanische
- chemisch-biologische
- elektro-magnetische
- thermodynamische

Ausprägungen unterschieden werden. Eine mechanische Ausprägung einer Ursache beinhaltet definitionsgemäß mechanische Zustände und ein mechanisches Verhalten zum Auslösen einer Gefährdung. Als Beispiele können rotierende Teile oder kinetische Energien von Objekten im Wirkungskreis von Personen sein. Analog sind die weiteren Ausprägungen erklärbar.

Neben den rein physikalischen Ursachen aus dem System selbst oder der angrenzenden Umwelt, die zu einer Gefährdung führen können, ist, bei vorausgesetzter vorhandener Mensch-Maschine-Schnittstelle eines technischen Systems, das menschliche Verhalten eine häufig anzutreffende Gefährdungsursache. Dabei können sowohl menschliche Unzulänglichkeiten als auch Fehlhandlungen eine Gefährdung auslösen bzw. sogar eine ausgelöste Gefahrenabwehr oder Auswirkungsminderung behindern. Diese Fehlhandlungen bzw. Unzulänglichkeiten können unterschiedlich begründet sein. Während eine vorsätzliche Handlung eher einem Sabotageakt gleichkommt, kann eine Unkenntnis der Bediener z.B. aufgrund fehlender Ausbildung, kurzfristige Unaufmerksamkeit, Fahrlässigkeit oder beruflicher, politischer, persönlicher Belastungen zu menschlichem Versagen führen. Dieser Bereich der Gefährdungsuntersuchung wird weitestgehend mit dem Begriff “Human Factors” oder „Human Errors“ assoziiert. Einen sehr guten Überblick und detaillierte Untersuchungen im Bereich der Psychologie des sicheren Handelns liefert [BS08].

In den folgenden drei Unterabschnitten werden die drei Sicherheitsstrategien Gefahrenvermeidung, Gefahrenabwehr und Auswirkungsminderung anhand von kurzen Beispielen erläutert.

3.4.2 Gefährdungsverhinderung als Gefahrenvermeidung

Abbildung 3.11 zeigt die Implementierung einer Sicherungsfunktion, die bei intakter Funktion einen Ausfall der korrekten lokalen Systemfunktionalität erkennt und durch geeignete Maßnahmen in einen sicheren Ausfallzustand (hier Fail-Safe) überführt. Durch Instandsetzungsmaßnahmen wird die korrekte lokale Systemfunktionalität wieder hergestellt, ohne dass der globale sichere Systemzustand in den gefährlichen wechselt. Zu

berücksichtigen sind bei dieser Forderung der betrachtete Systemaufbau und die Funktionsstruktur des Systems. Für die erforderliche Systemsicherheit ist es nicht ausreichend einzelne (Teil-)Systeme diesem Sicherheitskonzept zu unterstellen, sofern sie einem Gesamtsystem unterliegen. Selbst bei jeweils fehlerfrei (im Sinne eines "lokalen" Sicherheitskonzeptes) arbeitenden Systemen können fehlerhafte Systemeingaben zu Fehlfunktionen aus dem Gesamtsystem führen und schwerwiegende Gefahrenzustände hervorrufen und katastrophale Folgen nach sich ziehen. Erst ein vollständiges "globales" Sicherheitskonzept auf Gesamtsystemebene unter Berücksichtigung der jeweiligen Teilfunktionen kann gefährliche globale Systemzustände ausschließen, bzw. deren Eintrittswahrscheinlichkeit auf ein akzeptables Maß reduzieren. Dies erfordert eine umfangreiche Analyse der Funktionen und Funktionsabhängigkeiten innerhalb eines Systems sowie eine genaue Kenntnis der jeweilig möglichen intakten und nicht-intakten Zustände, um das Systemverhalten durch so geartete Sicherungsfunktionen entsprechend zu beeinflussen bzw. zu steuern. Der Zusammenhang zwischen dem lokalen und globalen Systemverhalten ist dabei essenziell (vgl. Unterabschnitt 3.2.2).

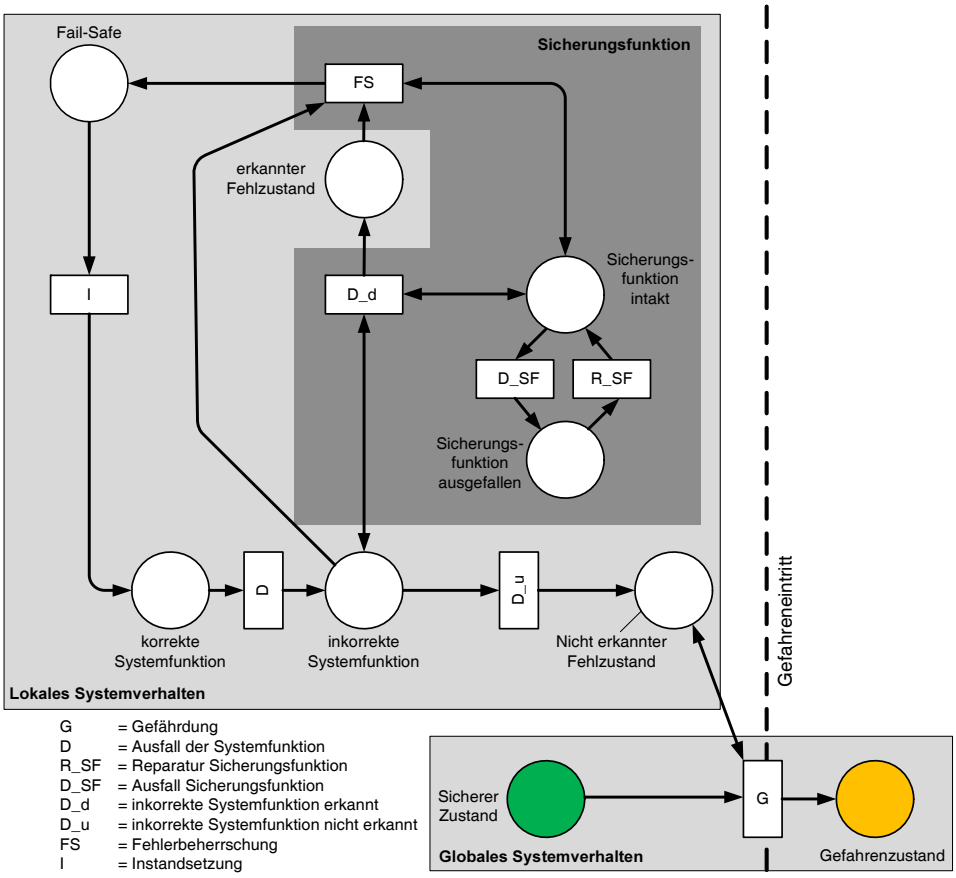


Abbildung 3.11: Sicherheitsimplementierung durch Vermeidung von Gefahren

Ein ausschließliches Vertrauen auf die vollständige Gefahrenvermeidung ist allerdings bei steigender Komplexität ggf. nicht ausreichend. Eine gewisse Eintrittswahrscheinlich-

keit von möglichen Gefahrenzuständen ist somit anzunehmen. Im folgenden Unterabschnitt wird das Eintreten von Gefahrenzuständen mit einer gewissen Wahrscheinlichkeit angenommen und der Fokus auf die Vermeidung des Schadenseintritts durch eine gezielte Gefahrenabwehr gerichtet.

3.4.3 Gefahrenabwehr

Abbildung 3.12 zeigt diesbezüglich den bereits eingetretenen globalen Gefahrenzustand, der potenziell zu einem Schaden führen kann. Implementierte Sicherungsfunktionen, nach vorgestelltem Sicherheitskonzept, erkennen diesen Gefahrenzustand und übernehmen weiter die Aufgabe schnellstmöglich einen sicheren Globalzustand des Systems wiederherzustellen. Dabei ist die Funktionsfähigkeit des Systems meist von untergeordneter Bedeutung, so dass ein Systemstillstand mit einigen Ausnahmen der angestrebte Zustand im Fehlerfall ist. Systeme wie Flugzeuge im Luftverkehr, Magnetbahnen, aber auch Chemieanlagen sind einige zu nennende Ausnahmen, die durch eine Systemabschaltung aufgrund eines Fehlers nicht grundsätzlich unmittelbar in den Systemstillstand als sicheren Zustand wechseln, sondern durch gezielte Maßnahmen zur Gefahrenabwehr einen sicheren aktiven Ausfallzustand anvisieren, um eine weitere Schadensausbreitung zu vermeiden.

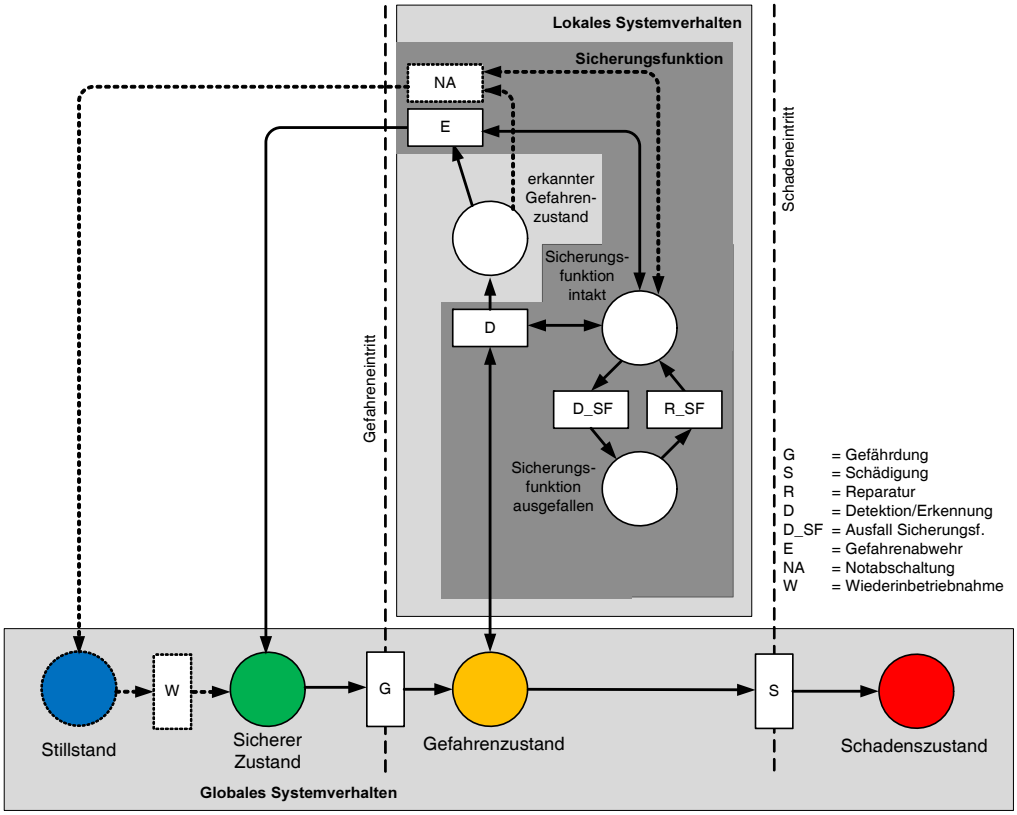


Abbildung 3.12: Sicherheitsimplementierung durch Abwehr von Gefahren

Der globale Systemzustand „Gefahr“ kann jedoch sehr vielfältig sein und bedarf einer ausführlichen Gefahrenidentifikation, die sich beispielsweise auf die Erkennung von gefährlichen Konstellationen lokaler Zustände konzentrieren kann. Bei einer unvollständigen Gefahrenidentifikation ist die Möglichkeit begrenzt, auf existente Gefahren gezielt zu reagieren, so dass bei Vernachlässigung der zufälligen Risikoreduktion, z.B. menschliche intuitive Reaktionen, ein Schadenseintritt unumgänglich wäre. Sicherheitsimplementierungen, die auf dem Prizip der Gefahrenabwehr aufsetzen, sind jedoch grundsätzlich geeignet existente Gefahrenzustände durch nicht beherrschte lokale Fehlfunktionen z.B. über erkannte eingetretende Gefährdungen gezielt zu erkennen und abzuwehren, bevor der Schadenszustand über die Schädigung eintritt.

3.4.4 Auswirkungsminderung

Die implementierte Auswirkungsverminderung kann als passive oder aktiv risikoreduzierende Maßnahme verstanden werden, die zwar einerseits die Häufigkeit der Schadensfälle nicht reduziert, die Schwere der Schäden aber zu mindern bestrebt sind. Abbildung 3.13 zeigt eine Sicherungsfunktion, die den globalen Gefahrenzustand erkennt und durch geeignete Maßnahmen den **nicht zu vermeidenden** Schaden in seiner Ausprägung reduziert.

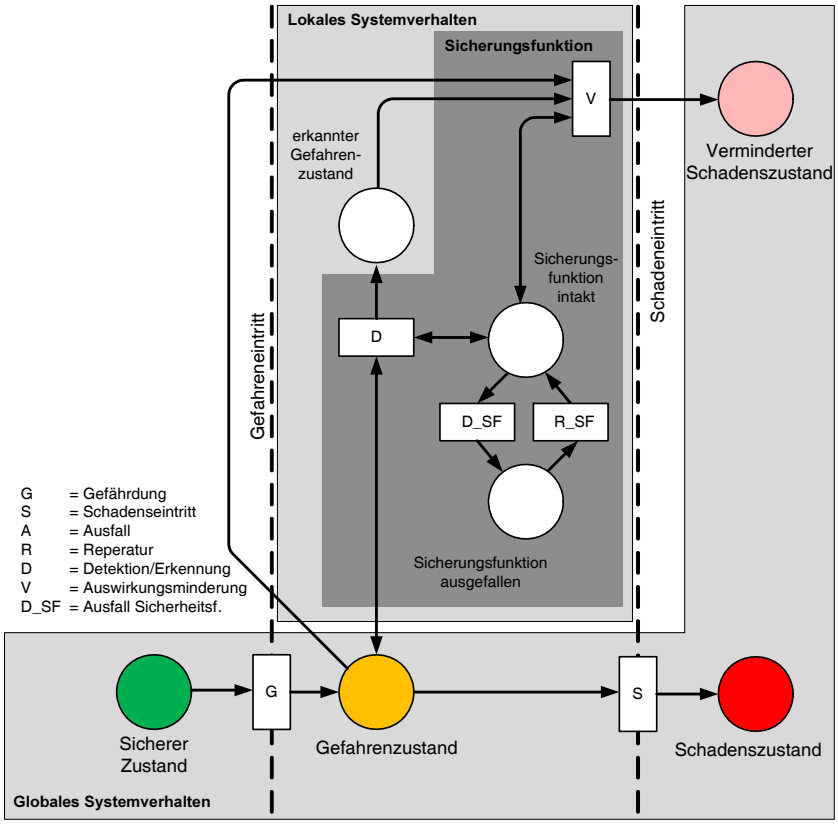


Abbildung 3.13: Sicherheitsimplementierung durch Auswirkungsminderung

Bei nicht intakter Sicherungsfunktion wäre eine Schadensreduzierung nicht möglich. Eine so geartete Sicherheitsimplementierung ist dazu geeignet auf Gefahrenzustände zu reagieren, die z.B. nicht selbstbestimmt sind, sondern i.d.R. durch andere Systeme oder Systemnutzer zu verantworten und nicht abzuwehren sind. Beispiele dafür sind drohende Unfälle im Straßenverkehr, bei denen die Hauptverantwortung beim Systemnutzer liegt und eine Vermeidung des Schadenseintritts ausschließlich durch eine vollständige Übernahme der Verantwortung durch das System zu realisieren wäre.

Historisch gesehen sind diese Systeme die klassischen Sicherheitssysteme, die vorwiegend ihre Anwendung als passive Systeme fanden, um einem möglichen Ausfall der Sicherungsfunktion entgegenzuwirken. Vorwiegend in der Automobilbranche wurden diese Systeme unter der Bezeichnung „Passive Sicherheit“ implementiert. Dazu zählt u.a. die Einführung der Knautschzone als passives System, während die Einführung von Airbags als aktiv reagierendes System zu nennen ist. Beide Systeme können einen Gefahrenzustand nicht abwehren und lediglich das Ausmaß der Schäden reduzieren.

3.5 Entwicklung und Umsetzung von Sicherungsimplementierungen

Bei der Planung und Realisierung von Implementierungskonzepten kann zwischen technischen systembezogenen und nicht-technischen prozessbezogenen Lösungen unterschieden werden. Während die technischen Lösungen zur Implementierung sich auf das System/Produkt selbst konzentrieren, zielen die nichttechnischen Lösungen auf die „sichere“ System-/Produktentstehung, vom ersten Konzept über die Inbetriebnahme sowie darüber hinaus bis zur Entsorgung, ab. Die technischen Realisierungen beinhalten dabei sowohl konstruktive als auch prozessorientierte Lösungen des Systems.

Die unterschiedlichen Sicherungsimplementierungskonzepte können entsprechend ihrer Prüfbarkeit/Nachweisbarkeit der „Gefährlichkeit“ eingeordnet werden. Während der Zustand und das (gefährliche) Systemverhalten von einfachen Systemen auch größtenteils nach Fertigstellung des Systems in der Regel zerstörungsfrei oder durch Prüfmuster prüfbar sind, lassen sich eine sicherheitsgerichtete Struktur oder spezifizierte Sicherungsfunktionen, die ein sicheres Teilsystemverhalten beschreiben, bei komplexen Systemen (z.B. elektronische Systeme) nur schwer nachträglich ohne die Nachvollziehbarkeit des vollständig dokumentierten „sicheren“ Entwicklungsablaufes beurteilen.

Aus diesem Grund wird die Strategie der Sicherungsimplementierungen hier in *Technische Sicherheit* im Sinne der Produktsicherheit und *Technisch Funktionale Sicherheit* im Sinne einer prozessorientierten Entwicklungssicherheit unterschieden. Zusätzlich kann, als weiteres Beispiel für nicht-technische Realisierungen, die *betrieblich-regulatorische Sicherheit*, die sich primär auf Gesetze, Verordnungen sowie Regularien und Handbücher stützt und teilweise umgangssprachlich auch als „Papierverschluss“ bezeichnet wird, die beiden Implementierungsstrategien erweitern, soll aber hier aufgrund der nur bedingten Zuverlässigkeit dieser Maßnahmen und der vorwiegend technischen Ausrichtung dieser

Arbeit nicht weiter betrachtet werden.

3.5.1 Technische Sicherheit - Produktsicherheit

Im Allgemeinen wird unter dem Begriff der *Technischen (Produkt-)Sicherheit* die Unwahrscheinlichkeit des Auftretens einer Gefahr durch die gefährlichen Eigenschaften eines technischen Systems verstanden. Dabei steht die strukturelle und konstruktive Gestaltung des Produktes meist im Vordergrund. In die Bereiche der Technischen Sicherheit fallen u.a. Vorschriften und Verordnungen wie z.B. die europäische Maschinenrichtlinie 2006/42/EG [Eur06] oder nationale Betriebssicherheitsverordnungen [Bun02]. Die europäischen Mitgliedsstaaten haben sich gemäß Artikel 26 der Maschinenrichtlinie verpflichtet, Rechtsvorschriften zur nationalen Umsetzung der Richtlinie bis zum 29. Juni 2008 zu erlassen und zu veröffentlichen. Eine Übergangsfrist bis zur abschließenden Anwendung der nationalen Vorschrift, also der künftigen Maschinenverordnung, ist ab dem 29. Dezember 2009 vorgesehen.

Grundsätzlich spielen bei den genannten Verordnungen unmittelbare Kriterien, wie eine mögliche Gesundheitsgefahr durch Giftstoffe, das Verletzungsrisiko durch eine unvorteilhafte Bauweise (z.B. scharfe Kanten) oder durch unsachgemäße Bedienung (z.B. eine ggf. erforderliche Zweihandbedienung bei Werkstattmaschinen) eine vordergründige Rolle. Ein besonderes Augenmerk bei der Betrachtung der technischen (Produkt-) Sicherheit liegt zudem auf der Produkthaftung, die im Falle einer Nichteinhaltung der geltenden Richtlinien und Vorschriften negative finanzielle und rechtliche Folgen für das produzierende Unternehmen haben kann. Die Folge sind u.a. Rückrufe und Schadensersatzforderungen in zum Teil beträchtlichem Ausmaß.

Jede in Verkehr gebrachte Maschine muss die grundlegenden Sicherheits- und Gesundheitsanforderungen erfüllen. Diese werden ebenfalls im Anhang der Maschinenrichtlinie beschrieben und umfassen zum Teil harmonisierte Normen. Sind allerdings keine harmonisierte Normen vorhanden, können auch nationale Normen herangezogen werden. Maßgeblich sind aber die grundlegenden aufgeführten Anforderungen, die auch auf andere Weise erfüllt werden können.

Jeder Hersteller muss prüfen, ob neben der Maschinenrichtlinie auch andere Richtlinien zu berücksichtigen sind, wie z.B. die Niederspannungsrichtlinie oder die EMV-Richtlinie (Elektromagnetische Verträglichkeit). Diese Einhaltung der Richtlinien (Konformität) muss der Hersteller einer Maschine vor dem in Verkehrbringen nachweisen und kennzeichnen.

Ein weit bekanntes Merkmal zur Kennzeichnung der Einhaltung dieser Verordnungen ist das CE-Zeichen:

Abbildung 3.14: CE-Kennzeichen

CE steht für Communautes Européennes (Europäische Gemeinschaft). Jede Maschine, die nach dem 1.1.1995 in der EU in Verkehr gebracht wird, muss mit dem CE-Zeichen versehen werden. Das CE-Zeichen zeigt, daß der Hersteller für die Maschine eine Konformitätserklärung abgegeben hat, bei besonders gefährlichen Maschinen (siehe Anhang IV der EG-Maschinenrichtlinie) zusätzlich eine EG-Baumusterprüfung von einer benannten Stelle durchzuführen lassen hat, zumindest noch so lange, bis harmonisierte Normen für diese Maschinen von der EG verabschiedet werden.

Die Vorraussetzung für die Kennzeichnung ist die technische Dokumentation, die unter anderem einen s.g. "Sicherheitstechnischen Steckbrief" enthält, der einer Analyse möglicher Gefahren und deren Vermeidung gleichkommt und eine Aufstellung der geltenden Anforderungen aus EU-Richtlinien, relevanten harmonisierten und nationalen Normen und technischen Spezifikationen enthält. Zusätzlich ist eine Gegenüberstellung der getroffenen Maßnahmen zur Erfüllung dieser Anforderungen erforderlich.

Die Umsetzung der Sicherheit bzw. die Abwehr möglicher erkannter Gefahren hat gemäß der Gesetzgebung mit unterschiedlichen Prioritäten zu erfolgen. Erkannte Gefahren müssen in erster Instanz konstruktiv vermieden werden, d.h. der gefährliche Zustand des Systems ist auszuschließen (vgl. Gefahrenvermeidung). Sollte jedoch dieser gefährliche Zustand z.B. aufgrund von negativen funktionalen Einschränkungen (Vermeidung rotierender Teile bei einer Drehmaschine) nicht sinnvoll realisierbar sein, ist eine Schutzvorrichtung im Sinne einer Isolation vorzusehen, um eine unmittelbare Gefährdung des Menschen zu vermeiden (vgl. Gefahrenabwehr). Erst wenn auch diese Sicherheitsmaßnahme nicht ausreichend realisierbar ist, kann durch entsprechend ausgelegte Kennzeichungen, Warnschilder und Anleitungen etc. auf die existente Gefahr beim Anwender hingewiesen werden. Dabei gilt die Unterscheidung zwischen informeller (Information, Warnung) und physikalischer (Schutzeinrichtung) Einflussnahme.

Für die meisten Produkte ohne komplexen Sicherheitsbezug ist diese Art der Gefahrenbetrachtung und Umsetzung der Sicherheit ausreichend. Die Sicherheit der Produkte wird in der Regel durch intensive Tests und Prüfverfahren nachzuweisen versucht. Dazu werden zum einen umfangreiche Testfälle spezifiziert, mit dem Ziel gefährliche lokale Zustände künstlich zu erzeugen und damit das sichere Verhalten des Gesamtsystems (Überführung des Systems in einen sicheren Zustand - Gefahrenabwehr) zu bestätigen und zum anderen Bedientests mit Prüfkörpern (z.B. Dummies) durchgeführt, um während der gesamten spezifizierten Bedienung ein Verlassen des sicheren globalen Zustands bzw. das Erreichen eines inakzeptablen Schadenszustands (Auswirkungsminderung) ausschließen zu können. Diese Bedientests schließen oft auch offensichtliche Fehlbedienungen mit ein.

Der Schwerpunkt liegt dabei vorwiegend beim Testen und lässt sich grundlegend an einem einfachen Entwicklungsprozess veranschaulichen. Der in Abbildung 3.15 dargestellte Entwicklungsprozess, der auch als Wasserfallmodell bekannt ist, beinhaltet die Betrachtung von Sicherheitsanforderungen während der Anforderungs- und Analysephase, um auch aus wirtschaftlichen Gesichtspunkten ein „sicheres“ Produkt nach den Forderungen der Produktsicherheit zur Vermeidung von Produkthaftungen zu entwickeln. Diese Anforderungen basieren auf einer gewünschten Funktionalität und beschreiben grundsätzliche sicherheitstechnische Belange, die das Produkt bei der Auslieferung erfüllen soll. Die

sicherheitsrelevanten Anforderungen stützen sich allerdings meist auf die Gefahrenbetrachtung des Produktes im direkten Kontakt mit den potenziell Geschädigten. Beispiele für potenzielle Risiken sind Gefahren mit dem Potenzial für Verbrennungen, Klemmen, Quetschen und Verletzungen aufgrund beweglicher Teile, chemische, biologische oder elektrische Schädigung von Systemnutzern. Auffällig ist hierbei das ausschließlich abschließende Testen des implementierten Produkts. Überprüfungen von systeminternen Verhalten oder die Validierung von internen Teilfunktionen bzw. die Verifikation der Anforderungsverfolgung oder der durchgeführten Gefährdungsanalysen, die sich überwiegend nicht vollständig im Nachherein realisieren lassen, bleiben zum großen Teil unberücksichtigt.

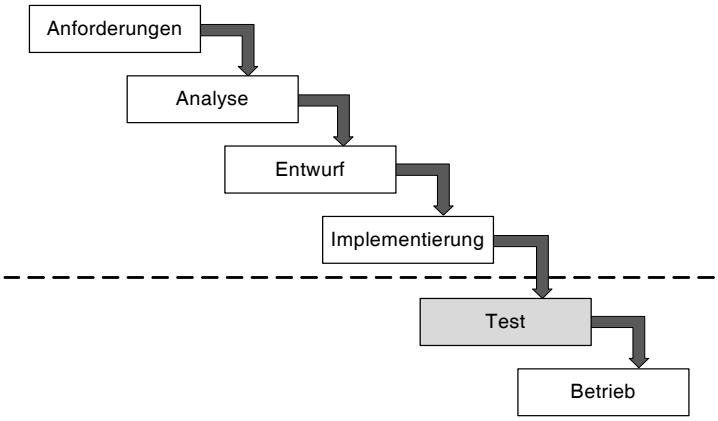


Abbildung 3.15: Phasenorientierter Entwicklungsprozess

Fraglich bleibt aus diesem Grund, insbesondere für komplexe Systeme, ob durch die alleinige Konzentration auf einen ungefährlichen äußerlichen Zustand bei Auslieferung und ein offensichtlich unbedenkliches Verhalten, sowie eine konstruktiv und materiell unbedenkliche Beschaffenheit eine indirekte Gesundheitsgefährdung aufgrund systematischer bzw. funktionaler Fehler ausreichend ausgeschlossen werden kann. Die Gewährleistung einer ausreichenden Sicherheit für einen Betreiber / Anwender ist nicht möglich bzw. eine Wahrscheinlichkeit in dem sicheren Zustand zu verweilen kann nicht garantiert werden.

Ein komplexes System mit direkter Sicherheitsverantwortung, z.B. ein Stellwerk zum Stellen und Sichern der Fahrwege im Schienenverkehr, das nach diesen Richtlinien geprüft würde, kann zwar mit ausreichender Wahrscheinlichkeit direkte Schäden (z.B. Körperschluss am Bediener) ausschließen und wird auch mit großer Wahrscheinlichkeit adäquat auf zufällige vor allem zuverlässigkeitsbedingte Fehler reagieren können, schließt aber die systematische Betrachtung unzulässiger Systemzustände wie z.B. falsch projektierte Signalstellungen und damit die Möglichkeit einer Zugkollision oder Entgleisung sowie Softwarefehler aufgrund fehlerhafter Systemeingaben oder systematischer Fehler nicht grundsätzlich mit ein.

Durch die gesteigerte Komplexität der Systeme ist eine pragmatische Analyse der Systemfunktionaliät und damit die ausreichende Berücksichtigung sämtlicher Systemgefahren allein durch abschließendes Testen nicht mehr möglich. Aus diesem Grund sind

systematische zum Teil formale Beschreibungsmittel, Methoden und Werkzeuge erforderlich, die eine gezielte Analyse der Sicherheit/Gefährdungen unter Berücksichtigung der Funktionalität in Verbindung mit sämtlichen möglichen und denkbaren Fehlern, bereits während der Entwicklung, ermöglichen. Auf diese Weise werden bereits während der Entwicklung erkannte potenzielle Gefahren durch sichere Strukturen bzw. durch zu implementierende Sicherungsfunktionen systematisch berücksichtigt, vermieden oder beherrscht. Allgemein ist dieses unter der Bezeichnung "Funktionale Sicherheit" bekannt.

3.5.2 Technisch Funktionale Sicherheit - Entwicklungssicherheit

Ziel der Funktionalen Sicherheit ist es, Systeme und Teilsysteme für sicherheitskritische Anwendungen zu entwickeln, die für den zu kontrollierenden/steuernden Prozess angemessen sind und das Gesamtsystem unter Einbezug der jeweiligen Umwelt während des gesamten Lebenszyklus ausreichend sicher gestalten. Dabei werden die Maßnahmen und Methoden der Technischen (Produkt-)Sicherheit durch zusätzliche Schritte erweitert. Unter den Begriff: Funktionale Sicherheit fällt u.a. der eng verknüpfte Begriff der Zuverlässigkeit, der als "Funktionieren unter allen Bedingungen" in [Bör06] definiert wird. Aufgrund der bereits erwähnten Komplexität vieler Systeme und dem unumgänglichen natürlichen Zerfall von Bauteilen ist eine vollständige Zuverlässigkeit jedoch nicht möglich. Während sich zufällige Bauteilausfälle, z.B. durch Redundanzen, beherrschen lassen, stellt die Behandlung von systematischen Fehlern in Softewaresystemen einen weitaus höheren Anspruch und erfordert in der Regel ein systematisches strukturiertes Vorgehen, die Verwendung von angemessenen Methoden, Beschreibungsmitteln oder Werkzeugen sowie ggf. den Einsatz diversitäter Systeme (sowohl SW als auch HW-Diversität). Gerade systematische Fehler in Softwarefunktionen können nicht vollständig ausgeschlossen werden und stellen ein erhöhtes Potenzial dar, ein systematisches Fehlverhalten zu ermöglichen. Trotz begrenzter Zuverlässigkeit und den daraus ggf. resultierenden Fehlern kann ein System dennoch als sicher gelten, solange es auch unter diesen Umständen keine Gefahren erzeugt bzw. die Wahrscheinlichkeit der Gefahren innerhalb akzeptabler Grenzen liegt und dieses Verhalten nachweisbar ist.

Der Lebenszyklus von Systemen (Abbildung 3.16 zeigt ein Beispiel der Softwareentwicklung) und der daraus resultierende Entwicklungsprozess stehen bei der Funktionalen Sicherheit aus diesem Grund im Mittelpunkt. Sicherheitsgerichtete Systeme erfordern die Einhaltung besonderer Sicherheitsanforderungen, die auf funktionale und nicht-funktionale Anforderungen aus der Systementwicklung aufbauen, um einen sicheren Zustand während eines definierten Prozesses im Fehlerfall schnellstmöglich einzunehmen. Die Analyse und Erfüllung dieser Anforderungen wird in der Regel in einem gesonderten beweisähnlichen Dokument während der Entwicklung erfasst, dem s.g. Sicherheitsnachweis. Der Sicherheitsnachweis weist das sichere Verhalten von Systemen bei möglichen Gefährdungen nach. Aus diesem Grund geht in einer Sicherheitsanalyse dem Nachweis der Sicherheit eine umfangreiche entwicklungsbegleitende Risiko-/ und Gefährdungsanalyse voraus. Während die Risikoanalyse das implementierungsfreie Risiko der Applikation/Funktion bestimmt, durch Akzeptanzkriterien dieses auf ein akzep-

tables Maß begrenzt, dadurch die Systemsicherheitsanforderungen definiert, ist das Ziel der Gefährdungsanalyse der Nachweis der Einhaltung dieser Anforderungen durch die beabsichtigte Entwicklung. Gleichzeitig sind während der Gefährdungsanalyse weitere aus der Implementierung resultierende Gefährdungen zu identifizieren und im Rahmen der Risikoakzeptanz zu beherrschen. Die Gefährdungsanalyse liefert folglich zusätzliche Sicherheitsanforderungen für das zu entwickelnde System, die auf den jeweiligen Detaillierungstiefen zu validieren sind. Die zu spezifizierenden Anforderungen werden dabei in funktionale und nichtfunktionale Anforderungen sowie in sicherheitstechnische Anforderungen unterschieden.

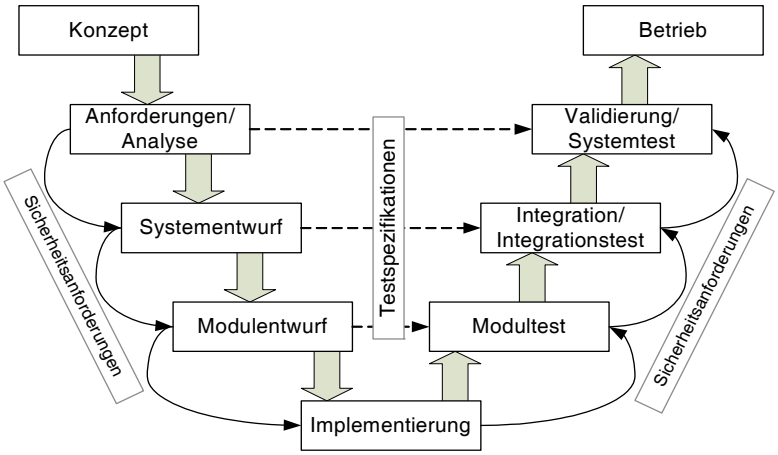


Abbildung 3.16: Entwicklungslebenszyklus sicherer Software-Systeme

Basis dieses sicherheitsgerichteten Vorgehens ist eine anforderungsgestützte Entwicklung, die durch ein geeignetes Anforderungsmanagement und ein geeignetes Sicherheitsmanagement unterstützt wird. Ziel dieser Entwicklung ist die Erfassung und Analyse konsistenter Anforderungen, die in weiteren Entwicklungsschritten verfeinert und konsequent umgesetzt, verifiziert und validert werden.

Dabei findet die Verifikation und Validierung phasenorientiert statt. Die Verifikation als Mittel zur Prüfung der jeweiligen Phasenprodukte auf Vollständigkeit, Konsistenz und Korrektheit gewährleistet einen durchgängigen korrekten Entwicklungprozess, während die Validierung die (Teil-)Produkte gegen die jeweiligen Anforderungen evaluiert. Auf diese Weise lassen sich Anforderungen auf Bauteilebene bereits frühzeitig testen, die ggf. zu einem späteren Zeitpunkt nicht zerstörungsfrei durchführbar wären. Die Durchgängigkeit der Anforderungen auf unterschiedlichen Detaillierungsebenen ist dabei eine Grundvoraussetzung. Gerade im Bezug auf die Implementierung der Sicherheit spielt eine durchgehende Anforderungsverfolgung eine große Rolle, um erkannte Gefährdungen kontrolliert und nachweislich über spezifizierte Anforderungen und folglich über Ressourcen implementierte Funktionen gezielt zu vermeiden.

Je nach Domäne lassen sich dabei unterschiedliche Normen anwenden. Die wohl bekanntesten Normen der Funktionalen Sicherheit sind die IEC 61508 [Deu02] für allgemeine elektrische, elektronische und programmierbare elektrische Systeme sowie die für

Bahnanwendungen geltenden CENELEC Normen EN 50126 [Deu00], EN 50128 [Deu01] und EN 50129 [Deu03b]. Eine gültige Norm zur Funktionalen Sicherheit, explizit für Anwendungen im Automobilbereich, ist in Bearbeitung und derzeit als Entwurf (ISO CD 26262) verfügbar.

4 Verkehrssicherheit als spezifische Systemeigenschaft

Aufbauend auf die detaillierte Analyse der begrifflichen Bestandteile, des Umfangs und der Zusammenhänge um den Begriff *Sicherheit*, sowie der vorgestellten Formalisierung in Verbindung mit Implementierungsansätzen im vorangegangenen Kapitel folgt die Anwendung und Verfeinerung der Erkenntnisse in Bezug auf das System *Verkehr*.

Verkehr als soziotechnisches System wird im Folgenden systematisch analysiert und analog zum Begriffssystem Sicherheit ebenfalls als vereinfachtes Begriffssystem dargestellt. Die Verkehrssicherheit als Eigenschaft des Systems Verkehr versteht sich somit als Konkretisierung der Sicherheit als allgemeine Systemeigenschaft eines generischen Systems.

Die Verkehrssicherheit läßt sich nach den in Kapitel 3 vorgestellten Ansätzen ebenfalls als Begriffssystem darstellen und formalisieren. Folglich lassen sich unterschiedliche Sicherungsimplementierungkonzepte für Verkehrssysteme ableiten.

Das Kapitel gliedert sich in eine allgemeine Interpretation und Darstellung des Verkehrs als Begriffssystem, die begriffliche Konzentration auf die Systemeigenschaft „Verkehrssicherheit“ und die Analyse möglicher Sicherungsimplementierungen im System Verkehr. Abschließend werden konventionelle und neue verkehrsspezifische Sicherheitsmaße vorgestellt.

4.1 Verkehr als Systembegriff

Das System Verkehr kann, wie grundsätzlich alle Systeme, aus unterschiedlichen Perspektiven betrachtet werden. Wird eine rein assoziative und wissensbasierte Betrachtung verfolgt, ergeben sich zwar weitläufig etablierte Definitionen, Umfänge und Geltungsbereiche, die jedoch bei genauerer Betrachtung zum großen Teil nicht auf terminologischen Grundlagen basieren und somit zu Konsistenzproblemen führen können, wie sie ausführlich in Abschnitt 2.3 beschrieben sind.

Die begriffliche Analyse erfolgt nach dem in Abschnitt 2.4 beschriebenen Konstruktionsprinzip in Anlehnung an [Sch02b].

Darauf aufbauend wird in einem weiteren Unterabschnitt, unter Verwendung von geeigneten Beschreibungsmitteln und Systemkonzepten, das System Verkehr sowohl in seiner statischen Struktur als auch in seinem dynamischen Verhalten in Ansätzen formalisiert. Eine ähnliche Vorgehensweise kann auch in [Mül98] betrachtet werden, wenngleich

dort Verkehr u.a. mit ERD (Entitiy Relationship Diagram) systematisch dargestellt wird.

4.1.1 Analyse des Begriffs Verkehr

Dieser Unterabschnitt befasst sich mit der begrifflichen Analyse des Begriffs *Verkehr* unter Verwendung der erweiterten Konstruktionsmethode zur Erstellung von Begriffssystemen aus Abschnitt 2.4. Analog zu der Begriffsanalyse des Begriffs *Sicherheit* wird auch hier erneut mit der Bestandsaufnahme begonnen und über die Bestandsuntersuchung eine Bestandsfestlegung durchgeführt, die in der Darstellung eines Begriffssystems mündet. Der inhaltliche Rahmen beschränkt sich dabei auf die systemorientierte funktionale Sichtweise des Verkehrs und lässt dabei die Unterscheidung zwischen den einzelnen konkreten Verkehrssystemen bewusst außer Betracht. Dabei existiert eine Fülle von Literaturquellen, die jedoch nicht über die Grenzen des jeweiligen Verkehrssystems hinaus gehen und Verkehr isoliert für den einzelnen Verkehrsträger als Begriff verwenden. Ein systemübergreifender Ansatz und die damit verbundene ganzheitliche Fokussierung wird dadurch erschwert. Die Bestandsausfnahme beschränkt sich aus diesem Grund auf die Angabe nur weniger Literaturquellen, wenngleich eine Vielzahl unterschiedlicher Quellen gesichtet wurden.

Bestandsaufnahme: Verkehr

Unabhängig von bereits manifestierten Interpretationen und Definitionen werden in diesem Unterabschnitt zitierte Begriffsbeschreibungen vorgestellt, die zu großen Teilen aus wissenschaftlichen Publikationen oder normativen bzw. regulatorischen Dokumentationen entnommen wurden. Das Ziel dieser Bestandsaufnahme ist die Konzentration auf eine interessierende Begriffsmenge um den zentralen Begriff *Verkehr*.

Verkehr: Prozesse bzw. Vorgänge der Interaktion zwischen verschiedenen sozialen Akteuren; der soziale Umgang zwischen Menschen (z. B. er verkehrt in besseren Kreisen). Im weitesten Sinn gehören dazu: Geschlechtsverkehr, Geschäftsverkehr, Verkehr im juristischen Sinne, Fremdenverkehr im ursprünglichen Sinne des Wortes.
Quelle: Glossar Verkehrswesen [AH06]

Die Ortsveränderung von Objekten (z. B. Güter, Personen, Nachrichten) in einem definierten (Verkehrs-)System.
Quelle: Glossar Verkehrswesen [AH06]

Verkehrssystem: Als Verkehrssystem bezeichnet man eine bestimmte Menge funktionell miteinander verknüpfter Komponenten, welche nach bestimmten Merkmalen aus der Gesamtheit aller im Verkehrswesen vorhandenen Systemelemente abgegrenzt werden. Die Abgrenzung erfolgt z. B. nach räumlichen, zeitlichen, technischen, organisatorischen, politischen, juristischen oder betrieblichen Gesichtspunkten und dient der Vereinfachung des Umgangs mit den komplexen Strukturen des Verkehrswesens. Es gibt offene oder geschlossene Verkehrssysteme. Die isolierte Betrachtung

eines Verkehrssystems unter Vernachlässigung der Systemumgebung kann zu fehlerhaften Schlussfolgerungen führen.
Quelle: Glossar Verkehrswesen [AH06]

Ein Verkehrssystem verkörpert das Zusammenwirken von Verkehrsmitteln zwecks Raumüberwindung von Personen, Gütern und Nachrichten, wobei die Systemkomponenten durch funktionale Zusammenhänge miteinander verknüpft sind, so dass ein komplexes Gebilde aus verschiedenen Verkehrszweigen, Verkehrsmärkten usw. entsteht, auf dem Verkehrsunternehmen mit drei Aktionsparametern auftreten können: Variation von Preis, Menge und Güte von Verkehrsdienstleistungen.
Quelle: Voigt, F. [Voi65]

Verkehrsprozess: Der Begriff Verkehrsprozess (auch Transportprozess, Synonym bzw. Kurzform Verkehr) bezeichnet eine dynamische Aufeinanderfolge verschiedener Zustände eines Verkehrssystems zur meist zielgerichteten und zweckbestimmten Bewegung von Personen, Gütern oder Nachrichten in einem örtlich, zeitlich oder sachlich definierten Raum, i. d. R. unter Zuhilfenahme von Verkehrsmitteln, zwischen einer Verkehrsquelle (Start) und einer Verkehrssenke (Ziel). Der Verkehrsprozess stellt die operative Komponente bzw. die eigentliche Ausführung der am Verkehrsmarkt als Produktions- bzw. Konsumgut gehandelten Verkehrsdienstleistung dar. Die wissenschaftliche Untersuchung und Bewertung des Verkehrsprozesses, z. B. hinsichtlich Verfügbarkeit, Zuverlässigkeit, Ressourceneffizienz, erfolgt mittels besonderer Mess- und Kenngrößen der Verkehrsmaßlehre durch die Verkehrstheorie. Oft synonym verwendet für Fahrt, Reise oder Weg im Personenverkehr oder Transport(-prozess) im Gütertransport. Verkehrsprozesse setzen die Existenz von Verkehrsbedürfnissen, Verkehrsobjekten und Verkehrsmitteln (das Verkehrswesen) voraus und bilden als Gesamtprozess eine Einheit aus Haupt- und Hilfsprozessen. Der Gesamtprozess ist eine Kette aus Teilprozessen, die zeitlich und räumlich nacheinander ablaufen.
Quelle: Glossar Verkehrswesen [AH06]

Personenverkehr: Die allgemeine Bezeichnung für die Ortsveränderung (Beförderung) von Personen umfasst die technischen, technologischen organisatorischen und ökonomischen Erscheinungen der Personenbeförderung und die zu befördernden Personen selbst, einschl. Fußgängerverkehr.
Quelle: Glossar Verkehrswesen [AH06]

Transport: Ein Prozess zur Ortsveränderung von Personen oder Gütern von einem Ort zu einem anderen. Der Begriff beschreibt die räumliche Standortveränderung physischer Transportobjekte mittels verschiedener Verkehrsmittel (je nach Abgrenzung auch als Transportmittel bezeichnet). Im Unterschied hierzu ist der Begriff Verkehr allgemeiner zu verstehen, weil im Verkehrsprozess nicht unbedingt eine physische Sache „hinübergetragen“ werden muss.
Quelle: Glossar Verkehrswesen [AH06]

Verkehrsmittel: Die Verkehrsmittel (je nach Abgrenzung auch Transportmittel) sind

i. w. S. die Gesamtheit der stationären bzw. mobilen sowie der materiellen bzw. immateriellen Arbeits- bzw. Produktionsmittel, welche die Bewegung von Gütern, Personen und Nachrichten ermöglichen und damit als „verkehrswirtschaftliche Produktionsfaktoren“ zur Produktion von Verkehrsdienstleistungen genutzt werden, so z. B. Verkehrsanlagen (insbes. Verkehrsweg, Stationen, Nebenanlagen), mobile Einheiten, wie Zug- und Tragtiere, Flug-, Schwimm- oder Fahrzeuge und Gefäße (Wagen, Schiffe, Luftfahrzeuge, Behälter wie Tanks und Container usw.) einschließlich der zugehörigen Verkehrsobjekte.
Quelle: Glossar Verkehrswesen [AH06]

Die Menge aller Fortbewegungsmöglichkeiten, einschl. Fußgänger und privater motorisierter Verkehr, v. a. im Zusammenhang mit der Verkehrsmittelwahl
Quelle: Verkehrslogistik, Schubert [SS00]

Verkehrsobjekt: Das Verkehrsobjekt ist der Arbeitsgegenstand im Verkehrsprozess. Umfasst bewegliche Sachen, wie Personen (Reisender), Transportgut/Güter (einschließlich Energie), Information (Nachrichten und Daten). Unterscheide Transportobjekt, Nachrichtenverkehrsobjekt.
Quelle: Glossar Verkehrswesen [AH06]

Verkehrsinfrastruktur: Der Begriff Verkehrsinfrastruktur kann folgende Bedeutungen haben: die Menge aller Grundeinrichtungen personeller, materieller und institutioneller Art, welche den Transport von Gütern (Gut), die Beförderung von Personen und die Übertragung bzw. Übermittlung von Nachrichten ermöglichen, also bedeutungsgleich mit Verkehrswegen. Ugs. die Menge der baulichen bzw. ortsfesten Anlagen im Verkehrswesen (Verkehrsanlagen) und damit ein stationäres Produktionsmittel (Verkehrsmittel) zur Produktion von Verkehrsdienstleistungen.
Quelle: Glossar Verkehrswesen [AH06]

Verkehrsweg: Der Verkehrsweg (unterscheide davon Weg) ist für ein für die Nutzung durch Verkehrsmittel reserviertes, teilweise spezialisiertes (ausgebautes), relativ dauerhaft genutztes Raumsegment in verschiedenen Verkehrsmedien zwischen einem Start und einem Ziel, worauf Verkehrsprozesse zum Zwecke einer effektiven und effizienten Ortsveränderung gebündelt und durchgeführt werden. Landverkehr: Pfad, Weg, Straße; Schifffahrt: Seeweg, Binnenwasserstraße; Luftverkehr: Luftstraße bzw. Luftverkehrskorridor.
Quelle: Glossar Verkehrswesen [AH06]

Verkehrsorganisation: Die Verkehrsorganisation wird - individuell und aktuell - von menschlichen Verkehrsmittelführern (Fahrer, Pilot) und Weisungspersonal (Polizei, Ordnungskräfte) oder von technischen Einrichtungen wie Autopilot, Fahrerassistenzsystemen, Lichtsignalanlagen oder Stellwerken wahrgenommen und ausgeführt. Die jeweilige Implementierung der Verkehrsorganisation (Prozess) kann innerhalb der drei Klassen (Ressourcen) Verkehrswegeinfrastruktur, Verkehrsmittel oder Verkehrsobjekte durchgeführt werden.
Quelle: Verkehrsleittechnik [Sch07]

Verkehrsqualität: Verkehrsqualität ist die Gesamtheit von Merkmalen der Verkehrsdienstleistung bezüglich ihrer Eignung, festgelegte und vorausgesetzte Anforderungen des Nutzers zu erfüllen. Die Verkehrsqualität lässt sich mittels der Verkehrswertigkeit eines Verkehrssystems ermitteln, indem den dort aufgeführten Dienstleistungseigenschaften die entsprechenden Anforderungen des Nutzers gegenübergestellt werden. Im Gegensatz zur Verkehrsaffinität ist die Verkehrsqualität eine operative Größe zur Bewertung einer bestimmten Verkehrsdienstleistung. Gütekriterien für die Verkehrsqualität können z. B. sein:

- Sicherheit - das Risiko der aus der Verkehrsqualität resultierenden Gefahren bleibt bei Berücksichtigung von Wirtschaftlichkeit und Leistungsfähigkeit (Sicherheit vs. Verfügbarkeit) unter einer gewissen Toleranzgrenze (Verkehrssicherungswesen)
- Wirtschaftlichkeit - der ökonomische Nutzen des Verkehrs bleibt gewahrt, Renditeerwartungen sollten mit der Sicherheit abgewogen werden
- Leistungsfähigkeit - die meisten Verkehrsbedürfnisse können unter Berücksichtigung von Sicherheit und Wirtschaftlichkeit durch das Verkehrssystem befriedigt werden
- Nachhaltigkeit - das Verkehrssystem fügt sich in seine natürliche und anthropogene Umgebung möglichst harmonisch ein, ohne ungewollte direkte und indirekte Nebenwirkungen (Ressourcenbedarf, Umweltschäden, Sozialkonflikte) in andere Räume und Zeiten zu verlagern sowie unter Berücksichtigung kultureller, ethischer bzw. sozialer Standards des jeweils beeinflussten Gemeinweisens.

Während Sicherheit, Wirtschaftlichkeit und Leistungsfähigkeit im Verkehr allgemein anerkannte Gütekriterien sind, wird die Forderung nach Nachhaltigkeit gegenwärtig insbes. in Verkehrswissenschaft und Verkehrspolitik erhoben.
Quelle: Glossar Verkehrswesen [AH06]

Verkehrszustand: Der Verkehrszustand (Verkehrsstromzustand) ist die Summe aller Eigenschaften, die einen Strom aus sich bewegenden Objekten charakterisieren, so z. B. Art und Häufigkeit des Auftretens: stochastischer oder deterministischer Massen- oder Einzelverkehr. Gegenseitige Beeinflussung der Verkehrsobjekte: freier Verkehr, teilgebundener Verkehr, gebundener Verkehr, gestauter Verkehr.
Quelle: Glossar Verkehrswesen [AH06]

Bestandsuntersuchung: Verkehr

Die Bestandsaufnahme aus dem vorangegangenen Abschnitt zeigt lediglich einen Ausschnitt des möglichen Umfangs und Inhalts des Begriffs Verkehr und repräsentiert die interessierende Begriffsmenge. Ziel der Bestandsuntersuchung ist die Einordnung und Abgrenzung dieser in Teil- und Unterbegriffe über die kontextbezogene Analyse. Gleichzeitig werden dabei nicht relevante Begriffe entfernt und Relationen zu anderen Begriffen kontextbezogen beschrieben.

Analyse der nicht-sprachlichen Kontexte

Die einzelnen Inhalte und Umfänge der jeweiligen Begriffe werden in Tabelle 4.1 bis Tabelle 4.3 für jeden Begriff einzeln aufgeführt. Die aufgeführten Unter- und Teilbegriffe sind nur exemplarisch und keinesfalls vollständig erfasst worden. Die Auswahl fiel auf die, aus Sicht des Autors, wichtigsten Begriffe zur Klärung des Umfangs und Inhalts des jeweiligen Begriffs.

Tabelle 4.1: Nicht-sprachliche Begriffskontexte zum Verkehr

Verkehr	
Unterbegriffe	Teilbegriffe (Merkmale)
Personenverkehr	Verkehrsprozessqualität
Güterverkehr	Verkehrsqualität
Datenverkehr	Verkehrssicherheit
Verkehrssystem	
Unterbegriffe	Teilbegriffe (Merkmale)
Personenverkehrssystem	Verkehrssystemstruktur
Güterverkehrssystem	Verkehrssystemqualität
	Verkehrssystemsicherheit
Verkehrsmittel	
Unterbegriffe	Teilbegriffe (Merkmale)
Fahrzeuge	Kapazität für Verkehrsobjekte
Zug-, Tragtiere	Geschwindigkeit, Reichweite
Fußgänger	Instandhaltbarkeit
	Zuverlässigkeit

Tabelle 4.2: Nicht-sprachliche Begriffskontexte zum Verkehr (Fortsetzung 1)

Verkehrsobjekt	
Unterbegriffe	Teilbegriffe (Merkmale)
Reisender	Vulnerabilität
Transportgut/Güter	Wert
Informationen/Daten	Verderblichkeit
Energien	Dringlichkeit
Verkehrinfrastruktur	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrsweg	Kapazität für Verkehrsmittel
Verkehrsanlagen	Zuverlässigkeit
	Instandhaltbarkeit
Verkehrsorganisation	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrslenkung	Automatisierungsgrad
Verkehrsleittechnik (VLT)	
Verkehrssicherung	Leistung
Verkehrsregelung	Verfügbarkeit
Verkehrsüberwachung	
Verkehrsprozess	
Unterbegriffe	Teilbegriffe (Merkmale)
Transportprozess	Prozessdauer
Fahrt	Prozessqualität
Reise/Weg	Prozesseffizienz
Transport	
Unterbegriffe	Teilbegriffe (Merkmale)
Peronentransport	Transportqualität
Gütertransport	Transportdauer
Datentransport	Transportkosten
Energietransport	

Tabelle 4.3: Nicht-sprachliche Begriffskontexte zum Verkehr (Fortsetzung 2)

Verkehrsqualität	
Unterbegriffe	Teilbegriffe (Merkmale)
Personenverkehrsqualität Güterverkehrsqualität	Verkehrssicherheit Verkehrswirtschaftlichkeit Verkehrsleistungsfähigkeit Verkehrsnachhaltigkeit
Verkehrzustand	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrsstromzustand	Verkehrsverfügbarkeit Verkehrssicherheit Verkehrsdichte (z.B. Staugrad) Verkehrsstärke

Analyse der begrifflichen Relationen

Werden die in der Bestandsaufnahme ermittelten sprachlichen Kontexte und die im vorangegangenen Unterabschnitt ermittelten nicht-sprachlichen Kontexte der Begriffe betrachtet, ergeben sich bereits verschiedene Bezüge zwischen einzelnen Begriffen auf Merkmalsebene, lassen aber weitere Relationen offen, die in diesem Abschnitt analysiert werden.

„Verkehr“ wird im klassischen Sinn durch ein „Verkehrssystem“ umgesetzt/produziert (i.w.S. Genetizität r_2). Gleichzeitig wird das „Verkehrssystem“ durch die Art des Verkehrs geprägt. Wird beispielsweise der schienengebundene Verkehr betrachtet, prägen diverse Eigenschaften und Merkmale dieser Verkehrsart das „Verkehrssystem“ (i. w. S. Genetizität r_1). Aufgrund der Annahme, dass „Verkehr“ als generischer Begriff für die Umsetzung von Verkehrs-/Transportprozessen verstanden werden kann, kann daraus eine partitive Relation zwischen den Begriffen „Verkehr“ und „Transport“ (Meronymie r_{17}) abgeleitet werden. Der „Transport“ ermöglicht die Ortsveränderung von „Verkehrsobjekten“ (Assoziation r_{18}), die zu diesem Zweck die „Verkehrsmittel“ nutzen (Assoziation r_8) und den „Verkehr“ charakterisiert (Assoziation r_{16}). Die „Verkehrsmittel“ wiederum nutzen die „Verkehrsinfrastruktur“ (Assoziation r_{11}). In umgekehrter Betrachtungsrichtung trägt die „Verkehrsinfrastruktur“ die „Verkehrsmittel“ (Assoziation r_{12}), welche „Verkehrsobjekte“ transportieren (Assoziation r_{15}). Sowohl „Verkehrsobjekte“, „Verkehrsmittel“ als auch die „Verkehrsinfrastruktur“ und der „Transport“ an sich werden in ihrem Verhalten vom „Verkehrsprozess“ (Assoziationen r_{20}, r_{23}, r_{21} und r_{19}) geprägt. Die Ausprägung des „Verkehrsprozesses“ bzw. des darin enthaltenen „Trans-

portprozesses“ definiert gleichzeitig den „Transport“ als Begriff (Assoziation r_{22}). Des Weiteren beeinflusst der Prozess den „Verkehrszustand“ und die „Verkehrsqualität“ mit ihrer Merkmalsmenge (Assoziationen r_{27} und r_{24}) die beide ebenfalls in einer assoziativen Relation zueinander stehen (r_{26}). Die „Verkehrsqualität“ beschreibt dazu qualitativ die Auswirkungen des „Verkehrsprozesses“ (Assoziation r_{25}). Der „Verkehrsprozess“ hingegen wird durch die „Verkehrsorganisation“ gesteuert bzw. geregelt (Assoziation r_7). Die einzelnen Verkehrskonstituenten „Verkehrsobjekt“, „Verkehrsmittel“ und „Verkehrsinfrastruktur“ werden durch die „Verkehrsorganisation“ beeinflusst (Assoziationen r_5, r_9 und r_{13}) und organisieren damit den „Verkehr“ (Assoziation r_4). Folglich realisiert das „Verkehrssystem“ durch die Implementierung der Organisationsfunktionen die „Verkehrsorganisation“ (Genetizität r_3) indem die Konstituenten „Verkehrsobjekt“, „Verkehrsmittel“ und/oder „Verkehrsinfrastruktur“ als Funktionsträger agieren (Genetizität r_6, r_{10} und r_{14}). Eine tabellarische Zusammenfassung der beschriebenen Relationen wird in Tabelle 4.4 sowie in Tabelle 4.5 dargestellt.

Tabelle 4.4: Darstellung direkter Relationen der verkehrsrelevanten Begriffsmenge

		Senke									
		Verkehr	Verkehrssystem	Verkehrsmittel	Verkehrsobjekt	Verkehrsinfrastruktur	Verkehrsorganisation	Verkehrsprozess	Transport	Verkehrsqualität	Verkehrszustand
Quelle	Verkehr	X	r_1	-	-	-	-	-	r_{17}	-	-
	Verkehrssystem	r_2	X	-	-	-	r_3	-	-	-	-
	Verkehrsmittel	-	-	X	r_{15}	r_{11}	r_{10}	r_{23}	-	-	-
	Verkehrsobjekt	-	-	r_8	X	-	r_6	r_{20}	-	-	-
	Verkehrsinfrastruktur	-	-	r_{12}	-	X	r_{14}	r_{21}	-	-	-
	Verkehrsorganisation	r_4	-	r_9	r_5	r_{13}	X	r_7	-	-	-
	Verkehrsprozess	-	-	-	-	-	-	X	r_{22}	r_{24}	r_{27}
	Transport	r_{14}	-	-	r_{18}	-	-	r_{19}	X	-	-
	Verkehrsqualität	-	-	-	-	-	-	r_{25}	-	X	-
	Verkehrszustand	-	-	-	-	-	-	-	-	r_{26}	X

Tabelle 4.5: Relationen der verkehrsrelevanten Begriffsmenge im Detail

Relation	Relationsbenennung	Relationsart	math. Relation
r_1	prägt	Genetizität	transitiv
r_2	setzt um	Genetizität	transitiv
r_3	realisiert	Genetizität	transitiv
r_4	organisiert	Assoziation	-
r_5	beeinflusst	Assoziation	-
r_6	kann umsetzen	Genetizität	transitiv
r_7	regelt, steuert	Assoziation	-
r_8	nutzt	Assoziation	-
r_9	beeinflusst	Assoziation	-
r_{10}	kann umsetzen	Genetizität	transitiv
r_{11}	nutzt	Assoziation	-
r_{12}	trägt,leitet	Assoziation	-
r_{13}	beeinflusst	Assoziation	-
r_{14}	kann umsetzen	Genetizität	transitiv
r_{15}	transportiert	Assoziation	-
r_{16}	charakterisiert	Assoziation	-
r_{17}	beinhaltet	Meronymie	reflexiv, antisymmetrisch, transitiv
r_{18}	ermöglicht Ortsveränderung	Assoziation	-
r_{19}	folgt	Assoziation	-
r_{20}	folgt	Assoziation	-
r_{21}	folgt	Assoziation	-
r_{22}	definiert	Assoziation	-
r_{23}	folgt	Assoziation	-
r_{24}	beeinflusst	Assoziation	-
r_{25}	beschreibt	Assoziation	-
r_{26}	beschreibt	Assoziation	-
r_{27}	beeinflusst	Assoziation	-

Bestandsfestlegung: Verkehr

Über die aus der Bestandsuntersuchung abgeleiteten sowohl sprachlichen, nichtsprachlichen als auch Begriffssystemkontexte kann ein konsistentes Begriffsystem modelliert werden und damit ein systematisches Grundverständnis des Begriffs *Verkehr* ermöglicht werden. Abbildung 4.1 zeigt dieses exemplarische Begriffssystem.

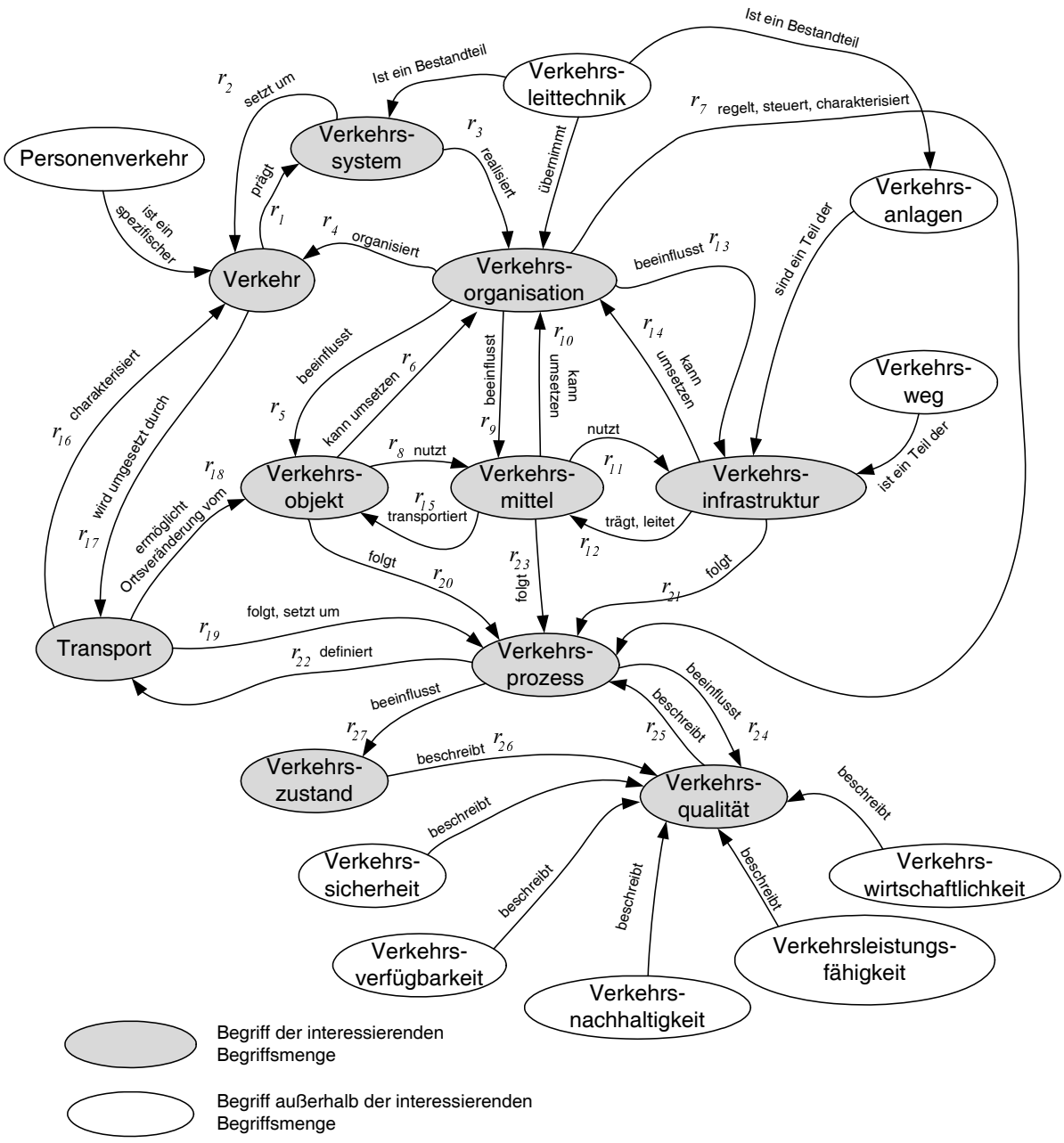


Abbildung 4.1: Erweiterte Darstellung des verkehrsbezogenen Begriffssystems

Aus dem dargestellten Begriffssystem wird durch die ausgeprägten Begriffsbeziehungen deutlich, dass eine starke Vernetzung zwischen den einzelnen Konstituenten (Verkehrsmittel, Verkehrsobjekt, Verkehrsinfrastruktur und Verkehrsorganisation) vorliegt. Eine Einordung und Abgrenzung der einzelnen Verkehrskonstituenten lässt sich durch diese Art der Analyse strukturiert und systematisch auf begrifflicher Ebene durchführen. Die aus der Bestandsaufnahme ermittelte interessierende Begriffsmenge läßt sich durch diese kontextbezogene Analyse konsistent und in einem engen Zusammenhang durch die angegebenen Relationen definieren.

Deutlich wird in dem Begriffssystem auch die zentrale Rolle der Verkehrsorganisation und des Verkehrszustands, die in einer unmittelbaren Relation zueinander stehen und den am stärksten ausgeprägten Begriffssystemkontext durch zentrale Relationen zu den übrigen aufgeführten Begriffen besitzen. Der Transport, hier als Instanziierung des Verkehrs betrachtet, weist eine relativ schwache direkte Relation zu den einzelnen Konstituenten auf. Gleiches gilt auch für die Verkehrsverlässlichkeit, die stark von den einzelnen Verkehrszuständen abhängt.

Ein Vergleich mit einem Modell über die Ausprägungen des Verkehrs in [Mül98] zeigt gewisse Überschneidungen und Überdeckungen, lässt aber keine Inkonsistenzen erkennen. Das zitierte Beispiel beschreibt ein dynamisches Gesamtverkehrsmodell und zeigt die Zusammenhänge ausführlich mittels eines s.g. semi-formalen Entity Relationship Diagramms (ERD). Im Folgenden wird auf eine konsequente Formalisierung durch die Verwendung verschiedener UML-Diagramme und Petrinetze fortgefahren.

4.1.2 Formalisierung des Verkehrsbegriffssystems

Die Formalisierung des Verkehrs erfolgt in diesem Abschnitt unter Berücksichtigung der begrifflichen Analyse aus Unterabschnitt 4.1.1.

Aus der Darstellung lassen sich sowohl die einzelnen Akteure und Bestandteile des Verkehrs ableiten, als auch die statischen und dynamischen Zusammenhänge analysieren. Unabhängig vom spezifischen Verkehrssystem können dadurch Verkehrsmittel, Verkehrsobjekte, Verkehrswegeinfrastruktur als Hauptakteure bestimmt werden. Zusätzlich wird hier die Verkehrsorganisation eingeführt, die wie in der begrifflichen Analyse identifiziert, als Bindeglied zwischen den drei dort aufgeführten physischen Verkehrskonstituenten agiert.

Die Zusammenhänge aus dem festgelegten Begriffsmodell werden hier zunächst in einem semi-formalen statischen Modell als Klassendiagramm dargestellt und über Zustands- und Verhaltensbeschreibung um den dynamischen Anteil erweitert. Bezugnehmend auf die Systemaxiome aus Unterabschnitt 2.2.2 können dabei aus der Darstellung der statischen Zusammenhänge die Struktur abgeleitet und somit das Struktur- und Dekompositionsprinzip angewendet werden. Die dynamischen Zusammenhänge zeigen dabei die unterschiedlichen Zustände und das globale Verhalten des Systems Verkehr. Hierauf sind die Prinzipien der Kausalität und Temporalität anwendbar. Die Darstellung der Funktion des Verkehrs, im Sinne einer Realisierung einer Ortsveränderung von Verkehrsobjekten, lässt sich allerdings nur durch die Kombination beider Modelle ableiten. Die beiden

einzelnen angesprochenen Modelle werden in den folgenden Abschnitten dargestellt und erläutert.

Darstellung als vereinfachtes Klassendiagramm

Eine vollständige Erfassung sämtlicher Facetten des Verkehrs in einem einzigen Modell würde zum einen die Möglichkeiten der Darstellung im Rahmen dieser Arbeit überschreiten und zum anderen ein nicht abschätzbares endloses Unterfangen sein. Eine einfache Strukturierung der einzelnen (Verkehrs-)Aspekte aus der Begriffsanalyse kann jedoch bereits einen ersten Ansatz zur Beherrschung der Komplexität bieten. Aus diesem Grund wird hier vorerst lediglich die Struktur der Verkehrskonstituenten als Untermenge der interessierenden Begriffsmenge formalisiert.

Zur Klärung der systematischen Eigenschaften des Systems Verkehr wird dieses zuerst strukturell nach Maßgabe der Objektorientierung analysiert: Die Konstitutenten des Verkehrs werden als Klassen in einem Klassendiagramm dargestellt, welches die Struktur in Form von Relationen aufzeigt (Abbildung 4.2).

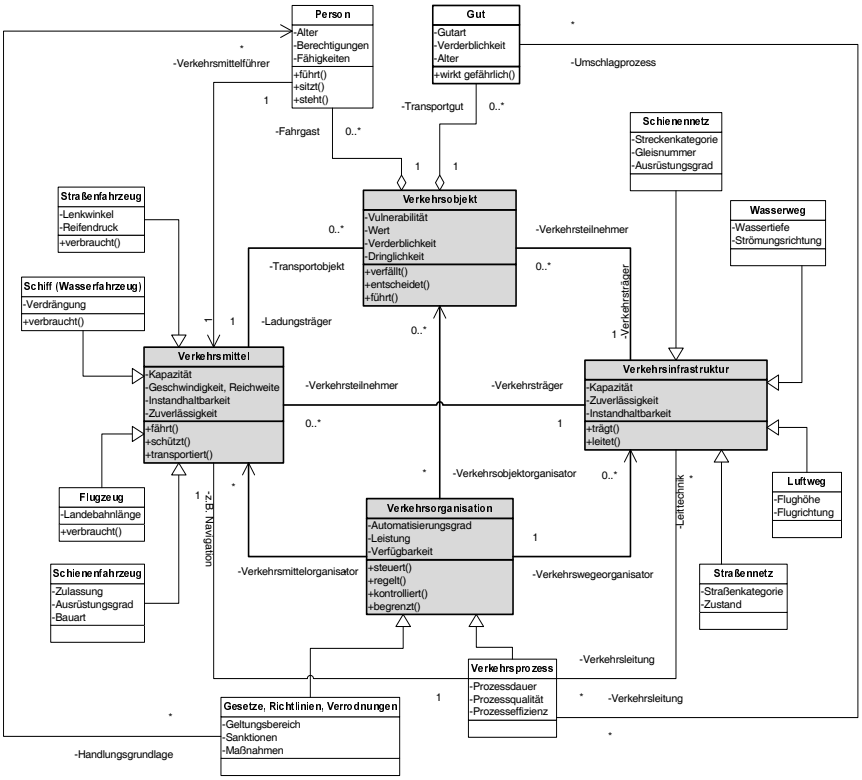


Abbildung 4.2: Die Konstituenten des Verkehrs als Klassendiagramm

Das Verkehrssystem selbst besteht axiomatisch aus den elementaren Konstituenten *Verkehrsobjekt*, *Verkehrsmittel*, *Verkehrswegeinfrastruktur* und *Verkehrsorganisation*, die wiederum Bezüge zu den obigen allgemeinen Aspekten wie auch untereinander aufweisen. Reisende (Personen) oder Güter natürlicher oder technischer Herkunft werden als

Verkehrsobjekte betrachtet, die in *Verkehrsmitteln* (Flugzeuge, Schiffe, Straßen- oder Schienenfahrzeuge) auf Luft-, Wasser- oder Landstraßen bzw. Schienenwegen, als *Verkehrsinfrastruktur* zusammengefasst, verkehren. Die *Verkehrsorganisation* stellt die organisierende virtuelle Instanz zwischen den physischen Konstituenten dar.

Das Klassendiagramm zeigt die drei Konstituenten „Verkehrsobjekt“, „Verkehrsmittel“ und „Verkehrsinfrastruktur“, die durch die vierte Konstituente „Verkehrsorganisation“ vervollständigt werden und folgt dem Ziel, Verkehr möglichst verkehrssystemunabhängig zu betrachten, ohne dabei die grundsätzliche Struktur und Funktionalität des Verkehrs zu vernachlässigen. Die jeweilige Implementierung der Verkehrsorganisation (z.B. in Form von technischen Lösungen) kann innerhalb der drei Klassen (Ressourcen) Verkehrswegeinfrastruktur, Verkehrsmittel oder Verkehrsobjekte umgesetzt werden. Die klassische Verkehrsleittechnik als exemplarische Implementierung (Ressource) der (Funktion) Verkehrsorganisation innerhalb der Verkehrsinfrastruktur nimmt neben der verkehrsobjektseitigen Implementierung der Verkehrsorganisation mittels der z.B. durch den Verkehrsmittelführer beachteten Gesetze und Regularien derzeit einen wichtigen Anteil des Verkehrsgeschehens ein. Eine weitere Möglichkeit der Implementierung der Verkehrsorganisation kann generell auch über die Verkehrsmittel erfolgen (vgl. Abbildung 4.3) und existiert derzeit bereits im Straßenverkehr in Form von fahrzeugseitigen Navigationslösungen und im Schienenverkehr durch Konzepte fahrzeugautarker Ortung [PBB+08] und unterschiedliche Fahrzeugsicherungskonzepte, die jedoch zu großen Teilen auf Funktionen innerhalb der Infrastruktur angewiesen sind. Eine Verschiebung dieser Implementierungsallokation kann durch unterschiedliche Anforderungen aus dem Umfeld des Verkehrs (Wirtschaft, Gesellschaft, Technik, Umwelt und Wissenschaft) jederzeit begründet sein.

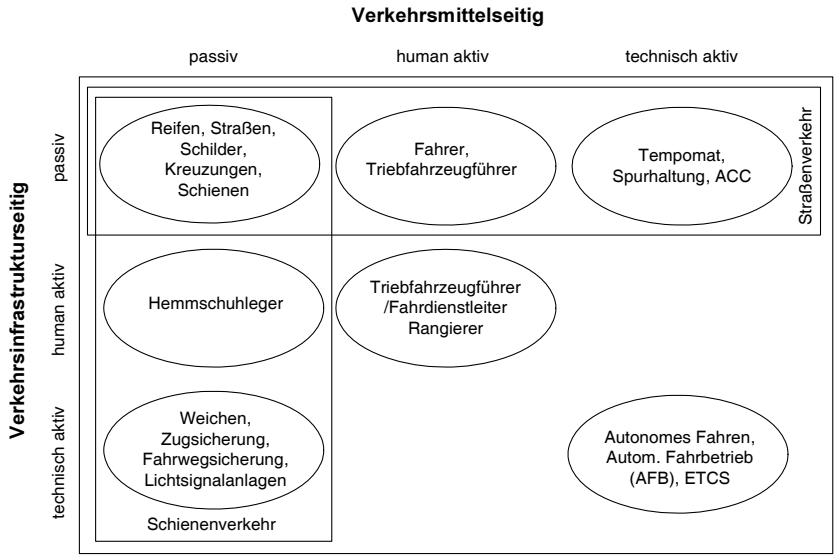


Abbildung 4.3: Allokation der Verkehrsorganisation auf die Verkehrselemente [Sch03]

Abbildung 4.3 zeigt exemplarisch verschiedene Allokationen von Funktionen der Ver-

kehrsorganisation auf verschiedene Ressourcen (vgl. Trennung Funktion - Ressource in Abbildung 2.7). Dabei werden die konstituentenbezogenen Ressourcen „Verkehrsmittel“ und „Verkehrsinfrastruktur“ unterschieden und jeweils der Grad der Automatisierung hinzugefügt. Der Ressourcenanteil der „Verkehrsobjekte“ ist je nach deren Zugehörigkeit als human aktiver Bestandteil integriert worden. In der Darstellung wird die unterschiedliche Präsenz der aktiven Funktionen durch Umsetzung als Ressource im Straßen- bzw. Schienenverkehr deutlich und zeigt die Infrastrukturorientierung des Schienenverkehrs im Gegensatz zu der Verkehrsmittelorientierung des Straßenverkehrs, welches auf die zentrale bzw. dezentrale Funktionsausrichtung der Verkehrsorganisation zurückzuführen ist.

Verkehrsverhalten als vereinfachtes dreifach-hybrides dynamisches Zustandsmodell

Dieser Abschnitt beschreibt das Verhalten des Verkehrs in einer abstrahierten Form, basierend auf einer Fahrzeugbewegung. Verwendet wird hierzu die vereinfachte Zustandsraumdarstellung der variablen Geschwindigkeit und des zurückgelegten Wegs der Fahrzeugbewegung in Richtung eines festen Hindernisses [Sch03], vgl. Abbildung 4.4.

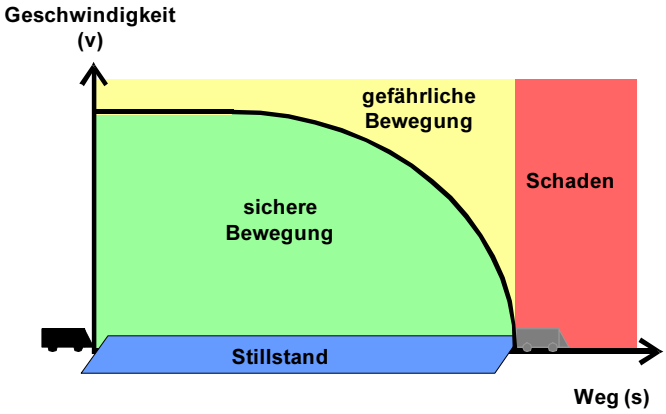


Abbildung 4.4: Fahrzeugbewegung in Zustandsraumdarstellung und globale Zustandsbereiche

Der Zustandsvektor innerhalb des Zustandsraums (Trajektorie) beschreibt bei fortlaufender Zeit die jeweils aktuellen Zustände der Geschwindigkeit im Bezug zu dem aktuell zurückgelegten Weg. Dieses einfache Modell soll die grundlegenden zu unterscheidenden Zustände und Zustandsübergänge des Verkehrs in einer stark vereinfachten Darstellung verdeutlichen. Abbildung 4.4 zeigt den Verlauf der Geschwindigkeit über dem zurückgelegten Weg in der Ausprägung einer Bremsparabel eines Fahrzeugs in dem beschriebenen Geschwindigkeits-Weg-Diagramm. In dieser Darstellung können vier grundsätzlich verschiedene globale diskrete Zustandsbereiche identifiziert werden. Während eine Geschwindigkeit mit dem Betragswert von Null einem „Stillstand“ gleichkommt, können

Bewegungen innerhalb der z.B. durch die Bremskurve begrenzten Fläche als „sichere Bewegung“ interpretiert werden. Ein Übertreten dieser durch die Geschwindigkeit limitierten Grenze kann, ohne gleichzeitig die durch den Weg limitierte Grenze zu überschreiten, als „gefährliche Bewegung“ verstanden werden. Beim Durchbrechen der Weg-Grenze führt jedoch die damit verbundene zeitliche Überschneidung der örtlichen Zustände beider abgebildeter Objekte zu einem durch eine Kollision verursachten „Schadenszustand“ in der Analogie zu der in Unterabschnitt 3.3.1 in Abbildung 3.6 gezeigten Grenze zum Schadenseintritt bzw. zum Gefahrenzustand.

Abbildung 4.5 zeigt die abstrahierte Darstellung der einzelnen abgeleiteten Globalzustände aus der Fahrzeugbewegung, die in Abbildung 4.4 identifiziert wurden, und verbindet diese mit möglichen Zustandsübergängen. Diese Zustandsübergänge werden im Kontext der technischen Zuverlässigkeit stochastisch attributiert exemplarisch mit λ für eine Ausfallrate und mit μ für eine Reparaturrate bezeichnet. Angenommen wird der mögliche Übergang aus dem Stillstand in eine sichere Bewegung, die wiederum zurück in den Stillstand wechseln kann. Aus der sicheren Bewegung kann durch Überschreiten von Grenzen (vgl. Unterabschnitt 3.2.3 – z.B. Geschwindigkeit) eine gefährliche Bewegung ausgeführt werden, die beim angenommenen schadensfreien Verlassen des gefährlichen Zustandsraums einerseits wieder in eine sichere Bewegung übergehen, andererseits im Sinne einer Fail-Safe-Funktion auch in den direkten Stillstand münden kann (z.B. Not-/Zwangsbremsung). Wird aus der gefährlichen Bewegung weder die Überführung in den Stillstand noch in die sichere Bewegung initiiert, resultiert daraus zwangsläufig der Eintritt eines Schadens, der ausschließlich über eine angenommene mögliche Instandsetzung wieder in den (sicheren) Stillstand überführt werden kann.

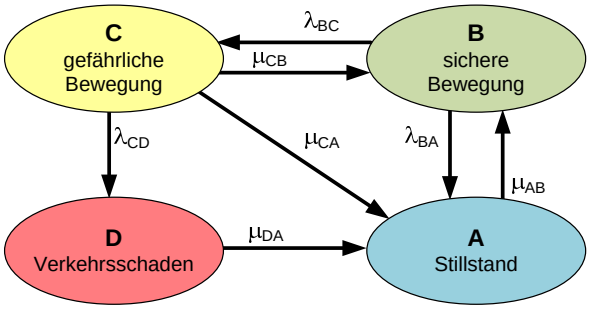


Abbildung 4.5: Hybrides Zustandsmodell nach [Sch03]

Innerhalb der jeweiligen globalen Zustände kann ein kontinuierliches Systemverhalten vorausgesetzt werden, da sich die lokalen Zustände einer sicheren Bewegung (z.B. Geschwindigkeit und zurückgelegter Weg) stetig ändern. Der Übergang bzw. der Durchtritt durch die entsprechenden Grenzflächen im Zustandsraum wird hingegen als diskret aufgefasst, so dass dieses Modell auch als hybrides, d.h. kontinuierlich-diskretes System mit vier Globalzuständen bezeichnet werden kann.

Werden die Zustandsübergänge in Form von stochastischen Zustandsübergangsraten sek^{-1} und die globalen Zustände mit Wahrscheinlichkeitsgrößen belegt, kann hier zusätz-

lich auch von einem dreifach hybriden Zustandsmodell gesprochen werden, welches sowohl diskretes als auch kontinuierliches sowie stochastisches Verhalten in einem Modell vereint. Dieses Modell bildet neben der Formalisierung des abstrakten vereinfachten Verkehrsverhaltens die Basis für die quantitative Analyse der Verkehrssicherheit, die sich im folgenden Abschnitt anschließt.

4.2 Verkehrssicherheit als Begriffssystem

Die Verkehrssicherheit wird begrifflich je nach Domäne und Fokus unterschiedlich interpretiert. Während beispielsweise [RS01] ausschließlich auf die Ursachen, Ausprägungen und Auswirkungen des Straßenverkehrs bezüglich der Sicherheit der beteiligten Personen eingeht, konzentrieren sich andere vorwiegend auf eine verkörperte, eher technische Sicherheit im Sinne von Abwehr- oder Vermeidungsmaßnahmen, ohne die Sicherheit ganzheitlich zu thematisieren. Dabei existieren in sämtlichen Verkehrssystemen eine Vielzahl von domänenspezifischen wissenschaftlich dokumentierten Analysen zu detaillierten Fragestellungen mit dem Ziel, Unfälle systemspezifisch wirksam zu vermeiden. Die Bezeichnung „Verkehrssicherheit“ findet sich dabei allerdings vorwiegend im Bereich des Straßenverkehrs wieder, wie es [Bit67], [HS95], [Eva04] und [RS01] verdeutlichen, die diesen Begriff, bzw. das englische Synonym „Traffic Safety“, verwenden. Eine Abgrenzung bzw. ein konkreter Bezug zum jeweiligen Verkehrssystem hat sich jedoch in der Literatur durch die Verwendung der spezifischen Sicherheitsbezeichungen „Flugsicherheit“ in der Luftfahrt als auch im Schienenverkehr mit der Bezeichnung „Eisenbahnsicherheit“ entwickelt. Die Umsetzung von Maßnahmen bzw. die Einflussnahme in die systemspezifische Sicherheit wird dort primär durch die mit dem Begriff der Sicherung in Relation stehenden Bezeichnungen „Flugsicherung“ bzw. „Eisenbahnsicherung“ dokumentiert [FNT03]. Allgemein prägt [AH06] den Begriff des „Verkehrssicherungswesen“, der diesen als Aufgabenbereich zur Gewährleistung der Sicherheit im Verkehrsprozess, also dem gefährdungs- und gefahrlosen sowie unfallfreien Verkehrsablauf beschreibt ohne ein spezifisches Verkehrssystem in den Vordergrund zu heben.

Um der Zielrichtung dieser vorliegenden Arbeit treu zu bleiben und den systemischen Kontext zu wahren, wird die Verkehrssicherheit hier begrifflich systemübergreifend verstanden, so dass hier entwickelte Sicherungsstretegien ihre ganzheitliche Anwendung finden können.

4.2.1 Begriffsanalyse der Verkehrssicherheit

Die Verkehrssicherheit setzt sich, wie bereits in der Einleitung erwähnt, aus den Wortteilen *Verkehr* und *Sicherheit* zusammen, die jeweils als Begriff in den vorangegangenen Abschnitten bzw. vorangegangenen Kapiteln ausführlich betrachtet, analysiert und formalisiert wurden. Dieser Abschnitt fügt die einzelnen Teile konsequent zusammen und beschreibt unter Bezugnahme auf die jeweiligen Textstellen sowohl die Begriffsanalyse

als auch die Formalisierung sowie mögliche Implementierungen der systemunspezifischen *Verkehrssicherheit*.

Die Verkehrssicherheit wird analog zu den beiden isolierten Wortbestandteilen, basierend auf den bereits vorgestellten erweiterten Analysen, begrifflich definiert. Zur eingänglichen Klärung des Begriffsinhaltes (charakterisierender Bestandteil des Begriffs) wird eine systematische Analyse der interessierenden Begriffsmenge um den Begriff Verkehrssicherheit in Form einer kurzen Bestandsaufnahme durchgeführt.

Die Bestandsaufnahme konzentriert sich dabei vorwiegend auf die in den vorangestellten Begriffsanalysen erzeugten Begriffssysteme und identifizert Schnittstellen, die für die Verkehrssicherheit von Bedeutung sind.

Eine Analyse unterschiedlicher Begriffsbezeichnungen (z.B. Synonyme, Homonyme, etc.) wird hier analog zu den bisher durchgeführten Begriffsanalysen vernachlässigt, da sie in dem Kontext eines Grundsatzverständnisses nicht weiterführt.

Die Relationen, die zwischen den Teilbegriffen/Merkmalen selbst und anderen Begriffen existieren, werden aufgrund ihrer Bedeutungsschwere systematisch in der Bestandsuntersuchung analysiert und in der Bestandsfestlegung zu einem Begriffssystem zusammengefasst.

Bestandsaufnahme: Verkehrssicherheit

Aus den Begriffsanalysen zu den Begriffen „Sicherheit“ und „Verkehr“ und einer daraus abgeleiteten Bestandsaufnahme ergibt sich folgende interessierende Begriffsmenge, die zu einem großen Teil aus eigenen Interpretationen besteht:

Verkehrssicherheit: *Zusammengesetzt aus „Verkehr“ und „Sicherheit“*
Freiheit von unvertretbaren Risiken und Gefahren bei der Ortsveränderung von Personen oder Sachgütern (Verkehrsobjekte), die z.B. in Verkehrsmitteln unter Einbezug der Verkehrsinfrastruktur und Verkehrsorganisation transportiert werden.

Verkehrobjektsicherheit: *Zusammengesetzt aus „Verkehrsobjekt“ und „Sicherheit“*
Die Sicherheit (Freiheit von unvertretbaren Risiken und Gefahren) bezogen auf die Verkehrsobjekte (z.B. Fußgänger/Reisende, Sachgüter/ Ladung). Darunter fällt sowohl die Sicherheit im Sinne von nicht vorhandenen ausgehenden Gefährdungen von den Verkehrsobjekten, als auch die Sicherheit im Sinne der Vulnerabilität (Unverletzbarkeit) der Verkehrsobjekte z.B. durch Schutzmaßnahmen.

Verkehrsmittelsicherheit: *Zusammengesetzt aus „Verkehrsmittel“ und „Sicherheit“*
Die Sicherheit (Freiheit von unvertretbaren Risiken und Gefahren) bezogen auf die Verkehrsmittel (z.B. Fahrzeuge, Trag-/Zugtiere). Darunter fallen nach [Kra06] sowohl aktive unfallvermeidende Maßnahmen (Fahrsicherheit, Konditionssicherheit, Bedienungssicherheit und Wahrnehmungssicherheit) als auch passive Unfallfolgen mindernde Maßnahmen (Selbstschutz, Kontrahentenschutz) an Verkehrsmitteln um diese Freiheit zu erzielen. Durch diese Definition werden die Bereiche Fahrzeugsicherheit und Fußgängersicherheit mit einbezogen.

(Verkehrs-)Unfall: Ein Ereignis, bei dem die Abweichung zwischen vorgegebener Fahraufgabe und deren Erfüllung ein zulässiges Maß überschreitet (nicht bewältigte Regelaufgabe) und in dessen unmittelbarer Folge ein (Verkehrs-)Schaden bestimmter Art und Schwere eintritt.
Quelle: Kramer [Kra06]

Wird hier im Sinne einer „Schädigung“ von Verkehrsobjekt, Verkehrsmittel oder Verkehrsinfastruktur verstanden.

Verkehrsschaden: *Zusammengesetzt aus „Verkehr“ und „Schaden“*
Physische Verletzung oder Schädigung der Gesundheit von Verkehrsobjekten (Menschen oder Sachgüter), entweder direkt oder indirekt als ein Ergebnis von Schäden von Verkehrsobjekten, Verkehrsmitteln, Verkehrsinfastruktur oder der Umwelt.
Ein Verkehrsschaden beinhaltet somit gleichermaßen Transportschäden (Schaden an Ladung) als auch Personenschäden (Schäden an Reisenden) oder Fahrzeug- bzw. Infrastruktur- oder Umweltschäden.

Verkehrsgefahr: *Zusammengesetzt aus „Verkehr“ und „Gefahr“*
Sachlage, bei der das Verkehrsrisiko größer als das Grenzrisiko ist, wobei unter Grenzrisiko das größte noch vertretbare Risiko im Verkehr verstanden wird. Komplementär zur Verkehrssicherheit.

Verkehrsgefährdung: *Zusammengesetzt aus „Verkehr“ und „Gefährdung“*
Verhalten des Verkehrssystems, das zu einer Verkehrsgefahr führen kann, wenn es nicht beherrscht wird und einen Schaden an Verkehrsobjekten (Reisenden) direkt oder indirekt hervorrufen kann.

Verkehrsrisiko: *Zusammengesetzt aus „Verkehr“ und „Risiko“*
Eine Kombination der Wahrscheinlichkeit und des Schweregrads der möglichen Verletzung oder Gesundheitsschädigung in einer durch den Verkehr verursachten oder befindlichen Gefährdungssituation. Wahrscheinlichkeitsaussage, die quantitativ die zu erwartende Häufigkeit $H_{Verkehr}$ des Eintritts eines zum Verkehrsschaden führenden Ereignisses und das bei Ereigniseintritt zu erwartende Verkehrsschadensausmaß $S_{Verkehr}$ zusammenfasst.

Bestandsuntersuchung: Verkehrssicherheit

Die aufgeführten Begriffe werden nachfolgend in Tabelle 4.6 und Tabelle 4.7 bzgl. deren Kontexte (nicht-sprachlicher und Begriffssystemkontext) analysiert.

Tabelle 4.6 und Tabelle 4.7 zeigen die verschiedenen nicht-sprachlichen Kontexte der einzelnen Begriffe zu dem Begriffsumfeld der Verkehrssicherheit. Die wichtigsten Begriffssystemkontexte (Relationen) werden nachfolgend zuerst textuell beschrieben und

anschließend tabellarisch dargestellt. Relationen, die bereits in den vorangegangenen Begriffsanalysen/-systemen beschrieben wurden, werden hier nicht explizit wiederholt.

Tabelle 4.6: Nicht-sprachliche Begriffskontexte zur Verkehrssicherheit

Verkehrssicherheit	
Unterbegriffe	Teilbegriffe (Merkmale)
Straßenverkehrssicherheit	Verkehrssicherheitsmaß
Schienenverkehrssicherheit	Verkehrsgefährdungsrate
Transportsicherheit	Verkehrsgefahrenvermeidungspotenzial
Verkehrsobjektsicherheit	
Unterbegriffe	Teilbegriffe (Merkmale)
Insassensicherheit	Vulnerabilität
Ladungssicherheit	Head Injury Criterion (HIC)
Fußgängersicherheit	Abreviated Injury Scale (AIS)
Verkehrsmittelsicherheit	
Unterbegriffe	Teilbegriffe (Merkmale)
Fahrzeugsicherheit	EURO NCAP Sterne
Zweiradsicherheit	Index aktiver Sicherheit (AkSIx) [Kra06]
Fußgängerschutz	Index passiver Sicherheit (PaSIx) [Kra06]
Crash-Sicherheit	
Verkehrssschaden	
Unterbegriffe	Teilbegriffe (Merkmale)
Transportschaden	Verkehrsschadensausmaß
Personenschaden	Verkehrsschadensart
Infrastrukturschaden	Verkehrsschadenseintritt (Unfall)
Verkehrsgefahr	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrsobjektgefahr	Verkehrsschadenspotenzial
Verkehrsmittelgefahr	Gefahrenart/-richtung
	Vermeidungspotenzial

Tabelle 4.7: Nicht-sprachliche Begriffskontexte zur Verkehrssicherheit (Fortsetzung)

(Verkehrs-)Unfall	
Unterbegriffe	Teilbegriffe (Merkmale)
Fahrunfall	Verkehrsschadenspotenzial
Abbiegeunfall	Unfallvermeidungspotenzial
Kreuzungsunfall	Unfallhäufigkeit
Verkehrsgefährdung	
Unterbegriffe	Teilbegriffe (Merkmale)
Verkehrsmittelgefährdung	Verkehrsgefährdungsrate
Verkehrsobjektgefährdung	Gefährdungsresistenz
Verkehrsinfrastrukturgefährdung	Verkehrsgefährdungsart
Verkehrsrisiko	
Unterbegriffe	Teilbegriffe (Merkmale)
Unfallrisiko	Verkehrsschadensschwere
Personenschadensrisiko	Verkehrsschadenseintritt (Unfall)
Verletzungsrisiko	Verkehrsrisikoakzeptanz

Die „Verkehrssicherheit“ kann als Eigenschaft des „Verkehrssystems“ betrachtet werden (Meronymie r_1). Die „Verkehrsorganisation“ als ein Bestandteil (Verkehrskonstituent) des „Verkehrssystems“ nutzt verschiedene „Sicherungstechniken“ (Assoziation r_2), die verschiedene „Sicherungsfunktionen“ produzieren/implementieren (i. w. S. Genetizität r_3). Dadurch setzt die „Verkehrsorganisation“ diese „Sicherungsfunktionen“ um (Genetizität r_4). Die „Sicherungstechnik“ wird durch die Bestandteile des „Verkehrssystems“ (Verkehrsobjekte, Verkehrsmittel oder Verkehrsinfrastruktur) implementiert (i. w. S. Genetizität r_5) indem die „Sicherungstechnik“ den „Verkehrsprozess“ beeinflusst (Assoziation r_6) und entweder direkt das „Schadensausmaß“ reduziert (Genetizität r_7) oder über die „Sicherungsfunktionen“ „Verkehrsunfälle“ (Synonym zu Verkehrsschadenseintritt) vermeidet (Assoziation r_8). Die Umsetzung von „Sicherungsfunktionen“ kann die Gefährdungsrate reduzieren, indem „Gefahrenquellen“ beherrscht (Assoziation r_9) und „Verkehrsgefährdungen“ und damit „Verkehrsgefahren“ nach Möglichkeit verhindert werden (Assoziation r_{10} und Kausalität r_{12}). Das Vorhandensein bzw. das Fehlen von „Sicherungsfunktionen“ im Verkehr, die den „Verkehrsprozess“ beeinflussen, definiert somit das aktuelle „Verkehrsrisiko“ (Assoziation r_{11}). Die „Verkehrsorganisation“ kann demnach einen großen Beitrag zur Reduzierung des „Verkehrsrisikos“ und zur Erhöhung der „Verkehrssicherheit“ beitragen. Tabelle 4.8 fasst die beschriebenen Relationen zusammen.

Tabelle 4.8: Verkehrssicherheitsrelevante Relationen

		Senke											
		Verkehrssystem	Verkehrssicherheit	Verkehrsorganisation	Sicherungstechnik	Verkehrsprozess	Sicherungsfunktion	Verkehrsunfall	Verkehrsgefährdung	Verkehrsgefahr	Verkehrsrisiko	Schadensausmaß	Schadensausmaß
Quelle	Verkehrssystem	X	-	-	r_5	-	-	-	-	-	-	-	-
	Verkehrssicherheit	r_1	X	-	-	-	-	-	-	-	-	-	-
	Verkehrsorganisation	-	-	X	r_2	-	r_4	-	-	-	-	-	-
	Sicherungstechnik	-	-	-	X	r_6	r_3	-	-	-	-	r_7	-
	Verkehrsprozess	-	-	-	-	X	-	-	-	-	-	-	-
	Sicherungsfunktion	-	-	-	-	-	X	r_8	r_{10}	-	r_{11}	-	r_9
	Verkehrsunfall	-	-	-	-	-	-	X	-	-	-	-	-
	Verkehrsgefährdung	-	-	-	-	-	-	-	X	r_{12}	-	-	-
	Verkehrsgefahr	-	-	-	-	-	-	-	-	X	-	-	-
	Verkehrsrisiko	-	-	-	-	-	-	-	-	-	X	-	-
	Schadensausmaß	-	-	-	-	-	-	-	-	-	-	X	-
	Gefahrenquelle	-	-	-	-	-	-	-	-	-	-	-	X

Bestandsfestlegung: Verkehrssicherheit

Aus der vorangegangenen integrierten Bestandsaufnahme und -untersuchung ist sowohl der inhaltliche Kontext der einzelnen Begriffe als auch begriffsübergreifende Zusammenhänge zwischen unterschiedlichen Begriffen aufgeführt. Die Bestandsfestlegung stellt diese in einem Begriffssystem grafisch dar.

Tabelle 4.9: Relationen der verkehrssicherheitsrelevanten Begriffsmenge im Detail

Relation	Relationsbenennung	Relationsart	math. Relation
r_1	ist Merkmal von	Meronymie	reflexiv, antisymmetrisch, transitiv
r_2	nutzt	Assoziation	-
r_3	implementiert	Genetizität	transitiv
r_4	setzt um	Genetizität	transitiv
r_5	implementiert	Genetizität	transitiv
r_6	beeinflusst	Assoziation	-
r_7	reduziert	Genetizität	transitiv
r_8	vermeidet	Assoziation	-
r_9	beherrscht	Assoziation	-
r_{10}	verhindert	Assoziation	-
r_{11}	definiert	Assoziation	-
r_{12}	führt zu	Kausalität	irreflexiv, antisymmetrisch, transitiv

Abbildung 4.6 zeigt die grafische Umsetzung der identifizierten und analysierten Relationen aus Tabelle 4.9. In dem dort dargestellten Begriffssystem können grundlegende Bestandteile der unterlagerten Begriffssysteme zu den Wortteilen „Verkehr“ und „Sicherheit“ wiedergefunden werden. Interessant ist die bedeutende Rolle der Verkehrsorganisation als Lieferant von Sicherungsfunktionen, die in Form von Sicherungstechniken in den einzelnen Verkehrskonstituenten implementiert werden. Über die Darstellung der Beherrschung von Gefahrenquellen und der damit verbundenen Verhinderung von Gefährdungen sowie die Reduktion von Verkehrschadensausmaßen kann die Verkehrssicherheit verbessert werden. Dabei wird die Verkehrssicherheit in diesem Kontext als Wahrscheinlichkeit des Verkehrssystems, sich weder in einem gefährlichen noch in einem Schadenszustand zu befinden, verstanden. Diese Interpretion der Verkehrssicherheit wird im folgenden Abschnitt ansatzweise formalisiert.

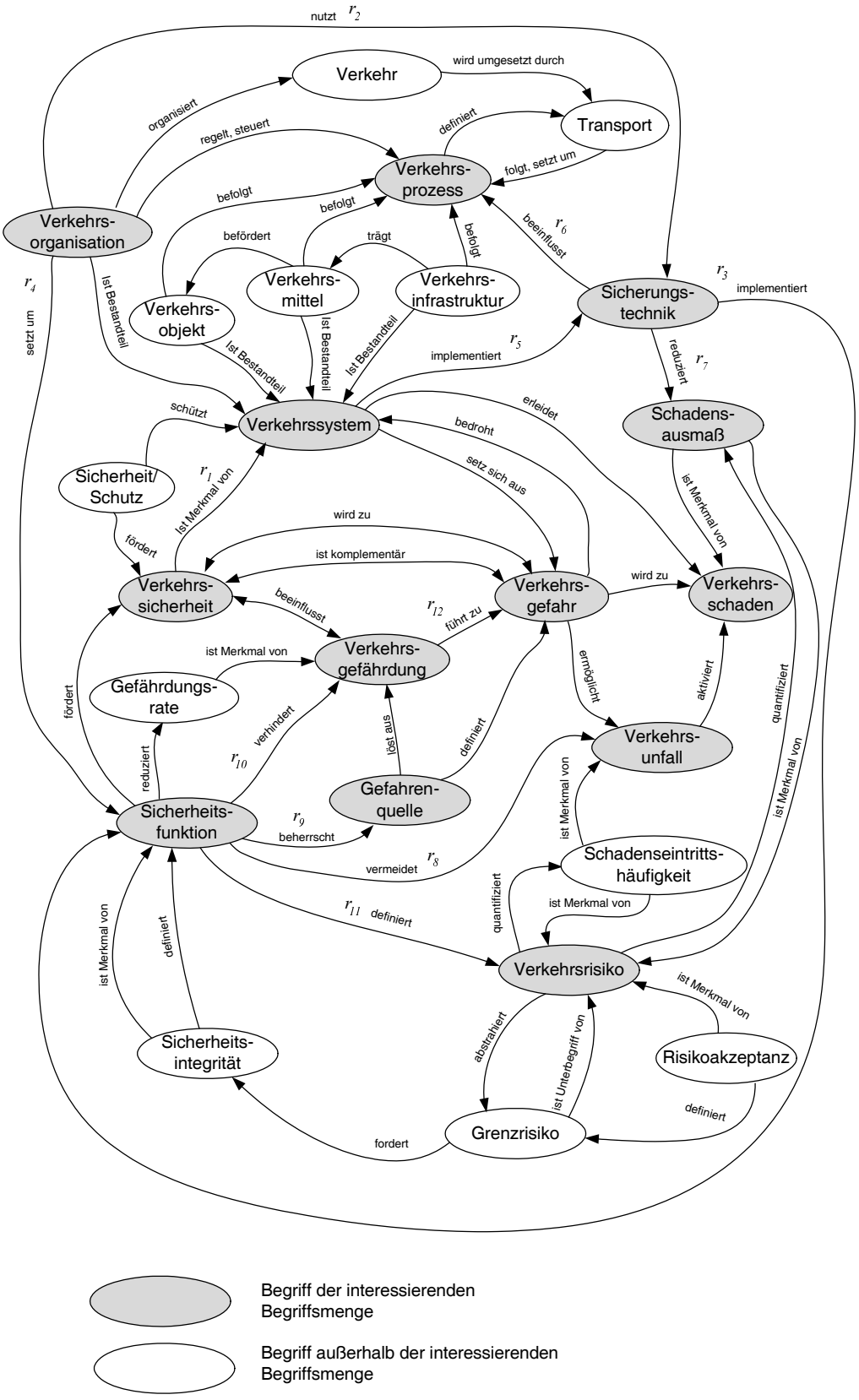


Abbildung 4.6: Begriffssystem: Verkehrssicherheit

4.2.2 Formalisierung der Verkehrssicherheit

Die Verkehrssicherheit als instanziierte Sicherheit und qualitative Eigenschaft des Verkehrs kann in einfachen Modellen konzeptionell formalisiert werden. Dazu wird ausgehend von den zentralen Begriffen der Verkehrsgefahr der Zustandsraum des Verkehrs betrachtet. Diese Zustandsmenge muss in einem engen Zusammenhang mit dem Verkehr als System verstanden werden und schließt somit die Struktur der Verkehrskonstituenten, die einzelnen Zusammenhänge zwischen diesen und dem daraus resultierenden Verhalten zur Erfüllung der primären Funktionen des Verkehrs (Durchführung von Transporten über realisierte Fahrzeugbewegungen) mit ein.

Abbildung 4.7 zeigt die vier bekannten Globalzustände des Verkehrs: Stillstand, sichere Bewegung, gefährliche Bewegung und Schaden, mit deren Zustandsübergängen aus Unterabschnitt 4.1.2. Diese Konstellation der Zustände spiegelt die enge Analogie zu der Formalisierung der Sicherheit, deren drei globale Zustände: sicherer Zustand, Gefahrenzustand und Schaden sowie deren Übergänge in Unterabschnitt 4.1.2 beschrieben wurden, und zeigt gleichzeitig das typische abstrakte Verhalten des Verkehrs.

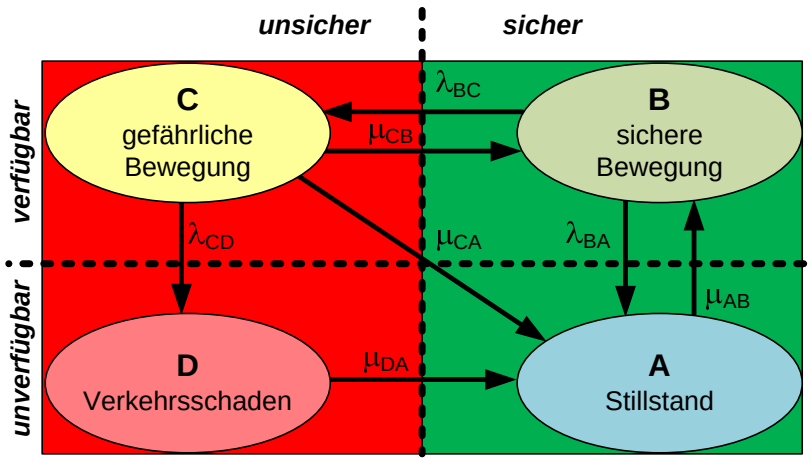


Abbildung 4.7: Verfügbarkeits-Sicherheits-Ebene mit vier Quadranten

Werden die vier globalen Systemzustände des dreifach hybriden Modells weiter zu deren Verlässlichkeitsmerkmalen abstrahiert, können daraus zwei, bzw. durch deren Negation vier, globale Verkehrsverlässlichkeitsmerkmale modelliert werden:

- Verkehrsverfügbarkeit (verfügbar)
- Verkehrsunverfügbarkeit (unverfügbar)
- Verkehrssicherheit (sicher)
- Verkehrsunsicherheit (unsicher)

Bezogen auf die Ergebnisse der Begriffsanalyse, die die Verkehrssicherheit als Wahrscheinlichkeit eines Systems definiert, während einer definierten Zeit in einem sicheren Zustand zu verharren, zeigt die Modellierung dieser globalen Zuverlässigkeitsgrößen eine ideale Übereinstimmung.

Über die Verknüpfung der einzelnen lokalen Zustandswahrscheinlichkeiten mit den jeweiligen Zustandsübergangsraten können Aussagen über die globalen chrakterisierenden Zustände Sicherheit (bzw. Unsicherheit) und Verfügbarkeit (bzw. Unverfügbarkeit) des Systems Verkehr getroffen werden. Die untergeordneten Zustände Stillstand und sichere Bewegung werden als sicher angenommen, während die gefährliche Bewegung und der Schaden als unsicher definiert werden. Gleichzeitig werden sichere und gefährliche Bewegung als verfügbarer und der Stillstand und der Schaden als unverfügbarer Zustand bezeichnet. Aus den Zustandswahrscheinlichkeiten der lokalen Verkehrszustände lassen sich die verlässlichkeitsspezifischen globalen Wahrscheinlichkeiten der Zustände Verkehrssicherheit und Verkehrsverfügbarkeit wie folgt ableiten.

Für die Sicherheit ergibt sich folgender Zusammenhang:

Die Menge aller Zustände sei Ω. Weiter sei die Sicherheit die Menge aller Zustände Z, die einen Stillstand (A) oder eine sichere Bewegung (B) spezifizieren.

$$\mathit{Sicherheit} := \{Z | Z \in A \cup B\}; \tag{4.1}$$

Entsprechend sei Unsicherheit die Menge aller Zustände Z', die eine gefährliche Bewegung (C) oder einen Verkehrsschaden (D) spezifizieren.

$$\mathit{Unsicherheit} := \{Z' | Z' \in C \cup D\}; \tag{4.2}$$

A, B, C, und D sind paarweise disjunkt und es gilt:

$$\mathit{Sicherheit} \cup \mathit{Unsicherheit} = \Omega \tag{4.3}$$

$$\mathit{Sicherheit} = \Omega \setminus \mathit{Unsicherheit} \tag{4.4}$$

$$A \cup B = \Omega \setminus (C \cup D) \tag{4.5}$$

Dann gilt:

$$P(A) + P(B) = 1 - [P(C) + P(D)] \tag{4.6}$$

Für die Verfügbarkeit analog:

$$P(B) + P(C) = 1 - [P(A) + P(D)] \tag{4.7}$$

Zusätzlich zu dieser Betrachtung der Verkehrssicherheit als Wahrscheinlichkeit, können mit einer abweichenden Modellierung Aussagen über die Schadenseintrittsrate getroffen werden, um daraus z.B. in Verbindung mit dem Schadensausmaß das Verkehrsrisiko zu bestimmen. Dazu kann der Schadenszustand entsprechend als globaler Zustandsbereich isoliert werden.

Für die Schadenswahrscheinlichkeit ergibt sich folgender Zusammenhang:

$$P(D) = 1 - [P(A) + P(B) + P(C)] \tag{4.8}$$

Für die vollständige Betrachtung sind die Übergangsraten zwischen den jeweiligen Zuständen zu berücksichtigen. Für die Schadenswahrscheinlichkeit ist dies in Form einer simulativen Markov-Analyse durchgeführt worden, um die Auswirkungen von Variationen der Übergangsraten darstellen zu können [Sch05].

In Abbildung 4.8 ist die Sicherheit (hier vereinfacht die Anzahl der Unfälle pro Stunde) über der Verfügbarkeit in % für die Simulation dargestellt [Sch05]. Die abgebildeten Funktionswerte zeigen die Sicherheit (hier Schadenshäufigkeit) und Verfügbarkeit bei Veränderungen der Übergangsraten in einer logarithmischen Skalierung.

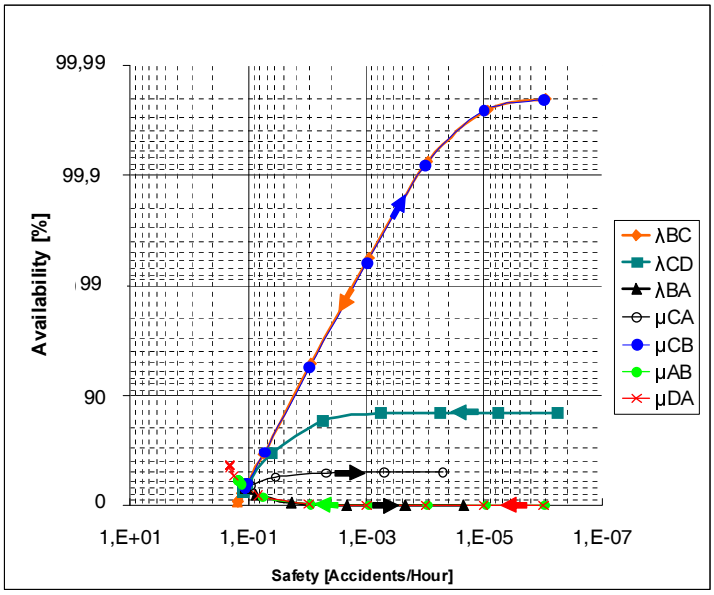


Abbildung 4.8: Maßnahmen auf die Verfügbarkeit und Sicherheit

Eine Veränderung der Übergangsraten zwischen der sicheren Bewegung und der gefährlichen Bewegung zeigt dabei die deutlichste Auswirkung auf die Sicherheit bei gleichzeitiger Beeinflussung der Verfügbarkeit. Bemerkenswert ist dabei die Erkenntnis, dass nur eine Reduktion der Übergangsrate zwischen sicherer und gefährlicher Bewegung (λ_{BC}) bzw. eine Erhöhung der Übergangsrate in umgekehrter Richtung (μ_{CB}) sowohl die Anzahl der resultierenden Schäden pro Zeiteinheit reduziert, als auch die Gesamtverfügbarkeit erhöht. Änderungen der Übergangsraten zwischen dem Stillstand und der sicheren Bewegung (λ_{BA} bzw. μ_{AB}) sowie zwischen der gefährlichen Bewegung und dem Schaden (λ_{CD}) haben zwar vergleichbare positive Auswirkungen auf die Sicherheit, wirken sich jedoch kaum negativ und z.T. auf die Verfügbarkeit aus.

Diese Art der Wirksamkeitsanalyse von Änderungen der Zustandsübergangsraten kann hilfreich für die Bewertung von Maßnahmen zur Steigerung der Sicherheit sein und ef-

fiziente Ansatzpunkte für Sicherungsfunktionen z.B. erweiterter Fahrerassistenzsysteme liefern und damit nachhaltig und messbar die Verkehrssicherheit erhöhen [Slo06].

4.3 Sicherungsimplementierungen im Verkehr

Dieser Abschnitt befasst sich mit möglichen Implementierungen der Verkehrssicherheit. Dabei werden die Grundlagen der Systemeigenschaften und insbesondere deren Zusammenspiel beschrieben, um die generischen Sicherungsimplementierungkonzepte (vgl. Abschnitt 3.4) im Verkehr zu realisieren.

4.3.1 Technisch-konstruktive Beeinflussung von Systemeigenschaften

Als **Technisch-Konstruktive** Maßnahmen werden hier die Maßnahmen bezeichnet, die sich bei der Implementierung der Sicherheitskonzepte vorwiegend auf die Struktur des jeweiligen Systems konzentrieren. Dabei sollen durch konstruktive Maßnahmen Gefährdungen vermieden, Gefahren abgewehrt oder Auswirkungen gemindert werden. Als Beispiele dafür können z.B. Schutzgehäuse um drehende Teile, abgerundete Stoßkanten, aber auch redundante und zuverlässige Funktionsstrukturen innerhalb von Sicherungssystemen betrachtet werden. Der Ausfall eines Systems, der in der Folge eine Gefährdung potenziell ermöglicht, soll durch eine verlässliche Konstruktion verhindert werden. Gleiches gilt insbesondere für die Implementierung von Sicherungsfunktionen durch entsprechende Funktionsträger. Die Konzipierung solcher Sicherungsfunktionen, inklusive der notwendigen Teilfunktionen zur Steuerung von Ereignissen, ist allerdings keine rein technisch konstruktive Maßnahme, da für einen steuernden bzw. sichernden Eingriff der Prozess (das Systemverhalten) ausreichend berücksichtigt werden muss.

Weitere technisch-konstruktive Maßnahmen können in Form von konkreter Abwehr bzw. erzeugter Resistenzen (Immunität) gegenüber einwirkenden Gefahrenquellen ermittelt werden. Bei der konstruktiven Beherrschung von gefährlichen Wirkungen von Gefahrenquellen am verletzbaren System (Immunisierung) liegt das verfolgte Ziel, bzw. das verfolgte Sicherungsimplementierungskonzept, in der Auswirkungsminderung und somit in der Vermeidung eines inakzeptablen Schadenszustands. Wird hingegen eine schädigende Ursache in der Gefahrenquelle beherrscht, so kann von einer Gefahrenabwehr gesprochen werden. Für die entsprechende Maßnahmenkonstruktion werden die folgenden gefährdenden Eigenschaften von Gefahrenquellen unterschieden:

mechanisch: gegenseitige physikalische Beeinflussung durch kinetische Energie. (z.B. Kollision mit einem Hindernis)

thermodynamisch: gegenseitige Beeinflussung durch thermische Energie. (z.B. Wärme-/Kältezufuhr, Brandfall)

elektro-magnetisch: gegenseitige Beeinflussung durch elektrische und magnetische sowie gekoppelte Felder/Energien inkl. Teilchenstrahlung (z.B. elektrischer Schlag, elektromagnetische Beeinflussung)

chemisch-biologisch: gegenseitige Beeinflussung durch chemische oder biologische Stoffe. (z.B. durch Chemikalien ausgelöste biologische Reaktionen)

Eine Grundlage dieser Gefahrencharakteristiken stellt der Anhang 1 der Norm DIN EN ISO 14121-1 „Sicherheit von Maschinen - Risikobeurteilung“ ausführlich dar [Int07]. Die dort angegebenen 10 Gefahrentypen sind hier aus Gründen der Vereinfachung und der teilweise nur sehr schwer voneinander abgrenzbaren Charakteristiken zu den vier o.a. Eigenschaften von Gefahrenquellen zusammengefasst worden.

Bezogen auf das System Verkehr mit den beteiligten Verkehrskonstituenten (vgl. Unterabschnitt 4.1.1) können auf diese Weise potenzielle Gefahren systematisch ermittelt werden. Abbildung 4.9 zeigt am Beispiel der Verkehrskonstituenten *Verkehrsobjekt* und *Verkehrsmittel* unterschiedliche Ausprägungen von Gefahren mit jeweils gegensätzlicher Ursache und Wirkung.

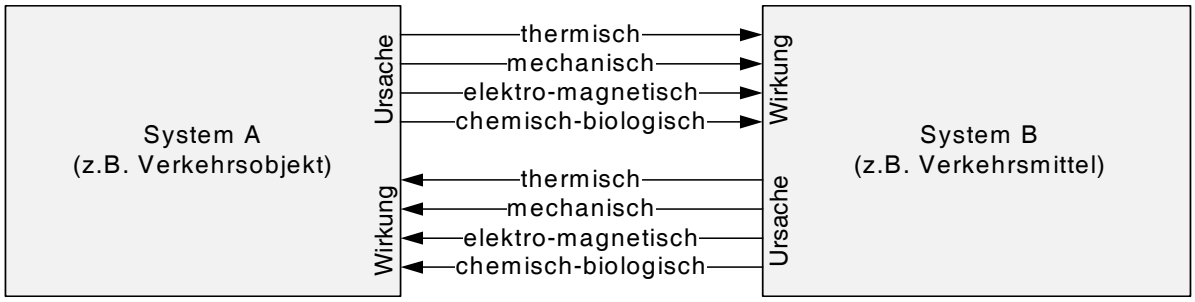


Abbildung 4.9: Ursache-Wirkungsrelationen von Gefahrenquellen/-senken

Tabelle 4.10 zeigt Ursachen- und Wirkungskombinationen und deren Ausprägungen am Beispiel der Verkehrskonstituenten *Verkehrsmittel* und *Verkehrsobjekt* (insb. Personen/Reisende). Werden technisch-konstruktive Sicherheitsmaßnahmen zur Vermeidung der Ursachen bzw. Auswirkungen implementiert, müssen die Sicherheitsmaßnahmen die jeweilige Auswirkung bzw. Ursache in der jeweiligen Ausprägung und in dem entsprechenden Betrag eliminieren. Wirkt ein System (hier: Verkehrsmittel) thermisch auf ein anderes System (hier: Verkehrsobjekt in der Instanz Reisender) und erwirkt dort eine chemisch-biologische Auswirkung (z.B. Kreislaufschädigung durch Hitzeschaden oder auch Vergiftungen durch Rauch) sind entsprechende Maßnahmen darauf abzustimmen. Eine potenzielle Maßnahme ist es zum einen die thermische Ausstrahlung des Verkehrsmittels auf den Fahrgast zu vermeiden oder zu reduzieren (z.B. automatische Klimaregelung, Verwendung halogenfreier Materialien) bzw. zum anderen die chemisch-biologischen Auswirkungen am Reisenden zu reduzieren (z.B. kühlende Schutzkleidung, Luftzufuhr). Die am häufigsten anzutreffenden Kombinationen aus Ursachen und Wirkungen im Verkehrssystem sind in der Regel auf mechanische Einflüsse zurückzuführen.

Tabelle 4.10: Beispielhafte Ursache-/Wirkungsbeziehungen

		Wirkungen bei System B			
		mechanisch	thermodyn.	elekt.-magn.	chem.-biol.
Ursache von System A	mechanisch	Verletzungen (Knochenbrüche)	Verbrennungen (durch Reibung)	-	-
	therm.	Verletzungen (Verbrennungen)	Verbrennung (direkt)	-	Rauch-vergiftung
	elekt.-magn.	Verletzungen (Tumorbildung)	Verbrennung (Strahlung)	gestörte Reizleitung	Verletzung (Strahlung)
	chem.-biol.	Verletzung (Verätzungen)	Verbrennung (chemisch)	-	Vergiftung

Die konstruktiven Maßnahmen konzentrieren sich dann meist auf energieabsorbierende Konstruktionen, wie die Einführung der „Knautschzone“ im Jahr 1952 durch Béla Barényi, die bis heute in verschiedenenen Verkehrssystemen etabliert ist, exemplarisch zeigt. Aber auch die Einführung der Helmpflicht für motorisierte Zweiradfahrer im Jahr 1976, bzw. der Helm als konstruktive Maßnahme am Verkehrsobjekt, trägt zur Minderung der Wirkungen (Auswirkungsminderung) aufgrund mechanischer Ursachen bei. In anderen Personentransportsystemen, z.B. Autobusse, Personenzüge, Flugzeuge sowie Schiffe, sind zudem diverse konstruktive Maßnahmen zur Beherrschung von Brandfällen eingeführt worden. Beispiel dafür sind teilweise feuerfeste und zumindest nichttoxische Materialien sowie ausreichende Rauchabzugsmöglichkeiten, um Schäden an Personal und Reisenden zu vermeiden. Anforderungen an den Brandschutz in Schienenfahrzeugen sind in normativer Form zusammengetragen worden [Deu03a].

4.3.2 Prozessorientierte Steuerung von Systemeigenschaften

Aus der Beschreibung von generischen Sicherungsimplementierungskonzepten sowie der Begriffsanalyse zur Verkehrssicherheit (vgl. Abschnitt 3.4 und Abschnitt 4.2) wird deutlich, dass die (Verkehrs-)Sicherheit, als Wahrscheinlichkeit betrachtet, das Komplement zur Wahrscheinlichkeit eines (Verkehrs-) Gefahrenzustands darstellt. Folglich kann daraus abgeleitet werden, dass zusätzlich zur kontruktiv-technischen Beeinflussung die gezielte Beinflussung des Systemverhaltens bzw. die gezielte Beeinflussung der Wahrscheinlichkeit des Zustands „Verkehrsgefahr“ die Verkehrssicherheit positiv beeinflusst.

Aus den in den Grundlagen erläuterten Systemeigenschaften (Unterabschnitt 2.2.2) wird zudem deutlich, dass das Verhalten eines Systems über Zustandsübergänge charakterisiert wird. Eine gezielte Beeinflussung von Zustandswahrscheinlichkeiten kann z.B. durch die Steuerung von Zustandsübergängen (Ereignissen) erreicht werden. Das Verhal-

ten (der Objektprozess) eines Systems kann auf diese Weise durch Steuerungsfunktionen, die den Steuerprozess beschreiben, kontrolliert und beeinlusst werden. Mittels geeigneter Strukturen bzw. durch Auswahl zuverlässiger Funktionsträger können verlässliche (Sicherheits-)Funktionen implementiert werden, die das Systemverhalten gezielt und sicherheitsgerichtet beeinflussen. Gleichzeitig unterliegen diese, durch die Funktionsträger implementierten, Sicherungsfunktionen zusätzlich einem funktionsträgerspezifischen Verlässlichkeitsverhalten, welches im Systemsicherheitskontext ebenfalls zu berücksichtigen ist.

In [Slo06] wird das s.g. *ProFunD* Konzept beschrieben, das den Prozess (Pro), die Steuerungsfunktion (Fun) und die jeweilige Zuverlässigkeit der Ressource (D) modellbasiert integrativ berücksichtigt. Die Abgrenzung zwischen Prozess und Funktion erfolgt in Abbildung 4.10 durch die Unterscheidung von Vekehrsprozess und Verkehrssteuerungsfunktion in der idealen (kontinuierlichen und deterministischen) Welt, sowie die jeweils dazugehörigen Verlässlichkeiten in der realen (diskreten und stochastischen) Welt. Es korrespondiert unmittelbar mit dem dreifach hybriden Zustandsmodell aus Abbildung 4.5.

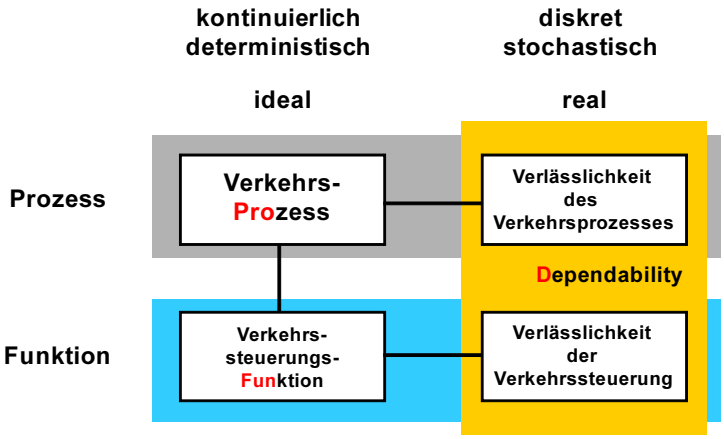


Abbildung 4.10: ProFunD-Konzept nach [Slo06]

Zur Verdeutlichung wird dieses Vorgehen am Beispiel einer Straßenverkehrskreuzung erläutert. Der Verkehrprozess wird unter Berücksichtigung der jeweiligen Fahrtrichtung in Abbildung 4.11 (oben) dargestellt. Die lokalen Zustände können je Fahrtrichtung als *Fzg. vor Kreuzung*, *Fzg. auf Kreuzung* und *Fzg. hinter Kreuzung* definiert werden. Die lokalen Zustandsübergänge (Ereignisse), die zwischen den lokalen Zuständen stattfinden lauten *Einfahren* (E_i) und *Verlassen* (V_i) sowie für ein zyklisches Verhalten das Ereignis *Nächstes Fahrzeug* (N_i). Integriert man zusätzlich die globalen Zustände (*sicher*, *Gefahr* und *Schaden*) analog zu Unterabschnitt 3.2.1 lassen sich diese mit den genannten Zuständen und Zustandsübergängen verknüpfen. Insgesamt lässt sich dadurch das Objekt-/Systemverhalten (der ungesteuerte Prozess) in Abbildung 4.11 (unten) modellieren.

Dieses ideale Modell lässt sich durch diskrete und stochastische Verhalten auf Prozess-

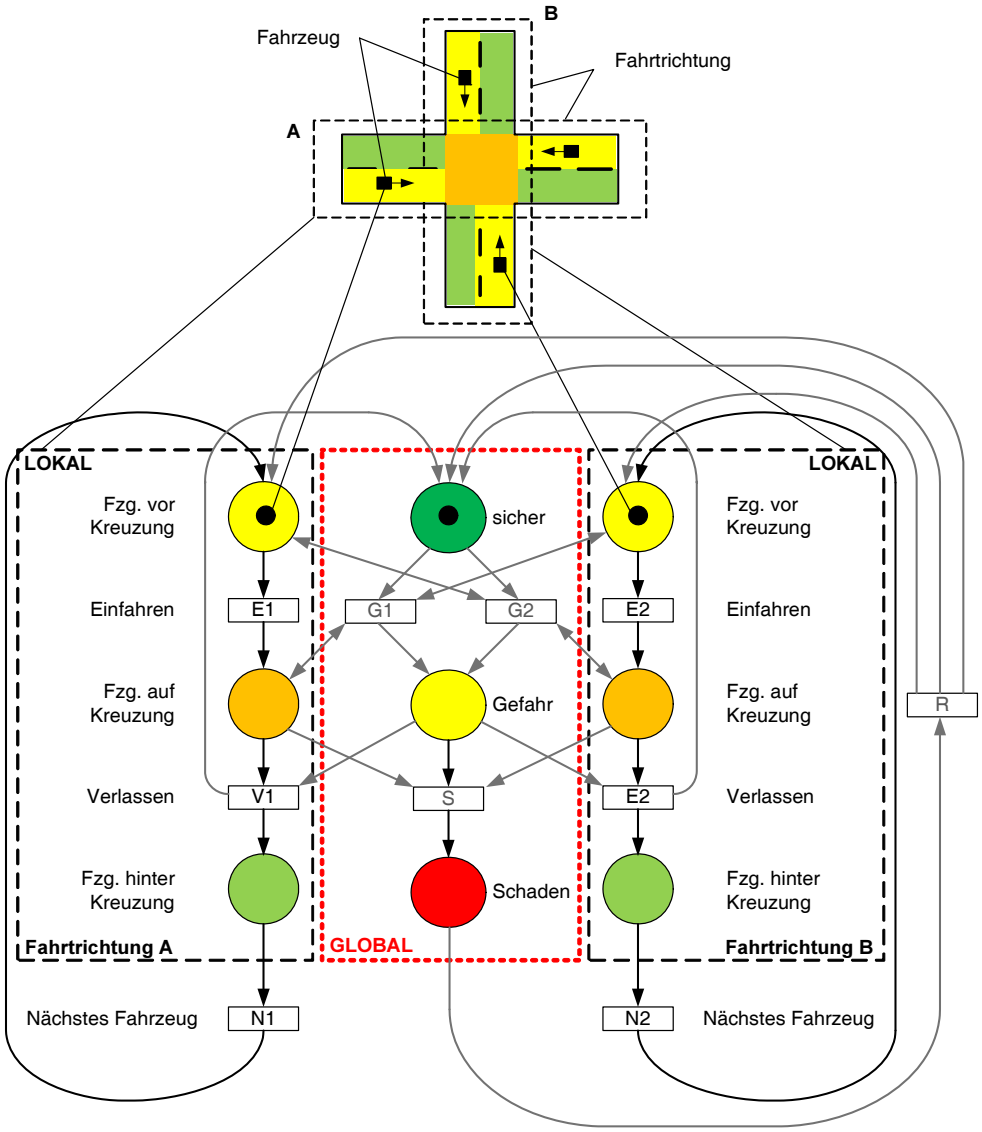


Abbildung 4.11: Prozess einer Straßenverkehrskreuzung

ebene erweitern, um das Modell an ein reales Verhalten anzunähern. Die Zustandsübergänge (Transitionen) des Modells werden dazu nach Vorgabe von zeitbewerteten Petrinetzen stochastisch attributiert. Eine detaillierte Erklärung dieser Modellierungsmethode ist in [Slo06] beschrieben. Zustandsübergänge können auf diese Weise mit spezifischen zeitlichen Verteilungsfunktionen belegt werden.

Das Verhalten von Fahrern, die aufgrund einer vorhandenen Gefahrensituation nicht in eine belegte Kreuzung einfahren, sowie Verhalten in denen Gefahrensituationen unterschätzt werden und trotz existenter Gefahr die belegte Kreuzung befahren wird, sind hierbei auf Modellebene abbildbar.

In Abbildung 4.12 ist das ProFunD Konzept auf den Prozess der Straßenverkehrskreuzung aus Abbildung 4.11 angewendet worden. Das Modell ist zum einen durch eine zusätzliche Funktionalität und zum anderen um Verlässlichkeitsaspekte erweitert worden. Im vorliegenden Beispiel ist eine Sicherungsfunktion, mit der Aufgabe den gegenseitigen Ausschluss der Kreuzungseinfahrt zu unterstützen, integriert worden und wird durch den Funktionsträger Lichtsignalanlage (LSA) implementiert. Dabei wurde aus Gründen der Übersichtlichkeit auf die Modellierung der Gelbphase verzichtet. Das gegenläufige Umschalten der Signale erfolgt über die zeitbehafteten Transitionen (T1) und (T2), welche die zeitlichen Ampelphasen symbolisieren. Diese Funktionalität beeinflusst bzw. bedingt die Zustandsübergänge *Einfahrt (Ei.*[*j..n*]*)* im betrachteten Prozess. Über die Transitionen (E1.1) und (E2.1) sind die Signale (A frei) und (B frei) aus der Funktionsebene verbunden. Neben dem eher idealen Verhalten, auschließlich bei einer autorisierten Freigabe in die Kreuzung einzufahren, kann das reale Verhalten verschiedener Fahrer über deren bereits erwähnte Verlässlichkeit im Modell berücksichtigt werden. Die stochastisch attributierten Transitionen (E1.2), (E2.2), (E1.n) und (E2.n) ermöglichen dazu mit einer spezifizierbaren Wahrscheinlichkeit das Einfahren in die Kreuzung trotz aktiver Belegtzustände (A bel.) oder (B bel.). Gleichzeitig aktiviert dieses Prozessverhalten (unautorisiertes Einfahren in die Kreuzung) den globalen Gefahrenzustand über die Gefährdungen (G1) und (G2). Das auf die menschliche Zuverlässigkeit zurückzuführende Verhalten wirkt sich insbesondere bei langen Rotphasen negativ aus, da aufgrund der stochastischen Verteilung die potenzielle Anzahl der unautorisierten Einfahrten zunimmt. Der Detaillierungsgrad dieser Modellierung kann je nach Bedarf weiter verfeinert werden, um z.B. die Bildung und Auswirkung von Warteschlagen etc. berücksichtigen zu können .

Zusätzlich zum Fahrer als Ressource ist auch die LSA einer spezifischen Verlässlichkeit ausgesetzt, die sich unter anderem durch stochastische Zustandswechsel in zwei unterschiedliche Ausfallzustände vereinfacht ausdrücken lässt. Hier wurde als Beispiel einerseits der sichere Ausfall (Ausfall 2), der sich in der gleichzeitigen Nichtautorisierung beider Fahrtrichtungen auswirkt, sowie andererseits der gefährliche Ausfall (Ausfall 1), der die Autorisierung beider Fahrtrichtungen zur gleichen Zeit bewirkt, unterschieden. Ebenfalls werden die Reparaturraten (Rep 1) und (Rep 2) zur Wiederherstellung des intakten Zustands der LSA im Modell als zeitbehaftete (deterministische) Transitionen berücksichtigt.

Das hier gezeigte Beispiel einer Sicherungsfunktion verfolgt das Sicherungsimplementierungskonzept der „Gefährdungsvermeidung“, indem durch gezielte Maßnahmen die

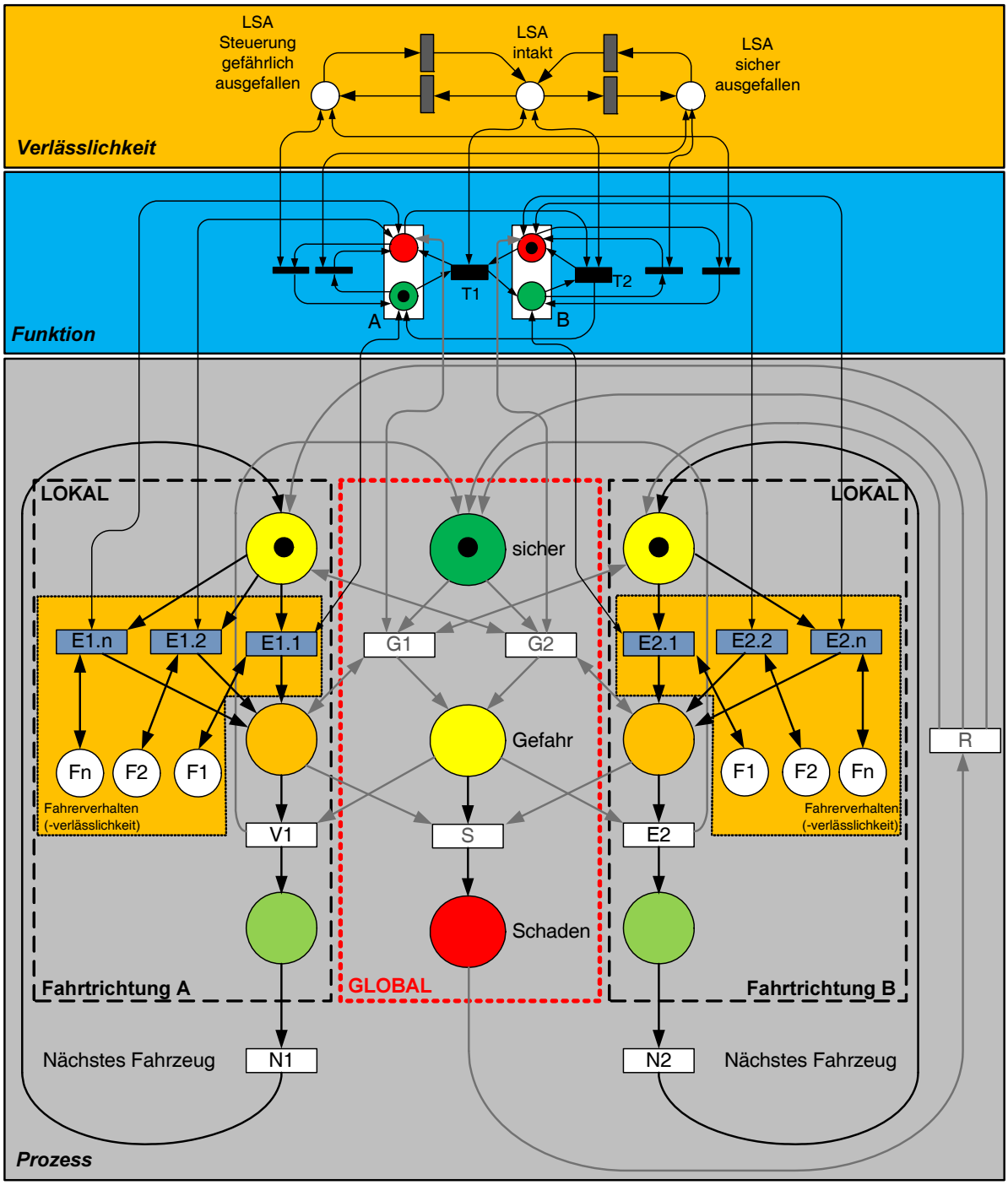


Abbildung 4.12: Prozess einer Straßenverkehrskreuzung nach ProFunD in PN-Darstellung

Vermeidung des Eintritts in den Gefahrenzustand (Gefährdung) beabsichtigt wird. Wie bereits zuvor erläutert zeigt dieses Beispiel, dass eine ausschließliche Verfolgung einzelner Sicherungsimplementierungskonzepte ggf. nicht ausreichend sein kann. Insbesondere die nur schwer beeinflussbare Verlässlichkeit des Fahrers beim Ein- und Ausfahren zeigt hier die Grenzen der Gefährdungsvermeidung auf. Weitere Maßnahmen z.B. der Gefahrenabwehr oder der Auswirkungsminderung könnten je nach Risikoakzeptanz ggf. erforderlich oder ratsam sein.

Für eine Beurteilung des Risikos ist eine Risiko- und Gefährdungsanalyse durchzuführen. In [Slo06] wurde auf dieser konzeptionellen Basis eine detaillierte Risiko- und Gefährdungsanalyse u.a. am Beispiel einer funktionsorientierten Bahnübergangsimplementierung durchgeführt und quantifiziert. Dabei wurde die Verlässlichkeit der Steuerungsfunktion mit einem Verlässlichkeitsmodell des Funktionsträgers (Ressource) sowie dem zugrunde liegenden Prozess modellbasiert verknüpft, um Aussagen über das erreichte Risiko in Verbindung mit der Systemverfügbarkeit auf Basis von unterschiedlichen Steuerungen mit verschiedenen Sicherheitsintegritätsstufen zu gewinnen. [BS02] zeigt dafür u.a. eine Herleitung von Sicherheits- und Verfügbarkeitsanforderungen für Leit- und Sicherungssysteme basierend auf verschiedenen Risikoakzeptanzkriterien.

4.3.3 Maßnahmenallokation auf Verkehrskonstituenten

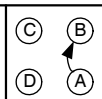
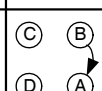
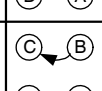
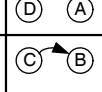
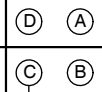
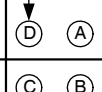
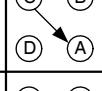
Wie im Vorausgegangenen als auch in Unterabschnitt 4.2.2 gezeigt wurde, haben die Zustandsübergangsraten einen großen Einfluss auf die jeweilige Zustandswahrscheinlicheit und somit auch auf die global ableitbaren Verlässlichkeitsgrößen *Sicherheit* und *Verfügbarkeit*. Gleichzeitig wird deutlich, dass verschiedene Veränderungen dieser Raten unterschiedliche Auswirkungen auf die Sicherheit und vor allem Verfügbarkeit haben. Da grundsätzlich der Verkehr die Ortsveränderung von Verkehrsobjekten beabsichtigt und damit die notwendig verfügbare Erfüllung der Transportfunktion impliziert, ist ein sicheres aber unverfügbares System genauso trivial wie auch aus Gründen der Verfügbarkeit inakzeptabel.

Zur Beeinflussung der Verkehrssicherheit können auf diese Weise verschiedene Maßnahmen, sowohl einzeln als auch in Kombination, abgeleitet werden. Tabelle 4.11 zeigt für die jeweilige Maßnahme (konkrete Veränderung der Übergangsrate von einem Zustand zu einem anderen gemäß des Ergebnisses aus Abbildung 4.8) verschiedene Implementierungsbeispiele differenziert nach den vier Verkehrskonstituenten. Das Vorzeichen des jeweiligen Implementierungsbeispiels ist mit einer Reduzierung (-) oder Vergößerung (+) der jeweiligen Übergangsrate gleichzusetzen.

Wie in Unterabschnitt 4.2.2 gezeigt, verfügen die Maßnahmenkategorien (3) und (4), die gemäß Abbildung 4.7 die Übergangsraten λ_{BC} und μ_{CB} beeinflussen, über das größte Potenzial, die Verkehrssicherheit und gleichzeitig die Verfügbarkeit zu erhöhen bzw. die Schadensrate zu reduzieren. Das verfolgte Sicherungsimplementierungkonzept der Maßnahmenkategorie (3) entspricht der Gefährdungsvermeidung, während bei der Maßnahmenkategorie (4) die Gefahrenabwehr verfolgt wird. Diese Maßnahmenkategorien lassen sich je nach Verkehrskonstituente unterschiedlich implementieren.

Um die Übergangsrate von der sicheren zur gefährlichen Bewegung zu reduzieren (3), können verkehrsobjektseitig z.B. Fahrertrainings, die das sichere Fahren schulen, bzw. eine optimierte Ladungssicherung implementiert werden. Verkehrsmittelseitig lassen sich dieser Kategorie Fahrerassistenzsysteme (FAS), die den Übergang in gefährliche Bewegungen verhindern, zuordnen. Beispiele für solche Fahrerassistenzsysteme sind Spur- oder Abstandshalteassistenten im Straßenverkehr, oder verschiedene Zugsicherungssysteme, die z.T. auch verkehrsinfrastrukturseitig bzw. in Kombination implementiert werden. Infrastrukturseitige Implementierungen können neben der abschreckenden Wirkung durch Geeschwindigkeitskontrollen und aktiver Leittechnik (Signalisierung von Richtgeschwindigkeiten) eine sichere Weggestaltung (weniger Kreuzungen, oder Vermeidung höhengleicher Bahnübergänge) zur Reduktion der Gefährdungsrate beitragen. Die Verkehrsorgansisation, als übergreifende Funktionalität zur Organisation der Verkehrsobjekte, Verkehrsmittel und Verkehrsinfrastruktur untereinander verstanden, kann durch organsiatorische funktionale Maßnahmen ebenfalls zu einer Gefährdungsvermeidung bei den Konstituenten beitragen. Diese funktionalen Maßnahmen werden dann i.d.R. durch die jeweilige Ressource in den Verkehrskonstituenten realisiert (vgl. Trennung Funktion und Ressource Unterabschnitt 2.2.2). Andere Möglichkeiten der Realisierung sind u.a. verkehrskonstituentenunabhängige Schulungsmaßnahmen oder Gesetzesänderungen.

Tabelle 4.11: Konstituentenbezogene Maßnahmen zur Sicherungsimplementierung

		Maßnahmen und Sicherheitsimplementierungen			
		Verkehrsobjekte	Verkehrsmittel	Verkehrsinfrastruktur	Verkehrsorganisation
1		- weniger Güter, Personen	- mehr ÖPNV	- Verkehrsystemwahl	- Verkehrsbündelung
		- weniger Transporte	- mehr Insassen pro Fzg.	- Fahrzeugverbund	- Car Sharing
				- größere Netze	- Zugangsbeschränkungen
					- Eignungstests
2		+ Fahrerlaubnisentzug	+ Stilllegung von Fzg.	+ Maut	+ Verkehrsbündelung
		+ Produktion vor Ort	+ mehr ÖPNV	+ Hohe Fixkosten	+ neue Produktionskonzepte
				+ Verbrauchskosten erhöhen	+ mehr Kontrollen
					+ Marktbeeinflussung
3		- Fahrertrainings (Proaktiv)	- FAS: Lane Keeping Ass.	- sichere Gestaltung	- Trajektorienregelung
		- Ladungssicherung	- Fahrzeugsicherheit erhöhen	- Sicherungstechnik	- Schulungsmaßnahmen
		- Öffentlichkeitsarbeit	- Höchstgeschwindigkeiten	- „Blitzer“	- Gesetzesänderungen
		- Sanktionen		- Leittechnik	- Gefahrenvermeidung
4		+ Fahrertrainings (Handling)	+ FAS: ESP etc.	+ sichere Gestaltung	+ Sanktionen (Bußgelder)
		+ Ladungskontrollen		+ Überwachung	+ gesetzl. Fahrertrainings
				+ Sicherungstechnik (z.B. ATP etc.)	+ Gefahrenabwehr
5		- Eigenschutz (Helm etc.)	- FAS: ABS, etc.	- Einbahnverkehre	- Gesetzesänderungen
		- Ladungssicherung	- bessere Crashsicherheit	-Geschwindigkeitsbegrenzung	- Auswirkungsminderung
			- weniger Bewegungsenergie		
			- besseres Fzg.handling		
6		+ Verkehrssünderkartei	+ autom. Notbremse	+ z.B. Zugsicherungssysteme	+ Sanktionen (Fahrverbot)
			+ z.B. Zugsicherungssysteme	+ Schotterbett (Nothalte)	+ Fail-Safe Konzepte
					+ Gefahrenabwehr
7		+ regelm. Ersthelferausbildung	+ Crashsicherheit	+ Notfallmelder (Säulen)	+ Rettungskonzepte
		+ ausr. Bergungskonzepte	+ Brandschutzkonzepte	+ keine Hindernisse etc.	+ Störfallkonzepte
		+ Notfallkonzepte	+ Rettungsmittelpflicht	+ Schutzeinrichtungen	+ Safety Management
			+ eCall Systeme		+ Notfallmanagement

Im Gegensatz zu den Maßnahmen zur Gefährdungsvermeidung sind Implementierungen der Maßnahmenkategroie (4) bestrebt, ausgehend vom Zustand der gefährlichen

Bewegung (Gefahrenzustand) die Übergangsrate zurück in die sichere Bewegung zu erhöhen, um damit die Wahrscheinlichkeit des unmittelbar bevorstehenden Schadenseintritts zu reduzieren. Das entspricht dem zuvor als Gefahrenabwehr bezeichneten Sicherungsimplementierungskonzept. Auch hier lassen sich für jede Verkehrskonstituente Beispiele aufzeigen. Dazu zählen Fahrertrainings im Straßenverkehr, die eine Beherrschbarkeit des eigenen Fahrzeugs in Gefahrensituationen verkehrsobjektseitig schult und den Fahrer ertüchtigt, mit geeigneten Gegenmaßnahmen die gefährliche Bewegung in eine sichere zu überführen. Eine optimierte Ladungssicherung trägt ebenfalls dazu bei, in Gefahrensituationen das Fahrzeug besser beherrschen und somit leichter in die sichere Bewegung überführen zu können. Verkehrsmittelseitig tragen Fahrerassistenzsysteme, die gefährliche Situationen erkennen und aktiv reagieren, wie z.B. das elektronische Stabilitätsprogramm (ESP)[1], zur Erhöhung der Übergangsrate in die sichere Bewegung bei. Die sichere Gestaltung der Verkehrswege, sowie eine Überwachung gefährlicher Bewegungen mit entsprechender Reaktion z.B. durch aktive Sicherungstechnik (Zugsicherung - ATP[2]) erhöht verkehrsinfrastrukturseitig die Übergangsrate zurück in die sichere Bewegung. Die funktionalen Maßnahmen der Verkehrsorganisation sind mit denen der Gefährdungsvermeidung zu vergleichen.

4.4 Maße der Verkehrssicherheit

4.4.1 Konventionelle Maße der Verkehrssicherheit

Ein übliches Maß für das Verkehrsrisiko auf Systemebene ist die Mortalität, welche sich im Verkehr dann als akkumulierte Zahl von tödlich Verunglückten N_D im Verkehr in bestimmten Gebieten und Zeiträumen ergibt, ggf. ergänzt um einen gewichteten Zuschlag von Leicht- und Schwerverletzten, bezogen auf die jeweilige Bezugspersonenzahl N. Eine gewisse Problematik ergibt sich durch die Bemessung der jeweiligen Bezugspersonenzahl, z. B. die gesamte Bevölkerung oder nur die jeweiligen Verkehrsmittelnutzer, insbesondere einer Verkehrsmode. Die Mortalität m entspricht begrifflich der menschlichen Ausfallrate λ bei technischen Systemen, welche dort idealerweise die Änderung der relativen Anzahl Betrachtungseinheiten pro Zeiteinheit charakterisiert [SD08].

$$m = \lambda = \lim_{T \to 0} \frac{N_D}{N \cdot T} \tag{4.9}$$

Allgemein hängt die Mortalität auch vom jeweiligen Lebensalter t ab, d. h. zuverlässigkeitstechnisch gesprochen treten Frühausfälle, zufällige und Spätausfälle auf.

Aus den statistischen Daten der Sterblichkeit und ihrer Ursachen resultiert die in Abbildung 4.13 dargestellte altersabhängige Mortalität $m(t)$ allgemein und der verkehrsbedingten Mortalität $m_T(t)$ bzw. $\lambda(t)$ in Abbildung 4.14.

[1] Nach aktueller EU Entscheidung müssen neu entwickelte Fahrzeuge, die nach November 2011 ausgeliefert werden mit einem ESP System ausgerüstet sein.

[2] Automatic Train Protection

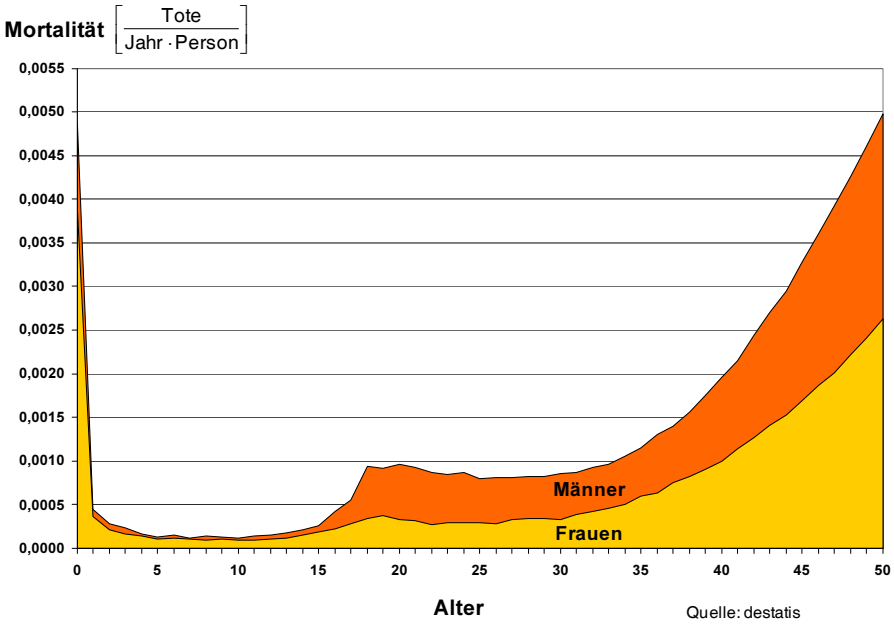


Abbildung 4.13: Mortalität in Deutschland 2002

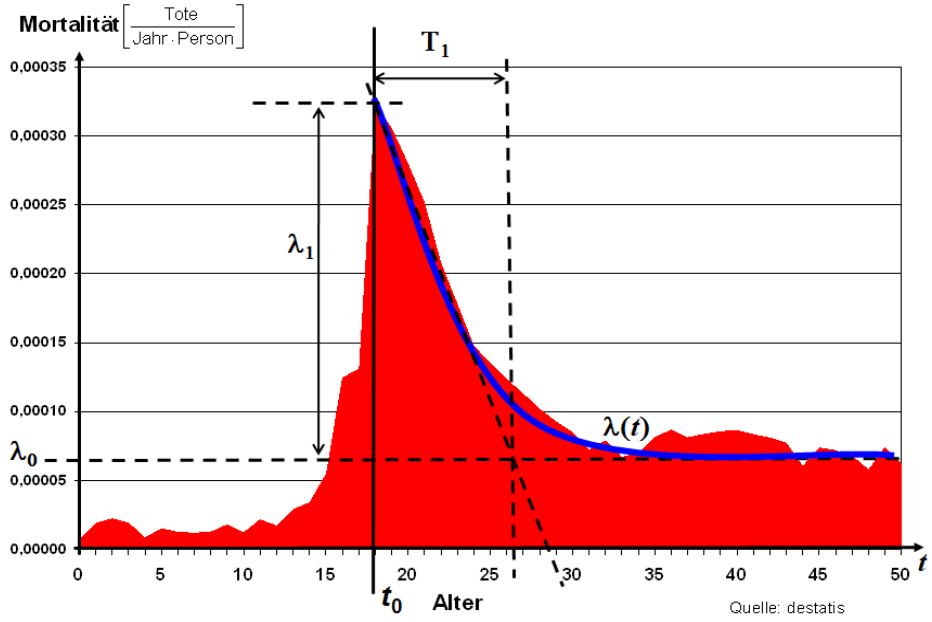


Abbildung 4.14: Verkehrsbedingte Mortalität in Deutschland 2002

Die Ausfallrate λ ist daher altersabhängig und wird in der Zuverlässigkeitstechnik üblicherweise durch eine Weibullverteilung beschrieben. Aus Sicht der Theorie der Zuverlässigkeit kann die Sterblichkeitsratenverteilung durch eine dreiparametrige Weibullverteilung bzw. durch einen vereinfachten Ansatz nach [Tsc05] analytisch beschrieben

werden.

$$\lambda(t) = \lambda_0 + \lambda_1 e^{-\frac{t-t_0}{T_1}} \quad \text{für} \quad t \geq t_0 \tag{4.10}$$

Nach der Zuverlässigkeitstheorie lässt sich über die zeitabhängige Mortalität $m(t)$ bzw. menschliche Ausfallrate $\lambda(t)$ auch die mittlere Lebensdauer T_L bestimmen. Für den Fall zeitabhängiger Ausfallraten muss die mittlere Lebensdauer durch Integration bestimmt werden. Zwischen mittlerer Lebensdauer T_L und mittlerer Mortalität $\bar{m}$ besteht ein reziproker Zusammenhang.

$$\bar{m} = \bar{\lambda} = \frac{1}{T_L} \tag{4.11}$$

Gemessen an der durchschnittlichen Lebenserwartung T_L entsprechend der Vitalität einer Gesellschaft ist im vorzeitigen Todesfall infolge von Unfällen eine individuelle bzw. mittlere Verkürzung der Lebenszeit (Brevitalität, brevis lat. kurz) ΔT anzusetzen. Dieses Risikomaß korrespondiert mit dem aus dem Gesundheitswesen bekannten Maß Years of Life Lost (YLL) [OEC01]. Dabei setzt sich die mittlere Lebenszeitverkürzung ΔT aus dem Erwartungswert der Differenz zwischen mittlerer Lebensdauer und tatsächlichem Lebensalter t_i sowie den zeitlichen Erwartungswerten der Dauer der Verletzung T_{inj} und Behinderung T_{dis} zusammen.

$$\Delta T = E(T_L - t_i) + E(T_{inj}) + E(T_{dis}) \tag{4.12}$$

Bezogen auf die in Abbildung 4.13 für Deutschland dargestellte altersabhängige Sterblichkeitsverteilung ergibt sich nach Auswertung der verkehrsbedingten Todesfälle für das Jahr 2002 eine Verringerung der mittleren Lebensdauer von ca. 3 Monaten.

Mit der verkehrs- und modalspezifischen Angabe der verkürzten Lebensdauer (Brevitalität) liegt ein absolutes Maß des Risikos im Verkehr vor.

Hinsichtlich der Risiken an Leib und Leben wird damit trotz ihrer Verschiedenartigkeit eine einheitliche Bemessung möglich. Sie orientiert sich an der Zuverlässigkeitsberechnung technischer Systeme hinsichtlich ihrer uneingeschränkten Nutzungsdauer. Dort wird zwischen reparierbaren und nicht reparierbaren Systemen unterschieden, was der Unterscheidung zwischen Unfall mit Wiederherstellung durch Genesung bzw. mit Todesfolge entspricht. Im Krankheitsfall als Unfallfolge ist auch die uneingeschränkte Lebensteilhabe um die Genesungsdauer reduziert. Im Fall von schweren Verletzungen oder fortdauernden Behinderungen kann ihr Grad für die Verkürzung der weiteren uneingeschränkten Lebensteilhabe angesetzt werden.

Für verkehrsunfallbedingte Schäden an Leib und Leben ergibt sich danach ein Maß (Vitalität und Brevitalität) mit zeitbezogener Einheit. Zwischen der Mortalität und dem Verhältnis auf die mittlere Lebensdauer bezogene mittlere Lebensdauerverkürzung (relative Brevitalität) besteht folgender Zusammenhang:

$$T_L - \Delta T = \frac{1}{\bar{\lambda} + \Delta\lambda} \tag{4.13}$$

Hinsichtlich des Begriffs Sicherheit, insbesondere seines Begriffsumfangs, wird gern von einer hundertprozentigen Sicherheit in idealer Weise gesprochen. Diese Angabe hat zwei Aspekte, einmal ist der Sicherheitsbegriff explizit als Größe ausgewiesen und benannt, zum anderen ist sie hinsichtlich einer maximal erreichbaren Ausprägung quantitativ definiert, wenn auch relativ und damit verhältnisskaliert. Der zur Sicherheit emotional negativ belegte Risiko- bzw. komplementäre Gefahrenbegriff mit der ebenfalls negativ besetzten Größe Mortalität wird so vermieden. Es stellt sich die Frage, ob für die Verkehrssicherheit ebenfalls eine derartige positiv besetzte Begriffsbildung mit neutraler Dimension und quantitativ aufsteigender Skalierung in Korrelation zum Sicherheitsbegriff gefunden werden kann.

Ein sehr anschauliches Sicherheitsmaß wurde von Heilmann in [Hei02] im Gesundheitswesen vorgeschlagen. Dabei werden die spezifischen Todesfälle N_D in einem definierten Zeitraum auf die jeweilige Gesamtpopulation N bezogen. Als Sicherheitsgrad S_g definiert Heilmann den negativen dekadisch logarithmierten Quotienten, der bei höchster Sicherheit unbeschränkt wächst. Logarithmische Maße und Skalen sind in anderen Lebens- und Wissenschaftsbereichen etabliert, z. B. der pH-Wert in der Chemie, der dB-Wert in der Akustik, die Richter-Skala in der Seismologie. Der Heilmannsche Sicherheitsgrad ist auch mit der spezifischen Mortalitätsrate ermittelbar:

$$S_g = -\log \frac{N_D}{N} = -\log(\Delta\lambda \cdot 1Jahr) \in [0, \infty) \tag{4.14}$$

Dieses positiv besetzte, relative Sicherheitsmaß berücksichtigt allerdings noch keine nationalen oder kulturellen Unterschiede, wie es z. B. der Life Quality Index (LQI) vorsieht [Rac02]. Dieses allgemein positiv empfundene Maß für die Lebensqualität setzt sich in komplexer Weise aus mehreren Einzelindikatoren weitgehend multiplikativ zusammen. Einer seiner Faktoren ist die mittlere Lebenserwartung, die insgesamt für den Vergleich der Lebensqualität unterschiedlicher Nationen und Gesellschaften eine signifikante Rolle spielt. Auch diese kulturell unterschiedliche Wahrnehmung von Risiken wurde wissenschaftlich diskutiert, was auf verschiedene Bewusstseins- und gesellschaftliche Zustände hinweist. Dies kann u. U. erklären, warum Sicherheitskennzahlen national so verschieden sein können.

4.4.2 Neue Maße der Verkehrssicherheit

In [SD08] wurde daher als Sicherheitsmaß ein spezifischer Sicherheitsindex ψ vorgeschlagen, der die durch spezifische Ursachen, z.B. den Verkehr, verkürzte Lebenszeit auf die mittlere Lebensdauer einer Gesellschaft bezieht und aus diesem Verhältnis ein logarithmisches Maß bestimmt.

$$\psi = -\log \frac{\Delta T}{T_L} \approx \log \frac{\Delta\lambda}{\bar{\lambda}} \in [0, \infty) \tag{4.15}$$

Dieser Sicherheitsindex steigt monoton mit verringerter Lebensverlustzeit und hat derzeit für deutsche Verhältnisse den verkehrsspezifischen Wert 2,49 [SD08].

Durch einfache Umrechnung findet man auch hier den Heilmann-Sicherheitsgrad wieder, allerdings berücksichtigt der Sicherheitsindex auch die Umstände der örtlichen Lebensqualität durch die mittlere Lebensdauer T_L.

$$\psi = S_g - \log\left(\frac{T_L}{1 \cdot Jahr}\right) \tag{4.16}$$

Häufig werden für die Angabe des Verkehrsrisikos in jährlicher Folge nur die absoluten Werte für Verkehrstote oder Verletzte gemeldet, um deren fortlaufenden Rückgang hervorzuheben. Noch beeindruckender sind diese Zahlen im Verhältnis bezogen auf die modale jährliche Verkehrsleistung, zumeist in Fahrzeug- oder Personenkilometer pro Jahr, weil hier noch stärkere Rückgänge zu verzeichnen sind. Bei dieser Skalierung ist eine eindeutige qualitative Ordnung der Risiken der jeweiligen Verkehrsmoden klar erkennbar. Werden die absoluten Risikowerte auf den jeweiligen Zeitraum der Verkehrsmittelnutzung bezogen, ergibt sich jedoch eine andere Reihung. Der einseitige Bezug auf die Verkehrsleistung - für gewisse Verkehrsmoden durchaus vorteilhaft - verliert an Argumentationskraft, denn wissenschaftlich hängen die Werte jedoch durchaus zusammen und können ineinander überführt werden. Ansatz ist die Definition der obigen Risikomaße und ihr Verhältnis, aus dem sich die modalspezifische mittlere Reisegeschwindigkeit ergibt. Über den Modal Split und das fragliche Mobilitätsbudget lassen sich die Risikomaße ineinander überführen.

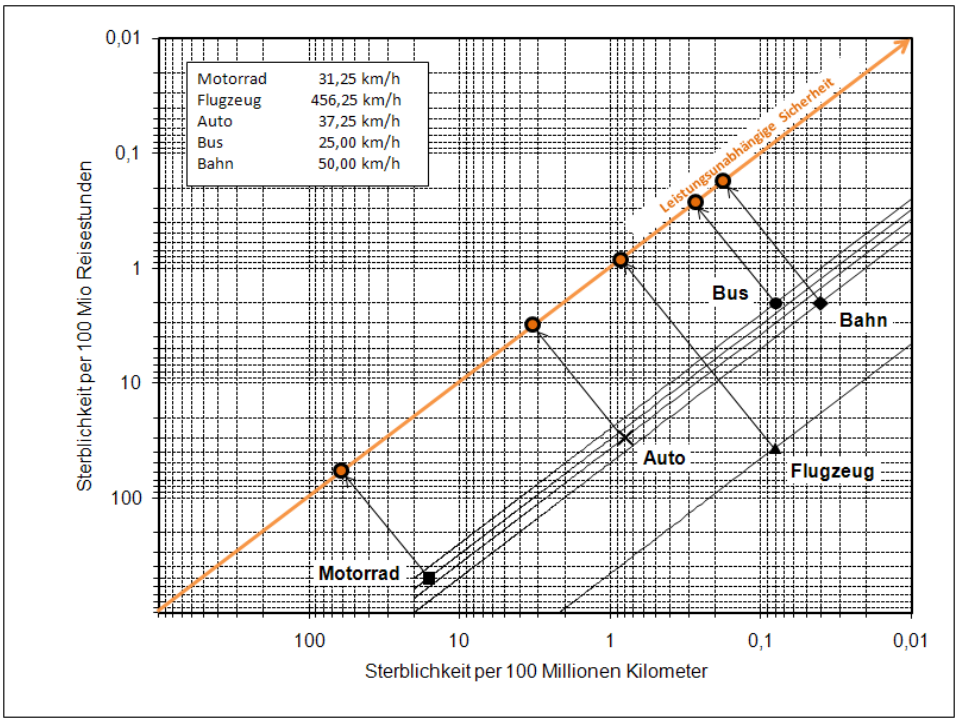


Abbildung 4.15: Verkehrsleistungs- und zeitliche verkehrsteilhabebezogene Risikowerte

Abbildung 4.15 zeigt die unterschiedliche Reihung der Verkehrsmoden und deren Über-

führung über die mittlere Reisegeschwindigkeit.

Die mittlere jährliche Reisedauer $\bar{\tau}_i$ pro Person lässt sich über den Modal Split V und das landesspezifische Mobilitätsbudget b bestimmen, welches für 2002 in Deutschland mit 85 min pro Person und Tag ermittelt wurde [Inf03].

$$\bar{\tau}_i = V \cdot \frac{b \cdot 365 Tage}{60 min} \tag{4.17}$$

Die mittlere jährliche Reiseentfernung $\bar{s}_i$ pro Person hängt mit der mittleren Reisedauer $\bar{\tau}_i$ über die mittlere modalspezifische Reisegeschwindigkeit zusammen.

$$\bar{v}_i = \frac{\bar{s}_i}{\bar{\tau}_i} \tag{4.18}$$

Aus den zumeist vorliegenden Werten der Verkehrsopfer N_{D_i}, Verkehrsleistung und mittleren Geschwindigkeit lässt sich dann auch die Ausfallrate berechnen. Dabei muss immer berücksichtigt werden, welche Expositionszeit zugrunde gelegt wird. Die Angabe der Verkehrsleistung berücksichtigt nur die tatsächliche Expositionszeit, d. h. Reisezeit τ. Die wegbezogenene Mortalität m_{T_s} hängt somit direkt über die mittlere Reisegeschwindigkeit und indirekt über das Mobilitätsbudget mit der zeitbezogenen Mortalität m_{T_τ} zusammen.

$$m_{\tau_s} = \frac{N_{D_i}}{N \cdot \bar{s}_i} \tag{4.19}$$

$$m_{\tau_t} = \frac{N_{D_i}}{N \cdot \bar{\tau}_i} \tag{4.20}$$

$$\frac{m_{T_\tau}}{m_{T_s}} = \bar{v}_i \tag{4.21}$$

$$\lg \frac{m_{T_\tau}}{m_{T_{t_0}}} = \lg \frac{v_i}{v_0} + \lg \frac{m_{T_s}}{m_{T_{s_0}}} \tag{4.22}$$

Die expositionszeitbezogenen Angaben sind für Risikoprognosen bedeutsam, die von Gefährdungsanalysen ausgehen, welche auf den grundsätzlich zeitbezogenen Ausfallraten von einzelnen Komponenten beruhen. Mit den Methoden der Technischen Zuverlässigkeit kann dann eine Systemgefährdungsrate ermittelt werden. Diese sollte unterhalb existierender Risikowerte liegen und ist nur so akzeptierbar. Das akzeptable Risiko wird dann durch die so genannte Tolerable Hazard Rate THR bestimmt.

4.4.3 Sicherheitsmaße der Verkehrskonstituenten

Im Laufe der Weiterentwicklung der verschiedenen Verkehrssysteme haben sich verschiedene Sicherheitsmaße innerhalb der einzelnen Verkehrsdomänen durchgesetzt. Während sich im Schienenverkehr eine eher risikoorientierte Denkweise auf Systemebene ausgeprägt hat, wird im Straßenverkehr vorwiegend die in unterschiedliche Schwereklassen eingeteilte Schädigung als Häufigkeit in den Vordergrund gestellt. Dabei wird in den

meisten Fällen zwischen Personenschäden sowie leichten und schweren Sachschäden unterschieden. Auffallend ist dort auch die stark isolierte konstituentenbezogene Ausrichtung der verschiedenen Kenngrößen im Straßenverkehr, die im Schienenverkehr auf diese Weise nicht vorzufinden ist.

Wird beispielsweise die Konstituente **Verkehrsmittel** betrachtet, werden im Straßenverkehr Sicherheitsbewertungen von Fahrzeugen auf Basis von standardisierten Unfallversuchen durchgeführt. Die Bemessung der Fahrzeugsicherheit wird mit einem auf die Überlebenswahrscheinlichkeit der Insassen abgestimmten Punktesystem und einer abschließenden Bewertung in Form von Sternen durchgeführt. Diese Überlebenswahrscheinlichkeit basiert auf der Auswertung von Messpunkten an unterschiedlichen Körperpartien eines künstlichen Versuchsmenschen (Dummy). Der s.g. 50%-Hybrid III Dummy, der beispielsweise für Frontalcrashversuche eingesetzt wird, verfügt über Messpunkte zur Aufnahme von Beschleunigungen, Kräften und Momenten an bis zu sechs unterschiedlichen Positionen (Kopf, Hals, Brust, Oberschenkel, Schienbein und Fuß) [Sei92].

Abbildung 4.16 zeigt eine Zusammenfassung der im EURO NCAP[1] am häufigsten verwendeten Prüfverfahren.

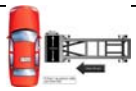
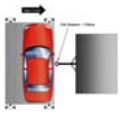
Frontalcrash 	40%-Offset mit deformierbarer Barriere	64km/h
Seitencrash 	Deformierbare Barriere auf Fahrermitte gerichtet	50km/h
Pfahlcrash 	Stahlpfahl auf Kopfmitte des Fahrers gerichtet	29km/h
Fußgänger 	Körperkomponente mit Fahrzeugfront / Motorhaube	40km/h
Kopfaufprall im Innenraum	Punkte auf Basis des angegurteten Fahrers	24km/h
Heckcrash 	Barriere auf das Heck in Fahrzeuglängsrichtung	50km/h
Überschlagtest 	Vom 23° geneigten Schlitten	50km/h

Abbildung 4.16: Tabellarische Zusammenfassung der Euro-NCAP Prüfverfahren

Zusätzlich zur Bewertung des reinen Insassenschutzes haben sich die Bewertung der Fahrzeugsicherheit und damit auch die Unfallversuche auf den Fußgängerschutz und die Kindersicherheit ausgerichtet und eigens darauf abgestimmte Bewertungen eingeführt,

[1]EURO NCAP - European New Car Assessment Programme ist eine Vereinigung europäischer Verkehrsministerien, Automobilclubs und Versicherungsverbänden.

die jedoch derzeit noch nicht in die Gesamtbewertung eines Fahrzeugs mit einbezogen werden. Kopfaufprall, Heckcrash und Überschlagtest sind nicht Bestandteil des Standard Euro NCAP und werden nach Bedarf entsprechend Amerikanischer Normen (FMVSS - Federal Motor Vehicle Safety Standard) durchgeführt [Kra06].

Derzeit existieren weltweit unterschiedliche Prüfverfahren zur Fahrzeugsicherheit, die sich in Euro NCAP, US NCAP (NHTSA), Japanese NCAP und Australian NCAP aufteilen. Abbildung 4.17 zeigt die einzelnen Prüfverfahren der einzelnen Programme und deren Unterschiede. Die einzelnen Prüfmethoden weichen teilweise erheblich voneinander ab, so dass Bestrebungen einer Zusammenführung zu einem World oder auch Global NCAP existieren, mit der Absicht, die Prüfverfahren zu harmonisieren und so eine objektive Vergleichbarkeit zu schaffen. Im Gegensatz zu den anderen NCAP verfolgt derzeit das Euro NCAP als einziges ein Prüfverfahren zum Fußgängerschutz. Beim Seitenaufprall werden grundsätzlich, mit Ausnahme des Australian NCAP, vergleichbare Verfahren angewendet. Im vorgeschlagenen World NCAP könnten sämtliche Prüfverfahren harmonisiert werden, um die größtmögliche Aussagekraft für die Bewertung der Fahrzeugsicherheit bieten zu können.

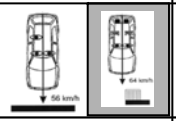
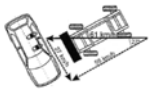
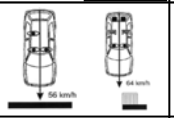
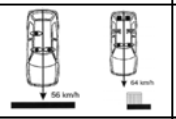
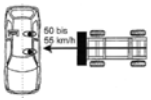
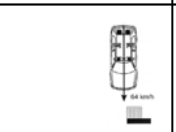
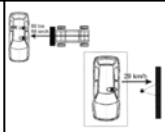
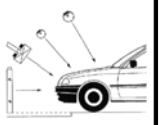
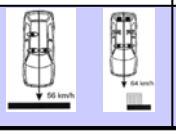
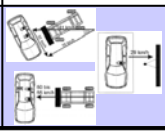
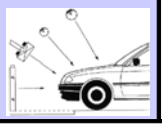
	Gründung	Bewertung	Frontalaufprall	Seitenaufprall	Fußgänger
US NCAP/ IIHS	1978	5 Sterne: Frontalaufprall Seitenaufprall			
Australian NCAP	1992	5 Sterne: Frontalaufprall			
Japanese NCAP	1996	1(bad)-6(good): Kombi. Frontal- Seitenaufprall			
Euro NCAP	1997	4/5 Sterne: Insassenschutz Fußgängerschutz Kindersicherheit			
World NCAP					

Abbildung 4.17: Bestehende internationale NCAP-Prüfverfahren im Überblick

Als Kenngrößen der **Verkehrsobjekte** lassen sich ebenfalls etablierte Beispiele finden. Es haben sich für die Personen- /Fahrgastsicherheit zwei grundlegende ineinander überführbare Bewertungen etabliert, die jedoch bei genauerem Hinsehen ebenfalls eher einer Bewertung des Insassenschutzes zugeordnet sein sollten. Das „Head Injury Criterion (HIC)“ und die „Abbreviated Injury Scale (AIS)“ bewerten nach einem ebenfalls standardisierten Verfahren zum Prüfablauf und Vermessung der Auswirkungen die Ver-

letzungsschwere des Fahrgastes. Die Klassifikation, die bei der Bewertung der Überlebenswahrscheinlichkeit durch die AIS-Skala getroffen wurde, ist unabhängig von der Art der Behandlung und Behandlungsqualität. Sie reicht von „Minor"-Verletzungen (AIS-Code 1), welches in etwa Schürfwunden entspricht, bis hin zu „nicht behandelbar" (AIS-Code 6) und somit zum Todesfall. Der Kopfverletzungs-Faktor (Head Injury Criterion - HIC) beschreibt indes ein Kriterium zur Bewertung von Kopfverletzungen in Folge eines Fahrzeugunfalls. Das HIC berechnet sich aus der resultierenden Kopfbeschleunigung a in g (Vielfaches der Erdbeschleunigung) in einem betrachteten Zeitintervall t_1 bis t_2.

$$HIC = [\frac{1}{t_2 - t_1} \int_{t_1}^{t_2} a(t)\mathrm{d}t]^{2,5}(t_2 - t_1) \tag{4.23}$$

Eine Bewertung der Sicherheit von Sachgütern ist nicht bekannt, sofern von den Gefahrgutklassen als eher komplementäres Maß abgesehen wird [Ver07].

Eine Sicherheitseinstufung der **Verkehrswegeinfrastruktur** hat sich erst in den letzten 10 Jahren durch Bewertungen von Straßennetzen entwickelt. Im Jahr 2005 wurde die durch den deutschen Automobilclub ADAC[1] maßgeblich in Form von Straßentests durchgeführte Bewertung „EuroRAP" (European Road Assessment Programme) eingeführt (vgl. http://www.eurorap.org vom Februar 2009) sowie die 2005 eingeführte Überprüfung der Tunnelsicherheit „EuroTAP" (European Tunnel Assessment Programme) (vgl. http://www.eurotap.eu vom Februar 2009). Im Rahmen dieser Straßentests wurden insgesamt 8000 km Straßen in Deutschland befahren und deren passive Sicherheit von Experten bewertet. Europaweit wurden 152 Tunnel durch systematische Tests, die aus rund 250 Prüfpunkten bestehen, beurteilt. Sicherheitsrelevante Kriterien für diese Bewertung der Straßenabschnitte sind beispielsweise das Vorhandensein von „Gegenverkehrstrennungen", „hindernisfreie Seitenräume", „Schutzeinrichtungen vor Hindernissen" an Kreuzungen sowie an den Knoten die „Ausbildung von Kreuzungen und Einmündungen mit Überführungsbauwerken oder Kreisverkehren". Die Bewertung der Straßenabschnitte erfolgt analog zum NCAP auf einer Skala von bis zu vier Sternen während die Sicherheit von Tunneln in fünf Güteklassen bewertet wird. Dabei ergibt sich die Gesamtnote aus dem Durchschnittswert der Einzelnoten zum Tunnelsystem, der Beleuchtung und Stromversorgung, der Verkehrsinformations- und leittechnik, den Kommunikationsmöglichkeiten, Fluchtweggestaltung, dem Brandschutzkonpzept, der Beleuchtung und dem vorhandenen Notfallkonzept. Ein Bezug zum tatsächlichen Unfallgeschehen wird allerdings weder in der Bewertung der Straßenabschnitte noch in der Tunnelbewertung hergestellt.

Auf Grundlage der von der Forschungsgesellschaft für Straßen und Verkehrswesen (FGSV) erstellten „Empfehlung für die Sicherheitsanalyse von Straßenverkehrsnetzen" wird ein s.g. „Sicherheitspotenzial" vorgestellt [For03]. Dieses Maß resultiert aus einem Verfahren, das für alle Straßenarten, unter Beürcksichtung des tatsächlichen Unfallgeschehens, die Abschnitte ermittelt, bei denen durch straßenbauliche Maßnahmen ein großes „Sicherheitspotenzial" gegeben ist. Dieses „Sicherheitspotenzial" errechnet sich aus der durch bauliche oder verkehrsregelnde Maßnahmen vermeidbaren Anzahl

[1] Allgemeiner Deutscher Automobil-Club

und Schwere der Straßenverkehrsunfälle, ausgedrückt durch die vermeidbaren volkswirtschaftlichen Verluste pro Kilometer und Jahr.

Eine etablierte Bewertung bzw. Kenngrößen der **Verkehrsorganisation** konnten im Rahmen der Arbeit nicht identifizert werden. Aufgrund der physischen Implementierung der zugehörigen Funktionen innerhalb der drei anderen Verkehrskonstituenten als Funktionsträger ist eine bisherige Fokussierung auch eher unwahrscheinlich.

5 Methode zur Identifikation generischer Gefahren

Eine Gefahr ist, wie bereits in Unterabschnitt 3.2.1 beschrieben, definiert als Situation, die potenziell zu einen Schaden führen kann. Ein häufig anzutreffendes Problem ist die Abgrenzung von Gefahren auf unterschiedlichen Systemebenen, z.B. zwischen Komponentenausfällen und Situationen (Zuständen) eines Systems zu differenzieren. Zu identifizierende Gefahren, deren Risiko im Rahmen einer Systementwicklung zu betrachten ist, sind auf einer definierten Systembebene zu identifizeren und so zu beschreiben, dass sie unmissverständlich von allen Beteiligten wahrgenommen und interpretiert werden können. In den folgenden Abschnitten wird eine Methode vorgestellt, die es ermöglicht aus einer Systemstruktur potenzielle Gefährdungen systematisch zu identifizieren, und potenzielle Auswirkungen zuzuordnen, um eine einheitliche Dokumentation von Gefahren(-situationen), unter Berücksichtigung der spezifischen Gefährdungen und Auswirkungen, zu erwirken.

5.1 Gefahrenartefakte am Beispiel Stellwerksapplikation

In der Systemsicherheitsdomäne existieren unterschiedliche Methoden zu Identifikation und Analyse von Gefahren. [Eri05] zeigt eine umfangreiche Auswahl von Methoden, die je nach Lebenszyklusphase und Zielsetzung ihre unterschiedliche Anwendung finden. Meist sind die Methoden jedoch nicht allein auf die Identifikation von Gefahren ausgelegt, sondern dienen gleichzeitig zur Gefahrenanalyse und -bewertung und erfordern oft eine nicht zu vernachlässigende hohe Disziplin, um sich nicht auf unterschiedlichen Systemebenen zu verzetteln.

Das primäre Problem der verfügbaren Methoden ist die leicht zu verlierende Systematik und eine schwer zu beurteilende Vollständigkeit des betrachteten Gefahrenumfangs im Vergleich zu dem theoretisch aus den Systemeigenschaften abbleitbaren Gefahrenumfang. Aus diesem Grund verwendet die vorgestellte Methode ein formales Systemmodell als Basis und konstruiert systematisch Gefahrensituationen, nachfolgend als Gefahrenartefakte bezeichnet. Eine Vermischung der unterschiedlichen Systemebenen (Detaillierungsebenen) wird unter der Voraussetzung eines konsistenten Systemmodells vermieden.

In einem ersten Ansatz werden domänenspezifische Situationen, die mit einem Schaden in Verbindung stehen, untersucht. Für das Beispiel Stellwerksapplikation lassen sich

die möglichen Schadensereignisse auf oberster Ebene in die Klassen „Kollisionen“, „Entgleisung“ und „Sonstige Unfälle“ einteilen, die verschiedene Ursachen als Auslöser haben können. Eine Entgleisung im Schienenverkehr kann beispielsweise durch einen Schienenbruch hervorgerufen werden. Allerdings führt nicht jeder Schienenbruch zwangsläufig zu einer Entgleisung inkl. Schaden. Zwischen dem Zustand der Gefahr und dem daraus möglicherweise resultierenden Schadenszustand ereignet sich ein Zustandsübergang, der generell mit dem Begriff “Unfallereignis”, welcher der in Unterabschnitt 3.2.3 beschriebenen „Schädigung“ entspricht, umschrieben wird. Diese Unfallereignisse lassen sich baumartig in weitere Untergruppen klassifizieren, die je nach Anwendungsdomäne unterschiedlich ausfallen können. Abbildung 5.1 zeigt eine angenommene Differenzierung der Unfallereignisse für den Schienenverkehr.

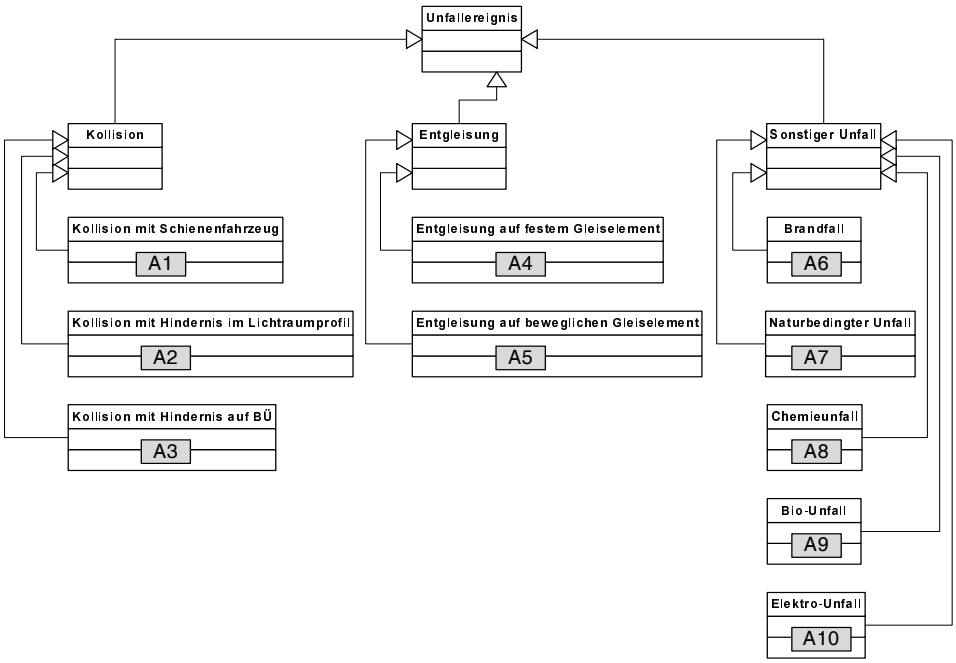


Abbildung 5.1: Differenzierung der Unfallereignisse im Schienenverkehr

Für die Festlegung möglicher Gefahrenzustände sind verschiedene Unfallursachen zu berücksichtigen. Für das Eintreten eines gefährlichen Zustandes (Gefahrenzustand) bedarf es einer spezifischen Anzahl von Bedingungen. Beispielsweise muss ein Schienenbruch mindestens mit der Möglichkeit von darüber verkehrenden Schienenfahrzeugen zusammentreffen, um eine Gefährdung auszulösen. Zusätzlich wird davon ausgegangen, dass wiederum jede Bedingung eine unbestimmte Anzahl von Vorbedingungen (Ursachen) hat, die jeweils erneut durch Vorbedingungen kausal verknüpft sind.

Die Kombinationen aus Gefahrenursache, als Auslöser einer Gefährdung (Gefahreneintritt), und möglichem daraus resultierenden Unfallereignis bilden somit die wesentlichen Bestandteile eines Gefahrenartefaktes. Die Definition eines Gefahrenartefaktes wird somit wie folgt beschrieben:

"Die Dokumentation einer Menge gefährlicher Bedingungen (Gefährdung), die zu einem gefährlichen Zustand (Gefahr) mit dem Potenzial der Schädigung für Personen und Gegenstände (Schadenszustand) aufgrund eines Unfallsereignisses führen."

5.1.1 Struktur- und Funktionsanalyse

Bei einem formalen, systematischen Vorgehen zur vollständigen Auflistung von Gefahren ist ein umfangreiches Systemwissen mit einer eindeutigen Systemdefinition erforderlich. Hier wird daher die statische Systemstruktur der logischen Funktionen und physischen Elemente (Ressourcen) eines generischen Stellwerks in einem Strukturdiagramm (vgl. Abbildung 5.2) zusammengestellt. Elemente wie Signale, Weichen, Bahnübergang, Gleissperre u.v.m. werden allgemeingültig einbezogen und stellen weder die implementierte Architektur von Software noch von Komponenten dar. Die Darstellung der Struktur beschreibt eine Sicht auf die beteiligten Elemente und deren Zusammenhänge innerhalb einer Stellwerksapplikation. Entscheidend bei der Einteilung dieser Systemstruktur sind die Relationen zwischen den einzelnen Objekten, die dadurch das Zusammenwirken beschreiben und somit die Funktionalität des Gesamtsystems widerspiegeln.

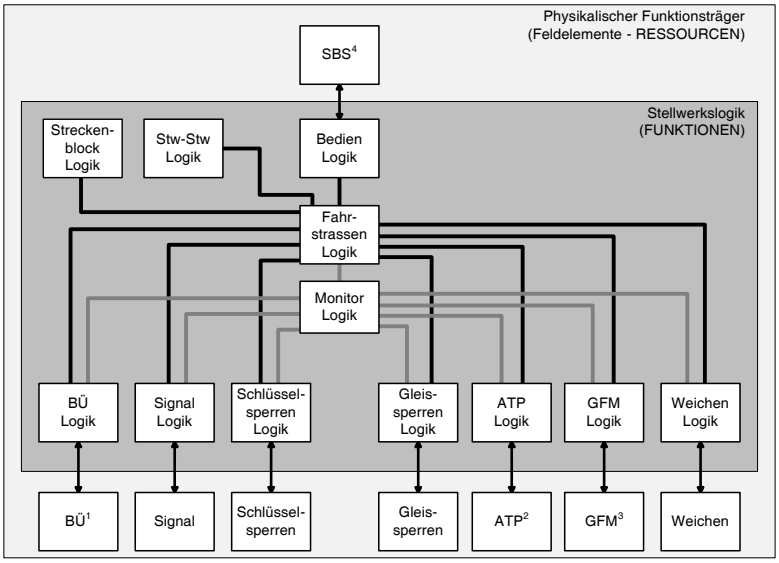


Abbildung 5.2: Abstrakte Struktur des Systems "Stellwerk"

Die in der Eisenbahnfachwelt weit verbreitete Vorgehensweise, Systeme auf der Komponentenebene Bottom-Up zu analysieren, ist hier durch eine Analyse der einzelnen

[1]BÜ - Bahnübergang, trifft nur zu bei signalabhängiger Einbindung in Fahrstraßen.
[2]ATP - Automatic Train Protection (Zugsicherungssystem), trifft nur zu bei direkt mit dem Stellwerk verbundenen Systemen.
[3]GFM - Gleisfreimeldeeinrichtung, z.B. Gleisstromkreise, Achszählsysteme etc.)
[4]SBS - Standard Bedienschnittstelle, Schnittstelle zum Bedienplatz des Fahrdienstleiters

Funktionen aus Stellwerkssicht ersetzt worden. Funktionen werden dabei durch Abläufe unterschiedlicher Prozesse vereinfacht betrachtet. Beispielsweise werden für einen Weichenantrieb die Funktionen der Weichenlagenänderung mit anschließender Endlagenerkennung festgelegt. Der interne Aufbau der Komponenten bleibt dabei unberücksichtigt, da dies im späteren Aufgabenbereich des jeweiligen Herstellers liegt. Grundsätzlich liegt der Betrachtung dabei stets das in Abbildung 5.3 skizzierte, an einen geschlossenen Regelkreis angelehnte, Prinzip zugrunde.

Unterschieden werden dort die vier Blöcke: „Logische Funktionen“, „Stellgrößen/-befehle“, „Ausführung“ und „Meldungen“. Dabei werden als “Meldungen” die vorhandenen Systemzustände sowohl der physikalischen Elemente (z.B. Weichenendlage) als auch der logischen Elemente (z.B. Variablen) erkannt. Die „Logische Funktion“ setzt die so erkannten Ist-Systemzustände mit den erforderlichen Soll-Systemzuständen (z.B. aus Vorschriften, Signalisierungsprinzipien, Flankenschutzregeln, Vorgaben etc.) in Beziehung, um mit den daraus ggf. resultierenden Abweichungen entsprechende Entscheidungen zu treffen (z.B. notwendiges Umlaufen einer Weiche für erforderlichen Flankenschutz). Diese Entscheidungen werden in Form von Kommandos bzw. Befehlen (hier: „Stellgrößen/-befehle“ an das jeweilige (Feld-)Element übertragen (z.B. Befehl: Richtungsänderung an Weiche), welches diese entsprechend ausführt (hier: „Ausführung“).

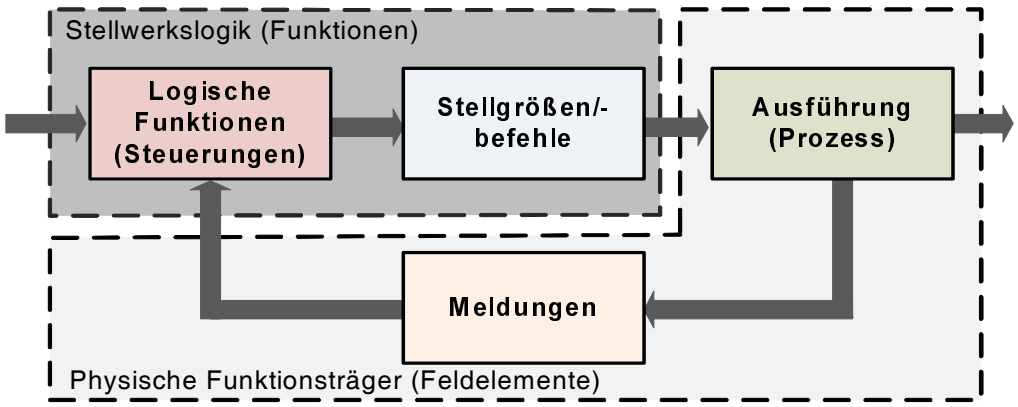


Abbildung 5.3: Regelkreisstruktur als Basis funktionaler Analysen

Nach einem Überblick über die allgemeine Systemstruktur sowie deren funktionale Regelkreisstruktur wird das Verhalten tiefer gehend in der Form untersucht, dass die funktionsinternen Prozesse sowie die zwischen den Prozessen auszutauschenden Informationen analysiert werden. Erkennbar ist in Abbildung 5.4 die Interaktion des physischen Feldelements “A” (z.B. Weiche mit dem physischen Prozess Weichenlagenänderung), mit der zugehörigen Stellwerkslogik „A“ mitsamt des internen Prozesses (z.B. Weichenlagenentscheidung). Die zwischen den Prozessen auszutauschenden Informationen stellen die Stellgrößen und Meldungen zur Gewährleistung der Funktion dar.

Unter Berücksichtigung der Systemstruktur aus Abbildung 5.2 und den jeweiligen Funktionsstrukturen mitsamt der Prozesse, Stellgrößen und Meldungen werden sämtliche Informationen, die zwischen den logischen und physischen Elementen ausgetauscht

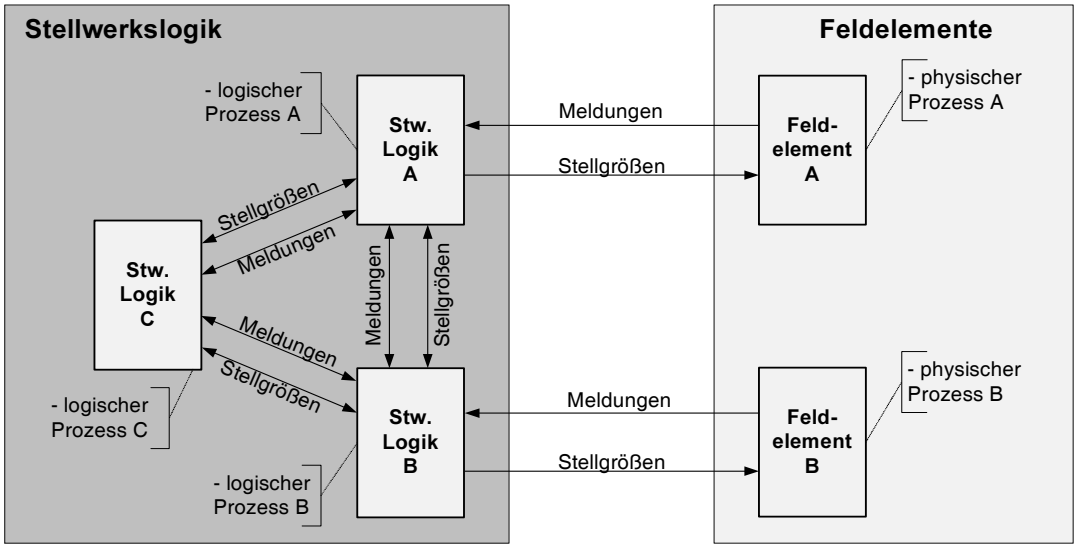


Abbildung 5.4: Funktionale Analyse unter Einbindung der Ressourcen (exemplarisch)

werden, systematisch ermittelt und in Form einzelner Kommunikationsdiagramme aufgestellt. Als Beipsiel ist in Abbildung 5.5 die Kommunikation und Funktionalität einer Weiche-Weichenlogik-Kombination abgebildet.

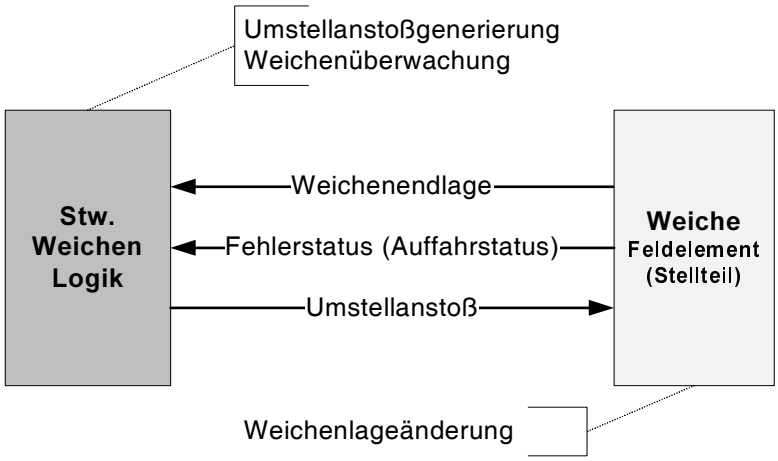


Abbildung 5.5: Informationsaustausch zwischen physischer und logischer Komponente

Wie aus der Struktur in Abbildung 5.4 zusätzlich zu erkennen ist, existiert ein Informationsaustausch nicht allein zwischen physischen und logischen Elementen, sondern auch zwischen den verschiedenen logischen Elementen selbst. Auszugsweise sind in Abbildung 5.6 die abstrakten Informationen aufgeführt, welche innerhalb der Fahrstraßenlogik eines Stellwerkes für eine Auswahl an Komponenten ausgetauscht werden. Den auf generischer Ebene in vier Phasen aufgeteilten logischen Prozess der Fahrstraßenbildung (Initialisierungs-, Verschluss-, Freigabe- und Auflösephase) ist hier durch die

farbigen Bereiche innerhalb des Blocks *Stw. Fahrstraßen Logik* ausgedrückt. Der Austausch von Informationen (Stellgrößen und Meldungen) ist hier jeweils mit den einzelnen logischen Teilprozessen des Elements der Fahrstraßenlogik verknüpft.

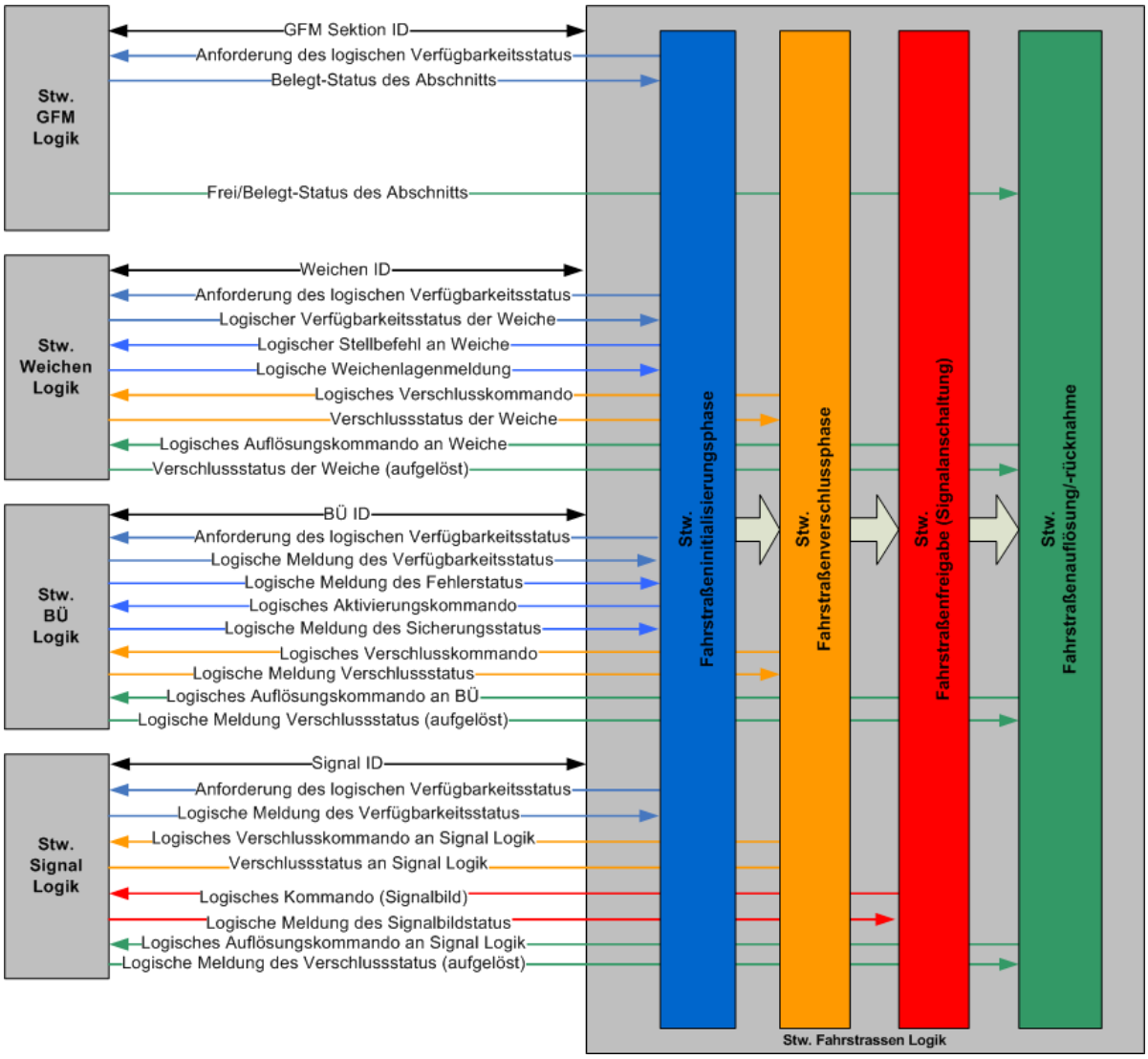


Abbildung 5.6: Informationsaustausch logischer Elemente

Im weiteren Verlauf müssen für das Gesamtsystem aus Abbildung 5.2 sämtliche generischen Funktionen und Informationen aufgestellt, analysiert und auf Vollständigkeit in mehreren Iterations- und Evaluationsschritten überprüft werden. Dabei sollte fallweise auf Expertenwissen zurückgegriffen werden, wobei an dieser Stelle der einzelne Fachexperte jeweils einen übersichtlichen – nicht allzu komplexen – Systemteil betrachtet und somit ein verteiltes Arbeiten möglich ist.

5.1.2 Gefährdungsstrukturierung

Nach der Aufstellung der System- und Funktionsstruktur kann davon ausgegangen werden, dass die analysierte Funktionalität der Stellwerksapplikation mit ihren Prozessen und Informationen eine derzeit größtmögliche Vollständigkeit auf einer einheitlichen Detaillierungstiefe aufweist. Zur Ermittlung der potenziellen Gefährdungen werden die analysierten Kommunikationsdiagramme herangezogen und einzeln betrachtet. Unter der Annahme, dass sämtliche Teilprozesse und Informationsaustausche potenziell nicht erfüllt werden, entstehen, analog zur beschriebenen Gefahrendefinition, potenziell angenommene gefährliche Bedingungen. Bei dieser Annahme werden ausschließlich einzelne "Nicht-Erfüllungen" mit tabellarischer Unterstützung betrachtet. Wird eine Nicht-Erfüllung eines Teilprozesses angenommen, wird davon ausgegangen, dass sämtliche vorausgehenden und nachfolgenden Teilprozesse – isoliert betrachtet – korrekt und folgerichtig ablaufen. Fehlerhafte Weichenlageninformationen könnten dazu führen, dass z.B. der Fahrstraßenlogik eine tatsächlich nicht vorhandene Weichenlage mit gewährendem Flankenschutz übermittelt würde. Basierend auf diesen fehlerhaften Informationen könnten Fahrstraßen unwissentlich ohne vorhandenen Flankenschutz gebildet werden, die als Folge zu einem erhöhten Risiko führen würden.

Die Tabelle in Abbildung 5.7 zeigt einen Auszug des Vorgehens am Beispiel des Elementes "Weiche". Auf der linken Tabellenseite ist das zu betrachtende Objekt aufgeführt – in diesem Fall die Weiche. Der linke obere Tabellenteil beinhaltet, bezogen auf den Kommunikationspartner (hier: Weichen (Logik) im Stellwerk), sämtliche anfallenden Meldungen, logische Prozesse, Stellgrößen und physische Prozesse, die zuvor in den kommunikationsdiagrammen ermittelt wurden. Dabei lassen sich Meldungen und physische Prozesse den Feldelementen, Stellgrößen und logische Prozesse der Stellwerkslogik zuordnen.

Zur einfacheren Zuordnung wurden die jeweiligen Gefährdungen (Ursachen sind potenzielle Fehler der Meldungen, Prozesse oder Stellgrößen) mit eindeutigen Nummerierungen versehen, z.B. "F1" etc., welche in einer späteren Gefahrenliste als Gefährdungen wieder zu finden sind und dort die Nicht-Erfüllung des Teilprozesses und die damit verbundenen Auswirkungen näher textuell aus Sicht des Fachexperten beschreiben.

Eine Beschreibung einer Gefährdung (z.B. „F1"), die durch einen Fachexperten durchgeführt wird, könnte wie folgt lauten:

„F1: die Weiche liefert eine inkorrekte aber plausible Weichenendlage (meldet Linkslage, liegt aber faktisch in Rechtslage). Dies könnte in der Stellwerkslogik zum Einlaufen von kollidierenden Fahrstraßen führen und eine Kollision mit anderen Schienenfahrzeugen, Hindernissen auf Bahnübergängen oder Entgleisungen auf beweglichen Gleiselementen führen"

Mit Hilfe der Tabelle können den jeweiligen Gefährdungen die Auswirkungen in Form von Unfallereignissen [A1] bis [A10] zugeordnet werden. Im gezeigten Beispiel für die Gefährdung „F1" sind die Unfallereignisse „A1", „A2", „A3" und „A5" zutreffend. Diese Felder sind durch ein Kreuz mit einer eindeutigen Nummerierung gekennzeichnet (1-1, 1-2, 1-3 und 1-5). Diese können nachfolgend als Gefahrenartefakt strukturiert dokumentiert werden.

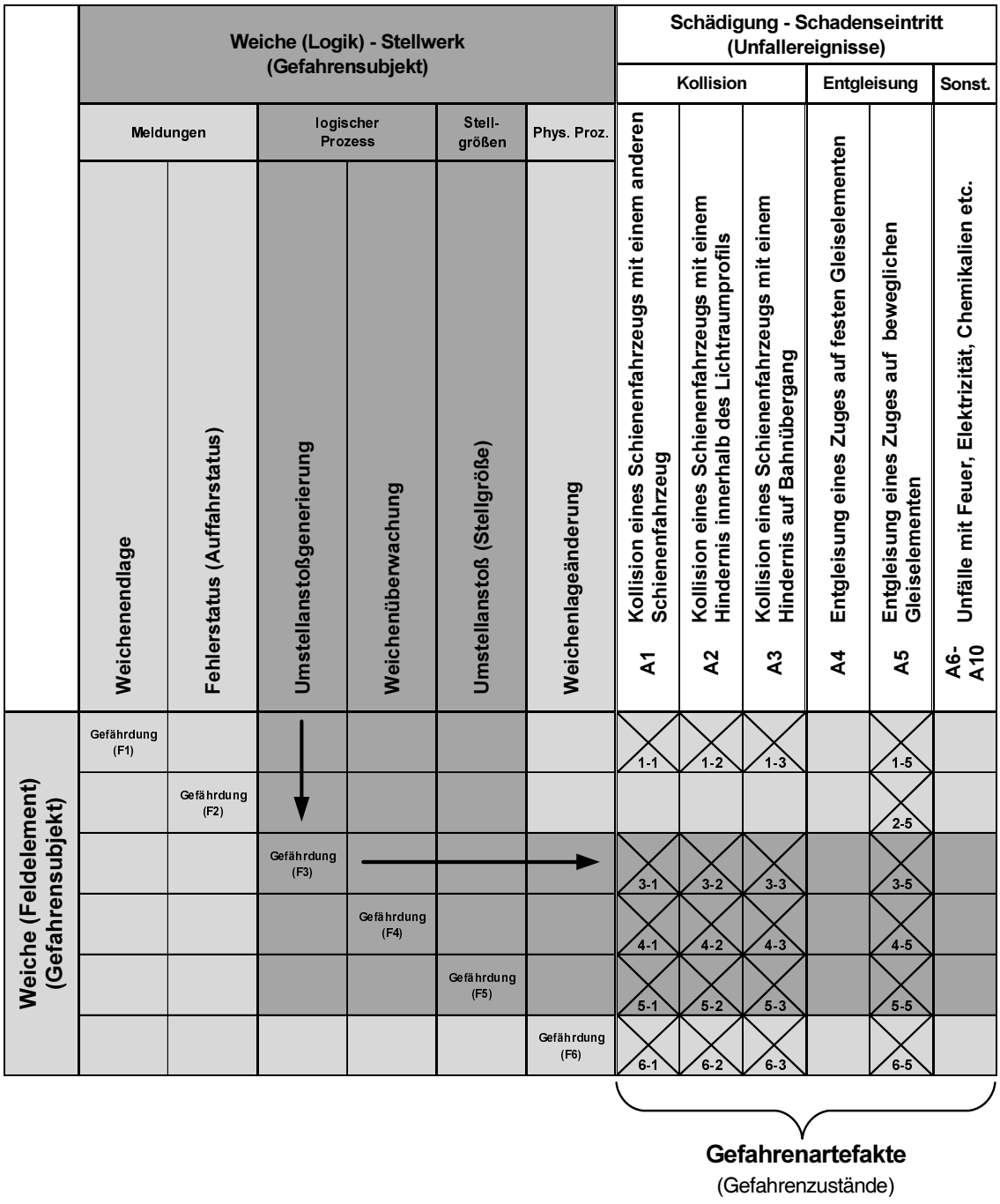


Abbildung 5.7: Hazard-Analyse und Unfallzuordnung

Die so verwendete Struktur ähnelt in ihrem konzeptionellen Aufbau Entscheidungstabellen und dem methodischen Vorgehen einer FMEA[1] und liefert so einen Beitrag zur Vollständigkeit der Analyse. Dieses Vorgehen lässt sich mit den zuvor auf Basis der begrifflichen Analyse erbrachten Formalisierungen der Sicherheit in Einklang bringen. Abbildung 5.8 zeigt dazu den Zusammenhang zwischen der Modellierung einer Gefahrensituation aus Unterabschnitt 4.1.2 und der Beschreibung eines Gefahrenartefakts nach der hier gezeigten Methode.

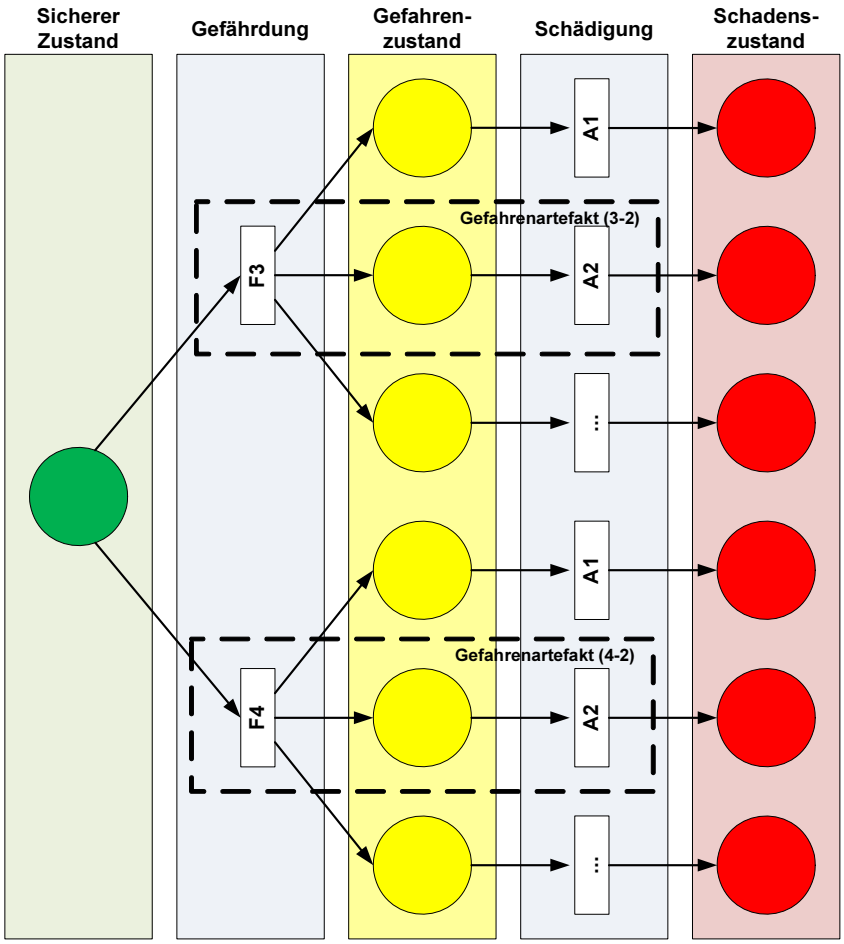


Abbildung 5.8: Bezug zur Formalisierung der Systemsicherheit

5.1.3 Dokumentation von Gefahrenartefakten

Mit Hilfe der Tabellen können unter systematischer Nutzung einer eindeutigen Syntax sowie unter Einbezug von Schlüsselwörtern die Gefahrenartefakte für das analysierte

[1]FMEA - Failure Mode and Effect Analysis

System, wie in Tabelle 5.1 gezeigt, zusammengestellt werden. Dabei setzt sich ein Gefahrenartefakt aus der angenommenen Gefährdung, als ursächliches Ereignis, und dem potenziellen Unfallereignis zusammen. Um die einzelnen konstruierten Gefahrenartefakte systematisch voneinander abgrenzen zu können, wird zusätzlich das Gefahrensubjekt, als Auslöser der Gefährdung, in die Beschreibung integriert. Somit ergibt sich für die Beschreibung eines Gefahrenartefakts folgende Syntax:

Mögliches [**Unfallereignis**] aufgrund einer [**Gefährdung**] eines [**Gefahrensubjekts**].

Tabelle 5.1: Generische Syntax für Gefahrenartefakte mit Beispielen

ID	Mögliches **Unfallereignis** **[A1] bis [A10]**	aufgrund einer **Gefährdung** **(F_i)**	eines **Gefahrensubjekts**
1-1	Mögliche Kollision eines Schienenfzgs. mit einem anderen Schienenfzg. [A1]	aufgrund einer inkorrekten Weichenendlagenmeldung (F1)	des physischen Elements Weiche.
1-2	Mögliche Kollision eines Schienenfzgs. mit einem Objekt im Lichtraumprofil [A2]	aufgrund einer inkorrekten Weichenendlagenmeldung (F1)	des physischen Elements Weiche.
...	...	...	...
2-5	Mögliche Entgleisung eines Schienenfzgs. auf beweglichen Gleiselementen [A5]	aufgrund einer inkorrekten Fehlerstatusmeldung (F2)	des physischen Elements Weiche.
...	...	...	...

Durch die Berücksichtigung der Unfallereignisse erhöht sich zwar die Anzahl der einzelnen Gefahren auf den ersten Blick, die Vorgabe der Folgen gibt dem späteren Bearbeiter so aber einerseits weniger Spielraum zu Spekulationen und Fehlern und andererseits ist die Abschätzung möglicher Unfallereignisse durch den Fachexperten für spätere Risikobewertungen hilfreich.

Aufgrund der eindeutigen Syntax der Gefahrenartefakte ist neben der einfacheren Verwendung für den Bearbeiter auch eine elektronische Verarbeitung möglich, wodurch

begründet ist, weshalb zur Strukturierung die Listenform und nicht etwa Baumstrukturen o.ä. gewählt wurden. Auch bietet die beschriebene allgemeingültige Methode zur Erstellung von Gefahrenartefakten dadurch das Potenzial für verschiedene technische – auch nicht eisenbahnspezifische – Anwendungsfelder.

5.2 Zusammenfassung und Anwendungspotenziale

Die vorgestellte Methode zeigt die strukturierte Vorgehensweise zur Identifikation von Gefahren und deren Dokumentation als Gefahrenartefakte. Die Zuordnung der Methode zur Verkehrssicherheit ist unter Verwendung des formalisierten Modells zur Verkehrssicherheit in Abbildung 5.9 dargestellt worden.

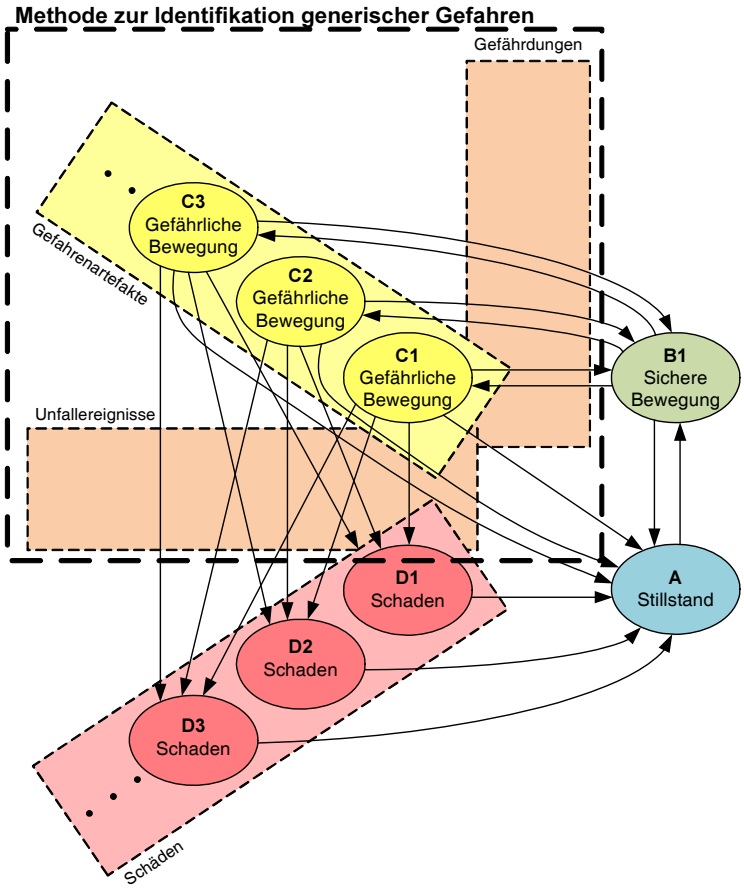


Abbildung 5.9: Einordung und Umfang der vorgestellten Methode

Generische Gefahrenartefakte und dadurch generierte Gefahrenlisten können Projekte zur Gefahren-/Gefährdungsidentifikation unterstützen, die Bearbeiter entlasten und insbesondere Kosten reduzieren. In der Phase der sicherheitsanalytischen Projektbearbeitung kann die gezeigte Methode herangezogen werden, um strukturiert und durch ver-

teilte Bearbeiter eine umfangreiche Liste möglicher Gefahrenartefakte auf einheitlicher Detaillierungstiefe zu erstellen. Basierend auf den so definierten Gefahrenartefakten, die potenzielle Unfallereignisse beinhalten, kann z.B. durch Quantifizerung des potenziellen Schadensausmaßes und der Häufigkeit das jeweilige Risiko analysiert werden. Lediglich die, für das zu bearbeitende Projekt relevanten (oberhalb des akzeptierten Grenzrisikos liegenden) Gefahrenartefakte werden anschließend ausgewählt, nicht relevante Gefahren werden gestrichen bzw. bleiben unbeachtet. Sollte beispielsweise das zu analysierende Stellwerk keine Anbindung von Gleissperren vorsehen, entfallen sämtliche Gefahrenartefakte in Bezug auf das Gefahrensubjekt Gleissperre; entsprechend verhält es sich bei anderen Elementen.

Im Rahmen von projektbegleitenden Sicherheitsanalysen ist es erforderlich, sicherheitsrelevante Anforderungen (vgl. Unterabschnitt 3.5.2) für das zu betrachtende System aufzustellen. Mit Hilfe der generischen Gefahrenartefakte können aufgrund der beschriebenen eindeutigen Syntax, ebenfalls elektronisch gestützt, durch einfachen Satzumbau die erforderlichen sicherheitsrelevanten Anforderungen (safety requirements) generiert werden. Da sowohl bei den Bahnen als Betreiber und Ersteller der Risikoanalysen als auch bei den Herstellern der Stellwerkssysteme meist firmeninterne Gefahrenlisten existieren, dient eine nach dieser Methode erstellte Liste u.a. als Referenzvorlage zur Vollständigkeitsprüfung und zum Abgleich bestehender Listen.

Neben der nachträglichen Analyse bestehender Anforderungen an ein System können durch frühzeitigen Einsatz dieser Methode Gefahren begleitend je nach Entwicklungsstand auf unterschiedlichen Detaillierungsstufen identifiziert werden und in Form von sicherheitsrelevanten Anforderungen mit in die Systementwicklung einfließen. Die Übernahme der Gefahrenartefakte z.B. in ein Requirements Management Tool (z.B. DOORS), mit dem Ziel Sicherheitsanforderungen mit diesen zu verknüpfen, kann einer durchgehenden Verfolgbarkeit von Anforderungen von der Realisierung bis zu deren dadurch begründbaren Entstehung dienen.

Die Methode ist grundsätzlich skalierbar und lässt sich sowohl für abstrakte rein funktional spzifizierte als auch konkrete technische Systemrealisierungen umsetzen und bestimmt durch die Wahl der Systemdetaillierung die resultierende Detaillierung der Gefahrenartefakte.

Aufgrund der generischen Struktur der so methodisch generierbaren Gefahrenliste ergeben sich keine Auswirkungen auf bestehende Betriebsvorschriften, Normen etc. Die allgemeingültige Ebene dieser Liste lässt jedem Anwender die Freiheit sämtliche zusätzlichen erforderlichen Betriebsvorschriften, Normen (z.B. CENELEC EN 50126, ff.) etc. heranzuziehen ohne Auswirkungen auf das mit Hilfe der vorgestellten Methode erstellte Ergebnis zu befürchten. Der aufgezeigte „Top-Down“-Ansatz zur Entwicklung generischer Gefahrenlisten soll durch die Ausführungen dazu beitragen, zukünftig verifizierbare, hochgradig vollständige Gefahrenlisten für technische Systeme einfacher und kostengünstiger zu erzeugen.

Die vorgestellte Methode ist u.a. in [SSF+07] durch Methoden und Beschreibungsmittel der UML weiter verfeinert worden. Zur Verbesserung der Konsistenz, der Verfolgbarkeit, Vollständigkeit und Ergonomie werden dort aus einer formalen statischen Struktur (UML Klassendiagramm), die inhaltlich und strukturell dem Funktions- und Struktur-

diagramm entspricht, automatisiert Kommunikationsdiagramme (Sequenzdiagramme) nach dem hier vorgestellten methodischen Muster erstellt und die erforderlichen Tabellen zur Hazard-Analyse inhaltlich vorbereitet. Zusätzlich wurde der Schritt der Gefährdungsanalyse (Beschreibung der ursächlichen Fehler) durch Anwendung s.g. Leitworte (Guidewords) aus dem HAZOP[1] Verfahren ergänzt. Dadurch lassen sich allein basierend auf einer formalen Struktur- und Verhaltensbeschreibung in Verbindung mit Expertenwissen systematische Gefährdungsanalysen erfolgreich und umfassend durchführen.

[1]HAZOP - Hazard and Operability Studies ist eine in der IEC 61882 standardisierte Methode zur systematischen Identifizierung von Fehlern und produktivitätsmindernden Betriebsstörungen. [Int01]

6 Methode zur sicherheitsgerichteten Anforderungsanalyse

Eine retrospektive Analyse erfordert grundsätzlich eine umfangreiche Verfügbarkeit relevanter Daten für das zu analysierende System. Die hier gezeigte Vorgehensweise basiert auf der Voraussetzung einer umfangreichen Datenlage für ein existierendes Verkehrssystem mit existenten, nicht akzeptablen Risiken, das im Sinne einer „Anpassentwicklung“ auf System- oder Subsystemebene „sicherer“ gestaltet werden soll. Die Identifizierung von Anforderungen für eine solche Gestaltung ist das Ziel dieser Methode. Aufgrund umfangreicher statistischer Aufzeichnungen ist es dadurch möglich, Schwachstellen im Verkehr (hier: Straßenverkehr) zu identifizieren und durch geeignete Maßnahmen wirksam die Sicherheit zu erhöhen. Im folgenden Abschnitt wird diese Methode exemplarisch vorgestellt, die es ermöglicht durch Unfallanalysen systematisch Anforderungen an Maßnahmen im Sinne von Assistenzsystemen zu ermitteln und gleichzeitig die Wirksamkeit von bestehenden Sicherungsfunktionen (hier: Assistenzsystemfunktionen) zu bewerten.

6.1 Unfallbasierte Anforderungsanalyse für Fahrerassistenzsysteme

Ein Ansatz die Verkehrssicherheit zu erhöhen ist es, aus Unfällen zu lernen und diese Erkenntnisse in zukünftige Produkte und Entwicklungen einzubeziehen [DB07], [VBD06]. Dabei sollen umfangreiche Unfallanalysen Aufschluss über Defizite des bisherigen Systems geben und ggf. Ansatzpunkte für Assistenz/Automatisierung oder ggf. Regulierung herleiten. Entscheidend bei diesem Ansatz ist die jeweilige Wirksamkeit der Maßnahme bezüglich einer resultierenden Senkung der Unfallereignisse bzw. der Schadenszustände in Abhängigkeit des Schadensausmaßes. Die folgenden Abschnitte schildern detailliert einen Ansatz zur Ableitung von Anforderungen an Fahrerassistenzsysteme im Straßenverkehr, der basierend auf Unfallanalysen wirksame Sicherungsfunktionen ermittelt [Kra06].

6.1.1 Unfallstatistik als Ausgangslage

In Deutschland werden jährlich ca. 2,3 Mio. Unfälle im Straßenverkehr polizeilich registriert (siehe Tabelle 6.1), von denen ein Großteil auf Fehler des Fahrers zurückzuführen

ist. Lt. [Bun06] lagen von den Unfallursachen 86% im Fehlverhalten der Fahrzeugführer, 4,2% im Fehlverhalten der Fußgänger, 4,5% in Straßenverhältnissen sowie jeweils weniger als 1% in Hindernissen (z. B. Wild) auf der Fahrbahn, in technischen bzw. Wartungsmängeln und in Witterungseinflüssen. Fehler aufgrund mangelnder Fahrzeugzuverlässigkeit im Sinne der Technischen Sicherheit (vgl. Unterabschnitt 3.5.1) sind demnach vergleichsweise gering vertreten.

Tabelle 6.1: Unfallstatistik in Deutschland für die Jahre 2005 und 2006

Spezifikation	**2005**	**2006**
gemeldete Unfälle	2 253 992	2 232 167
davon mit Sachschaden	1 917 373	1 904 331
davon mit Personenschaden	336 619	327 836

Mit der Absicht, die Verkehrssicherheit im Straßenverkehr nachhaltig und effizient positiv zu beeinflussen, besteht die Annahme, dass moderne und intelligente Fahrerassistenzsysteme den Fahrer unterstützen können, um unfallverursachende Situationen zu entschärfen (vgl. Gefahrenabwehr) oder gar vollständig zu vermeiden (vgl. Gefährdungsvermeidung). Maßnahmen mit dem Ziel der Auswirkungsminderung sind diesbezüglich aufgrund ihrer Systemverfügbarkeitseinschränkung nicht als alleinige Maßnahme ratsam, sondern sollten nur als ergänzende Funktion angesehen werden. Die Allokation der Assistenz ist bei allen Sicherungsimplementierungskonzepten nicht zwangsweise an den Fahrer (Verkehrsobjekt) bzw. an das Fahrzeug (Verkehrsmittel) gebunden, sondern durchaus, wie in Abschnitt 4.3 erläutert, im Bereich der Fahrwege (Verkehrsinfrastruktur) als Fahrwegassistenz genauso denkbar wie eine verteilte verkehrskonstituentenübergreifende Implementierung.

Um die Wirksamkeit vorhandener und neuer Fahrer- bzw. auch Fahrwegassistenzsysteme zu bewerten ist es notwendig, die Handlungsdefizite des Fahrers (als primäre Unfallursache) beim Führen (korrekt: Regeln) des Fahrzeugs zu analysieren. Protokolle aufgenommener Unfälle im Straßenverkehr liefern dabei ausgiebige Informationen zum Verlauf und zu den möglichen detaillierten Ursachen. In Deutschland werden sämtliche polizeilich aufgenommenen Unfälle statistisch ausgewertet und in einer Datenbank geführt. Diese Statistik unterliegt dem deutschen Statistikgesetz [Bun07] und erlaubt aus Datenschutzgründen lediglich Abfragen und Auswertungen, die die Anonymität der Beteiligten gewährt und eine Rückverfolgbarkeit mittels Datensatzkombination ausschließt.

Bei der polizeilichen Erfassung der Unfälle wird grundsätzlich eine Kategorisierung der Unfälle in unterschiedliche Unfalltypen durchgeführt, die eine systematische Einteilung und damit auch Erfassung in einer einheitlichen Statistik erlaubt. Diese in einer Datenbank abgelegten Datensätze werden vom statistischen Bundesamt geführt und stehen in unterschiedlicher Detaillierung der Öffentlichkeit zur Verfügung.

Die verfügbaren Zeitreihen des Statistischen Bundesamtes (destatis) lassen eine Analyse bis in die 50er Jahre zu und geben so einen guten Überblick über das Verkehrsgeschehen und insbesondere über das Unfallgeschehen. Neben der reinen polizeilichen Erfassung und statistischen Aufbereitung der Straßenverkehrsunfälle in Deutschland führen die Bundesanstalt für Straßenwesen (BaSt) und die Forschungsvereinigung Automobiltechnik e.V. (FAT) eine gemeinsame Datenbank mit detaillierten Unfallanalysen, die mittels eines strikten Stichprobenplans eine sehr detaillierte und vor allem repräsentative Übersicht der Unfälle und der (medizinischen) Unfallfolgen in Deutschland bietet. Auch diese Unfalldatenerhebung (GiDAS - German In-Depth Accident Study) kategorisiert die Unfälle entsprechend der bereits erwähnten Unfalltypen. Ein besonderer Fokus dieser Datensätze liegt dabei auf medizinischen Auswirkungen verschiedener Unfalltypen und wird daher von der medizinischen Hochschule Hannover betreut. Durch die Einbindung der medizinischen und monetären Folgen ließen sich typische Unfallereignisse entsprechenden Schweregraden (Schadensausmaß) zuordnen, sofern eine einheitliche Skalierung zwischen monetären und medizinischen Maßen vorläge.

Um verschiedene Statistiken miteinander in Bezug setzen zu können verwenden beide Datenbanken (GiDAS und destatis), wie bereits erwähnt, eine einheitliche Grobkategorisierung der Unfallsituationen [Kra06].

In der deutschen Unfallstatistik wird die Unfallsituation durch den sog. Unfalltyp gekennzeichnet. Dieser beschreibt den Verkehrsvorgang (z.B. Fahren in einer Kurve) sowie die jeweilige Konfliktsituation (z.B. Fahrzeug/Fußgänger von rechts/links), aus welcher der Unfall entstanden ist. Die amtliche Unfallstatistik unterscheidet hier sieben Typen von Unfällen auf der ersten Detaillierungsebene:

1. Fahrunfall: Um einen Fahrunfall handelt es sich, wenn ein Fahrer die Kontrolle über das Fahrzeug verliert, weil er die Geschwindigkeit nicht entsprechend der Situation gewählt hat.

2. Abbiegeunfall: Um einen Abbiegeunfall handelt es sich, wenn der Unfall durch einen Konflikt zwischen einem Abbieger und einem aus gleicher oder entgegengesetzter Richtung kommenden Verkehrsteilnehmer ausgelöst wurde.

3. Einbiegen/Kreuzen-Unfall: Um einen Einbiegen/Kreuzen-Unfall handelt es sich, wenn der Unfall durch einen Konflikt zwischen einem einbiegenden oder kreuzenden Wartepflichtigen und einem Vorfahrtberechtigten ausgelöst wurde.

4. Überschreiten-Unfall: Um einen Überschreiten-Unfall handelt es sich, wenn der Unfall durch einen Konflikt zwischen einem die Fahrbahn überschreitenden Fußgänger und einem Fahrzeug ausgelöst wurde - sofern das Fahrzeug nicht abgebogen ist.

5. Unfall durch ruhenden Verkehr: Um einen Unfall durch ruhenden Verkehr handelt es sich, wenn der Unfall durch einen Konflikt zwischen einem Fahrzeug des fließenden Verkehrs und einem auf der Fahrbahn ruhenden, d. h. einem haltenden oder parkenden Fahrzeug ausgelöst wurde.

6. Unfall im Längsverkehr: Um einen Unfall im Längsverkehr handelt es sich, wenn der Unfall durch einen Konflikt zwischen Verkehrsteilnehmern ausgelöst wurde, die sich in gleicher oder entgegen gesetzter Richtung bewegten - sofern dieser Konflikt nicht die Folge eines Verkehrsvorganges war, der einem anderen Unfalltyp entspricht.

7. Sonstiger Unfall: Hierunter fallen alle Unfälle, die nicht einem der Unfalltypen (1-6) zuzuordnen sind.

Eine genauere Beschreibung liefert die Erweiterung des Unfalltypenkatalogs entsprechend der Klassifizierung des HUK-Verbands [ON02], die über eine dreistellige Codierung die Unfallsituation genauer berücksichtigt.

Tabelle 6.2: Unfallklassifizierung in Deutschland gemäß HUK-Unfalltypen

Unfalltyp	**Fahrsituation**	**Konfliktsituation**	**Erklärung**
1	10	101	Fahrunfall in einer Linkskurve
		102	Fahrunfall in einer Rechtskurve
	11	111	Fahrunfall bei abknickender Vorfahrt (links)
		112	Fahrunfall bei abknickender Vorfahrt (rechts)
	...	...	...
2	20	201	(Links-) Abbiegeunfall mit auffahrendem Nachfolger
		202	(Links-) Abbiegeunfall mit kollidierendem Nachfolger
	21	211	(Links-) Abbiegeunfall mit durchfahrendem Gegenverkehr
		212	(Links-) Abbiegeunfall mit abbiegendem Gegenverkehr
	...	...	...
...	...	...	...

Die erste Ziffer dieser Kodierung (vgl. Tabelle 6.2 entspricht dem beschriebenen und in der amtlichen Statistik etablierten Unfalltyp. Mit der zweiten und dritten Ziffer werden die jeweiligen Fahr- und Konfliktsituationen genauer beschrieben. Beispielsweise wird beim Fahrunfall **(1)** die Erweiterung zu **(10)** dem Fahrunfall in der Kurve erfasst, die Erweiterung zu **(101)** spezifiziert die Kurve zu einer Linkskurve, bzw. **(102)** zu einer Rechtskurve. Diese Unfalltypkategorisierung eignet sich sehr gut als primärer Schritt für die Gruppierung von Unfällen hinsichtlich des Unfallhergangs, da jedem Unfalltyp bestimmte Fahrmanöver und spezifische Randbedingungen zuordbar sind und damit das Unfallverhalten (den Unfallprozess) detailliert beschreibt.

In [VBD06] ist eine detaillierte statistische Analyse auf Basis statistischer Unfalldaten durchgeführt worden. Als Datenbasis dienten dort zum einen eine 50% Stichprobe vom Statistischen Bundesamt über Unfälle, die ausschließlich durch PKWs verursacht wurden und bei denen der Verkehrsmittelführer über 18 Jahre alt war, und zum anderen polizeilich erfasste Unfälle der Stadt Braunschweig, die ebenfalls in einer 50% Zufallsstichprobe des selben Jahres herangezogen wurden, um anhand dieser eine In-depth Analyse durchzuführen. Aufgrund zahlreicher merkmalsbezogener Angleichungen sind merkmalsähnliche Datenbasen erzeugt worden. Insgesamt wurden in der zitierten Analyse 185 004 Unfälle aus Deutschland 993 schweren Unfällen aus Braunschweig gegenübergestellt. Das tatsächliche Unfallgeschehen in Deutschland umfasst für das Jahr 2002 insgesamt 2 279 613 polizeilich erfasste Unfälle, von denen 491 838 Unfälle mit Personenschäden bzw. schwerwiegenden Sachschäden gezählt wurden. In Braunschweig wurden für das Jahr 2002 insgesamt 9 347 Unfälle polizeilich erfasst, die Gesamtanzahl der Unfälle mit schweren bzw. Personenschäden ist unbekannt.

In einem merkmalsbasierten Gewichtungsverfahren werden in der zitierten Analyse die Unfälle aus Braunschweig, für die ein detaillierter Unfallbericht für eine In-depth Analyse vorlag, an den bundesdeutschen Durchschnitt angeglichen. Über dieses Verfahren erhielten einzelne Unfallgruppen entsprechende Gewichtungsfaktoren, die bei einer späteren Beurteilung der potenziellen Vermeidbarkeit von Bedeutung sind.

Für die weitere Beschreibung der Methode wird allerdings von einer vollständigen statistischen Datenlage ausgegangen. Eine umfangreiche Gewichtung, die in [VBD06] für eine repräsentative Beurteilung und Auswertung der örtlichen Unfallberichte über In-depth Analysen notwendig war, wäre somit bei dieser Annahme nicht erforderlich.

6.1.2 Fahrerverhalten und -zuverlässigkeit

Jeder der im vorangegangenen Abschnitt betrachteten Unfalltypen kann durch eine funktionale Analyse unterschiedlichen Fahrmanövern zugeordnet werden. Aus diesem Grund werden nachfolgend die Struktur und die Dynamik des Systems Straßenverkehr und insbesondere der Fahraufgabe detailliert untersucht. Grundlegend werden dabei in Tabelle 6.3 verschiedene Handlungsebenen nach [Sch07] und [Fay99] unterschieden und diesen organisatorischen Ebenen entsprechende Teilfunktionen zugeordnet.

Die Struktur dieser Teilfunktionen und Ebenen wird als kaskadiertes Funktionsmodell angenommen, so dass jede Entscheidung innerhalb einer Ebene Auswirkungen auf das

Tabelle 6.3: Einordnung der Fahraufgaben in das organisatorische Ebenenmodell

Ebene	**Beispielfunktion**
Strategische Ebene	Fahrzeugauswahl
Dispositive Ebene	Routennavigation
Taktische Ebene	Trajektorienregelung
Operative Ebene	Fahrzeugdynamikregelung

funktionale Verhalten innerhalb einer unterlagerten Ebene bewirken kann. Für jede Ebene resultiert aufgrund dieser konzeptionellen Annahme ein klassischer Regelkreis, bestehend aus einer notwendigen Situationserkennung (Sensor), einer Entscheidungsfunktion (Regler), einer Ausführungsfunktion (Aktor) sowie der klassischen Regelstrecke.

Die verwendete kaskadierte Regelkreisstruktur ist in Abbildung 6.1 abgebildet. Aufgrund der vorliegenden Tatsache, dass die betrachteten Unfälle vorwiegend aufgrund menschlicher Fehlhandlungen verursacht wurden, wird nachfolgend ausschließlich die taktische und operative Ebene, als maßgebliche Ebene für die Funktion der Fahrzeugbewegung, näher betrachtet. Unterschieden werden können auf taktischer Ebene die Trajektorienregelung, Positionserkennung und Hindernis/Umgebungserkennung und in der operativen Ebene die Funktionen der Längs- und Querdynamik mit ihren Funktionsblöcken: Längs-/Querregelung, Längs-/Queraktorik und der Fahrzeugdynamik sowie die jeweilige Situationserkennung der Fahrzeugbewegung (Sensorik).

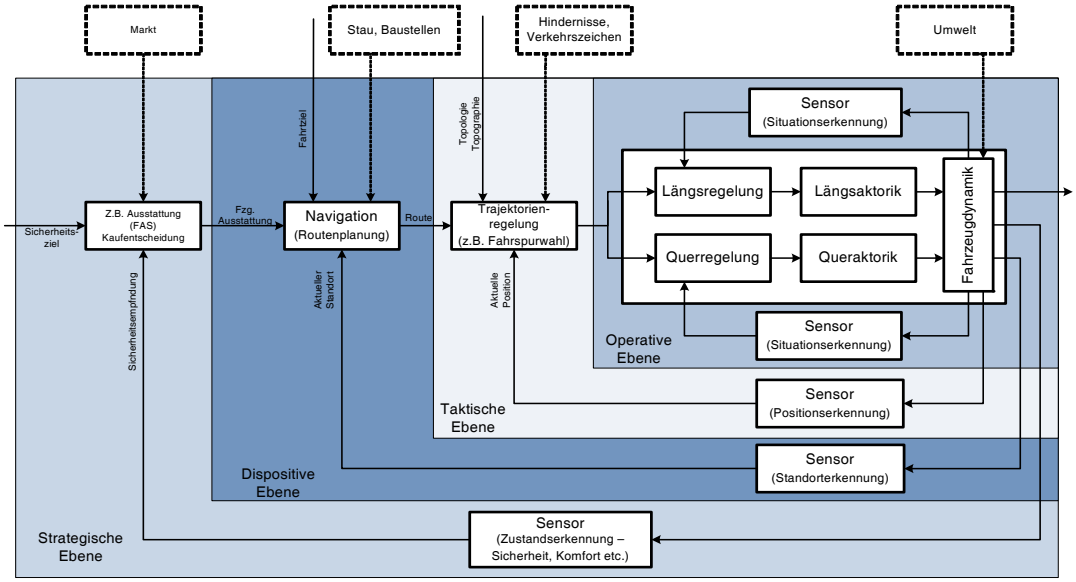


Abbildung 6.1: Kaskadierte Regelkreisstruktur zur Darstellung der Fahraufgabe

Die gezeigte Struktur ist ein vereinfachtes Modell von in der Realität eher komplexen Beziehungen zwischen Kunden-, Fahrer- und Fahrzeugdynamiken. Die meisten existierenden Modelle (vgl. [Sch03]) konzentrieren sich in der Regel auf Details einer Organsiationsebene bzw. nutzen unterschiedliche zum Teil inkompatible Beschreibungsmittel wie z.B. Regelkreise, System Dynamics, Petrinetze, Flussdiagramme usw. Die Zielsetzung dieses vereinfachten Modells ist die mögliche Zuordnung der menschlichen Ressource als Funktionsträger für die jeweiligen Funktionen zur Ausführung der Prozesse. Gelingt es über statistische Unfallanalysen den Unfalltypen menschliche Fehlhandlungen prozentual zuzuordnen, kann über die Implementierung von Sicherungsfunktionen zur Vermeidung von menschlich bedingten Gefährdungen (Fehlhandlungen) ein Rückschluss über die Unfallreduzierung vorgenommen werden.

In der konventionellen Fahraufgabe lassen sich die Funktionen der operativen und taktischen Ebene menschlichen Handlungen zuordnen. Tabelle 6.4 zeigt einige Beispiele für typische Aufgaben beim Führen eines Straßenfahrzeugs.

Tabelle 6.4: Einordnung der (Fahr-)Handlungen auf taktischer und operativer Ebene

Funktionsblock	**Beispiel**
Positionserkennung	Erkennen der aktuellen Position des eigenen Fahrzeugs
Umgebungserkennung	Erkennen der Umgebung: Straßenzustand, Hindernisse, andere Fahrzeuge etc.
Trajektorienregelung	Entscheidung über Soll-Trajektorie des Fahrzeugs
Längsregelung	Entscheidung über Soll-Beschleunigung / Gaspedalstellung / Soll-Geschwindigkeit
Querregelung	Entscheidung über Soll-Lenkwinkel / Kurvenverhalten
Längsaktorik	Betätigen des Gaspedals / Einstellen der Geschwindigkeit
Queraktorik	Lenken / Lenkbewegung / Einstellen des Lenkwinkels
Fahrzeugdynamik	Fahren mit Ist-Geschwindigkeit / Fahren in einer Ist-Richtung (Kurve/Geradeaus) / Reagieren auf Aktoriken
Sensor (Situationserkennung)	Erkennen der Ist-Geschwindigkeit / Ist-Lenkwinkel / Fahrzeugbewegung / Fahrzeugverhalten

Ein wesentlicher Faktor, der die Bedeutungsschwere des menschlichen Handelns in Bezug auf die analysierten Unfallereignisse charakterisiert, ist die menschliche Zuverlässigkeit in der Ausführung dieser Handlungen.

[JT08] und [Her03] definieren die menschliche Zuverlässigkeit als “die angemesse-

ne Erfüllung einer Arbeitsaufgabe über eine bestimmte Zeitdauer hinweg und unter zuverlässigen Bedingungen, die ebenfalls zeitveränderlich sein können". Eine ähnliche allgemeine Definition liefert Bubb [Bub90] "Zuverlässigkeit (Reliability) ist die Wahrscheinlichkeit, dass ein Element eine definierte Qualität während eines vorgegebenen Zeitintervalls und unter vorgegebenen Bedingungen erbringt".

Anders als die technische Zuverlässigkeit wird somit die menschliche Zuverlässigkeit durch die Wahrscheinlichkeit beschrieben, eine Aufgabe unter vorgegebenen Bedingungen für ein gegebenes Zeitintervall im Akzeptanzbereich durchzuführen. Der grundsätzliche Unterschied zwischen der technischen und der menschlichen Zuverlässigkeit liegt in der Ausführung einer spezifizierten Funktion (technisch) bzw. Ausführung einer Aufgabe (menschlich). Der Mensch arbeitet dabei typischerweise im Gegensatz zu einer Maschine zielorientiert (intelligent) und ist dabei in der Lage, trotz hoher Wahrscheinlichkeit fehlerhaften Ausführens einzelner Handlungsschritte, das Ziel dennoch mit hoher Wahrscheinlichkeit zu erreichen. Eine spezifizierte technische Funktion beschreibt das spezifizierte Verhalten des Systems innerhalb von spezifizierten Grenzen. Ein diskretes Überschreiten dieser Grenzen durch das Verhalten eines technischen Systems wird i.d.R. als Fehlverhalten bzw. Nichterfüllung der Funktion gewertet. Konventionelle Systeme versuchen diesbezüglich in der Regel nicht eigenständig (intelligent) andere Lösungwege zu finden, um dennoch ein sicheres Ziel zu erreichen, wenngleich ein interessanter Ansatz für intelligentes Handeln künstlicher Systeme in Form von Multiagentensystemen für den Einsatz in dispositiven Aufgaben verfügbar ist [Kön05].

Problematisch wird das intelligente Handeln von Menschen allerdings in sogenannten sicherheitskritischen Anwendungen. Fehleinschätzungen der Situation oder bzgl. des eigenen Könnens sowie nicht ausreichende Ausführung geplanter Handlungen oder sogar mutwillige Übersteuerung von sicherheitsgerichteten Funktionen lassen unter gewissen Umständen eine korrigierende notwendige Handlung bei Erkennen des Gefahrenzustands nicht mehr zu und führen unverweigerlich zum Unfallereignis.

Als Ergebnis der detaillierten Unfallanalysen aus [VBD06] lassen sich ebenfalls folgende grundsätzliche menschliche Fehlhandlungen als Ursache für Verkehrsunfälle feststellen:

- (C1) Fehlinterpretation der aktuellen Situation
- (C2) Fehleinschätzung des Verhaltens anderer
- (C3) Fehlanpassung der eigenen Fahrmanöver an die Situation
- (C4) Missachtung oder Ausbleiben bestimmter Fahraufgaben
- (C5) fehlerhafte Ausführung
- (C6) Bewusstes Überschreiten und Akzeptieren des Risikos

In Tabelle 6.4 ist ein Bezug zwischen Funktionen der Fahraufgabe und möglichen Fehlhandlungen hergestellt worden.

Tabelle 6.5: Menschliche Fahraufgaben und Fehlhandlungen

Funktion/Aufgabe	**menschliche Fehlhandlung**	**Index**
Umgebungserkennung	-Fehlinterpretation der aktuellen Situation	(C1)
	-Fehleinschätzung des Verhaltens anderer	(C2)
Positionserkennung	-Fehlinterpretation der aktuellen Situation	(C1)
Trajektorienregelung	-Fehlanpassung der eigenen Fahrmanöver an die Situation	(C3)
	-Bewusstes Überschreiten und Akzeptieren des Risikos	(C6)
Situationserkennung	-Fehlinterpretation der aktuellen Situation	(C1)
Querregelung	-Fehlanpassung der eigenen Fahrmanöver an die Situation	(C3)
	-Bewusstes Überschreiten und Akzeptieren des Risikos	(C6)
Längsregelung	-Fehlanpassung der eigenen Fahrmanöver an die Situation	(C3)
	-Bewusstes Überschreiten und Akzeptieren des Risikos	(C6)
Längsaktorik	-Missachtung oder Ausbleiben bestimmter Fahraufgaben	(C4)
	-fehlerhafte Ausführung	(C5)
Queraktorik	-Missachtung oder Ausbleiben bestimmter Fahraufgaben	(C4)
	-fehlerhafte Ausführung	(C5)
Fahrzeugdynamik	keine menschliche Fehlhandlung	

Jede dieser Funktionen beeinhaltet wiederum einzelne Detailhandlungen. Die Umgebungserkennung beinhaltet u.a. die Hinderniserkennung, die Verkehrszeichenerkennung, Witterungserkennung, die Einschätzung des Verhaltens anderer Verkehrsteilnehmer sowie viele weitere Aufgaben die die aktuelle Situation unter Berücksichtigung der Umgebung beschreiben. Dabei können einzelne Merkmale sowohl fehlerhaft wahrgenommen (z.B. aufgrund Sehschwächen) als auch fehlerhaft interpretiert werden (z.B. die Absicht eines Verkehrsteilnehmers anzuhalten). Die Ursachen der inkorrekten Umgebungswahrnehmung liegt in der Regel bei einer gestörten Wahrnehmung des Menschen (z.B. Nachtblindheit, Überlastung etc.).

Die aufgeführten Regelungsaufgaben beinhalten sowohl tatsächliche Entscheidungen (z.B. Spurwechsel in der Trajektorienregelung) als auch intuitive Reaktionen, die innerhalb des menschlichen Gehirns gespeichert sind, wie z.B. die Spurhaltung bei der Querregelung, die weitestgehend ohne direkte Fokussierung/Konzentration des Menschen erfolgt. Mögliche Fehlhandlungen basieren hier in erster Linie auf mangelnder Erfahrung (z.B. Fahranfänger, schlechtes Fahrzeughandling etc.), fehlerhaftem Regelverständnis (z.B. Unkenntnis von Verkehrsregeln) sowie die beabsichtigte Übertretung von Grenzen und damit Akzeptieren von Risiken aufgrund fehlerhafter Selbsteinschätzung. Ursachen für diese Unzuverlässigkeit des Menschen können beispielsweise Überlastung oder mentale bzw. physische Untauglichkeit (z.B. Unaufmerksamkeit, Müdigkeit, Drogeneinfluss etc.) sein. Die Auswirkungen einer fehlerhaften Regelungsaufgabe werden unmittelbar auf deren Ausführung (Aktorik) übertragen.

Die Ausführung der in den Regelungsaufgaben getroffenen Entscheidungen wie z.B. Stellgrößen (Lenkradeinschlag etc.) basiert auf der Annahme einer korrekten Entscheidung in den Regelungsaufgaben. Zusätzlich ist es möglich, diese Ausführung fehlerhaft durchzuführen, wobei auch hier unzureichende Fertigkeiten, mentale oder physische Untauglichkeit (z.B. Müdigkeit oder Drogeneinfluss) als Hauptfehlerquellen für eine inkorrekte Ausführung der Stellgrößen identifizierbar sind.

Um eine quantifizierte Auswertung dieser Fehlhandlungen durchzuführen sind die statistischen Unfalldaten jeder Unfallkategorie entsprechend der Fehlhandlungskategorien (C1) bis (C6) zu ermitteln.

Tabelle 6.6 zeigt am Beispiel der Fahrunfälle (Unfalltyp 1) basierend auf [VBD06] die Verteilung der menschlichen Fehlhandlungen.

In der zitierten Quelle werden die Fehlhandlungen zusätzlich weiter detailliert und für jeden Unfalltyp analysiert und gegenübergestellt. Die Fahrunfälle werden nach der Gruppe der Einbiegen/Kreuzen-Unfälle (Unfalltyp 3) als die Gruppe mit der zweitgrößten Unfällhäufigkeit identifiziert. Deutlich ist in Tabelle 6.6 zu erkennen, dass die *Fehlanpassung der eigenen Fahrmanöver an die Situation* die Ursache mit den meisten Unfallereignissen in der Kategorie der Fahrunfälle ist.

Eine explizite Vermeidung dieser identifizierten menschlichen Fehlhandlung durch entsprechende Sicherungsfunktionen würde demnach einen großen Beitrag zur Vermeidung von Fahrunfällen als direkte Ursachenbekämpfung (Gefährdungsvermeidung) leisten, während beispielsweise Maßnahmen, die eine fehlerhafte Ausführung unterstützend vermeiden (z.B. Fahrertrainings) ggf. nur geringe Effizienz bei der Vermeidung der Unfallursache versprechen.

Tabelle 6.6: Menschliche Fehlhandlungen im Zusammenhang mit Fahrunfällen

Menschliche Fehlhandlung als Ursache von Fahrunfällen	**Anteil Fahrunfälle**
(C1) Fehlinterpretation der aktuellen Situation	n.v.
(C2) Fehleinschätzung des Verhaltens anderer	n.v.
(C3) Fehlanpassung der eigenen Fahrmanöver an die Situation	84,6 %
(C4) Missachtung oder Ausbleiben bestimmter Fahraufgaben	9,8 %
(C5) fehlerhafte Ausführung	2,8 %
(C6) Bewusstes Überschreiten und Akzeptieren des Risikos	n.v.
keine Zuordnung bzw. ausgeschlossene Unfälle	2.8 %

6.1.3 Assistenzstrategien

Werden die grundlegenden Sicherungsimplementierungskonzepte aus Abschnitt 3.4 referenziert, lassen sich Assistenzstrategien mit dem Ziel der Gefährdungsvermeidung, Gefahrenabwehr und Auswirkungsreduzierung definieren. Im Folgenden sind unterschiedliche Strategien aus [VBD06] zur Unterstützung des Fahrers berücksichtigt worden.

- (S1) Bereitstellung von Informationen für den Fahrer
- (S2) Anzeige von Informationen während der Situationserkennung
- (S3) Warnen vor potenziellen akuten Gefahren bei Regelungsaufgaben
- (S4) Eingriff in der Aktorik
- (S5) Übernahme der Regelungsfunktion und/oder Aktorik

Die optionale passive Bereitstellung von notwendigen Informationen für den Fahrer (S1), ohne diese eigenständig anzuzeigen, ermöglicht dem Fahrer eine ausreichende Wahrnehmung der Umgebung und der eigenen Situation unter Einbezug verfügbarer Hilfsmittel und nimmt somit die Strategie mit der geringsten Autorität ein. Eine durch den Fahrer aktivierbare Außentemperaturanzeige dient beispielsweise einer besseren Einschätzung möglicher bevorstehender Gefährdungen durch überfrierende Nässe und trägt somit indirekt zur Gefährdungsvermeidung bei, stützt sich dabei allerdings auf den aktiven Abruf und die folgende Auswertung der Informationen durch den Fahrer, sowie auf dessen sicherheitsgerichtete Entscheidung. Aus diesem Grund wird diese Strategie als indirekt und passiv eingestuft. Eine Gefahrenabwehr ist bei dieser Strategie als

unwahrscheinlich anzunehmen, da die Interpretation des aktuellen Zustands als Gefahrenzustand durch den Fahrer nur zufällig erfolgt und nicht durch die Assistenzstrategie gefördert wird.

Eine vom System aktivierte dynamische Anzeige von Informationen (S2) zeigt dem Fahrer in der jeweiligen Situation die für eine Regelungsaufgabe notwendigen Informationen an, um eine in der Situation korrekte Interpretation der angezeigten Informationen und damit eine adäquatere Entscheidung bestmöglich zu unterstützen. Hierzu zählen beispielsweise eine automatische Verkehrszeichenanzeige im Fahrzeugcockpit oder der aktuelle Abstand zu anderen Verkehrsteilnehmern. Auch hier kann eine indirekte, passive Gefährdungsvermeidung angenommen werden, die aber im Vergleich zur Assistenzstrategie (S1) über eine größere Autorität verfügt.

Sofern gefährliche Situationen entstehen (eingetretene Gefährdungen, die für das Fahrzeug und den Fahrer ein potenzielles Risiko darstellen), kann eine unterstützende Warnung des Fahrers bei existenter Gefahrensituation bei Regelungsaufgaben (S3) die Aufmerksamkeit des Fahrers auf die Gefahrensituation lenken und den Fahrer ggf. zu entsprechenden Handlungen animieren, das Unfallereignis abzuwehren. Dazu zählen beispielsweise Warnungen bei unzulässigen Geschwindigkeitsübertretungen, Abstandsunterschreitungen oder bei unangekündigten gefährlichen Spurwechseln. Das verfolgte Sicherungsimplementierungskonzept ist hier primär die direkte aber passive Gefahrenabwehr, die zur tatsächlichen Abwehr der Gefahrensituation weiterhin das aktive Handeln des Fahrers benötigt.

Der aktive Eingriff des Assistenzsystems in die Aktorik des Fahrzeugs (S4) übernimmt ausbleibende Handlungen des Fahrers nicht, sondern unterstützt lediglich fehlerhaft bzw. nicht ausreichend ausgeführte Aktionen. Zu dieser Art von Eingriffen gehören das klassische elektronische Stabilitätsprogramm (ESP) oder das Anti-Blockiersystem (ABS), die beide bei unzureichender Fahrzeugstabilisierung durch den Fahrer dessen Funktion unterstützen. Aber auch die Anpassung des optimalen Bremsdrucks zur jeweiligen Situation zählt zu dieser Strategie. Vorraussetzung für die eingreifend unterstützenden Systeme ist die ständig verfügbare Möglichkeit diese Funktionen zu deaktivieren oder zumindest eine Gegenreaktion auszuführen, so dass die Hauptverantwortung der Fahraufgabe beim Fahrer verbleibt. Strategien dieser Art übernehmen dadurch die Funktion der direkten aktiven Gefahrenabwehr. Eine indirekte aktive Auswirkungsreduzierung erfolgt indes durch Systeme, die eine Erhöhung der Bremswirkung und damit einen gezielten Energieabbau ermöglichen. Eine vollständige Übernahme der Fahraufgabe durch das System ist jedoch durch diese Strategie nicht vorgesehen.

Die Strategie, die diese Grundsätze der Übersteuerbarkeit gezielt ausschließt, ist die vollständige Übernahme der Regelungs- und Aktorikaufgabe durch das System (S5). Systeme dieser Art entscheiden selbstständig entsprechend der erkannten Position, Situation und Umgebung über bevorstehende Gefährdungen oder eine ggf. bereits aktive Gefahrensituation und erzeugen angemessene sichere bzw. sichernde Stellgrößen (z.B. Trajektorie für Ausweichmanöver, Kommando für Notbremsungen, notwendige Lenkwinkel etc.), die durch eine entsprechende Aktorik selbstständig in entsprechende Handlungen (Einstellen der Lenkwinkel, Erzeugen des Bremsdrucks etc.) die Gefährdung vermeiden oder existente Gefahren abwehren. Bei dieser Art von Assistenz wird ein wesentlicher

Schritt in Richtung autonomes Fahren getan und eine direkte aktive Gefährdungsvermeidung ist neben der direkten aktiven Gefahrenabwehr möglich. Derzeit sind Systeme dieser Art in der allgemeinen Diskussion und stoßen an die Grenzen der gesetzlichen Vertretbarkeit, da die Haftung des Fahrers bzw. auch Halters im Schadensfall fraglich bleibt. Insbesondere, wenn dieser durch die Übernahme der Fahrhandlung durch das Assistenzsystem erfolgt ist sind Fragen der Produkthaftung zu klären [VBD06].

Der Vergleich mit den Sicherungsimplementierungskonzepten ist in (Tabelle 6.7) durchgeführt worden.

Tabelle 6.7: Sicherheitsgerichtete Assistenzstrategien und -konzepte

	Assistenzstrategien	**Sicherheits-implementierungskonzepte**
(S1)	Bereitstellung von Informationen	(indirekte, passive) Gefährdungsvermeidung
(S2)	Anzeige von Informationen während der Erkennung	(indirekte, passive) Gefahrenabwehr (indirekte, passive) Gefährdungsvermeidung
(S3)	Warnen vor akuten Gefahren bei Regelungsaufgaben	(indirekte, aktive) Gefahrenabwehr
(S4)	Eingriff in der Aktorik	(direkte, aktive) Gefahrenabwehr, (indirekte, aktive) Auswirkungsreduzierung
(S5)	Übernahme der Regelungs-funktionen und/oder Aktorik	(direkte, aktive) Gefährdungsvermeidung (direkte, aktive) Gefahrenabwehr

6.1.4 Ableitung von Anforderungen

Aus dem vorangegangenen Abschnitt wird deutlich, dass insbesondere für die Vermeidung von Fahrunfällen die bedeutungsschwerste Ursache „(C3) Fehlanpassung der eigenen Fahrmanöver an die Situation“ vermieden werden muss. Aus der Allokation der Assistenzstrategien zu den Fehlhandlungen in Tabelle 6.8 wird zudem deutlich, dass die Assistenzstrategien „(S3) Warnen vor potenziellen akuten Gefahren bei Regelungsaufgaben“, „(S4) Eingriff in der Aktorik“ und „(S5) Übernahme der Regelungsfunktion und/oder Aktorik“ wirksame Sicherungsimplementierungskonzepte realisieren können. Deutlich lässt sich in Tabelle 6.8 ein Zusammenhang zwischen dem Grad der Fehlhandlung und dem erforderlichen Grad an Assistenz anhand einer diagonalen Schwerpunktbildung von (C1)/(S1) nach (C6)/(S5) erkennen. Während die Fehlhandlungen (C1), (C2) eher auf die menschliche Unzuverlässigkeit zurückzuführen sind, zeigt (C3), (C4)

und (C5) eine gewisse Fahrlässigkeit und die Fehlhandlung (C6) sogar eine Vorsätzlichkeit des Fahrers. Somit kann der Grad der Vorsätzlichkeit als Skala der Fehlhandlungen festgestellt werden. Die Assistenzstrategien sind entsprechend ihrer Überstimmbarkeit bzw. ihres Handlungseingriffs geordnet. Während (S1), (S2) und (S3) lediglich informelle, alarmierende Eigenschaften besitzen greift (S3) aktiv in die Funktion des Fahrers ein und kann durch S5 vollständig übersteuert werden. Die ansteigende Vorsätzlichkeit bei den Fehlhandlungen im Bezug zu der ansteigenden Übersteuerung der Assistenzstrategien erklärt somit diese Schwerpunktbildung in der Diagonalen.

Tabelle 6.8: Allokation der Assistenzstrategien auf menschliche Fehlhandlungen

		Assistenzstrategien				
		(S1)	(S2)	(S3)	(S4)	(S5)
Fehlhandlungen	(C1)	X	X	X		
	(C2)	X	X	X		
	(C3)			X	X	X
	(C4)		X	X	X	X
	(C5)			X	X	X
	(C6)					X

Eine Gegenüberstellung der Fehlhandlungen zu den Funktionsblöcken und entsprechenden Assistenzstrategien zeigt (Tabelle 6.9).

Tabelle 6.9: Unterstützung von Funktionen durch Assistenzstrategien

Funktion/Aufgabe	**menschliche Fehlhandlung**		**Assistenzstrategien**
Trajektorienregelung	(C3)	-Fehlanpassung der eigenen Fahrmanöver an die Situation	(S3), (S4), (S5)
Querregelung	(C3)	-Fehlanpassung der eigenen Fahrmanöver an die Situation	(S3), (S4), (S5)
Längsregelung	(C3)	-Fehlanpassung der eigenen Fahrmanöver an die Situation	(S3), (S4), (S5)

Für die Entwicklung von Assistenzsystemen, die das Unfallgeschehen wirksam reduzieren können, lassen sich daraus die folgenden funktionalen Anforderungen auf oberster

Ebene ableiten:

Anforderung 1: Das Assistenzsystem soll die Fehlanpassung der Fahrmanöver an die Situation durch den Fahrer durch eine geeignete Kombination aus aktiver Warnmeldung von potenziellen Gefahren und Übernahme der Regelungsfunktion während der Trajektorienregelung verhindern, um Fahrunfälle zu reduzieren.

Anforderung 2: Das Assistenzsystem soll die Fehlanpassung der Fahrmanöver an die Situation durch den Fahrer durch eine geeignete Kombination aus aktiver Warnmeldung von potenziellen Gefahren und Übernahme der Regelungsfunktion während der Querregelung verhindern, um Fahrunfälle zu reduzieren.

Anforderung 3: Das Assistenzsystem soll die Fehlanpassung der Fahrmanöver an die Situation durch den Fahrer durch eine geeignete Kombination aus aktiver Warnmeldung von potenziellen Gefahren und Übernahme der Regelungsfunktion während der Längsregelung verhindern, um Fahrunfälle zu reduzieren.

Diese Anforderungen sind im Verlauf der Entwicklung weiter zu detaillieren, um daraus Systemanforderungsspezifikationen und insbesondere Systemsicherheitsanforderungen (vgl.Unterabschnitt 3.5.2) abzuleiten.

6.1.5 Fahrerassistenzsysteme

Während der letzten Dekade sind viele unterschiedliche Systeme für den Einsatz in Straßenfahrzeugen mit der Absicht entwickelt worden, den Fahrer in ungünstigen bzw. unkomfortablen Situationen durch Assistenzfunktionen zu unterstützen. Grundsätzlich können die Fahrerassistenzsysteme in Sicherheitsassistenz und Komfortassistenz unterschieden werden. Jedoch ist sowohl eine sicherheitsfördernde als auch eine gefährdende Wirkung von Komfortsystemen über die Reduzierung bzw. Erhöhung der Belastung des Fahrers indirekt möglich und wird bereits ausführlich in der Domäne der Verkehrspsychologie thematisiert [Wei06], [WS02].

Eine Auswahl von unterschiedlichen bereits etablierten und innovativen Fahrerassistenzsystemen kann wie folgt zusammengefasst werden.

- Abstandsregeltempomat - Adaptive Cruise Control (ACC)
- Bremsassistent - Braking Assistance (BA)
- Anti Blockiersystem - Antilock Braking System (ABS)
- Anti Schlupf Regelung - Anti Slip Regulation (ASR) bzw. Traction Control System (TCS)
- Elektronisches Stabilitätsprogramm - Electronic Stability Program (ESP)
- Parkassistenz - Parking Assistance System (PAS)

- Spurhalteassistent - Lane Departure Warning (LDW)
- Intelligente Lichtsteuerung - Intelligent (Front) Light System (ILS)
- Nachtsichtassistent - Night Vision (NV)
- Abstandsregeltempomat Stop'n'Go (ACC Stop'n'Go)
- Kollisionswarnungsassistent - Collision Warning System (CWS)
- Kollisionsvermeidungsassistent - Advanced Collision Avoidance System (ACA)
- Automatische Notbremse - Automatic Emergency Brake (AEB)
- Intelligente Geschwindigkeitsführung - Intelligent Speed Adaption (ISA)
- Spurwechselassistent - Lane Changing Assistance (LCA)
- Kreuzungsassistent - Intersection Assistance System (IAS)

Die gezeigten Fahrerassistenzsysteme können den jeweiligen bereits systematisch aufgeführten Assistenzstrategien sowie den ursprünglichen Fehlhandlungen des Fahrers zugeordnet werden [SBDG04]. Sicherheitsrelevante Fahrerassistenzsysteme sollen den Fahrer in seiner Sicherungsfunktion unterstützen und möglichen gefährlichen Fehlhandlungen entgegenwirken. Um die Sicherheitseffizienz der Assistenzsysteme abschätzen zu können, werden Fahrerassistenzsysteme exemplarisch qualitativ analysiert indem sie der Regelkreisstruktur in Abbildung 6.2 gegenübergestellt werden.

Eine funktionale Dekomposition der entsprechenden Akteure und Assistenzsysteme ist dafür hilfreich und wurde bereits durch verschiedene Disziplinen mit unterschiedlichen Zielsetzungen und unterschiedlichen Modellierungstiefen erfolgreich realisiert. Dazu zählen funktionale Modelle des Fahrers und der Assistenzsysteme aus dem Bereich der Regelungs- und Automatisierungstechnik, die das Ziel verfolgen, unterschiedliche Regelalgorithmen zu optimieren bzw. deren Robustheit zu stärken [Gan04], [Hel03]. Des weiteren existieren umfangreiche empirische Analysen aus dem Bereich der Psychologie mit dem Bestreben ergonomische Aspekte von Komfortsystemen und menschliche Faktoren im Sinne von *Human Erros* zu erforschen [Ras85], [Ras82].

Betrachtet man beispielsweise den einfachen Bremsassistenten *Braking Assistance*, der ausschliesslich die erforderliche Bremskraft in Abhängigkeit von der Bremspedalbedienung zur Verfügung stellt, dann vermeidet dieses System nur bestimmte menschliche Fehlhandlungen (hier: fehlerhafte Ausführung vgl. Tabelle 6.5 (C5)) im Bereich der Längsdynamikausführung (Längsaktorik) durch einen entsprechenden Eingriff in die Aktorik (dies entspricht dem Index (S4) in Tabelle 6.8). Eine ähnliche Überdeckung und Zuordnung kann für die anderen Assistenzsysteme auf gleiche Weise festgestellt werden.

Werden die Angaben der Häufigkeit von fehlerhaften Ausführungen in Bezug auf die Fahrunfälle (hier 2,8 %) auf die Anzahl der Unfälle durch fehlerhafte Bremspedalbetätigung (Pedalkraft) weiter heruntergebrochen, ergibt sich eine noch kleinere Zahl an Unfällen, die potenziell durch einen Bremsassistenten vermieden werden könnten. Die

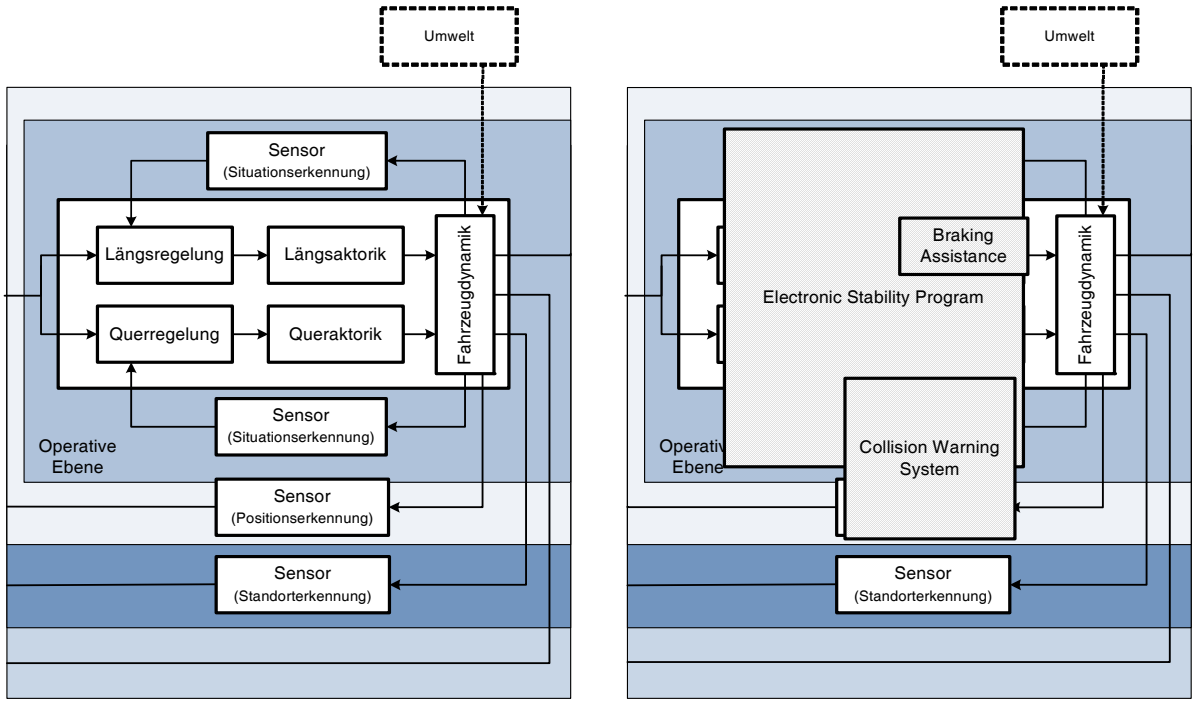


Abbildung 6.2: Implementierte Unterstützung der Fahraufgaben durch Assistenzsysteme

Wirksamkeit, bezogen auf die Anzahl potenziell vermeidbarer Unfälle, ist somit als eher gering einzustufen.

6.2 Zusammenfassung und Anwendungspotenziale

Die Einordnung und der Umfang der vorgestellten Methode wird unter Verwendung des formalisierten Modells zur Verkehrssicherheit in Abbildung 6.3 dargestellt.

Die Methode ermöglicht die Ableitung von Anforderungen an Systeme die zur Förderung der Sicherheit im Verkehr beitragen könnnen. Am Beispiel von Fahrerassistenzfunktionen ist dies umgesetzt worden.

Ein solches Vorgehen ermöglicht die Fokussierung von Fehlhandlungen und deren Vermeidung durch wirksame Assistenzstrategien für zukünftige Entwicklungen bzw. die Förderung der Integration von sicherheitsrelevanten Assistenzsystemen. So könnten bezogen auf das Beispiel potenziell 84,6 % und damit der Großteil der Fahrunfälle, die aufgrund verschiedener Fehlanpassungen der eigenen Fahrmanöver an die jeweilige Situation (C3) durch systematisch implementierte Assistenzstrategien (S3), (S4) und (S5) vermieden bzw. in ihren Auswirkungen reduziert werden. Somit ist dieses Verfahren gleichermaßen interessant für Systemhersteller, die sicherheitsbewusste Fahrer als Kunden gewinnen möchten, als auch für Vertreter von volkswirtschaftlichen oder gesellschaftlichen Belangen mit der Möglichkeit sicherheitsfördernde Systeme finanziell oder durch eine darauf ausgerichtete Gesetzgebung zu fördern.

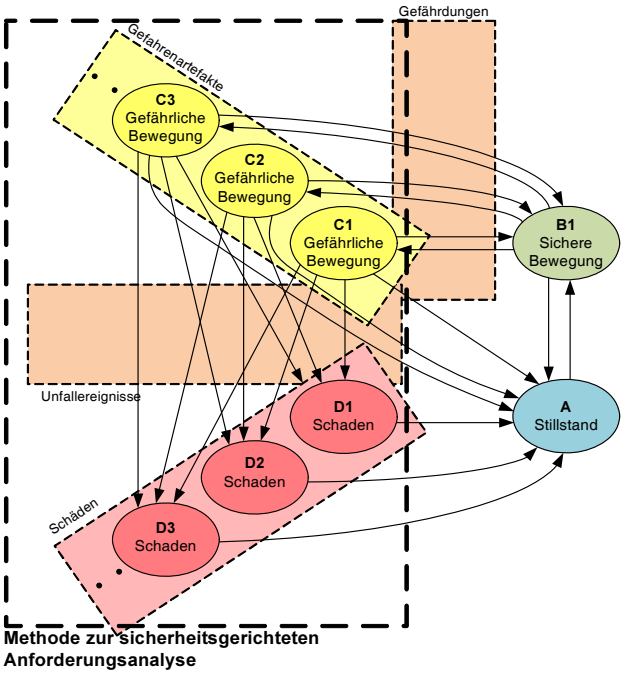


Abbildung 6.3: Einordnung und Umfang der vorgestellten Methode

Im folgenden Kapitel wird ein anforderungsgestützter Entwicklungsprozess für sicherheitsgerichtete Systeme erläutert, der bei einer Umsetzung von z.B. auf diese Weise gewonnenen Anforderungen angewendet werden kann.

7 Beispiel eines sicherheitsgerichteten Entwicklungsprozesses

Die in den vorangegangenen Kapiteln gezeigten Beispiele zur zielgerichteten systematischen Identifikation von Gefahren und Ermittlung sicherheitsrelevanter funktionaler Anforderungen basieren insbesondere für das Beispiel der Fahrerassistenzsysteme auf einem retrospektiv iterativen Ansatz. Dabei wird das vorhandene bereits entwickelte System (dort: Straßenverkehr) basierend auf einer Sicherheitsdefizitanalyse an seinen Schwachstellen unterstützt. Die vorgestellte Methode zur Identifikation von generischen Gefahrenartefakten basiert ebenfalls auf einer vorliegenden Systemstruktur sowie auf einem ausreichend und konsistent spezifizierten Systemverhalten.

In diesem Kapitel wird ein systematischer sicherheitsgerichteter Entwicklungsprozess beschrieben, der sich insbesondere in der Enwicklung von Systemen mit Sicherheitsverantwortung in der Schienenverkehrsdomäne weitestgehend etabliert hat.

Die Vorgehensweise basiert auf der Verfolgung eines strukturierten Entwicklungsprozesses, der potenzielle Gefahren des zu entwickelnden Systems bei dessen Anwendung identifizert, die möglichen Risiken abschätzt und daraus abgeleitete Sicherheitsanforderungen an das System zur Vermeidung nicht akzeptabler Risiken erstellt und kontrolliert umsetzt, verifiziert, validert und dokumentiert nachweist.

Ein immer wieder anzutreffendes Problem bei der Anwendung des normativ definierten lebenszyklusorientierten Entwicklungsprozesses ist die komplexe Vernetzung und in Folge dessen Vermischung von allgemeinen, sicherheitsrelevanten und dokumentierenden Aktivitäten. Klar definierte und eindeutig beschriebene Schnittstellen zwischen Produktentwicklung und Sicherheitsanalysen sowie der begleitenden Sicherheitsnachweisführung sind derzeit nicht vorhanden und liegen in der Verantwortung des jeweiligen Akteurs. Aus diesem Grund wird nachfolgend ein synchronisierter Entwicklungsprozess in Übereinstimmung mit den geltenden Normen vorgestellt.

7.1 Ein synchronisierter Entwicklungsprozess am Beispiel der EN 5012x

Eine Orientierung am Lebenszyklus von Systemen trägt dazu bei, die gesamte Wertekette sicher zu gestalten und damit nicht nur die Betriebsphasen in den Vordergrund zu stellen [WK06]. Die Betreiber von technischen Systemen müssen, bedingt durch die Einhal-

tung verschiedener sicherheitsrelevanter Normen (z.B. IEC 61508 [Deu02], DIN EN 50126 [Deu00], DIN EN 50128 [Deu01] oder DIN EN 50129 [Deu03b]), die u.a. den Stand der Technik prägen und bei deren etablierter Anwendung die anerkannten Regeln der Technik darstellen, während des gesamten Lebenszyklus geeignete Maßnahmen ergreifen, um die notwendige Sicherheit des Systems zu gewährleisten. Im Vordergrund stehen dabei die Fehlerursachen, die ebenfalls durch festgelegte Maßnahmen erkannt und entweder gänzlich oder zum größten Teil eliminiert werden können. Grundsätzlich wird bei der Entwicklung das systematische Vorgehen anhand eines V-Modells empfohlen. Das aus der EN 50126 entnommene und an das V-Modell angelehnte Modell des Systemlebenszyklus ist in Abbildung 7.1 abgebildet.

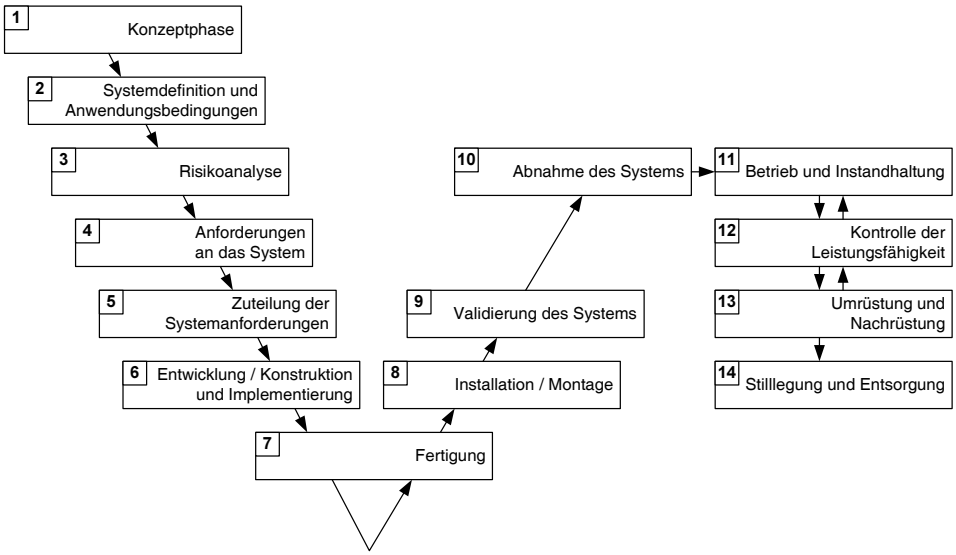


Abbildung 7.1: Lebenszyklusphasen für System im Schienenverkehr [Deu00]

Dieser Systemlebenszyklus wird in der Regel durch entsprechende Projektlebenszyklen umgesetzt und entsprechend instanziiert. Die Verteilung auf Projektlebenszyklen unterschiedlicher Akteure (Stakeholder) ist insbesondere nach erfolgter Zuteilung der Anforderungen auf Subsysteme von großer Bedeutung, um eine spätere reibungslose Integration dieser Subsysteme zu ermöglichen. Die Steuerung eines Projektlebenszyklus erfordert ein sicherheitsorientiertes Projektmanagement und ein kontinuierliches Anforderungsmanagement, die durch die Einführung eines Sicherheitsmanagementsystems erfolgen kann. In diesem Kontext wird in anderen Domänen oft von einem s.g. Functional Safety Management gesprochen, dessen Aufgabe die Planung und Ausführung des "Sicherheits-Controllings" darstellt. Nach [VDI07a] sind dabei folgende Arbeitsschritte durchzuführen:

- Übertragung der sicherheitstechnischen Anforderungen in Projekt- und Systemspezifikationen bezogen auf den gesamten Lebenszyklus des Produktes
- Erstellung sicherheitsbezogener Anforderungen an die Gestaltung des Systems und seiner Module/Baueinheiten

- Planerische Festlegung der Umsetzungsschritte
- Festlegung der Sicherheitsanforderungen, die der Nachweisführung zur Einhaltung der öffentlichen Sicherheit unterliegen
- Festlegung der Sicherheitsanforderungen, die zur Erlangung der Betriebsgenehmigung erforderlich sind
- Erstellung des Sicherheitsplans
- Erfahrungsrückführung

Diese Aktivitäten sind nach [Sch02a] durch eine anforderungsorientierte und durchgängige ganzheitliche Entwicklungsplanung zu erreichen. Dazu gehören ein Anforderungsmanagement, das neben der reinen Anforderungsentwicklung und Durchführung die Steuerung und Verwaltung von Anforderungen umfasst. Zusätzlich ist ein mit der Entwicklung eng verknüpftes Änderungsmanagement, Risikomanagement und Umsetzungsmanagement von entscheidender Bedeutung. Werden sicherheitsrelevante Anforderungen ohne ein entsprechendes Änderungsmanagement und darauf abgezieltes Risikomanangement geändert, können schwerwiegende Fehler bei der Umsetzung entstehen und bei einer mono-kausalen Betrachtung nicht erkennbare Gefahren systematisch „hinein-implementiert“ werden.

Die angesprochene erforderliche enge Vernetzung der allgemeinen und spezifischen Entwicklungs-, Sicherheits-, Dokumentations- und Managementtätigkeiten führt zu dem Anlass ein Prozessmodell für die lebenszyklusorientierte Entwicklung von Eisenbahnsystemen nach EN 50126 und EN 50128 zu erstellen, welches diese Aktivitäten beinhaltet und sinnvoll vernetzt. Insbesondere die Dokumentation von Sicherheitsnachweisen für signaltechnische Sicherungssysteme gemäß der EN 50129 lässt sich bestimmten allgemeinen und Sicherheitsaktivitäten zuordnen.

7.2 Ein integriertes Prozessmodell nach EN 5012x

Abbildung 7.2 bis Abbildung 7.5 zeigen die Unterscheidung der allgemeinen und sicherheitsrelevanten Aktivtäten der Phasen 1 bis 14 sowie deren jeweiligen Abhängigkeiten. Zusätzlich sind die Verknüpfungen zu den Kapiteln eines Sicherheitsnachweises nach EN 50129 aufgeführt.

Phase 1 - Konzeptphase: Das Ziel der Konzeptphase ist es, ein Verständnis für das zu erstellende System zu entwickeln sowie die Ideen und Visionen zu dokumentieren. Das Ergebnis der allgemeinen *Konzepterstellung* ist ein *Konzept*, welches den Umfang, den Zusammenhang und den Zweck des Systems enthält. Es beschreibt zusätzlich die Systemumgebung aus verschiedenen Perspektiven. Dazu gehören z.B.

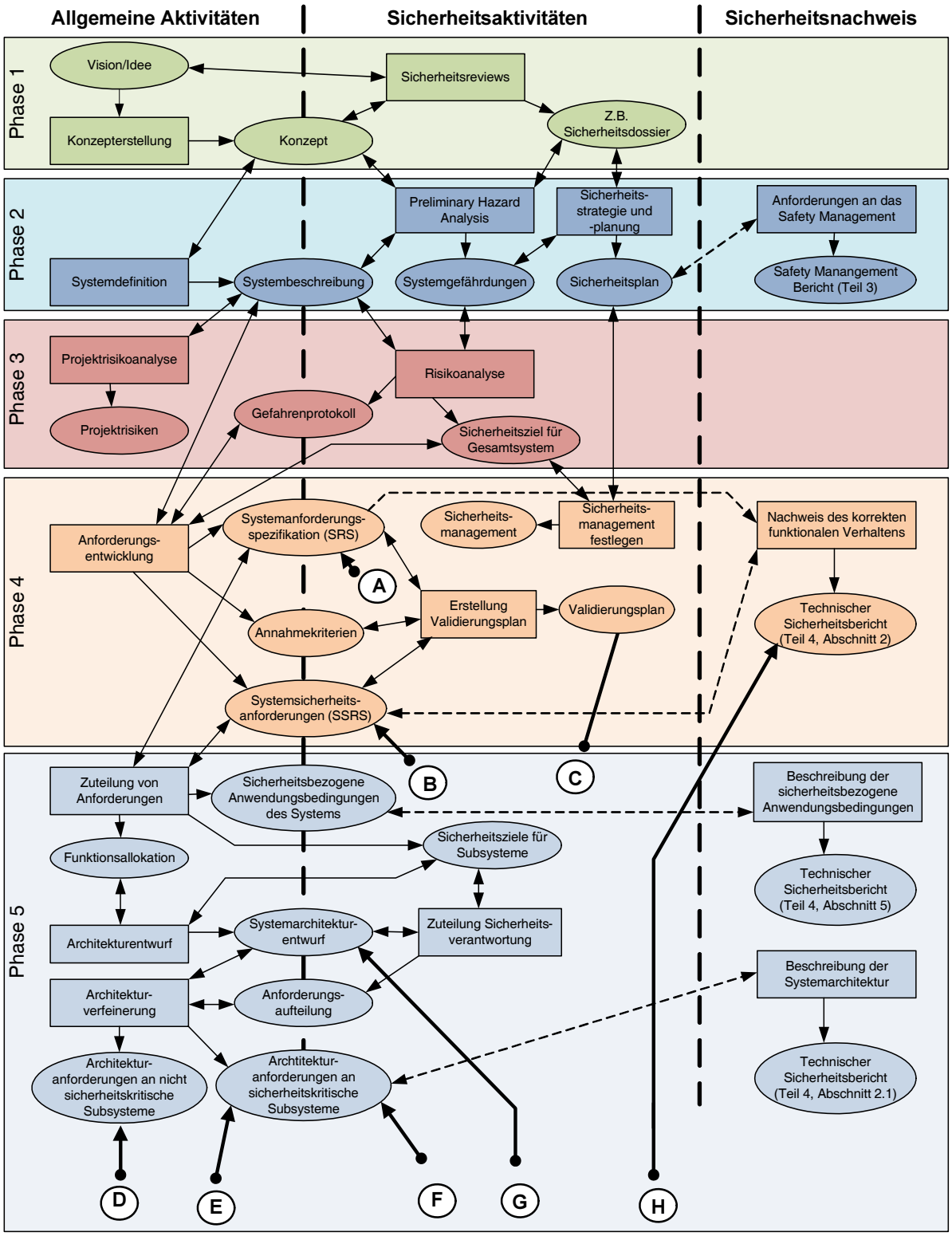


Abbildung 7.2: Aktivitäten im Projektlebenszyklus

die Klärung politischer, juristischer, sozialer und wirtschaftlicher Fragen sowie Fragen bzgl. vorhandener Schnittstellen zu anderen Systemen. Aus sicherheitsspezifischer Sicht werden im Rahmen eines *Sicherheitsreviews* ähnliche oder bereits vorhandene Systeme auf dort erreichte Sicherheitsziele, verfolgte Sicherheitsstrategien oder sonstige sicherheitsrelevante Randbedingungen in Form eines *Sicherheitsdossiers* dokumentiert.

Phase 2 - Systemdefinition und Anwendungsbedingungen: Das Ziel der Systemdefinition ist die Festlegung eines Betriebsaufgabenprofils in Form einer *Systembeschreibung*, welche aus dem *Konzept* der Phase 1 abgeleitet wird. Die Systembeschreibung soll u.a. Systemgrenzen und Anwendungsbedingungen festlegen und bereits erste Überlegungen bzgl. der späteren Instandhaltungsbedingungen berücksichtigen. Diese Ergebnisse fliessen in eine *vorläufige Gefahrenanalyse* ein, die auf Systemebene entsprechende *Systemgefahren* identifiziert. Gleichzeitig wird unter Berücksichtigung des *Sicherheitsdossiers* und der *Systemgefahren* ein erster *Sicherheitsplan* erstellt. Dieser stellt die spätere Basis für den *Sicherheitsmanagementbericht*, der als Teil 3 des Sicherheitsnachweises zu erbringen ist.

Phase 3 - Risikoanalyse: Die Risikoanalysephase verfolgt das Ziel, sowohl auf Projekt- als auch auf Systemebene Risiken zu bewerten. Dazu wird einerseits eine *Projektrisikoanalyse* basierend auf der *Systembeschreibung* durchgeführt und *Projektrisiken* identifiziert und bewertet. Diese können ggf. über die Weiterführung eines Projekts entscheiden. Die *Systemrisikoanalyse* nutzt die aus der Phase 2 gewonnenen Erkenntnisse über *Systemgefahren* und das zu erreichende *Systemsicherheitsziel* und dokumentiert die Ergebnisse unter Berücksichtigung von *Akzeptanzkriterien* in einem *Gefahrenprotokoll*. Das Gefahrenprotokoll führt projektbegleitend sämtliche Gefahren, deren Risikoeinstufung, sowie Maßnahmen und deren Realisierungstand, um ein durchgehendes Risikomanagement zu ermöglichen.

Phase 4 - Anforderungen an das System: Aufbauend auf der *Systembeschreibung* aus Phase 2, dem *Systemsicherheitsziel* und dem *Gefahrenprotokoll* der Phase 3 wird in dieser Phase das System in einer *Anforderungsentwicklung* spezifiziert. Ergebnisse sind eine *Systemanforderungsspezifikation*, *Systemsicherheitsanforderungen* sowie *Annahmekriterien* für eine spätere Validierung, die über die *Erstellung des Validierungsplans* geplant wird und als Dokument den *Validierungsplan* erzeugt. Die *Systemanforderungsspezifikation* und *Systemsicherheitsanforderungen* sind ebenfalls Eingangsgrößen für eine spätere Validierung. Gleichzeitig wird bereits in dieser Phase das *Sicherheitsmanagement* eingeführt, welches im *Sicherheitsplan* der Phase 2 entsprechen und dem *Systemsicherheitsziel* der Phase 3 genügen sollte. Die dokumentierten Anforderungen (insbesondere die Sicherheitsanforderungen) dieser Phase sind im Teil 4, Abschnitt 2 (Nachweis des korrekten funktionalen Verhaltens) des Sicherheitsnachweises nachzuweisen.

Phase 5 - Zuteilung der Anforderungen: Die in der vorangegangenen Phase erstellte *Systemanforderungsspezifiaktion* sowie die *Systemsicherheitsanforderungen* sind

die Eingangsgrößen dieser Phase, mit dem Ziel der *Zuteilung der Anforderungen* auf Subsysteme. Daraus resultieren eine *Funktionsallokation* und erste *Sicherheitsbezogene Anwendungsbedingungen* sowie *Sicherheitsziele für Subsysteme*. Diese werden in der Regel durch THRs[1] ausgedrückt. Der anschließende *Architekturentwurf* ist ein iterativer Prozess, der über die *Funktionsallokation* und die *Sicherheitsziele der Subsysteme* in mehreren Schritten über *Anfoderungsaufteilungen* und *Architekturverfeinerung* zu *Architekturanforderungen an nicht-sicherheitskritische Subsysteme* und *Architekturanforderungen an sicherheitskritische Systeme* mündet. Sowohl die *sicherheitsbezogenen Anwendungsbedingungen* als auch die *Architekturanforderungen an sicherheitskritische Subsysteme* sind im Sicherheitsnachweis zu beschreiben bzw. deren Erfüllung nachzuweisen.

Phase 6 - Entwicklung / Konstruktion und Implementierung: Die hier beschriebene Phase ist die umfangreichste Phase, da in dieser die gesamte Entwicklung, Konstruktion und Implementierung des Systems und der Subsysteme erfolgt. Basierend auf den *Architekturanforderungen für nicht-sicherheitheitskritische und sicherheitskritische Systeme* und dem gesamten *Systemarchitekturentwurf* werden einerseits die *Entwicklung unkritischer Systeme* und andererseits die *Entwicklung sicherheitskritischer Subsysteme* vorangetrieben. Aus einer *Gefahrenanalyse*, die insbesondere die Subsysteme bezüglich Einzelfehler, Mehrfachfehler und Fehler mit gemeinsamen Ursachen analysiert, resultieren *Anforderungen an die Unabhängigkeit der Betrachtungseinheiten*, die sowohl in den *Entwicklungsprozess sicherheitskritischer Subsysteme* als auch in die Sicherheitsnachweisführung (Teil 4, Abschnitt 3) eingeht. Gleichzeitig werden ggf. zusätzlich erkannte Gefahren in das *Gefahrenprotokoll* eingetragen. Als Ergebnis des *Entwurfs sicherheitskritischer Subsysteme* entstehen *Subsystemanforderungen an E/E/PE-Systeme*[1] und *Subsystemanforderungsspezifikationen anderer Technologien* auf deren Basis diese implementiert werden.

Für Funktionen der E/E/PE-Systeme werden *Sicherheitsintegritätsanfoderungen*[2] festgelegt, die je nach Stufe entsprechende weitere Maßnahmen während der Entwicklung bedingen. Über die *Zuteilung der Anforderungen auf Hardware und Software* entscheidet sich u.a. die weitere Verwendung zusätzlicher Normen, wie z.B. die EN 50128 [Deu01] und das weitere Vorgehen. Je nach Zuteilung und Randbedingung ergeben sich hier erneut *sicherheitsbezogene Anwendungsbedingungen*, die als Eingangsgröße für den Sicherheitsnachweis zu berücksichtigen sind.

Hardware-Anforderungen fließen in einen *HW-Entwurf*, während *Software-Anforderungen* in einen *SW-Entwurf* eingehen und gleichzeitig über die *Analyse der SW-Sicherheitsanforderungsstufen* die *Sicherheitsintegritätsanforderungen* umsetzt.

[1] THR - Tolerable Hazard Rate vgl. [Deu00]

[1] Elektrische, elektronische und programmierbar elektrische Systeme vgl. [Deu02]

[2] Sicherheitsintegritätsanforderungen werden in Stufen festgelegt (SIL1 bis SIL4) vgl.[Deu00]

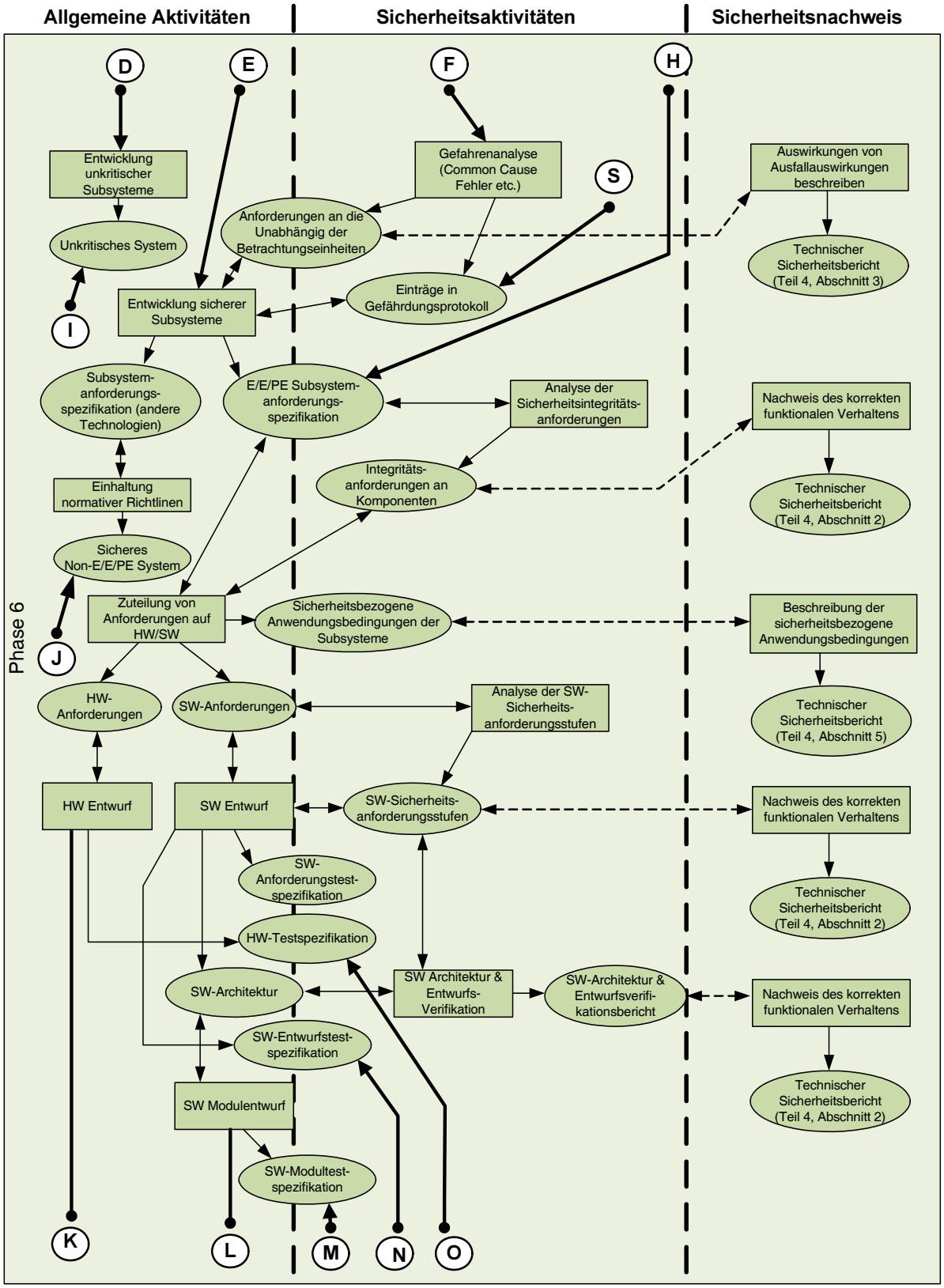


Abbildung 7.3: Aktivitäten im Projektlebenszyklus (Fortsetzung 1)

Die Ergebnisse des Hardwareentwurfs sind *HW-Spezifikationen* und *HW-Testspezifikationen* für die späteren *HW-Komponententests*. Der *SW-Entwurf* liefert die *SW-Spezifikation*, *SW-Testspezifikation* für die spätere SW-Validierung sowie die *SW-Architekturspezifikation* und zugehörige *SW-Entwurfstestspezifikation* bevor der *Modulentwurf* beginnt. Die in diesem Prozess entstehende *Modulspezifikation* wird einer *Modulverifikation* unterzogen, die in einem *Modulverifikationsbericht* dokumentiert wird. Der durch die *SW Codierung* anhand der *Modulspezifikation* erzeugte *SW-Quellcode* wird unter Verwendung der *Modultestspezifikation* den *Modultests* unterzogen, die in dem *SW-Modultestbericht* dokumentiert wird.

Nach erfolgter *SW-Integration* muss die *Software* entsprechende *SW-Integrationstests* durchlaufen, die ebenfalls in einem *Integrationstestbericht* dokumentiert werden. Die *HW/SW-Integration* zum fertigen Subsystem (*SW/HW-System*) wird ausgiebig in einer *SW-Validierung* über die *SW-Anforderungstestspezifikation* den Software-Anforderungen gegenübergestellt. Das Ergebis ist ein dokumentierter *SW-Validierungsbericht*.

Sämtliche Berichte dieser Phase fließen in die Sicherheitsnachweisführung zum Nachweis des korrekten funktionalen Verhaltens (Teil 4, Abschnitt 2) ein.

Phasen 7 und 8 - Fertigung, Installation und Montage: Diese Phasen haben als Zielsetzungen die *Systemimplementierung* eines Fertigungsprozesses, der validierte Subsysteme und Komponenten erzeugt, sowie der Zusammenbau und die Montage der Gesamtheit der Subsysteme und Komponenten, die erforderlich sind, um das *Gesamtsystem* zu bilden. Während dieser Implementierung und Fertigung wird weiterhin das *Gefahrenprotokoll* angewendet und ggf. durch unerwartet auftretende Gefahren ergänzt, die z.B. in Folgeentwicklungen einfließen, oder im schlimmsten Fall bei Nichtakzeptanz des Risikos einen Rückschritt in die Entwicklungs- und Konstruktionsphase (Phase 6) bedeutet.

Phase 9 - Validierung des Systems: Ziel der Validierung ist die Prüfung der gesamten Subsysteme, Komponenten und externen Maßnahmen zur Minderung von Risiken gegen die spezifizierten Anforderungen. Dabei wird in erster Linie das installierte System als Ganzes validiert und auf bereits auf Subsystemebene validierte Teile zurückgegriffen. Die *Systemvalidierung* folgt dem *Validierungsplan* aus Phase 4 und stellt die *Systemanforderungsspezifikation* und die *Systemsicherheitsanforderungen* dem installierten System gegenüber um die Realisierung zu bestätigen. In der Regel wird dieses durch entsprechende Feldtests umgesetzt. Gleichzeitig werden Subsystemvalidierungsberichte, z.B. *SW-Validierungsberichte*, mit einbezogen. Das Ergebnis der *Systemvalidierung* wird im *Validierungsbericht* dokumentiert, der als eine der wichtigsten Eingangsgrößen zum Nachweis des korrekten funktionalen Verhaltens dient.

Als allgemeine Aktivitäten werden in dieser Phase *Schulungen* des Bedien- und Instandhaltungspersonals während des *Probebetriebs* durchgeführt. Teilweise wird

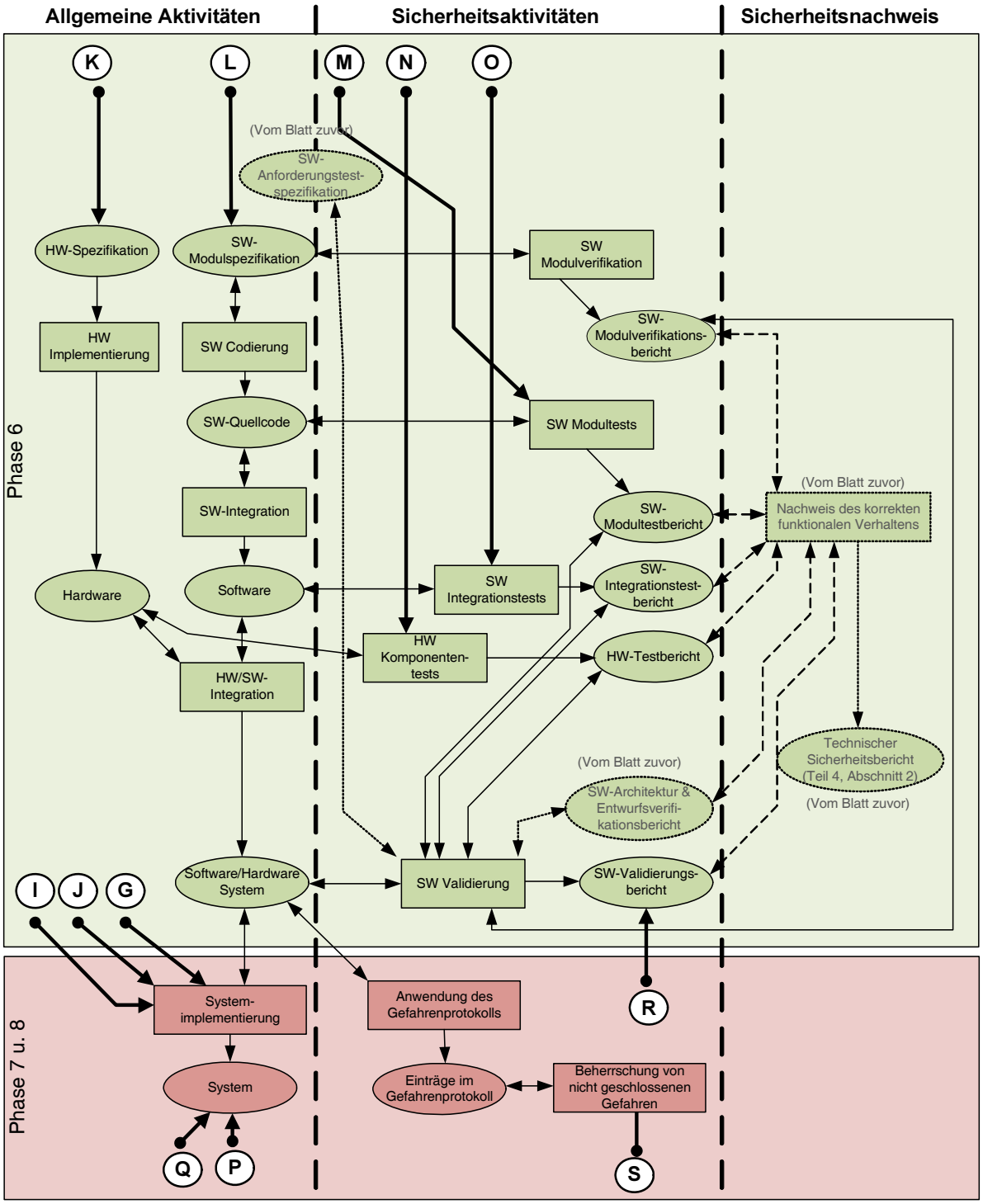


Abbildung 7.4: Aktivitäten im Projektlebenszyklus (Fortsetzung 2)

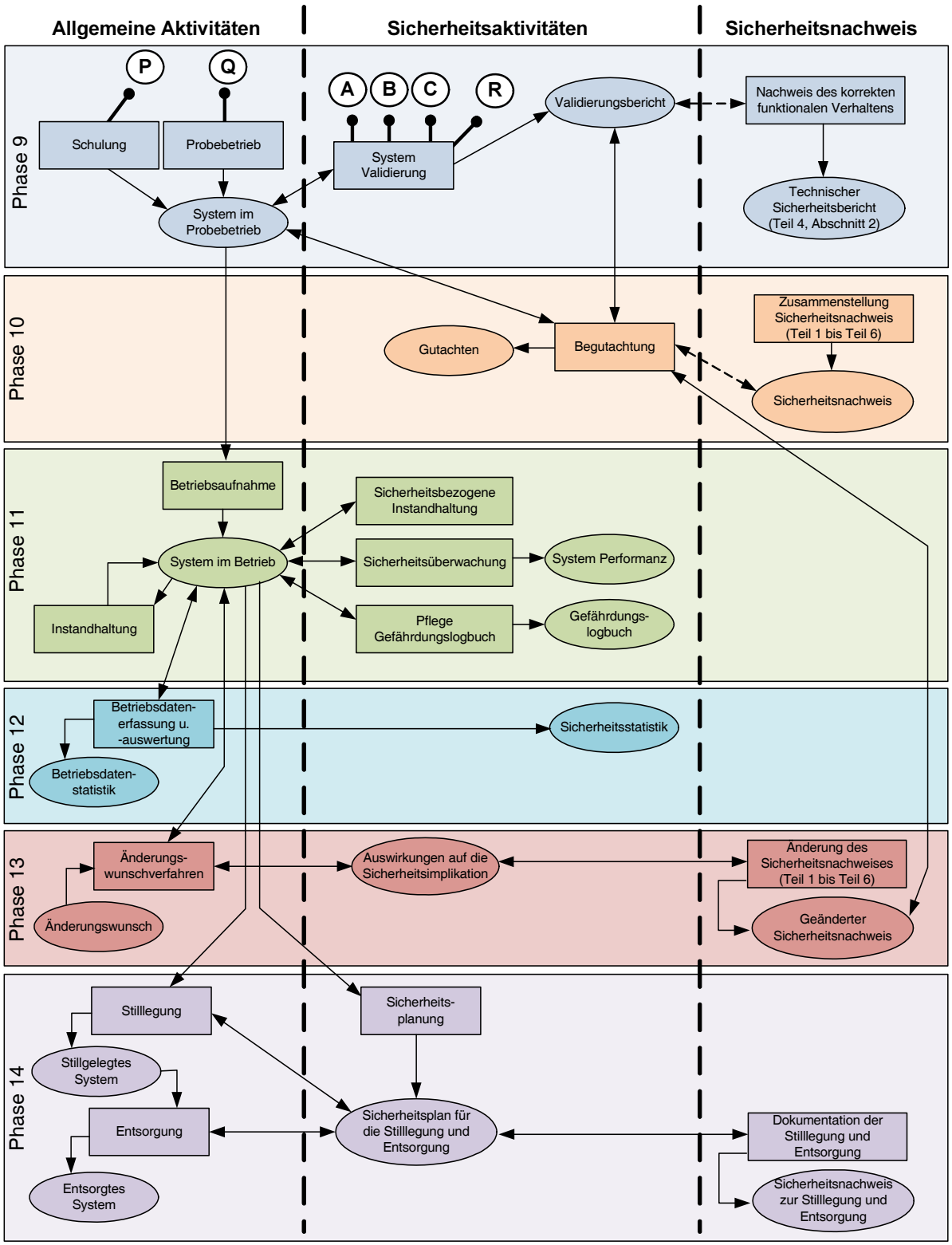


Abbildung 7.5: Aktivitäten im Projektlebenszyklus (Fortsetzung 3)

dem *Probebetrieb* ein s.g. Testbetrieb vorgelagert, in der die Validierung/Feldtests stattfinden. Der tatsächliche Probebetrieb wird dann erst nach offizieller Erklärung der Funktionsfähigkeit (HdF) durch den Hersteller, der den positiven Abschluss der Validierung bedeutet, begonnen.

Die Anforderungen der Phase 10, „Abnahme des Systems“, können mit den Anforderungen dieser Phase 9 zusammengefasst werden, wenn es zum betrachteten System passt. In diesem Fall müssen die Ergebnisdokumente dieser kombinierten Phase zeigen, dass bei der Realisierung von Phase 9 auch die Anforderungen von Phase 10 angemessen erfüllt werden.

Phase 10 - Abnahme des Systems: Die Abnahme des System erfolgt durch die Bewertung der Übereinstimmung sämtlicher Subsysteme, Komponenten und der externen Maßnahmen zur Minderung der Risiken bezüglich der System- und Systemsicherheitsanforderungen an das Gesamtsystem. In der Regel erfolgt dies bei vielen Systemen des Schienenverkehrs bereits in der Validierungsphase (Phase 9). Eine weitere Aktivität dieser Phase ist insbesondere bei Systemen des Schienenverkehrs die *Begutachtung*, die je nach Sicherheitintegritätsanforderung ein bestimmtes Maß an Unabhängigkeit aufweisen muss. Die *Begutachtung* evaluiert die Inhalte des *Sicherheitsnachweises* unter Einbezug der darin verwiesenen Dokumente (z.B. *Validierungsbericht* und erstellt ein *Gutachten*, welches in der Regel den jeweiligen nationalen Aufsichtsbehörden zur Systemzulassung vorgelegt werden muss. In einigen Fällen werden während der *Begutachtung* das im Probe-/Testbetrieb befindliche System mit einbezogen und einige Tests im Beisein der Gutachter wiederholt.

Phasen 11 bis 14 - Betrieb und Instandhaltung bis Stilllegung und Entsorgung: In der Phase 11 beginnt der eigentliche Betrieb des Systems mit der *Betriebsaufnahme* mit der laufenden *Instandhaltung*, die durch die *sicherheitsbezogene Instandhaltung* ergänzt wird. Diese überprüft z.B. im Rahmen von entsprechenden in den sicherheitsbezogenen Anwendungsregeln eines Systems definierten Wartungsintervallen sicherheitsrelevante Teile/Komponenten oder tauscht diese aus. Die laufende *Sicherheitsüberwachung* dokumentiert die erreichte *Systemleistungsfähigkeit*, die z.B. für eine entsprechende Qualifizierung eines Systems evtl. nachzuweisen ist. Gefahren, die während des Betriebs auftreten und nicht bereits im *Gefahrenlogbuch* dokumentiert sind, werden nachgetragen.

Die Phase 12 dient parallel zur Phase 12 der *Betriebsdatenerfassung* während des Betriebs um z.B. für weitere Projekte erforderliche *sicherheitsrelevante Statistiken* vorzuhalten. Bei z.B. durch auftretende Gefahren oder aufgrund von Kundenwünschen erforderlichen Änderungen am System wird gemäß Phase 13 ein s.g. *Änderungswunschverfahren* eingeführt, das *Änderungswünsche* unter Berücksichtigung der *Sicherheitsauswirkungen* und entsprechender *Sicherheitsnachweise* ermöglicht. Der *Sicherheitsnachweis* ist ggf. bei zulassungspflichtigen *Änderungen* erneut zu begutachten und durch eine nationale Aufsichtsbehörde zuzulassen.

Am Ende des Lebenszyklus befindet sich bei jedem System die *Stilllegung* und *Entsorgung* des Systems. Diese Aktivitäten sind ebenfalls entsprechend einer *Sicher-*

heitsplanung zu unterziehen und folgen einem dabei erstellen *Sicherheitsplan* für die Stilllegung und Entsorgung. Diese Sicherheitsplanung berücksichtigt eventuelle Auswirkungen auf angrenzende Systeme und durch die Stilllegung und Entsorgung ggf. auftretende Gefahren, die entsprechend zu beherrschen sind.

Der gezeigte Lebenszyklus stützt sich dabei in erster Linie auf einer sorgfältigen Systemanforderungsphase aus der sowohl funktionale Anforderungen, zur Erfüllung des gewünschten Objektverhaltens, als auch funktionale Sicherheitsanforderungen, die in Anforderungen an sichere Steuerungen und Prozesse übergehen und durch nicht-funktionale Sicherheitsanforderungen (z.B. Qualitätsanforderungen, quantitative Sicherheitsziele etc.) skaliert werden.

7.2.1 Kontinuierliches Anforderungsmanagement

Geplante Sicherheit muss, wie im vorangegangenen Abschnitt gezeigt, in Form von (Sicherheits-)Anforderungen in die Entwicklung eingehen, um entsprechend implementiert und validert werden zu können. Grundlage für ein solches Vorgehen ist ein kontinuierliches Anforderungsmanagement, welches neben der Spezifikation von Produktfunktionen insbesondere die Belange der Sicherheit (bzw. insgesamt RAMS) berücksichtigt.

Anforderungsmanagement wird lt. [Sch02a] und [Poh08] oft als Oberbegriff sowohl für alle Aufgaben zur Ermittlung und Definition von Anforderungen,als auch für die Steuerung, Kontrolle und Verwaltung dieser operativen Aufgaben benutzt. Die Vorteile einer gesteuerten und verwalteten Anforderungsentwicklung können wie folgt zusammengefasst werden:

- Anforderungen werden über den gesamten Lebenszyklus von der Konzeptphase über die Ermittlung der Anforderungen beim Kunden bis zur Umsetzung im Entwicklungsprojekt konsistent und für die Beteiligten transparent und verständlich verwaltet.

- Es existieren eindeutige Verantwortungsbereiche für den Umgang mit unterschiedlichen Anforderungen (z.B. Sicherheitsanforderungen, Qualitätsanforderungen, Umweltanforderungen etc.). Dadurch können Rollenkonflikte durch definierte Auftragnehmer-/Auftraggeberrollen im Sinne eines vertragsorientierten Vorgehens vermieden werden.

- Die Vollständigkeit und Robustheit der spezifizierten Anforderungen werden kontinuierlich überprüft, z.B. Validerung über kundenseitige oder behördliche Abnahmekriterien, die innerhalb des Anforderungsmanagements mit geführt werden.

- Fehler und Defizite in Anforderungen werden frühzeitig entdeckt und in einem definierten Prozess behoben. Die Entwicklungskosten können auf diese Weise optimiert werden, indem Fehlerkosten frühzeitig reduziert werden.

Anforderungen können grundsätzlich in drei Arten von Anforderungen unterteilt werden. Während die Kundenanforderungen die Belange und Wünsche des Kunden ausdrücken und vorwiegend die Funktionalität und Beschaffenheit des Produktes beschreibt, spezifizieren die Produktanforderungen zusätzliche Anforderungen an das Produkt, die entweder aus eigenen (Hersteller-)spezifischen Anforderungen oder aus externen Quellen resultieren. So können zusätzliche Anforderungen an die Umweltverträglichkeit, Sicherheit oder Rechtslage zu den Kundenanforderungen hinzukommen. Aber auch Anforderungen, die sich aus der Unternehmensstrategie oder dem Produktportfolio ergeben erweitern den Umfang der Produktanforderungen. Aus den Produktanforderungen lassen sich zusätzliche Projektanforderungen spezifizeren, die nicht direkt die Beschaffenheit des Produktes beeinflussen, sondern sich vorwiegend auf den Erstellungs-, Dokumentations- oder Verwaltungprozess konzentrieren. Diese Anforderungen lassen sich auch als Managementanforderungen verstehen. Im Bezug zur Sicherheit sind diese produktbegleitenden Prozesse in der Regel Prozesse der Nachweisführung, Begutachtung, Erprobung und Zulassung. Aber auch Prozesse des Marketings, der Entwicklungsdokumentation oder von produktspezifischen Schulungen usw. sind Anforderungen, die im Rahmen einer anforderungsorientierten Entwicklung zu spezifizieren sind.

Gerade im Hinblick auf sicherheitskritische Systeme und deren (Sicherheits-)Nachweisführung zeigt sich die Notwendigkeit einer durchgängigen Verfolgbarkeit von (Sicherheits-)Anforderungen von ihrer Entstehung aufgrund nicht akzeptabler Risiken bis zur Erfüllung durch das Produkt. Ohne den Bezug zu ihrer risikovermeidenden Aufgabe lassen sich Anforderungen insgesamt bzw. deren Änderungen nur schwer rückwirkend argumentieren. Änderungswünsche an Anforderungen, die in jedem Projekt mehr oder weniger aus unterschiedlichen Gründen häufig auftreten, unkontrolliert umzusetzten kann insbesondere bei sicherheitsrelevanten Anforderungen ggf. zu fatalen Auswirkungen führen, wenn keine oder nur eine mangelhafte Analyse der Rückwirkungsfreiheit durchgeführt wird. Abhilfe schafft dabei ein im kontinuierlichen Anforderungsmanagement fest installiertes Risiko-, Änderungs- und Umsetzungsmanagement, welches die Auswirkungen einer geplanten Änderung gezielt bewertet, freigibt oder verwirft und sorgfältig deren Umsetzung verfolgt.

Einen sehr guten Überblick zur Thematik des kontinuierlichen Anforderungsmanagements inklusive einer Bewertung unterschiedlicher Werkzeuge sowie die Beschreibung der grundsätzlichen Anforderungsentwicklung zeigt [Sch02a].

7.3 Bewertung und Anwendungspotenziale

Prozesse sind der wesentliche Kernpunkt um Sicherheit kontrolliert und qualitätsgesichert zu implementieren. Im Mittelpunkt dabei steht neben den fundierten Analyse- und Entwicklungsmethoden eine kontrollierende und regelnde Instanz, die den sinnvollen, korrekten und zielgerichteten Einsatz dieser Methoden und Verfahren plant, überwacht und steuert.

Eine durchgehende Sicherheitsnachweisführung kann die sorgfältige und angemesse-

ne Umsetzung von gewählten Sicherungsimplementierungskonzepten bestätigen. Durch den gezielten Einsatz von entsprechenden Methoden während des gezeigten Entwicklungsprozesses kann der iterative Aufwand bei der Entwicklung eines Systems mit Sicherheitsverantwortung optimiert werden. Eine klare und definierte Aufstellung eines Projektmanagements, welches durch ein kompetentes Sicherheits- und Qualitätsmanagement unterstüzt wird, sind dabei ein wichtiger Schlüssel zum wirtschaftlichen Erfolg, ohne dabei Sicherheitsbelange zu vernachlässigen.

Ein integriertes Prozessmodell für den jeweiligen Entwicklungprozess, welches insbesondere die Produktentstehung und die Sicherheitsaktivitäten, die sich in erster Linie durch Analysen und Dokumentation ausdrücken, sowie die Aktivitäten der Sicherheitsnachweisführung unterscheidet, kann für eine gesteigerte Transparenz sowohl bei Herstellern als auch bei Betreibern von Systemen mit Sicherheitsverantwortung führen. Diese Transparenz kann dabei helfen, menschliche Fehlhandlungen in der Entwickklungstätigkeit aufgrund der enormen Komplexität zu vermeiden und damit sichere und mit weniger Aufwand nachweisbare Systeme zu schaffen.

8 Zusammenfassung und Ausblick

8.1 Zusammenfassung

Die Verbesserung der Verkehrssicherheit als Ziel zu verfolgen, erfordert nicht nur ein umfangreiches Verständnis von Zusammenhängen, Strukturen und Funktionen des Systems Verkehr sondern benötigt zusätzlich die Kenntnisse von sicherem Systemverhalten oder die Definition sicherer oder gefährlicher Zustände von konkreten aber auch abstrakten technischen Systemen.

Diese Arbeit zeigt über eine ausführliche begriffliche Analyse sowohl die Facetten des Systems Verkehr, als auch formalisierte Zusammenhänge der Sicherheit als allgemeine übergreifende Systemeigenschaft. Die Systemsicherheit konnte im Rahmen dieser Arbeit auf Basis von Systemeigenschaften zustands- und verhaltensorientiert analysiert werden. Die Methoden und Beschreibungsmittel der Automatisierungstechnik wurden dazu unterstützend eingesetzt und führten zum Erfolg.

Aus der Verknüpfung dieser Erkenntnisse konnte ein ausgeprägtes Wissen über die Verkehrssicherheit generiert und formalisiert werden, welches in die Konstruktion und Modellierung von allgemeinen Sicherungsimplementierungkonzepten einfloss. Implementierungskonzepte, die auf generischer Systemebene entwickelt wurden, dienten der Analyse von verschiedenen Sicherungsimplementierungen im Verkehrssystem, die durch Beispiele belegt wurden. In der exemplarischen Anwendung dieser Erkenntnisse wurden verschiedene Methoden und Prozesse entwickelt, die maßgeblich die Sicherheit von Verkehrssystemen erhöhen können.

In der Beschreibung einer entwickelten Methode zur Identifikation generischer Gefahren, ist wurde ein Vorgehen gezeigt, welches auf Basis einer bekannten Systemstruktur und einem bekannten Systemverhalten eine systematische Konstruktion potenzieller Gefahrenartefakte ermöglicht. Die einheitliche Detaillierungtiefe hilf identifizerte Gefahren in einer festgelegten Syntax zu beschreiben. Durch die systematische Identifikation von potenziellen Gefahren können Anforderungen zu deren Vermeidung in Form von Sicherungsfunktionen zielgerichtet erstellt werden. Anhand eines Beispiels aus der Eisenbahnsicherungstechnik wurde die Methode erklärt und veranschaulicht.

Eine andere Methode wurde vorgestellt, die eine Ableitung von funktionalen Sicherheitsanforderungen auf der Grundlage von Unfallanalysen ermöglicht. Zur beispielhaften Ermittlung von Anforderungen an sicherheitsfördernde Fahrerassistenzsysteme wurden typische Fehlhandlungen von Fahrern im Straßenverkehr analysiert, quantifiziert und mit Funktionen zur Erfüllung der Fahraufgabe verknüpft. Den Fehlhandlungen wurden bekannte Assistenzstrategien von der einfachen Information bis zur vollständigen

Übernahme von Funktionen zugeordnet. Unter Berücksichtigung des Zusammenhangs zwischen Fehlhandlung und Unfallhäufigkeit und der damit verknüpften Funktion zur Erfüllung der Fahraufgabe sind Anforderungen an Assistenzsysteme abgeleitet worden, die das größte Unfallvermeidungpotenzial aufweisen würden, indem sie die auf die Fehlhandlungen abgestimmten Assistenzstrategien umsetzen.

In einem weiteren Beispiel ist ein durchgehender Entwicklungsprozess als integriertes Prozessmodell dargestellt worden. Diese Modell verbindet die allgemeinen Aktivitäten während einer Produkt-/Systementwicklung mit den Aktivitäten die zur Entwicklung eines „sicheren“ Produktes/Systems erforderlich sind. Dazu sind die phasenbezogenen Informationsquellen und Dokumentationsziele zur Sicherheitsnachweisführung am Beispiel der Europäischen Normen für Bahnanwendungen integriert worden. Die Transparenz und somit auch die Zuverlässigkeit des Prozesses über den gesamten Lebenszyklus werden zusätzlich in dem Beispiel durch den Vorschlag eines kontinuierlichen Anforderungsmanagements unterstützt.

8.2 Ausblick

Die Integration des hier gezeigten Wissens über Sicherungsimplementierungskonzepte und Methoden in einen vollständigen und transparenten Entwicklungsprozess ggf. unter Einbezug von geeigneten Werkzeugen zum Anforderungsmanagement, Qualitätsmanagement und Sicherheitsmanagement stellt eine Herausforderung für Hersteller, Dienstleister und forschende Einrichtungen im Bereich der Verkehrstechnik für die Zukunft dar.

Aufgrund der Forderung nach sicheren Systemen darf die Sicherheit nicht durch eine künstliche Komplexität während der Entwicklung gefährdet werden. Aus diesem Grund erscheint es als sinnvoll Prozesse, wie z.B. die Gefahrenidentifikation, Anforderungsentwicklung und die Sicherheitsnachweisführung sowohl methodisch als als durch neue Werkzeuge zukünftig zu unterstützen und vollständig in Sicherheitsmanagementsystemen zu integrieren.

Neue Wege in der Sicherheitsbetrachtung von Verkehrssystemen auf Basis von Analysen des sicheren/unsicheren Verhaltens und nicht auf Basis reiner Unfallstatistiken könnten neuen Sicherungsimplementierungsmöglichkeiten Auftrieb geben, sofern einheitliche skalierbare Sicherheitsmaße an Akzeptanz gewinnen.

Die in dieser Arbeit vorgestellten Methoden decken bereits einen Großteil der zur Analyse der Verkehrssicherheit erforderlichen Eigenschaften, Merkmale und Größen ab. Zur Vervollständigung sind jedoch noch weitere interessante Bestandteile des Modells durch weitere Methoden und Analysen zu bearbeiten. Abbildung 8.1 zeigt die abgedeckten Bereiche anhand des formalisierten Modells zur Verkehrssicherheit, die durch weitere Forschung bearbeitet werden könnten. Die Entstehung unterschiedlicher Gefährdungen aus verschiedenen sicheren Zuständen systematisch zu analysieren wäre neben der Beachtung von Schadensbehebungen ebenfall ein für die Domäne der Verkehrssicherheit wichtiger Beitrag.

Die Entwicklung sicherer Systeme kann ganzheitlich erfolgen und unkonventionelle Sicherungsimplementierungen, wie z.B. den Einbezug von allen Verkehrskonstituenten, berücksichtigen. Die verschiedenen Domänen, die an einem Verkehrssystem beteiligt sind müssen dafür gemeinsam aufeinander abgestimmt agieren. Eine Voraussetzung für das gemeinsame Handeln ist jedoch das gleiche Systemverständnis. Die Verwendung von einheitlichen domänenübergreifenden Terminologien, die auf Basis einer begrifflichen Analyse nach dem hier gezeigten Beispiel entstehen, können das Wissen harmonisieren und den Blick auf das Wesentliche, die Schaffung sicherer Systeme im Verkehr, freigeben.

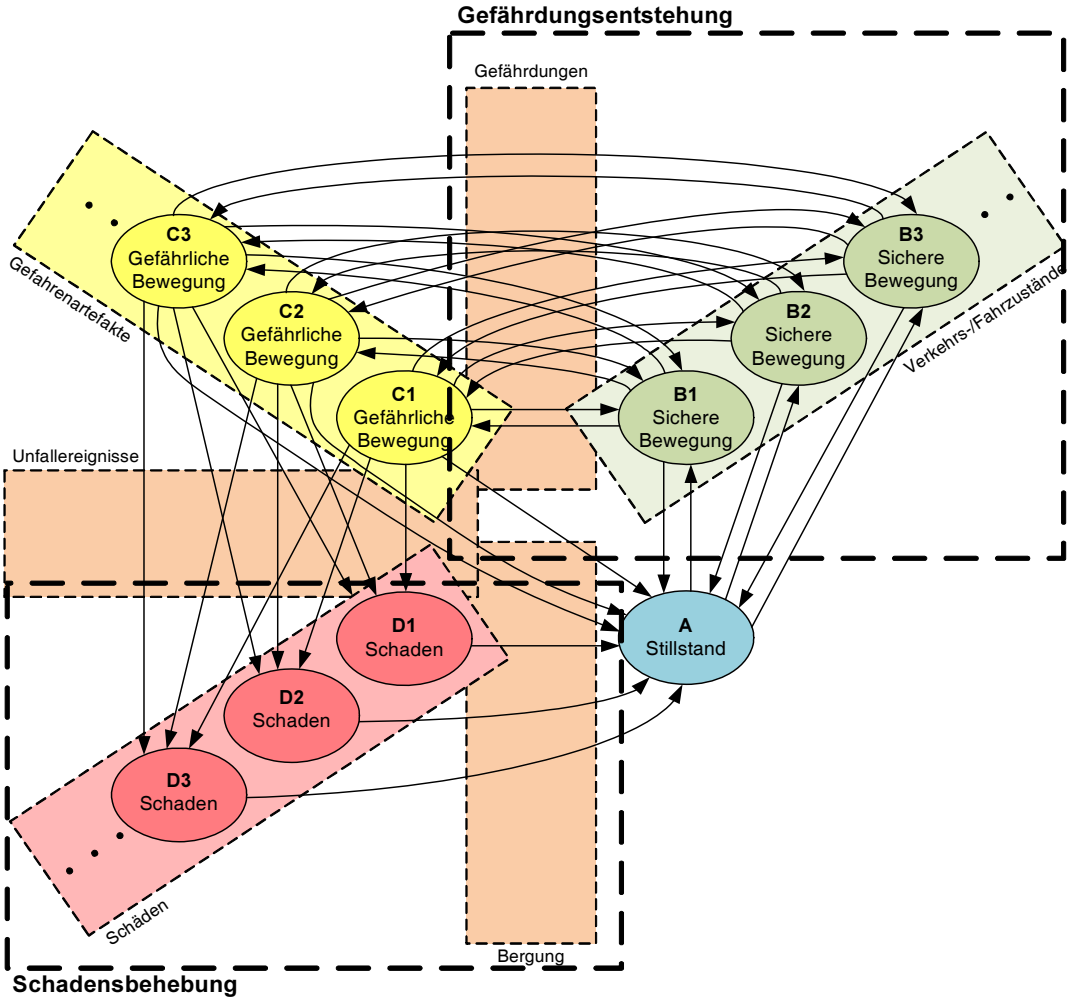


Abbildung 8.1: Einordung und Umfang für weitere Arbeiten

Literaturverzeichnis

[35400] 3542, VDI: *Sicherheitstechnische Begriffe für Automatisierungssysteme*. Oktober 2000

[40086] 4004, VDI: *Zuverlässigkeitskenngrößen*. September 1986

[AH06] Ammoser, Hendrik ; Hoppe, Mirko: *Glossar Verkehrswesen und Verkehrswissenschaften*. 2006 (Diskussionsbeiträge aus dem Institut für Wirtschaft und Verkehr ISBN 1233-626X)

[Ber69] Bertalanffy, Ludwig: *General System Theory - Foundations, Development, Applications*. Georg Brazilla, Inc., New York, 1969

[Bir06] Birkenbihl, Klaus: Standards für das Semantic Web. Version: 2006. http://dx.doi.org/10.1007/3-540-29325-6. In: Pellegrini, Tassilo (Hrsg.) ; Blumauer, Andreas (Hrsg.): *Semantic Web - Wege zur vernetzten Wissensgesellschaft*. Berlin/Heidelberg : Springer, 2006 (X.media.press). – DOI 10.1007/3–540–29325–6. – ISBN 978–3–540–29324–8, S. 73–88

[Bit67] Bitzl, Franz: *Der Einfluss der Strasseneigenschaften auf die Verkehrssicherheit*. Bundesminister f. Verkehr, Abteilung Strassenbau, 1967

[BJK07] Brock, Ditmar ; Junge, Matthias ; Krähnke, Uwe: *Soziologische Theorien von Auguste Comte bis Talcott Parsons*. Oldenbourg Verlag Miinchen Wien, 2007

[BLHL01] Berners-Lee, Tim ; Hendler, James ; Lassila, Ora: The Semantic Web - A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. In: *Scientific American* (2001), Mai

[BP06] Blumauer, Andreas ; Pellegrini, Tassilo: Semantic Web und semantische Technologien: Zentrale Begriffe und Unterscheidungen. Version: 2006. http://dx.doi.org/10.1007/3-540-29325-6. In: Pellegrini, Tassilo (Hrsg.) ; Blumauer, Andreas (Hrsg.): *Semantic Web - Wege zur vernetzten Wissensgesellschaft*. Berlin/Heidelberg : Springer, 2006 (X.media.press). – DOI 10.1007/3–540–29325–6. – ISBN 978–3–540–29324–8, S. 9–25

[Bör06] Börcsök, Josef: *Funktionale Sicherheit - Grundzüge sicherheitstechnischer Systeme*. Hüthig Verlag, Heidelberg, 2006

[Bro06] Brockhaus: *Der Brockhaus in drei Bänden, Enzyklopädie*. Bibliographisches Institut, Mannheim, 2006

[BS02] Bikker, Gert ; Schroeder, Martin: *Methodische Anforderungsanalyse und automatisierter Entwurf sicherheitsrelevanter Eisenbahnleitsysteme mit kooperierenden Werkzeugen*. Braunschweig, Technische Universität Braunschweig, Institut für Regelungs- und Automatisierungstechnik, Dissertation, 2002

[BS08] Badke-Schaub, Petra: *Human Factors : Psychologie sicheren Handelns in Risikobranchen ; mit 17 Tabellen*. Springer Medizin Verlag, Heidelberg, 2008

[BSMM95] Bronstein, Ilja N. ; Semendjajew, Konstantin A. ; Musiol, Gerhard ; Mühlig, Heiner: *Taschenbuch der Mathematik*. Verlag Herri Deutsch, 1995

[Bub90] Bubb, Heiner: *Bewertung und Vorhersage der Systemzuverlässigkeit - Ingenieurpsychologie, Enzyklopädie der Psychologie, Band 2*. Verlag für Psychologie, 1990

[Bun02] Bundesministerium: *Verordnung über Sicherheit und Gesundheitsschutz bei der Bereitstellung von Arbeitsmitteln und deren Benutzung bei der Arbeit, über Sicherheit beim Betrieb überwachungsbedürftiger Anlagen und über die Organisation des betrieblichen Arbeitsschutzes*. September 2002

[Bun06] Bundesamt, Statistisches: *Auszug aus Wirtschaft und Statistik 6/2005*. 6 2006

[Bun07] Bundesministerium: *Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz - BStatG)*. September 2007

[Car34] Carnap, Rudolf: *Logische Syntax der Sprache*. Wien, 1934

[DB07] Drewes, Jörn ; Becker, Uwe: Accident Based Requirements Analysis for Advanced Driver Assistance Systems. In: *IFAC Symposium Analysis, Design and Evaluation of Human-Machine Systems* (2007)

[Deu87] Deutsches Institut für Normung: *DIN 1463, Teil 1: Erstellung und Weiterentwicklung von Thesauri - Einsprachige Thesauri*. Berlin, November 1987

[Deu92] Deutsches Institut für Normung: *DIN 2342, Teil 1: Begriffe der Terminologielehre - Grundbegriffe*. Berlin, Oktober 1992

[Deu93] Deutsches Institut für Normung: *DIN 2330: Begriffe und Benennungen - Allgemeine Grundsätze*. Berlin, Dezember 1993

[Deu00] Deutsches Institut für Normung: *DIN EN 50126: Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)*. Berlin, März 2000

[Deu01] Deutsches Institut für Normung: *DIN EN 50128: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenübertragungssysteme, Software für Eisenbahnsteuerungs- und Überwachungssysteme.* Berlin, November 2001

[Deu02] Deutsches Insitut für Normung: *DIN EN IEC61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.* Berlin, November 2002

[Deu03a] Deutsches Institut für Normung: *DIN EN 45545-4 Bahnanwendungen - Brandschutz in Schienenfahrzeugen - Teil 4: Brandschutzanforderungen an die konstruktive Gestaltung von Schienenfahrzeugen.* 2003

[Deu03b] Deutsches Institut für Normung: *DIN EN 50129: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik.* Berlin, Dezember 2003

[Deu04] Deutsches Institut für Normung: *DIN 2342:2004-09 (Entwurf): Begriffe der Terminologielehre.* Berlin, September 2004

[Eri05] Ericson, Clifton A.: *Hazard Analysis Techniques for System safety.* Wiley Verlag, Fredericksburg, Virginia, USA, 2005

[Eur06] European Parliament and the Council of the European Union: *Directive 2006/42/EG (Maschinenrichtlinie).* Juni 2006

[Eva04] Evans, Leonard: *Traffic Safety.* Science Serving Society, 2004

[Fay99] Fay, Alexander: *Wissensbasierte Entscheidungsunterstützung für die Disposition im Schienenverkehr.* Braunschweig, TU Braunschweig, Dissertation, November 1999

[FNT03] Fenner, W. ; Naumann, P. ; Trinckauf, J.: *Bahnsicherungstechnik.* Publicis Corporate Publishing, 2003

[For03] Forschungsgesellschaft für Strassen-und Verkehrswesen: *Empfehlungen für die Sicherheitsanalyse von Straßennetzen (ESN).* 2003

[Fre02] Frege, Gottlob: *Funktion - Begriff - Bedeutung.* Vandenhoeck & Ruprecht, Göttingen, 2002

[Gan04] Ganzelmeier, Lothar: *Nichtlineare H-unendlich-Regelung der Fahrzeuglängsdynamik.* Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, Dissertation, 2004

[Hei02] Heilmann, Klaus: *Das Risiko der Sicherheit.* Hirzel Verlag, 2002

[Hel03] Helbig, Jörg: *Robuste Regelungsstrategien am Beispiel der PKW-Spurführung*. Braunschweig, Technische Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, Dissertation, 2003

[Her03] Herczeg, Michael: Sicherheitskritische Mensch-Maschine-Systeme: Rahmenbedingungen für sicherheitsgerichtetes Handeln. In: *Berichtsheft der Jahrestagung Kerntechnik*, 2003, S. 97–111

[Hir99] Hirschberg, Hans G.: *Handbuch Verfahrenstechnik und Anlagenbau. Chemie, Technik, Wirtschaftlichkeit*. Springer, 1999

[Hän08] Hänsel, Frank: *Zur Formalisierung technischer Normen*, Technische Universität Braunschweig, Insitut für Verkehrssicherheit und Automatisierungstechnik, Diss., 2008

[Hor05] Horstmann, Marc: *Verflechtung von Test und Entwurf für eine verlässliche Entwicklung eingebetteter Systeme im Automobilbereich*. Braunschweig, Intitut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, Dissertation, 2005. `http://www.digibib.tu-bs.de/?docid=00000006`

[HS95] Hilse, Hans-Günter ; Schneider, Walter: *Verkehrssicherheit. Handbuch zur Entwicklung von Konzepten*. Boorberg, 1995

[Inf03] Infas/DIW: *Mobilität in Deutschland 2002, Kontinuierliche Erhebung zum Verkehrsverhalten, Projektnummer 70.0681/2001*. 2003

[Int01] International Electrotechnical Commission: *IEC 61882: Hazard and Operability Studies*. Genf, May 2001

[Int07] International Organisation for Standardisation: *ISO 14121-1:2007 - Sicherheit von Maschinen - Risikobeurteilung - Teil 1: Leitsätze*. 2007

[ISO99] ISO/IEC: *Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen*. 1999

[Jan97] Janhsen, Axel: *Anthropozentrische Modellierung und Spezifikation komplexer Systeme am Beispiel von Eisenbahnleitsystemen*. Braunschweig, Intitut für Regelungs- und Automatisierungstechnik, Technische Universität Braunschweig, Dissertation, 1997

[JT08] Jürgensohn, Thomas ; Timpe, Klaus-Peter: *Kraftfahrzeugführung*. Springer Verlag, 2008

[Kön05] König, Stefan: *Middleware für evolutionäre Architekturen und Anwendungen für ein kooperatives Produktionskonzept im Schienengüterverkehr*. Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, Dissertation, 2005

[Kra06] Kramer, Florian: *Passive Sicherheit von Kraftfahrzeugen*. Vieweg Verlag, Wiesbaden, 2006

[Kuh81] Kuhlmann, Albert: *Einführung in die Sicherheitswissenschaft*. TÜV Rheinland Verlag, 1981

[Lar68] In: Larson, James L.: *The Species Concept of Linnaeus*. 1968, S. 291–299

[Mül98] Müller, Kai: *Verkehr in systemtechnischer Darstellung und ihre Anwendung auf ein multimodales Güterverkehrskonzept*, Technische Universität Braunschweig, Insitut für Verkehrssicherheit und Automatisierungstechnik, Diss., 1998

[MP02] Meyna, Arno ; Pauli, Bernhard: *Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik: Quantitative Bewertungsverfahren*. Hanser Fachbuch, 2002

[Nöt99] Nöth, Winfried: *Handbuch der Semiotik*. Metzler Verlag, 1999

[OEC01] OECD: OECD Health Data 2001: A Comparative Analysis of 30 Countries - data sources, definitions and methods. (2001)

[ON02] Otte, D. ; Nehmzow, J. ; Hannover), H. Tscherne (Medizinische H. (Hrsg.): *Codierungs-Katalog zur Dokumentation von Verkehrsunfällen*. Bundesanstalt für Straßenwesen, Bergisch-Gladbach, 2002

[OR74] Odgen, Charles K. ; Richards, Ivor A.: *Die Bedeutung der Bedeutung*. Suhrkamp Verlag KG, 1974

[PBB+08] Poliak, Jan ; Beisel, Daniel ; Becker, Uwe ; Hänsel, Frank ; May, Jörg ; Schnieder, Eckehard: Vehicle Localisation on Secondary Railway Lines Utilising Satellite Based Technologies. In: *Company PSKD - Operation and Structures of Rail Transport*, 2008

[Poh08] Pohl, Klaus: *Requirements Engineering: Grundlagen, Prinzipien,Techniken*. dpunkt.Verlag GmbH, 2008

[Rac02] Rackwitz, Rüdiger: Optimization and risk acceptability based on the Life Quality Index. In: *Structural Safety* 24 (2002), Nr. 2-4, S. 297–331

[Rak02] Rakowsky, Uwe K.: *System-Zuverlässigkeit : Terminologie, Methoden, Konzepte*. LiLoLe-Verlag, Hagen-Westfalen, 2002

[Ras82] Rasmussen, Jens: Human errors: A taxonomy for describing human malfunction in industrial installations. In: *Journal of Occupational Accidents* Volume 4 (1982), S. 311,333

[Ras85] Rasmussen, Jens: *Human Error Data - Facts or Fiction, Report M-2499*. Riso National Laboratory, 1985

[Rat98] Rath, Ingo W.: *Aristoteles - Die Kategorien.* Reclams Universal Bibliothek, Stuttgart, 1998

[RS01] Robatsch, Klaus ; Schrammel, Erwin: *Grundlagen der Verkehrssicherheit.* Österreichischer Kunst- u. Kulturvlg, 2001

[SBDG04] Schnieder, E. ; Becker, U. ; Drewes, J. ; Ganzelmeier, L: Maße und Messbarkeit der Fahrzeug- und Verkehrssicherheit und ihre Bestimmung. In: *VDI/VW Gemeinschaftstagung: Integrierte Sicherheit und Fahrerassistenzsysteme* Nr. 21 (2004), S. 325–342

[Sch99] Schnieder, Eckehard: *Methoden der Automatisierung.* Braunschweig, Wiesbaden : Vieweg & Sohn Verlagsgesellschaft, 1999. – ISBN 3–528–06566–4

[Sch02a] Schienmann, Bruno: *Kontimuierliches Anfoderungsmanagement - Prozesse - Techniken - Werkzeuge.* Addison-Wesley Verlag, 2002

[Sch02b] Schrick, Dirk van: *Entepetives Management - Konstrukt, Konstruktion, Konzeption.* Aachen, Universität Wuppertal, Habilitation, 2002

[Sch03] Schnieder, Eckehard: Control for Traffic Safety - Safety of Traffic Control. In: *CTS 2003 - Preprints*, 2003, S. 1–13

[Sch05] Schnieder, Eckehard: Ist Verkehrssicherheit berechenbar? In: *Jahrbuch 2004 der Braunschweigischen Wissenschaftlichen Gesellschaft* (2005), S. 155–178

[Sch07] Schnieder, Eckehard: *Verkehrsleittechnik - Automatisierung des Straßen- und Schienenverkehrs.* Springer-Verlag, 2007

[SD08] Schnieder, Eckehard ; Drewes, Jörn: Bemessung und Kenngrößen der Verkehrssicherheit. In: *Zeitschrift für Verkehrssicherheit. 54(3)* 3 (2008), S. 117–123

[Sei92] Seiffert, Ulrich: *Fahrzeugsicherheit.* VDI Verlag, 1992

[Sei03] Seidewitz, Ed: What Models Mean. In: *IEEE Software* Bd. 20. Los Alamitos, CA, USA : IEEE Computer Society, 2003. – ISSN 0740–7459, S. 26–32

[Slo06] Slovak, Roman: *Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs.* Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, Dissertation, 2006

[SS00] Schubert, Werner ; Schmädicke, Jürgen: *Verkehrslogistik - Technik und Wirtschaft.* Vahlen, 2000

[SS04] Staab, Steffen ; Studer, Rudi: *Handbook on Ontologies.* Springer-Verlag, 2004 (International Handbooks on Information Systems). – ISBN 3–540–40834–7

[SS07] Schnieder, Lars ; Schnieder, Eckehard: Formalisierung von Begriffs- und Modellkonzepten zur Beschreibung der Funktionsimplementierung in Eisenbahnleit- und -sicherungssystemen. In: *Tagungsband der Verkehrswissenschaftlichen Tagung*, 2007

[SS08] Schnieder, Eckehard ; Schnieder, Lars: Axiomatik der Begriffe für die Automatisierungstechnik. In: *atp – Automatisierungstechnische Praxis* 10 (2008), S. 62 bis 73

[SSF+07] Schreiber, S. ; Schmidberger, T. ; Fay, A. ; Drewes, J. ; May, J. ; Schnieder, E.: UML-based safety analysis of distributed automation systems. In: *Proceedings of the EFTA 2007, Institute of Electrical and Electronics Engineering (IEEE)* (2007), S. n.n.

[Tsc05] Tschalabi, Iftikhar: Lebensdauerverteilung zur Beschreibung des Ausfallverhaltens von elektronischen Geräten und komplexem Bauteilen. In: *VDI Tagung Technische Zuverlässigkeit*, 2005, S. n.n.

[VBD06] Vollrath, Mark ; Briest, Susanne ; Drewes, Jörn ; Strassenwesen, Bundesanstalt für (Hrsg.): *Ableitung von Anforderungen an Fahrerassistenzsysteme aus der Sicht der Verkehrssicherheit*. Bd. Bandnummer F 60. Wirtschaftsverlag NW, 2006

[VDI05] VDI/VDE 3681: *Einordnung und Bewertung von Beschreibungsmitteln aus der Automatisierungstechnik*. Oktober 2005

[VDI07a] VDI ; VDI (Hrsg.): *Qualitaetsmerkmal - Technische Sicherheit*. Verein Deutscher Ingenieure, 2007

[VDI07b] VDI 4003: *Zuverlässigkeitsmanagement*. März 2007

[Ver07] Verkehr, Bau und S. f.: *Europäisches Übereinkommen über die internationale Beförderung gefährlicher Güter auf der Straße (ADR)*. August 2007

[Voi65] Voigt, Fritz: *Verkehr - Die Entwicklung des Verkehrssystems*. Duncker & Humblot, 1965

[Wei06] Weisse, Bernd: Fahrerinformation und Fahrerassistenz in der zukünftigen Theoretischen Fahrerlaubnisprüfung. In: *2. Sachverständigentag 2006*, 2006

[Wer85] Wersig, Gernot: *Thesaurus Leitfaden - Eine Einführung in das Thesaurus Prinzip in Theorie und Praxis*. DGD-Schriftenreihe, Frankfurt am Main, 1985

[Wil01] Willke, Helmut: *Systemisches Wissensmanagement*. Lucius & Lucius Verlagsgesellschaft, Stuttgart, 2001

[WK06] Wratil, Peter ; Kieviet, Michael: *Sicherheitstechnik für Komponenten und Systeme: Sichere Automatisierung für Maschinen und Anlagen*. Hüthig, 2006

[WS02] Weller, Gert ; Schlag, Bernhard: Kriterien zur Beurteilung von Fahrerassistenzsystemen. In: *Tagungsband: BDP-Kongress für Verkehrspsychologie*, 2002

[Wun85] Wunsch, Gerhard: *Geschichte der Systemtheorie - Dynamische Systeme und Prozesse*. Akademie Verlag, Berlin, 1985