Rafał Dorociak

Systematik zur frühzeitigen Absicherung der Sicherheit und Zuverlässigkeit fortschrittlicher mechatronischer Systeme

A systematics for the early assurance of reliability and safety of advanced mechatronic systems

Geleitwort

Ein Schwerpunkt unserer Arbeiten ist das Systems Engineering für mechatronische Systeme. Der stark gestiegene Anteil an Informations- und Kommunikationstechnik in diesen Systemen und deren zunehmende Vernetzung führt zu einer Steigerung der Komplexität dieser Systeme sowie deren Entwicklungsprozesse. Dies gilt in besonderem Maße für das Erreichen der Sicherheit und Zuverlässigkeit. Die zahlreichen Rückrufaktionen der letzten Jahre unterstreichen den in diesem Zusammenhang bestehenden Handlungsbedarf. Ziel ist es, diese Komplexität durch eine möglichst frühzeitige Absicherung der Sicherheit und Zuverlässigkeit in der Konzipierung zu beherrschen. Wesentlich sind hierbei der Aufbau eines ganzheitlichen Systemverständnisses für die an der Entwicklung beteiligten Fachdisziplinen, der frühzeitige Einsatz von Methoden der Sicherheits- und Zuverlässigkeitstechnik sowie deren effiziente Auswahl und Kombination.

Vor diesem Hintergrund hat Herr Dorociak eine Systematik zur frühzeitigen Absicherung der Sicherheit und Zuverlässigkeit fortschrittlicher mechatronischer Systeme entwickelt. Das Thema ist hochaktuell und vielerorts Gegenstand der Forschung. Die Systematik kommt in der frühen Produktentstehungsphase Konzipierung zum Einsatz. Sie ermöglicht erste grundlegende Aussagen zur Sicherheit und Zuverlässigkeit des Produkts. Kern der Systematik bilden ein Vorgehensmodell, eine Methodik zur Auswahl und Planung von Methoden, eine Sprache zur Spezifikation der Produktkonzeption unter besonderer Berücksichtigung von Sicherheits- und Zuverlässigkeitsinformationen sowie Methoden zur Analyse und Verbesserung der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit.

Mit seiner Arbeit leistet Herr Dorociak einen wertvollen Beitrag zum modellbasierten Systems Engineering unter besonderer Berücksichtigung von Sicherheit und Zuverlässigkeit.

Paderborn, im Dezember 2014 *Prof. Dr.-Ing. J. Gausemeier*

Systematik zur frühzeitigen Absicherung der Sicherheit und Zuverlässigkeit fortschrittlicher mechatronischer Systeme

zur Erlangung des akademischen Grades eines
DOKTORS DER INGENIEURWISSENSCHAFTEN (Dr.-Ing.)
der Fakultät Maschinenbau
der Universität Paderborn

genehmigte
DISSERTATION

von
M. Sc. Rafał Krzysztof Dorociak
aus *Ozorków, Polen*

Tag des Kolloquiums: 18. Dezember 2014
Referent: Prof. Dr.-Ing. Jürgen Gausemeier
Korreferent: Prof. Dr.-Ing. habil. Walter Sextro

Vorwort

Die vorliegende Dissertation entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Produktentstehung am Heinz Nixdorf Institut der Universität Paderborn. Sie ist das Ergebnis meiner wissenschaftlichen Arbeit im Rahmen von Forschungs- und Industrieprojekten, insbesondere im Sonderforschungsbereich 614 „Selbstoptimierende Systeme des Maschinenbaus“ (SFB 614).

Mein herzlicher Dank gilt Herrn Prof. Dr.-Ing. Jürgen Gausemeier, der mich stets forderte und förderte. Die vielen fachlichen Diskussionen, Anregungen und die stets konstruktive Kritik haben wesentlich zu meiner fachlichen und persönlichen Entwicklung beigetragen.

Herrn Prof. Dr.-Ing. habil. Walter Sextro vom Lehrstuhl Mechatronik und Dynamik der Universität Paderborn danke ich für die Übernahme des Korreferates.

Allen Kolleginnen und Kollegen des Lehrstuhls danke ich für die sehr gute Zusammenarbeit. Hervorheben möchte ich Dr.-Ing. Sascha Kahl, Dr.-Ing. Roman Dumitrescu, Peter Iwanek, Dr.-Ing. Lydia Kaiser und Anja Czaja. Ebenfalls danke ich Oleg Lurye, Jörg Hermes und Dr. Michael Brasse für die vielen fachlichen Diskussionen. Darüber hinaus gilt mein Dank Thorsten Koch, Benjamin Koch, Tobias Schulte, Daniela Stücker und Andreas Simon sowie allen weiteren Studierenden, die mich bei meiner Arbeit durch ihre Bachelor- und Masterarbeiten sowie ihre Tätigkeit als studentische Hilfskräfte unterstützt haben.

Mein größter Dank gilt meiner Familie. Meine Eltern haben mir meine Ausbildung ermöglicht und mich dabei jederzeit voll unterstützt. Meiner Frau Svitlana und meinem Sohn Viktor danke ich für das Verständnis, die zugehörige Geduld sowie die Kraft und Liebe, die sie mir jeden Tag schenken. Diese Arbeit ist Euch beiden gewidmet.

Paderborn, im Dezember 2014 *Rafał Dorociak*

Liste der veröffentlichten Teilergebnisse

[DDG+14] DOROCIAK, R.; DUMITRESCU, R.; GAUSEMEIER, J.; IWANEK, P.: Specification Technique CONSENS for the Description of Self-Optimizing Systems. In: GAUSEMEIER, J.; RAMMIG, F.-J.; SCHÄFER, W. (Hrsg.): Design Methodology for Intelligent Technical Systems Systems – Develop Intelligent Technical Systems of the Future. Springer-Verlag, Berlin, 2014

[DG14] DOROCIAK, R.; GAUSEMEIER, J.: Early Probabilistic Reliability Analysis of an Advanced Mechatronic System based on its Principle Solution. In: GAUSEMEIER, J.; RAMMIG, F.-J.; SCHÄFER, W.; SEXTRO, W. (Hrsg.): Dependability of Self-optimizing Mechatronic Systems. Springer-Verlag, Berlin, 2014

[DGG+13] DOROCIAK, R.; GAUKSTERN, T.; GAUSEMEIER, J.; IWANEK, P.; VAßHOLZ, M.: A Methodology for the Improvement of Dependability of Self-Optimizing Systems. In: Journal of Production Engineering – Research and Development, Vol. 7, Iss. 1, Springer-Verlag, Berlin, 2013

[DGG+12] DOROCIAK, R.; GAUKSTERN, T.; GAUSEMEIER, J.; IWANEK, P.: A Framework for the Improvement of Dependability of Self-Optimizing Systems. In: International Symposium on Systems-Integrated Intelligence – SysInt, 27.-29. Juni, Hannover, 2012

[SMD+12] SONDERMANN-WÖLKE, C.; MEYER, T.; DOROCIAK, R.; GAUSEMEIER, J.; SEXTRO, W.: Early Development of Advanced Condition Monitoring for the Self-Optimizing Guidance Module of a Railway Vehicle based on its Principle Solution. In: 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference – PSAM & ESREL, June 25-29, Helsinki, Finland, 2012

[DG12] DOROCIAK, R.; GAUSEMEIER, J.: Modeling of the Failure Propagation of an Advanced Mechatronic System within the Specification of its Principle Solution. In: Proceedings of the International Design Conference – DESIGN, May 21-24, Dubrovnik, Croatia, 2012

[PGD12] POOK, S.; GAUSEMEIER, J.; DOROCIAK, R.: Securing the reliability of tomorrow's systems with Self-Optimization. In: The Annual Reliability and Maintainability Symposium – RAMS, Jan. 23-26, Reno, Nevada, USA, 2012

[Dor12] DOROCIAK, R.: Early Probabilistic Reliability Analysis of Mechatronic Systems. In: The Annual Reliability and Maintainability Symposium – RAMS, Jan 23-26, Reno, Nevada, USA, 2012

[DG11] DOROCIAK, R.; GAUSEMEIER, J.: Absicherung der Zuverlässigkeit komplexer mechatronischer Systeme auf Basis der domänenübergreifenden Prinziplösung. In: 25. VDI-Fachtagung: Technische Zuverlässigkeit – TTZ, 11.-12. Mai, Leonberg bei Stuttgart, 2011

[GGD11] GAUSEMEIER, J.; GAUKSTERN, T.; DOROCIAK, R.: Integrierte Entwicklungsumgebung für die Konzipierung mechatronischer Systeme. In: VDI-Mechatroniktagung 2011, 31. März – 1. April, Dresden, 2011

[GDN10] GAUSEMEIER, J.; DOROCIAK, R.; NYßEN, A.: The Mechatronic Modeller: A Software Tool for Computer-Aided Modeling of the Principle Solution of an Advanced Mechatronic System. In: 11th International Workshop on Research and Education in Mechatronics – REM, Sep 9-10, Ostrava, Czech Republic, 2010

[GDK10] GAUSEMEIER, J.; DOROCIAK, R.; KAISER, L.: Computer-Aided Modeling of the Principle Solution of Mechatronic Systems: A Domain-Spanning Methodology for the Conceptual Design of Mechatronic Systems. In: Proceedings of IDETC/CIE 2010 ASME 2010 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference, Aug 15-18, Montreal, Quebec, Canada, 2010

[GDP+10] GAUSEMEIER, J.; DOROCIAK, R.; POOK, S.; NYßEN, A.; TERFLOTH, A.: Computer-Aided Cross-Domain Modeling of Mechatronic Systems. In: Proceedings of the International Design Conference - DESIGN, May 17-20, Dubrovnik, Croatia, 2010

[BDT10] BRANDIS, R.; DOROCIAK, R.; TERFLOTH, A.: Softwareunterstützte Modellierung der Prinziplösung – Ein neuer Ansatz für eine integrative Produkt- und Produktionssystementwicklung. In: Produkt Daten Journal, Nr. 2/2010, Darmstadt, ProSTEP iViP e.V., 2010

Systematik zur frühzeitigen Absicherung der Sicherheit und Zuverlässigkeit fortschrittlicher mechatronischer Systeme

Die Absicherung der Zuverlässigkeit und Sicherheit mechatronischer Systeme ist heute ein noch unzureichend gelöstes Problem. Indikatoren hierfür sind die vielen Rückrufaktionen der letzten Jahre. Die meisten der Ausfälle lassen sich auf eine unzureichende Abstimmung der beteiligten Disziplinen zurückführen. Hinzu kommt, dass etablierte Absicherungsmethoden einen detaillierten Systementwurf voraussetzen und vergleichsweise spät zum Einsatz kommen. Des Weiteren führt die zunehmende Interdisziplinarität zu einer höheren Systemkomplexität, die es zu beherrschen gilt. Einen Lösungsansatz zur Überwindung der skizzierten Herausforderungen stellt die frühzeitige Absicherung der Zuverlässigkeit und Sicherheit auf Basis der fachgebietsübergreifenden Spezifikation der Produktkonzeption dar.

Im Rahmen der vorliegenden Arbeit wird eine Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme erarbeitet. Sie umfasst fünf wesentliche Bestandteile: ein strukturiertes Vorgehensmodell, eine Methode zur Auswahl und Planung von Absicherungsmethoden, eine Spezifikationssprache zur Beschreibung der Produktkonzeption unter Berücksichtigung von Zuverlässigkeits- und Sicherheitsinformationen, Methoden zur Analyse und Verbesserung sowie ein Konzept für eine Werkzeugunterstützung.

Die Validierung der Systematik erfolgt anhand des am Lehrstuhl für Regelungstechnik und Mechatronik des Heinz Nixdorf Instituts entwickelten X-by-Wire-Versuchsfahrzeugs Chamäleon. Es wird gezeigt, dass mit Hilfe der Systematik Schwachstellen der Produktkonzeption hinsichtlich Sicherheit und Zuverlässigkeit bereits in der frühen Produktentstehungsphase Konzipierung identifiziert und behoben werden können.

A systematics for the early assurance of reliability and safety of advanced mechatronic systems

As for today, the assurance of the reliability and safety of mechatronic systems is still a problem not solved sufficiently. Indicators for this are the product recalls of the last years. The most of the failures result from insufficient communication and cooperation of the involved disciplines. In addition, the established assurance methods of today typically require a detailed system design as their input and are therefore applied at a comparatively late stage. Furthermore, the increasing interdisciplinarity leads to a higher system complexity that needs to be dealt with. A solution approach for overcoming the outlined challenges is the early assurance of reliability and safety based on the discipline-spanning specification of the product conception.

In this thesis, a *systematics for the early assurance of reliability and safety of advanced mechatronic systems* has been developed. It contains five main constituent parts: a structured procedure model, a method for the selection and planning of the assurance methods, a specification language for the description of the product conception with the consideration of reliability and safety related information, methods for analysis and improvement of the product conception as well as a concept for a software tool support.

The validation of the systematics takes place based on the X-by-Wire experimental vehicle Chamaeleon that has been developed on the Chair for Control Engineering and Mechatronics of the Heinz Nixdorf Institute. It is shown that the systematics supports the identification and removal of the weak points of the product conception with regards to safety and reliability.

Systematik zur frühzeitigen Absicherung der Sicherheit und Zuverlässigkeit fortschrittlicher mechatronischer Systeme

Inhaltsverzeichnis

Seite

Anhang

1 Einleitung

Die vorliegende Arbeit entstand im Rahmen des Sonderforschungsbereichs 614 „Selbstoptimierende Systeme des Maschinenbaus“ (SFB 614) der Universität Paderborn. Das Ziel des SFB 614 ist eine neue Schule des Entwurfs fortschrittlicher mechatronischer Systeme. Die vorliegende Arbeit ordnet sich in den Projektbereich „Entwurfsmethoden und -werkzeuge“ des SFB 614 ein und adressiert das Themenkomplex „Entwurf verlässlicher selbstoptimierender Systeme“ [SFB08, S. 468]. Sie beschreibt eine *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme*.

1.1 Problematik

Die technischen Erzeugnisse von heute sind zunehmend durch das symbiotische Zusammenwirken der Fachdisziplinen Mechanik, Elektrik/Elektronik, Regelungstechnik und Softwaretechnik geprägt, was durch den Begriff Mechatronik zum Ausdruck kommt. Mechatronische Systeme durchdringen den modernen Maschinenbau und verwandte Branchen wie die Automobiltechnik, die Bahntechnik und die Medizintechnik. Aufgrund der Beteiligung mehrerer Fachdisziplinen sind sie durch eine hohe Komplexität geprägt [VDI2206].

Der Entwurf derartiger Systeme ist herausfordernd. Dies gilt insbesondere für das Erreichen der Zuverlässigkeit und Sicherheit [BGJ+09]. Indikatoren hierfür sind die vielen Rückrufaktionen der letzten Jahre (z.B. Gaspedal-Rückrufaktion von Toyota im Jahre 2010 [Toy10-ol], Nissan-Massenrückruf vom Mai 2013, Massenrückrufe von General Motors Anfang 2014 etc.)[1]. Bild 1-1 zeigt die Anzahl der durch das Kraftfahrt-Bundesamt alleine in der Bundesrepublik Deutschland eingeleiteten Rückrufaktionen im zeitlichen Verlauf. Im Vergleich zum Jahre 1998 hat sich die Anzahl der Rückrufaktionen verdreifacht und verblieb in den letzten Jahren auf einem vergleichsweise gleichen, hohen Niveau. Für die Hersteller sind die Rückrufaktionen meist mit sehr hohen Kosten sowie Imageschäden verbunden [Spi12b-ol]. Die Folgen unzureichender Absicherung der Zuverlässigkeit und Sicherheit können zudem erst spät im Produktlebenszyklus zum Vorschein kommen und katastrophale Folgen mit sich ziehen (z. B. die Bahnkatastrophe von Eschede aus dem Jahre 1998 [Spi10-ol]).

Eine große Anzahl der Ausfälle lässt sich auf eine unzureichende Abstimmung der beteiligten Disziplinen zurückführen. Insbesondere werden die disziplinübergreifenden Ausfallausbreitungspfade unzureichend bzw. nicht rechtzeitig ins Kalkül gezogen [STP+12].

---

[1] Eine detailliertere Darstellung der Rückrufe der letzten Jahre in der Automobilindustrie erfolgt in Abschnitt 2.3.1.

Hinzu kommt, dass etablierte Methoden zur Absicherung der Zuverlässigkeit und Sicherheit einen detaillierten Systementwurf voraussetzen [BGJ+09]. Die aus der unzureichenden Abstimmung der involvierten Fachdisziplinen resultierenden Zuverlässigkeits- und Sicherheitsprobleme werden dann erst spät im Entwurf und Ausarbeitung bzw. bei der Integration der Beiträge der involvierten Disziplinen erkannt. Jedoch: Je später Fehler entdeckt werden, desto mehr kostet es, diese zu beheben, was Bild 1-2 eindrucksvoll zeigt. Der darin abgebildete Anstieg von Fehlerkosten aufgrund später, nachträglicher Änderungen vermittelt die sogenannte „Rule of ten“ [BL04, S. 4], [EKL07, S. 12]: Eine Änderung im Rahmen der frühen Konzipierungsphasen kostet z.B. 1 €, während der Entwicklung 10 €, während der Fertigungsvorbereitung 100 €, während der Fertigung 1 000 € und nach der Auslieferung 10 000 € [EKL07, S. 12].

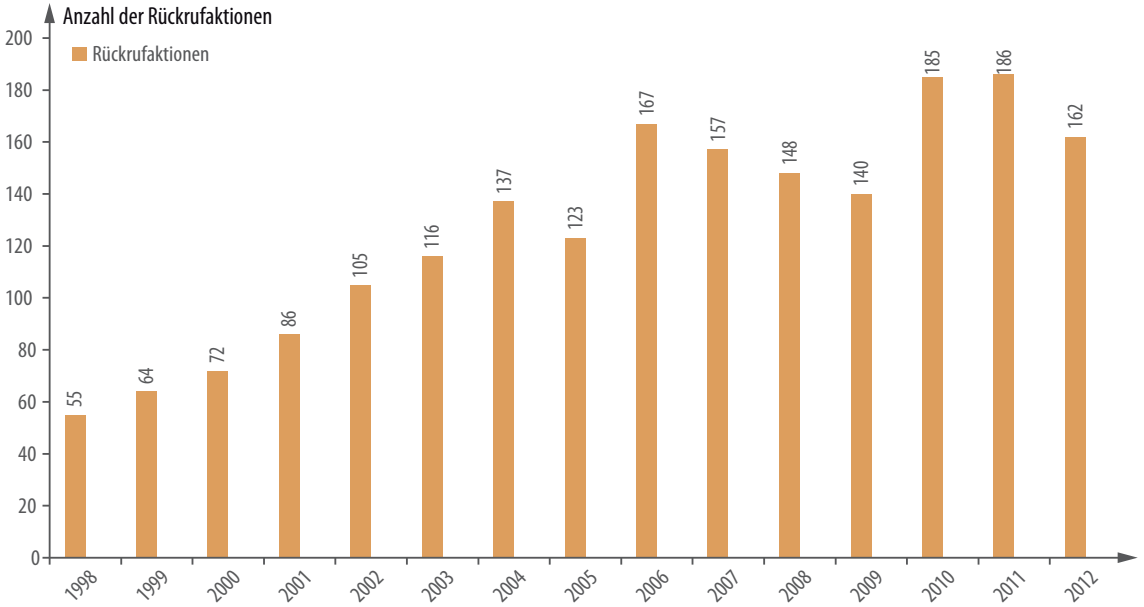


Bild 1-1: Anzahl der durch das Kraftfahrt-Bundesamt eingeleiteten Rückrufaktionen in den Jahren von 1998 bis 2012 (Quellen: Kraftfahrt-Bundesamt [KBA13-ol], Statista GmbH [Sta13-ol])

Aus der skizzierten Problemlage resultiert ein erheblicher Handlungsbedarf für eine Systematik, welche Methoden, Werkzeuge und ein Vorgehensmodell zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit[2] eines Produkts auf Basis der Produktkonzep-

[2] Verwendet wird in dieser Arbeit die Definition der Verlässlichkeit nach AVIZIENIS ET AL. [ALR+04]. Demnach ist Verlässlichkeit ein Oberbegriff für Zuverlässigkeit, Sicherheit, Verfügbarkeit, Instandhaltbarkeit, Vertraulichkeit und Integrität. Im Fokus der vorliegenden Arbeit stehen die Verlässlichkeitsaspekte Zuverlässigkeit und Sicherheit. Die englischen Begriffe „dependability“ und „reliability“ werden im deutschsprachigen Raum teilweise unterschiedlich übersetzt. In der einschlägigen Literatur werden diese als Verlässlichkeit und Zuverlässigkeit übersetzt (siehe z.B. [BL04, S. 20]). Die jüngsten Normen sehen eine Übersetzung als Zuverlässigkeit und Funktionsfähigkeit vor (siehe z.B. [VDI4001-2]). In diesem Beitrag wird die erstgenannte Nomenklatur verwendet. Eine detaillierte Vorstellung der wesentlichen Begriffsdefinitionen erfolgt in Abschnitt 2.1.

tion umfasst. Hierfür bedarf es einer modellbasierten Spezifikation der Produktkonzeption, welche den grundsätzlichen Aufbau, die Wirkungsweise und das gewünschte Verhalten des Produkts unter besonderer Berücksichtigung der Zuverlässigkeit und Sicherheit disziplinübergreifend beschreibt. Ebenso ist es notwendig, die etablierten Methoden der Zuverlässigkeits- und Sicherheitstechnik für die frühe Entwicklungsphase der Konzipierung verfügbar zu machen und in die Systematik zu integrieren. In diesem Zusammenhang sind Hilfsmittel von zentraler Bedeutung, die den Entwickler bei einer effektiven Auswahl und Planung der für seine Entwicklungsaufgabe adäquaten Methoden unterstützen.

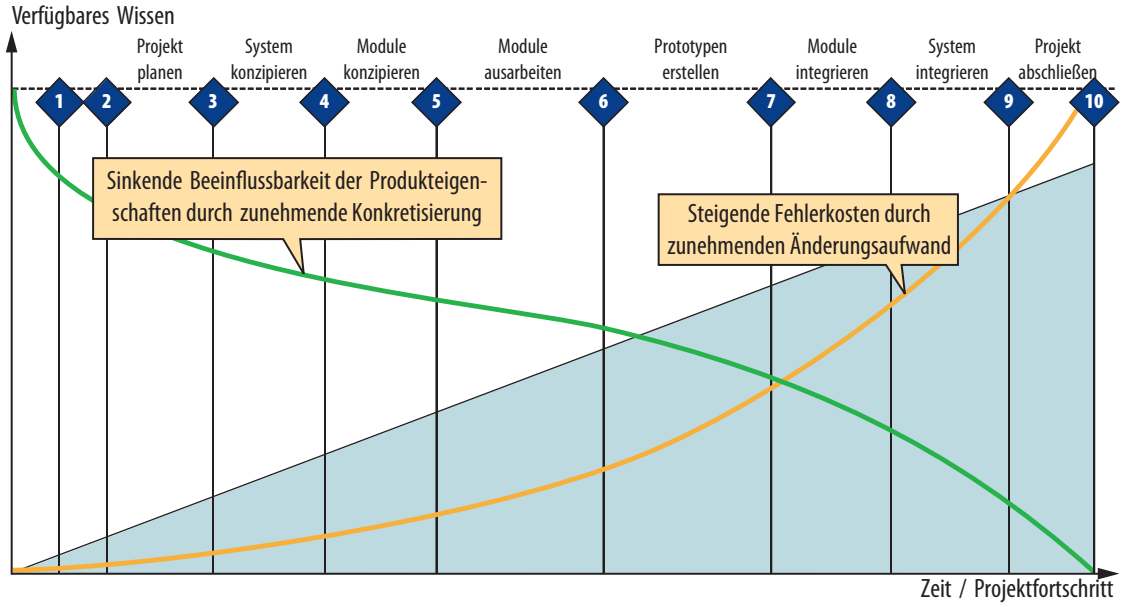


Bild 1-2: Entwicklung des Wissens und der Beeinflussbarkeit der Produkteigenschaften und der Fehlerkosten nach [BL04, S. 4], [EKL07, S. 12] (Graphische Darstellung in Anlehnung an [Gau10, S. 40])

1.2 Zielsetzung

Ziel der vorliegenden Arbeit ist eine *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme.* Sie ist so auszulegen, dass sie in der frühen Entwicklungsphase der Konzipierung angewendet werden kann. Die Systematik soll zum einen erste grundlegende Aussagen zur Zuverlässigkeit und Sicherheit des Produkts in der Konzipierung ermöglichen sowie die Identifikation von Schwachstellen unterstützen. Zum anderen ermöglicht die Systematik die Implementierung von Abstellmaßnahmen und damit einhergehend die Verbesserung der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit.

Die Anwendbarkeit der angestrebten Systematik ist anhand der Konzipierung eines Demonstrators des SFB 614 nachzuweisen. Für diesen Zweck wird das X-by-Wire-Versuchsfahrzeug Chamäleon herangezogen.

1.3 Vorgehensweise

Die Arbeit ist wie folgt strukturiert: die in Abschnitt 1.1 kurz skizzierte Problematik wird im Rahmen der Problemanalyse in **Kapitel 2** detaillierter erläutert. Ausgangspunkt ist die Darstellung der grundlegenden Begriffe und deren Zusammenhänge. Ferner werden die Eigenschaften fortschrittlicher mechatronischer Systeme und die damit verbundenen Herausforderungen im Hinblick auf die Absicherung ihrer Zuverlässigkeit und Sicherheit erläutert. Im Mittelpunkt steht dabei die frühe Entwicklungsphase der Konzipierung. Ebenso werden mögliche Negativfolgen für Unternehmen erklärt, die aus dem Nichterreichen der Zuverlässigkeits- und Sicherheitsziele resultieren können. Das Ergebnis der Problemanalyse sind Anforderungen an die angestrebte Systematik.

Eine detaillierte Analyse des Stands der Technik ist Gegenstand des **Kapitels 3**. Darin werden zunächst Vorgehensmodelle zur Entwicklung zuverlässiger und sicherer mechatronischer Systeme vorgestellt und beurteilt. Danach wird ein Überblick über ausgewählte Methoden der Zuverlässigkeits- und Sicherheitsanalyse gegeben. Darüber hinaus werden Hilfsmittel zur Unterstützung der Auswahl und Planung von Methoden sowie Modellierungssprachen zur Beschreibung der Produktkonzeption untersucht. Darauf aufbauend findet eine Analyse von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit auf Basis einer Beschreibung der Produktkonzeption statt. Außerdem erfolgt eine Untersuchung von verwandten Software-Werkzeugen. Abschließend wird der Stand der Technik auf die Erfüllung der in Kapitel 2 festgelegten Anforderungen hin beurteilt und der zugehörige Handlungsbedarf identifiziert.

Kapitel 4 beschreibt den Kern der vorliegenden Arbeit – die *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme*. Ausgangspunkt bildet ein Überblick über die Systematik, woraufhin die einzelnen Bestandteile der Systematik vorgestellt werden.

In **Kapitel 5** erfolgt die Validierung der Systematik. Diese geschieht anhand des X-by-Wire-Versuchsfahrzeugs Chamäleon, welches ein Demonstrator des SFB 614 ist. Dieses fortschrittliche mechatronische System weist eine hohe Sicherheitsrelevanz auf und ist zudem hochkomplex. Aufgrund dieser Eigenschaften eignet es sich sehr gut für den Nachweis des Nutzens der Systematik sowie der Erfüllung der aufgestellten Anforderungen.

Kapitel 6 gibt eine Zusammenfassung der vorliegenden Arbeit sowie einen Ausblick auf zukünftige Arbeiten. Im **Anhang** findet der Leser ergänzende Erläuterungen zur Problemanalyse, zum Stand der Technik, zu der Systematik sowie zum Anwendungsbeispiel Chamäleon.

2 Problemanalyse

Ziel der Problemanalyse sind Anforderungen an eine *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme*. Hierfür werden in Abschnitt 2.1 die grundlegenden Begriffe erklärt. Insbesondere werden die Begriffe Zuverlässigkeit und Sicherheit und deren Zusammenhang erläutert. Ebenso erfolgt ein kurzer Überblick über die wichtigsten Zuverlässigkeits- und Sicherheitskenngrößen sowie Ausfallratenmodelle. Danach wird in Abschnitt 2.2 der Aufbau und die Funktionsweise fortschrittlicher mechatronischer Systeme vorgestellt. Insbesondere wird auf klassische mechatronische Systeme, adaptive Systeme und selbstoptimierende Systeme eingegangen. Abschnitt 2.3 befasst sich mit den möglichen Negativfolgen für Unternehmen bei Nichterreichung von Zuverlässigkeits- und Sicherheitszielen. Anschließend wird in Abschnitt 2.4 die Problemabgrenzung für die vorliegende Arbeit vorgenommen. Die daraus resultierenden Anforderungen an die Systematik werden dann in Abschnitt 2.5 beschrieben.

2.1 Grundlegende Begriffe

Der Begriff einer Systematik leitet sich von dem Begriff der Konstruktionsmethodik[3] (engl. design methodology) ab:

> *„Unter Konstruktionsmethodik versteht man ein geplantes Vorgehen mit konkreten Handlungsanweisungen zum Entwickeln und Konstruieren technischer Systeme, die sich aus den Erkenntnissen der Konstruktionswissenschaft und der Denkpsychologie, aber auch aus den Erfahrungen in unterschiedlichen Anwendungen ergeben haben. Hierzu gehören Vorgehenspläne zur inhaltlichen und organisatorischen Verknüpfung von Arbeitsschritten und Konstruktionsphasen, die flexibel an die jeweilige Problemlage angepasst werden […]. Die Beachtung von generellen Zielsetzungen und die Verwirklichung von Regeln und Prinzipien […] insbesondere bei der Gestaltung […] sowie Methoden zur Lösung einzelner Konstruktionsprobleme oder -teilaufgaben […] sind notwendig“ [PBF+07, S. 10].*

Darauf aufbauend schlägt MÖHRINGER folgende Definition für den Begriff **Entwicklungsmethodik für mechatronische Systeme** vor:

> *„Instrumentarium zur Unterstützung des Produkterstellungsprozesses, das auf fünf wesentlichen Elementen besteht: 1) Vorgehensmodelle als*

[3] In der Literatur wird neben dem Begriff Konstruktionsmethodik oftmals der Begriff Entwicklungsmethodik verwendet. Beide Begriffe sind als synonym zu verstehen.

> *Planungs- und Problemlösungshilfe, 2) Methoden zur Lösung von Aufgaben in den einzelnen Entwicklungsschritten, 3) Spezifikationstechniken zur Beschreibung der Resultate, 4) Modellbildung und Werkzeuge zur Simulation der Systemeigenschaften und 5) Maßnahmen, die Einflüsse des Individuums, der Gruppe und der Organisation berücksichtigen (Mensch und Organisation). Das Instrumentarium ist auf die besonderen Anforderungen der Mechatronik ausgerichtet" [Möh04, S. 16].*

Aufbauend auf den zwei vorhergehenden Definitionen und in Anlehnung an DUMITRESCU wird unter einer (Entwicklungs-)**Systematik** im Kontext dieser Arbeit ein Instrumentarium verstanden, welches ein Vorgehensmodell sowie Methoden und Werkzeuge zur Erfüllung der angestrebten Entwicklungsaufgabe umfasst [Dum11, S. 6]. Dabei ermöglicht die Systematik „weder ein automatisiertes Entwickeln noch ist sie Ersatz für die kreative Lösung des Anwenders" [Dum11, S. 6]. Von dem Begriff Entwicklungsmethodik grenzt sich der Begriff der (Entwicklungs-)Systematik in folgenden zwei Punkten ab [Dum11, S. 6]: In eine Entwicklungsmethodik fließen zusätzlich denk- und arbeitspsychologische Untersuchungen ein. Ferner betrachtet die Entwicklungsmethodik zusätzlich organisatorische Aspekte [PBF+07, S. 10f.]. Eine (Entwicklungs-)Systematik adressiert die beiden Punkte nicht.

Demnach soll die angestrebte *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* Dritte in die Lage versetzen, fortschrittliche mechatronische Systeme zu entwickeln, die zuverlässig und sicher sind. Im Fokus soll dabei die frühe Entwicklungsphase der Konzipierung stehen. Bei der Erarbeitung der notwendigen Bestandteile der Systematik gilt es auf den etablierten Erkenntnissen, Methoden, Werkzeugen etc. aufzubauen bzw. diese neu zu entwickeln, falls keine geeigneten vorhanden sind.

Weitere relevante Begriffe sind die einer (Betrachtungs-)Einheit und eines Systems. Eine **(Betrachtungs-)Einheit** (engl. entity, item) ist definiert als ein „materieller oder immaterieller Gegenstand der Betrachtung" [DIN40041, S. 1]. Dabei wird zwischen nicht instandzusetzenden und instandzusetzenden Einheiten unterschieden. Eine **nicht instandzusetzende Einheit** ist eine Einheit, „die nach einem Ausfall nicht instandgesetzt wird" (z.B. eine Glühbirne) [IEV-191-01-03]. Eine **instandzusetzende Einheit** ist eine Einheit, die nach einem Ausfall instand zu setzen ist, wobei unter Instandsetzung eine Reparatur und kein vollständiges Ersetzen der Einheit gemeint ist [IEV-191-01-02], [Cas12].

Die Betrachtungseinheit ist Gegenstand der Zuverlässigkeits- bzw. Sicherheitsuntersuchungen. Dabei kann sie Teil eines Systems, das gesamte System bzw. ein Verbund von Systemen sein [VDI4003, S. 5]. Ein **System** (engl. system) ist „ein Satz von in Wechselbeziehung und Wechselwirkung stehenden Elementen" [DIN60812, S. 8], (nach [ISO9000, S. 20]). Es besitzt [DIN60812, S. 8]:

- einen vorgegebenen Zweck (definiert durch seine zu erfüllenden Funktionen),

- festgelegte Betriebs- und Einsatzbedingungen sowie
- eine definierte Begrenzung (Systemgrenze).

2.1.1 Verlässlichkeit als Oberbegriff für Sicherheit und Zuverlässigkeit

Die **Verlässlichkeit**[4] (engl. dependability) ist ein zusammenfassender Ausdruck zur Beschreibung von Zuverlässigkeit und Sicherheit sowie einiger weiterer Aspekte. In der vorliegenden Arbeit wird die Definition der Verlässlichkeit nach AVIZIENIS ET AL.[5] verwendet [ALR+04, S. 11]. Demnach umfasst Verlässlichkeit die Aspekte Sicherheit, Zuverlässigkeit, Verfügbarkeit, Vertraulichkeit, Integrität und Instandhaltbarkeit (Bild 2-1):

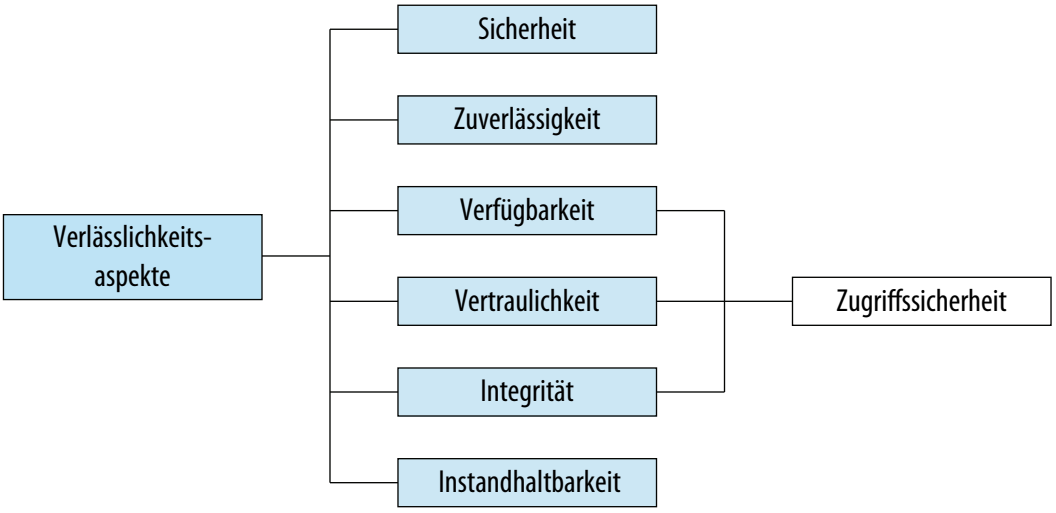


Bild 2-1: Verlässlichkeitsaspekte (in Anlehnung an AVIZIENIS ET AL.) [ALR+04, S. 14]

Sicherheit (engl. safety) bedeutet die Freiheit von unvertretbarem Risiko[6] in Bezug auf physische Verletzung oder Schädigung der Gesundheit von Menschen, Schädigung von

---

[4] Für die Übersetzung des englischen Begriffs „dependability" verwenden einige Autoren der einschlägigen Literatur den Begriff „Verlässlichkeit", als „Zuverlässigkeit" wird in diesem Fall der englische Begriff „reliability" übersetzt (siehe z.B. [BL04, S. 20], [Rei12, S. 253]). In den Normen DIN 40041 und IEV 191-02 sowie in weiteren darauf aufbauenden Normen wird „dependability" als Zuverlässigkeit und „reliability" als Funktionsfähigkeit übersetzt [DIN40041, S. 2f.], [IEV191-02-03], [IEV191-02-06].

[5] In der Norm IEV 191-02-03 wird die Verlässlichkeit als ein „zusammenfassender Ausdruck zur Beschreibung der Verfügbarkeit und ihrer Einflussfaktoren Funktionsfähigkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft" [IEV 191-02-03] definiert. Die Definition nach AVIZIENIS ET AL. geht über diese Definition hinaus [ALR+04, S. 11]. Denn die Begriffe Integrität und Vertraulichkeit werden ebenfalls betrachtet. Diese beiden Verlässlichkeitsaspekte gewinnen zunehmend an Bedeutung und müssen bei der Entwicklung zukünftiger hochvernetzter Systeme (Stichworte: Cyber-Physical Systems, Car-2-X-Communications, In-Vehicle-Services) mehr denn je zuvor berücksichtigt werden. Dies zeigt das jüngste Beispiel der Zerstörung von Irans Uranzentrifugen mit einem Cyber-Angriff (Stuxnet-Virus) [Spi13-ol] sowie die Tatsache, dass eine Neuauflage (Edition 2) der Sicherheitsnorm IEC 61508 sich dem Thema Zugriffssicherheit (engl. Security) zuwendet [IEC61508-1, 7.4.2.3, S. 27], [GB12, S.12]

[6] Im Bereich der Sicherheit wird Risiko als Produkt aus der Wahrscheinlichkeit des Eintretens eines zum Schaden führenden Ereignisses und dem beim Ereigniseintritt zu erwartenden Schadensausmaß definiert [ISO26262-1, S. 13], [SZ13, S. 96].

Gütern und Schädigung der Umwelt [DIN820-120, S. 11]. In diesem Zusammenhang wird eine potentielle Schadensquelle als eine **Gefahr** (engl. hazard) bezeichnet [DIN820-120, S. 11]. Beispiele: Gefahr durch elektrischen Schlag, Gefahr durch Stoß, Gefahr durch Feuer etc. Als **funktionale Sicherheit** (engl. functional safety) wird die Freiheit von unvertretbarem Risiko in Bezug auf Gefahren verstanden, die aus dem funktionalen Versagen eines Systems resultieren können (nach [ISO26262-1, S. 8]). Wenn im Rahmen dieser Arbeit von Sicherheit die Rede ist, ist stets die funktionale Sicherheit gemeint.

Der Begriff **Zuverlässigkeit** (engl. reliability) ist wie folgt definiert:

> *„Fähigkeit einer Einheit, eine geforderte Funktion unter gegebenen Bedingungen für ein gegebenes Zeitintervall zu erfüllen“* [7] *[VDI4001-2], [IEV-191-02-06], [BL04, S. 20].*

Auf die Ähnlichkeiten und Unterschiede zwischen Zuverlässigkeit und Sicherheit wird in Abschnitt 2.1.5 detailliert eingegangen.

Die **Verfügbarkeit** (engl. availability) ist definiert als:

> *„[die] Fähigkeit einer Einheit, zu einem gegebenen Zeitpunkt oder während eines gegebenen Zeitintervalls eine geforderte Funktion unter gegebenen Bedingungen erfüllen zu können, vorausgesetzt, dass die erforderlichen äußeren Hilfsmittel bereitgestellt sind“ [VDI4001-2], [IEV-191-02-05].*

Die Verfügbarkeit beschreibt also die Fähigkeit einer Einheit, die geforderte Funktion dann zu erfüllen, wenn dies erforderlich ist [BKL+06, S. 8]. Im Unterschied zur Zuverlässigkeit hängt die Verfügbarkeit stark von Instandhaltungsmaßnahmen ab [BKL+06, S. 8], [MP10, S. 50ff.], [BL04, S. 352ff.].

Die Teilaspekte Vertraulichkeit und Integrität ergeben zusammen mit dem Teilaspekt Verfügbarkeit nach AVIZIENIS ET AL die sogenannte **Zugriffssicherheit** (engl. Security) [ALR+04, S. 14]. (Informations-)**Vertraulichkeit** (engl. confidentiality) bedeutet das Verhindern einer unautorisierten Informationsgewinnung[8] [Eck08, S. 8]. (Daten-)**Integrität** (engl. integrity) bezieht sich auf das Verhindern einer unautorisierten Änderung

---

[7] Für nicht instandzusetzende Einheiten (z.B. eine Glühbirne) sind die Begriffe Verfügbarkeit und Zuverlässigkeit sowie die zugehörigen Kenngrößen äquivalent zueinander. Denn nicht instandzusetzende Einheiten sind so lange funktionsfähig bis sie nicht ausgefallen sind; nach einem Ausfall erfolgt keine Instandsetzung. Ein Unterschied zwischen den Begriffen der Verfügbarkeit und Zuverlässigkeit ergibt sich erst für instandzusetzende Einheiten, da diese nach einem Ausfall wieder instandgesetzt werden können.

[8] Nach NORTH sind Daten als Zeichen (Buchstaben, Ziffern, Sonderzeichen) in einer formalisierten und geordneten Form (Syntax) zu verstehen (z.B. die Zeichenkette „13°C“). Damit aus Daten Informationen werden, muss ein Bezug hergestellt werden (z.B. Außentemperatur 13°C). In diesem Zusammenhang ist Wissen der Prozess der zweckdienlichen Vernetzung von Informationen. Insgesamt ergibt sich die sogenannte Wissenstreppe [Nor11, S. 36]:

bzw. Entwendung von Daten [Eck08, S. 7]. Der Verlässlichkeitsaspekt der Verfügbarkeit spielt ebenfalls eine wichtige Rolle. In Bezug auf Zugriffssicherheit bedeutet Verfügbarkeit, dass autorisierte Benutzer in der Lage sind, das System zu verwenden [Eck08, S. 10]. ECKERT fügt den Teilaspekt Verbindlichkeit hinzu [Eck08, S. 11]: Verbindlichkeit (engl. non repudiation) bedeutet, dass die getätigten Aktionen im Nachhinein nachvollziehbar und beweisbar sind.

Schließlich ist die **Instandhaltbarkeit** (engl. maintainability) wie folgt definiert:

> *„Fähigkeit einer Einheit, unter gegebenen Anwendungsbedingungen in einem Zustand[9] erhalten bzw. in ihn zurückversetzt werden zu können, in dem sie eine geforderte Funktion erfüllen kann, wobei vorausgesetzt wird, dass die Instandhaltung unter den gegebenen Bedingungen mit den vorgeschriebenen Verfahren und Hilfsmitteln durchgeführt wird" [VDI4001-2], [IEV-191-02-07].*

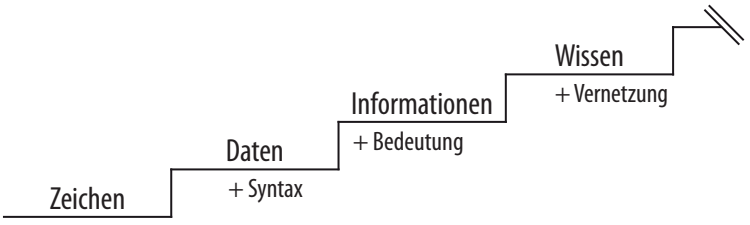
2.1.2 Beeinträchtigungen der Verlässlichkeit

Für die mit der Verlässlichkeit verbundenen **Beeinträchtigungen** (engl. threats) wird in dieser Arbeit die Unterscheidung in Fehlerursachen, Fehlzustände und Ausfälle nach AVIZIENIS ET AL. übernommen[10] [ALR+04] (Bild 2-2).

Eine **Fehlerursache** (engl. fault) ist ein Ereignis[11], welches das System in einen ungewünschten Zustand (Fehlzustand) versetzt. Hierbei kann es sich um einen internen Fehler oder um ein externes Ereignis handeln [ALR+04, S. 13].

Ein **Fehlzustand** (engl. error) ist wie folgt definiert:

> *„Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei durch Wartung oder andere geplante Handlungen*



Weitere Definitionen, Beispiele und Informationen hierzu findet der Leser in [Nor11, S. 35 ff.].

[9] Ein Zustand ist als die „Beschaffenheit einer Einheit zum Betrachtungszeitpunkt" definiert [DIN40041, S. 3]. Dabei ist die Beschaffenheit einer Einheit als Gesamtheit ihrer Merkmale und zugehöriger Merkmalswerte zu verstehen [DIN40041, S.2].

[10] Oft werden analog die Begriffe der Ausfallursache, Ausfallmöglichkeit und Ausfallauswirkung verwendet. Dies tritt insbesondere für die Methode FMEA zu (Fehlzustandsart- und auswirkungsanalyse; siehe Abschnitt 3.2.2.5).

[11] Ein Ereignis (engl. event) ist ein „Übergang von einem in einen anderen Zustand" [DIN40041, S. 3].

bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist“ [IEV191-05-01] [DIN60300-3-1] [DIN60812], [ALR+04, S. 13].

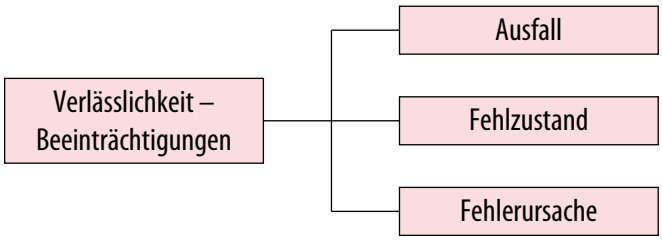


Bild 2-2: Beeinträchtigungen der Verlässlichkeit – die wichtigsten Begriffe (in Anlehnung an AVIZIENIS ET AL.) [ALR+04, S. 14]

Als **Fehlzustandsart** (engl. failure mode) wird „einer der möglichen Fehlzustände bezüglich der geforderten Funktion einer bestimmten Einheit“ bezeichnet [VDI4001-2, S. 18], [IEV 191-05-22]. Eine Einheit wird als **fehlerhaft** (engl. faulty) bezeichnet, wenn sie einen Fehlzustand aufweist [VDI4001-2, S. 16], [IEV191-05-23].

Ein **Ausfall** (engl. failure) ist:

„ein nach Beanspruchungsbeginn entstandenes Aussetzen der Ausführung einer Aufgabe einer Betrachtungseinheit aufgrund einer in ihr selbst liegenden Ursache und im Rahmen der zulässigen Beanspruchung“ [SZ13, S. 91].

Ein Ausfall bedeutet also die „Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen“ [IEV 191-04-01], [DIN60300-3-1]. Zu beachten ist, dass ein Fehlzustand ein Zustand des Systems beschreibt, während Fehlerursachen und Ausfälle Ereignisse sind. Bild 2-3 zeigt den Zusammenhang zwischen den Beeinträchtigungsbegriffen. Ein Fehlzustand eines Systemelements kann durch eine externe Fehlerursache (z.B. eine fehlerhafte Eingangsinformation) oder durch eine interne Fehlerursache verursacht werden. Eine interne Fehlerursache führt erst zu einem Fehlzustand, nachdem sie aktiviert wurde (z.B. durch den Beanspruchungsbeginn). Danach erfolgt die Fortpflanzung des Fehlzustands, die schließlich zu einem Ausfall des Systemelements führt. Dieser Ausfall kann sich weiter über die Verbindungen zu anderen Systemelementen fortpflanzen und einen Ausfall dieser verursachen. Der Ausfall eines Systemelements kann also in diesem Fall eine Fehlerursache für einen Ausfall eines anderen Systemelements darstellen. Eine derartige Fortpflanzung kann auch über Hierarchieebenen hinweg erfolgen. Zusammenfassend ergibt sich eine in Bild 2-3 dargestellte Ursache-Wirkungskette.

Dieser Zusammenhang wird an einem Beispiel aus der Automobiltechnik erklärt (Bild 2-4) [ISO26262-10, 4.3, S. 5]: Betrachtet wird das Gesamtsystem Fahrzeug, welches neben anderen Systemelementen das Subsystem Motor-Steuergerät umfasst. Die auf dem Mikrocontroller des Motor-Steuergeräts ausgeführte Software enthält einen systematischen Programmierfehler: Die Abbruchbedingung einer der Schleifen wurde fehlerhaft

programmiert (Fehlerursache). In gewissen Situationen kommt es nun zu einer Endlosschleife (Fehlzustand).

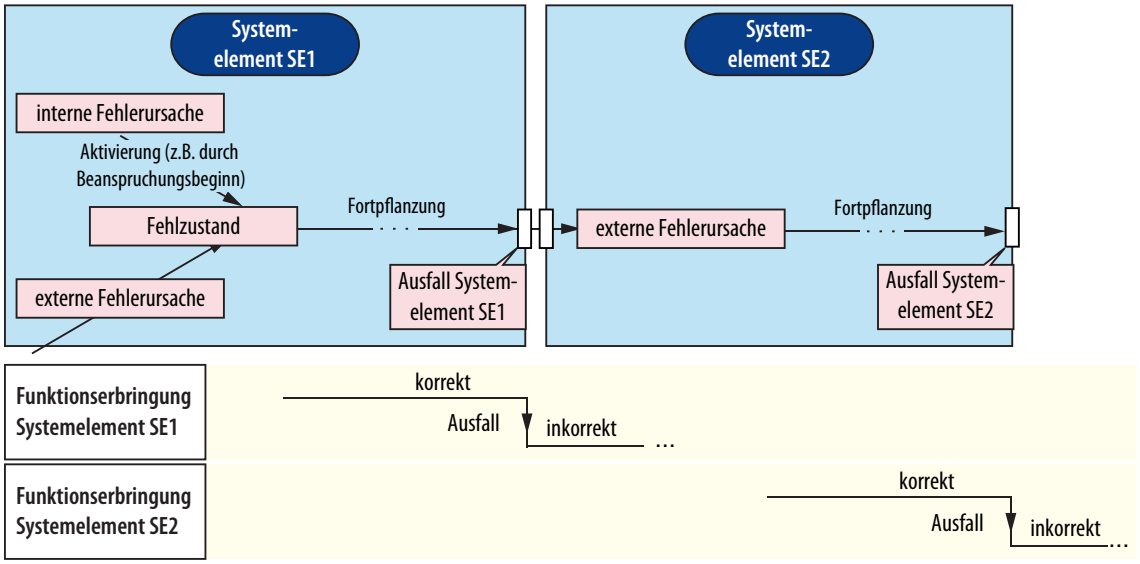


Bild 2-3: Beeinträchtigungskette (in Anlehnung an AVIZIENIS ET AL.) [ALR+04]

Die Eingrenzung und Behebung eines derartigen Fehlzustands ist oft mit hohem zeitlichem Aufwand verbunden. Denn die Situationen, in denen sich dieser äußert, typischerweise schwer zu reproduzieren sind. Es wird folglich durch den Watchdog[12] erkannt, dass sich der Mikrocontroller in einem Fehlzustand befindet. Als Konsequenz sendet der Watchdog ein Reset-Signal an den Mikrocontroller; der Mikrocontroller wird neu gestartet. Für die Zeit von der Reset-Anforderungen bis zum vollständigen Neustart wird der Normalbetrieb des Motor-Steuergeräts unterbrochen (Ausfall im Kontext des Motor-Steuergeräts). Konsequenz dieses Ausfalls des Motor-Steuergeräts ist eine Zündungsunterbrechung (Fehlzustand des Fahrzeugs) und das Ruckeln des Fahrzeugs (Ausfall auf Fahrzeugebene). Aus diesem Beispiel wird ersichtlich: was auf Ebene des Motor-Steuergeräts ein Ausfall war, ist auf der übergeordneten Ebene des Fahrzeugs eine Fehlerursache für einen anderen Ausfall. Abhängig vom jeweiligen Betrachtungskontext kann also ein Ereignis als eine Fehlerursache oder ein Ausfall angesehen werden.

Fehlerursachen bzw. Ausfälle unterscheiden sich u.a. durch ihre zeitliche Persistenz, ihre Ursache etc. [ALR+04, S. 15 ff.], [Rei12, S. 258] In Bezug auf die zeitliche Persistenz wird zwischen intermittierenden und andauernden Fehlerursachen bzw. Ausfällen unterschieden. **Andauernd** (engl. persistent, permanent) bedeutet, solange bestehend, „bis

[12] Die Watchdog-Funktion stellt einen speziellen Timer dar und dient zur Überwachung der korrekten Ausführung eines Software-Programms innerhalb eines Mikrocontrollers [Krü08, S. 196ff.]: Im Normalbetrieb wird der Watchdog in der Hauptschleife des Software-Programms regelmäßig zurückgesetzt. Findet dieses Zurücksetzen aufgrund eines Fehlers (z.B. einer Endlosschleife) nicht mehr statt, so läuft der Watchdog-Timer ab und löst einen RESET aus, um den Mikrocontroller und damit einhergehend das Software-Programm neu zu starten.

eine Instandsetzung ausgeführt ist“ [VDI4001-2, S. 17], [IEV191-05-16]. **Intermittierend** bzw. **transient** (engl. intermittent, volatile, transient) heißt „nicht zu jeder Zeit während der Prüfung reproduzierbar […] und [tritt] sporadisch [auf]“ [DIN61014, S. 13]. Der zugehörige Fehlzustand besteht für eine begrenzte Zeit. Von diesem Fehlzustand ausgehend „erlangt die Einheit [nach gewisser Zeit] ihre Funktionsfähigkeit wieder, ohne dass an ihr irgendeine Instandsetzungsmaßnahme vorgenommen wird“ [VDI4001-2, S. 17], [IEV191-05-17].

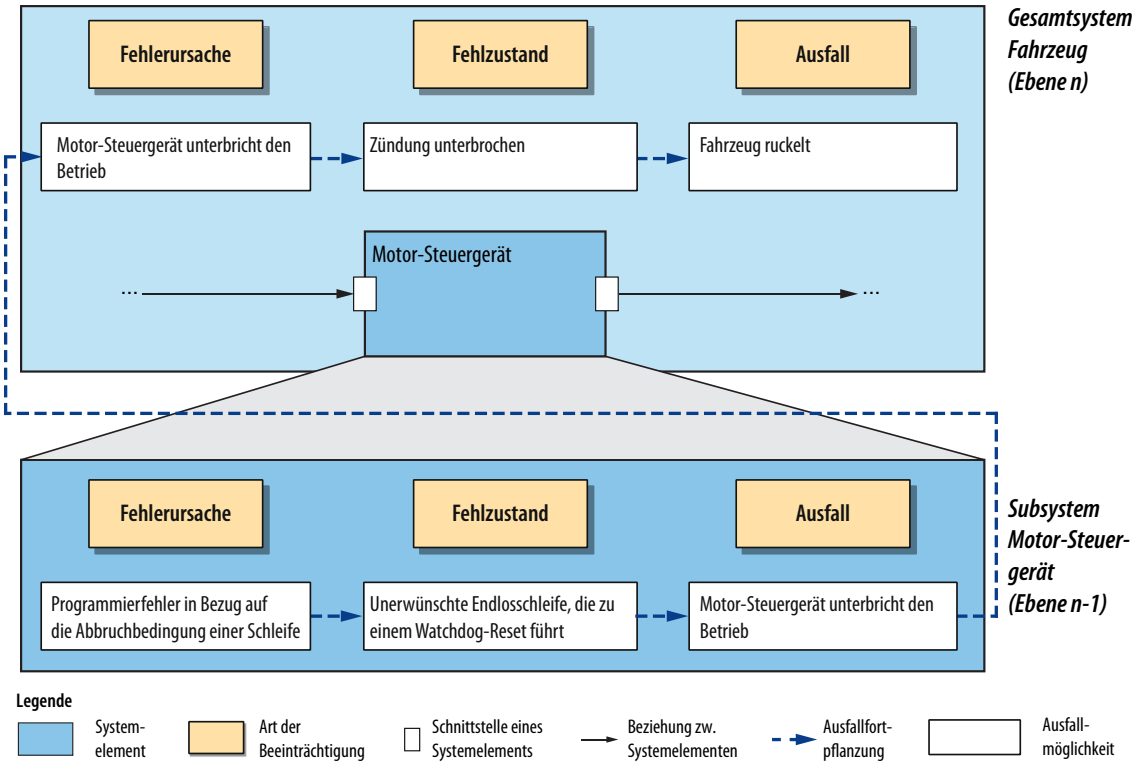


Bild 2-4: Ausfallfortpflanzung am Beispiel eines Fahrzeugs; eine Beeinträchtigung kann abhängig vom zugehörigen Kontext verschiedene Rollen (Fehlerursache, Ausfall) einnehmen [ISO26262-10, S. 6]

Die Ursache eines Ausfalls kann systematisch oder zufällig sein. Ein **systematischer Ausfall** (engl. systematic failure) ist jener, „bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Veränderung des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betreibens, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann.“ [VDI4001-2, S. 7], [IEV 191-04-19]. **Zufällige Ausfälle** (nicht systematische Ausfälle, engl. random failure) „sind jene, deren Ausfallmuster kein Wiederauftreten zeigt und dessen Ursachen nicht andeuten, dass ein Wiederauftreten wahrscheinlich ist“ [DIN61014, S. 32]. Softwarebedingte Ausfälle sind immer systematisch [DIN61014, S. 8].

Oft anzutreffen in der Literatur ist die Unterscheidung zwischen Einfach- und Mehrfachfehlerursachen. **Einfach-Fehlerursachen** (engl. single point faults) sind Fehlerursachen, die für sich alleine zur Verletzung eines Sicherheitsziels führen [ISO26262-1, S. 21].

Mehrfach-Fehlerursachen (engl. multiple point faults) sind Fehlerursachen, die zwar unabhängig voneinander sind, in Kombination mit anderen Fehlerursachen jedoch zu einem Ausfall führen [LPP10, S. 136]. Entsprechend gilt die Nomenklatur der Beeinträchtigungskette. Zum Beispiel wird ein Ausfall, der auf eine Kombination von mehreren voneinander unabhängigen Mehrfach-Fehlerursachen zurückzuführen ist, als ein Mehrfach-Ausfall bezeichnet. Für weitere Unterscheidungsmerkmale in Bezug auf Fehlerursachen, Fehlzustände und Ausfälle siehe die umfassende Darstellung in [ALR+04, S. 15ff.].

Im Zusammenhang mit der Absicherung der Zuverlässigkeit und Sicherheit technischer Systeme ist darüber hinaus der Begriff der **abhängigen Ausfälle** (engl. dependent failures) von Relevanz. Zwei Ausfälle sind (stochastisch) abhängig voneinander, wenn die Wahrscheinlichkeit ihres gleichzeitigen bzw. aufeinanderfolgenden Auftretens nicht als Produkt der Auftretenswahrscheinlichkeiten der einzelnen Ausfälle ausgedrückt werden kann [ISO26262-1, S. 4]. Andernfalls spricht man von unabhängigen Ausfällen. Für abhängige Ausfälle gilt:

$$P_{A\ und\ B} = P_A \cdot P_B$$

$P_{A\ und\ B}$: Wahrscheinlichkeit des gleichzeitigen bzw. aufeinanderfolgenden Auftretens von Ausfällen A und B

P_A: Wahrscheinlichkeit des Auftretens vom Ausfall A

P_B: Wahrscheinlichkeit des Auftretens vom Ausfall B

Gleichung 2-1: Definition abhängiger Ausfälle

Dabei werden zwei Klassen abhängiger Ausfälle unterschieden (Bild 2-5) [ISO26262-1, S. 4], [Eri05, S. 400ff.]:

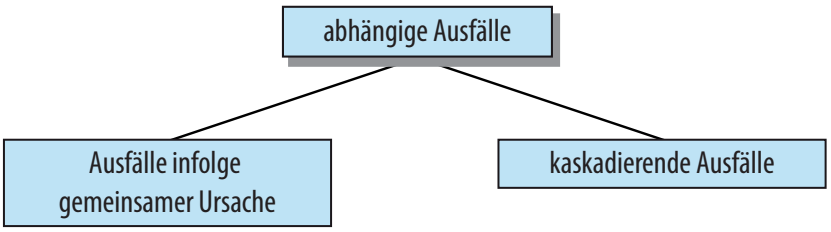


Bild 2-5: Klassen abhängiger Ausfälle

- **Ausfall infolge gemeinsamer Ursache** (engl. common cause failure, CCF): Ausfall von einem oder mehreren Systemelementen aufgrund einer gemeinsamen Ursache (z.B. Vibration, kosmische Strahlung, Ausfall einer gemeinsamer Stromversorgung).
- **Kaskadierender Ausfall** (engl. cascading failures): Ausfall eines Systemelements einer Betrachtungseinheit, welcher zum Ausfall eines bzw. mehrerer weiterer Systemelemente derselben Betrachtungseinheit führt. Beispiel: Ausfall einer Software-Komponente aufgrund des Zugriffs auf einen korrupten Speicherbereich, der infolge

eines Ausfalls einer anderen Software-Komponente korrumpiert wurde. Ein weiteres Beispiel: mehrere elektrische Systemelemente in einer Serienanordnung. Fällt eins der Systemelemente aus, kann es dazu führen, dass in der Schaltung ein höherer Strom fließt als vorgesehen, was einen kaskadierenden Ausfalleffekt in der restlichen Schaltung verursacht.

2.1.3 Mittel zur Erreichung der Verlässlichkeit

Mittel zur Erreichung der Verlässlichkeit sind gemäß Bild 2-6 Fehlerbeseitigung, Fehlertoleranz, Fehlerverhinderung und Fehlervorhersage.

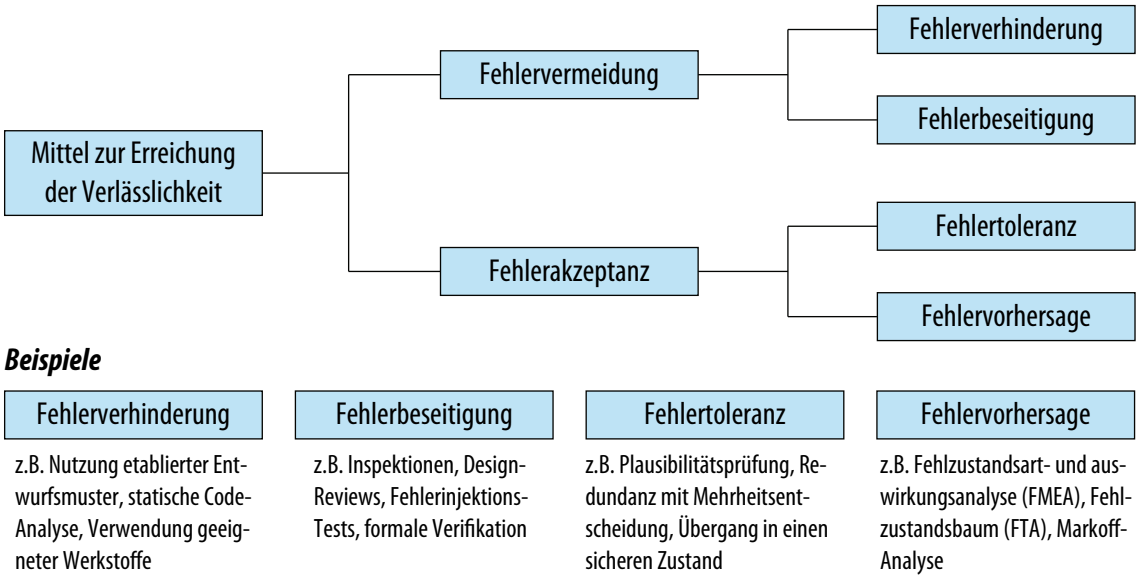


Bild 2-6: Mittel zur Erreichung der Verlässlichkeit (in Anlehnung an AVIZIENIS ET AL.) [ALR+04, S. 14]

Fehlervermeidung (engl. fault avoidance)

Fehlervermeidung umfasst Maßnahmen zur Steigerung der Verlässlichkeit im Entwicklungsprozess, um Fehler von Beginn an zu vermeiden [BGJ+09, S. 93], [Sto96, S. 13], [ALR+04, S. 19]. Diese betreffen den gesamten Entwicklungsprozess von der Konzipierungs- über die Entwurfsphase bis hin zu den Testphasen sowie die Nutzungsphase [Ise07a, S. 173]. Es wird in diesem Zusammenhang zwischen Maßnahmen zur Fehlerverhinderung und Fehlerbeseitigung unterschieden [ALR+04, S. 29].

Im Fokus der Maßnahmen zur **Fehlerverhinderung** (engl. fault prevention) stehen die Konzipierungs- und Entwurfsphasen des Entwicklungsprozesses [ALR+04, S. 24]. Beispiele sind Verbesserung der konstruktiven Maßnahmen, ein sorgfältigerer Entwurf (z.B. durch Einsatz von statischer Code-Analyse, MISRA-Regeln, Nutzung etablierter Entwurfsmuster und Codierungsrichtlinien im SW-Entwicklungsprozess etc.), Einsatz formaler Methoden zur Systemmodellierung, Verwendung von geeigneteren Werkstoffen, Verwendung verbesserter Herstellungstechniken [BGJ+09, S. 93], [ISO26262-6],

[ALR+04, S. 24]. Ziel der Maßnahmen zur **Fehlerbeseitigung** (engl. fault removal) ist die Reduktion der Anzahl und Schwere der potentiellen Fehler. Sie finden schwerpunktmäßig Anwendung in den Testphasen des Entwicklungsprozesses sowie der Nutzungsphase. Beispiele für Maßnahmen zur Fehlerbeseitigung während der Entwicklung sind eine erhöhte Anzahl von Review- und Testtätigkeiten (z.B. Inspektionen, Fehlerinjektions-Tests etc.), formale Verifikationsmethoden etc. [BGJ+09, S. 93], [ISO26262-6], [Sto96, S. 271ff.]. Maßnahmen zur Fehlerbeseitigung während der Nutzungsphase sind Instandhaltungsmaßnahmen: Instandsetzungsmaßnahmen (außerplanmäßige Instandhaltung) und Wartungsmaßnahmen (planmäßige Instandhaltung) [ALR+04, S. 28].

Fehlerakzeptanz (engl. fault acceptance)

Aufgrund der Komplexität technischer Systeme von heute ist die vollständige Vermeidung von Fehlern während der Entwicklung nicht mehr möglich, so dass der Umgang mit Fehlern im Betrieb ins Kalkül gezogen werden muss [BGJ+09, S. 368]. Hierzu dienen die Maßnahmen zur Fehlerakzeptanz [ALR+04, S. 29]. Es wird dabei zwischen Fehlertoleranz und Fehlervorhersage unterschieden [ALR+04, S. 29]:

Fehlertoleranz (engl. fault tolerance) bezeichnet die Fähigkeit einer Betrachtungseinheit ihre spezifizierte Funktion im Betrieb auch beim Vorhandensein einer begrenzten Anzahl von Fehlern zu erbringen [Sto96, S. 14], [BGJ+09, S. 93]. Die Fehlertoleranz wird im Allgemeinen durch die Kombination von Überwachung, Fehlererkennung und Fehlerbehandlung erreicht [SZ13, S. 98ff.], [BGJ+09, S. 368ff.]. **Überwachung** (engl. supervision) dient dazu, unerwünschte bzw. unerlaubte Abweichungen vom gewünschten Verhalten zu erkennen und – falls erforderlich – Gegenmaßnahmen einzuleiten [SZ13, S. 99]. Maßnahmen zur **Fehlererkennung** (engl. fault detection) dienen der Erkennung von Fehlern im Systembetrieb, so dass die Ausfallauswirkungen reduziert werden können [Sto96, S. 13], [BGJ+09, S. 368]. Beispiele für Maßnahmen zur Fehlerkennung für elektronische Systeme sind Plausibilitätsprüfung, Referenzwertüberprüfung durch Frage-Antwort-Spiel, Überprüfung anhand redundanter Werte, Senden einer Bestätigung [HK13, S. 22], [SZ13, S. 99f.]. Maßnahmen zur **Fehlerbehandlung** (engl. fault treatment) legen fest, wie auf bereits aufgetretene und erkannte Fehler reagiert wird [SZ13, S. [BGJ+09, S. 368]. Beispiele sind Verwendung von redundanten Werten oder Ersatzwerten, Übergang in einen sicheren Zustand (z.B. durch Abschaltung von Subsystemen bzw. des Gesamtsystems) und Neustart eines Systemelements (z.B. Reset eines Mikroprozessors durch eine Watchdog-Schaltung) [SZ13, S. 101].

Methoden der **Fehlervorhersage** (engl. fault forecasting) dienen der Evaluierung des Verhaltens der Betrachtungseinheit in Bezug auf Ausfallmöglichkeiten und die zugehörigen Ursache-Wirkungsketten [ALR+04, S. 28]. Sie kommen typischerweise in den Konzipierungs- und Entwurfsphasen des Entwicklungsprozesses zum Einsatz. Beispiele von Methoden zur Fehlervorhersage sind die Fehlzustandsart- und -auswirkungsanalyse (FMEA), Markoff-Analyse, Fehlzustandsbaumanalyse (FTA) und Ereignisablaufanalyse (ETA), die in Abschnitt 3.2 vorgestellt werden. Es wird dabei zwischen **induktiven** und

deduktiven Methoden unterschieden. Bei induktiven Methoden wird entlang der Fragestellung „Was wäre wenn?“ Bottom-Up vorgegangen [Eri05, S. 49]. Für jede Ausfallart wird ihre Auswirkung in der betrachteten Systemebene bestimmt [DIN60300-3-1, S. 11]. Induktiv sind beispielsweise die FMEA und die ETA. Bei deduktiven Methoden geht man entlang der Frage „Wie kann?“ Top-Down vor [Eri05, S. 49]. Ausgehend von einem unerwünschten Einzelereignis werden die hierzu beitragenden Ereignisse ermittelt und untersucht [DIN60300-3-1, S. 11]. Beispiele deduktiver Methoden sind die FTA und die Markoff-Analyse. Die meisten der Methoden können sowohl zur **qualitativen** als auch zur **quantitativen** Analyse herangezogen werden. Bei einer qualitativen Analyse werden Ausfallmöglichkeiten und die zugehörigen Ursache-Wirkungsketten ermittelt, klassifiziert und qualitativ bewertet (z.B. Beschreibung von Ursache-Wirkungsketten mit einer qualitativen FTA) [Eri05, S. 51ff.], [ALR+04, S. 28]. Eine quantitative Analyse geht darüber hinaus, da mit numerischen Werten (z.B. Ausfallraten) gearbeitet wird und eine numerische Aussage getroffen wird (z.B. Berechnung der Systemzuverlässigkeit mit einer quantitativen FTA) [Eri05, S. 51ff.], [ALR+04, S. 28].

Zusammenfassend lässt sich folgendes festhalten [ALR+04, S. 14]: Das Ziel der Maßnahmen zur Fehlerbeseitigung und Fehlervorhersage ist ein Nachweis, dass die an die Betrachtungseinheit gestellten funktionalen und verlässlichkeitsspezifischen Anforderungen sowie die zugehörige Spezifikation adäquat sind und dass die Betrachtungseinheit diese erfüllt. Ziel der Maßnahmen zur Fehlerverhinderung und Fehlertoleranz ist eine zuverlässige und sichere Erbringung der spezifizierten Funktion durch die Betrachtungseinheit im Betrieb.

Alle Formen der Fehlertoleranz beruhen auf **Redundanz** (engl. redundancy) [Sto96, S. 124]. Eine redundante Auslegung liegt dann vor, wenn das betrachtete Systemelement durch eine oder mehrere Systemelemente ergänzt wird, gewöhnlich in paralleler Anordnung, die im Normalbetrieb überflüssig sind [Ise07a, S. 173]. Ein Überblick über Arten der Redundanz gibt Anhang A1.1.

2.1.4 Grundlegende Begriffe des modellbasierten Systems Engineerings

Im Kontext der vorliegenden Arbeit sind einige Begriffe des modellbasierten Systems Engineerings wie semiformale Notation, Metamodell etc. von zentraler Bedeutung. Nachfolgend werden diese kurz erklärt.

Eine **Modellierungssprache**[13] dient der Beschreibung eines Sachverhalts, der als Modell zu repräsentieren ist. Die Sprachspezifikation einer Modellierungssprache umfasst ein Metamodell (abstrakte Syntax und statische Semantik) sowie die Definition der konkreten Syntax und der dynamischen Semantik [SVE+07].

---

[13] In dieser Arbeit werden synonym zum Begriff einer Modellierungssprache die Begriffe Spezifikationssprache und Beschreibungssprache verwendet.

Eine **Modellierungstechnik** besteht aus einer Modellierungssprache und einem Vorgehensmodell mit Modellierungsregeln zur Anwendung der Modellierungssprache.

Ein **Metamodell** umfasst die Definition der abstrakten Syntax und der statischen Semantik einer Modellierungssprache. Ein Modell ist eine Instanz des Metamodells; es ist beschrieben in der durch das Metamodell definierten Modellierungssprache.

Die **abstrakte Syntax** definiert, welche Modellelemente zur Verfügung stehen, welche Attribute diese besitzen und wie sie prinzipiell mit anderen Modellelementen in Beziehung gesetzt werden können [SVE+07]. Zum Beispiel ist ein Zustand ein Modellelement einer Zustandsmaschine. Ein Zustandsübergang stellt eine mögliche Beziehung zwischen zwei Zuständen dar.

Die **statische Semantik** definiert, wie ein Modellelement verknüpft werden muss, um eine Bedeutung zu haben. Es handelt sich hierbei insbesondere um Constraints, welche die Verwendung der Modellelemente, das Setzen deren Attribute sowie die Spezifikation der Beziehungen zwischen den Modellelementen einschränken. Zum Beispiel wird festgelegt, dass eine Zustandsmaschine über nur einen Startknoten verfügen darf.

Zusätzlich zur Definition des Metamodells umfasst die Sprachspezifikation einer Modellierungssprache die Definition der konkreten Syntax und der dynamischen Semantik:

Die **konkrete Syntax** legt fest, wie die Modellelemente und deren Beziehungen untereinander graphisch dargestellt werden. Zum Beispiel wird definiert, dass ein Zustand in einer Zustandsmaschine durch ein abgerundetes Rechteck dargestellt wird.

Die **dynamische Semantik** definiert die Bedeutung eines Modellelements bzw. einer Beziehung in einem konkreten mit der Modellierungssprache erstellten Modell. Zum Beispiel kann für Zustandsübergange mit mehreren Aktionen (auszulösenden Ereignissen) festgelegt werden, dass im Falle einer Auslösung des jeweiligen Zustandsübergangs alle Aktionen parallel zueinander ausgeführt werden[14]. Alleine für Zustandsmaschinen sind unterschiedliche Definitionen der dynamischen Semantik vorzufinden. Klassische Zustandsmaschinen nach HAREL weisen eine andere dynamische Semantik auf als die Zustandsmaschinen der UML [Har87], [OMG11]. Auch bei der UML fehlt die Eindeutigkeit. Zum Beispiel weicht die im Software-Werkzeug IBM Rational Rhapsody für UML-Zustandsmaschinen umgesetzte dynamische Semantik von der in der UML-Spezifikation beschriebenen ab [CD05].

Eine **informale Notation** ist nach ISO 26262 eine Modellierungssprache, deren Syntax nicht vollständig definiert ist. Eine **semiformale Notation** ist nach ISO 26262 eine Modellierungssprache mit einer vollständig definierten Syntax. Die Semantik (insbesondere

---

[14] Eine andere Möglichkeit stellt eine sequentielle Ausführung dar. Beispiel: Ist ein Zustandsübergang mit den Aktionen x := x + 1; y := x * 5 versehen, so wird unter der Annahme von x = 0 bei einer parallelen Ausführung das Resultat x = x + 1 = 0 + 1 = 1 und y = x * 5 = 0 * 5 = 0 sein. Bei einer sequentiellen Ausführung sieht das Ergebnis anders aus: x = x + 1 = 0 + 1 = 1 und y = x* 5 = 1* 5 = 5.

die dynamische) muss nicht vollständig definiert sein. Ein Beispiel ist die Systems Modeling Language (SysML) (vgl. auch Abschnitt 3.4.2). Eine **formale Notation** ist nach ISO 26262 eine Modellierungssprache mit einer vollständig definierten Syntax und einer vollständig definierten Semantik. Beispiele sind die Z Notation und die Vienna Development Method. [ISO26262-1]

2.1.5 Zuverlässigkeit und Sicherheit technischer Systeme

Im Folgenden wird auf die Zuverlässigkeit und Sicherheit technischer Systeme eingegangen. In Abschnitt 2.1.5.1 findet zunächst eine Begriffsklärung statt; die Ähnlichkeiten und Unterschiede zwischen Zuverlässigkeit und Sicherheit werden erklärt. In Abschnitt 2.1.5.2 werden dann die grundlegenden Kenngrößen der Zuverlässigkeit vorgestellt. Darauf basierend werden in Abschnitt 2.1.5.3 die Kenngrößen der Sicherheit eingeführt. Abschließend gibt Abschnitt 2.1.5.4 einen kurzen Überblick über Ausfallratenmodelle.

2.1.5.1 Zuverlässigkeit und Sicherheit – Begriffsklärung

Die beiden Verlässlichkeitsaspekte Zuverlässigkeit und Sicherheit stehen im Mittelpunkt der vorliegenden Arbeit. Der wesentliche Unterschied zwischen den beiden Verlässlichkeitsaspekten besteht in ihrem jeweiligen Fokus [Eri11, S. 18]: Zuverlässigkeitsbetrachtungen fokussieren die Ausfallrate einer Betrachtungseinheit. Vereinfacht ausgedrückt beschreibt die Ausfallrate die durchschnittliche Zeit, in der die Betrachtungseinheit unter gegebenen Bedingungen funktionsfähig ist, bevor sie ausfällt. Ziel der Absicherung der Zuverlässigkeit ist es demnach, durch geeignete Maßnahmen zu erreichen, dass die Betrachtungseinheit und deren Bestandteile die geforderte Ausfallrate erreicht und nicht übersteigt. Je niedriger die Ausfallrate, desto höher die Zuverlässigkeit [Eri11, S. 18].

Im Fokus der Sicherheitsbetrachtungen steht die Vermeidung potentieller Gefahren und der daraus möglicherweise resultierenden Unfälle. Je niedriger das Sicherheitsrisiko, desto sicherer ist die Betrachtungseinheit [Eri11, S. 18], [Dou09, S. 6]. Im Gegensatz zur Zuverlässigkeit, steht bei der Sicherheit die Funktionsfähigkeit der Betrachtungseinheit nicht im Mittelpunkt [SZ13, S. 96].

Im Falle eines sogenannten Fail-Safe-Systems[15] sind Sicherheit und Zuverlässigkeit oft gegenläufige Ziele. Die Zuverlässigkeit eines derartigen Systems erhöht sich, wenn dieses möglichst lange funktionsfähig bleibt, auch wenn dies zu Gefahren und als Konsequenz zu Unfällen führen kann. Die Sicherheit eines solchen Systems erhöht sich, wenn im Fehlerfall ein Übergang in seinen sicheren Zustand eingeleitet wird, auch wenn dies oft das Ausschalten des Systems bedeutet. In diesem Fall erhöht sich die Sicherheit des

[15] Ein Fail-Safe-System ist dadurch gekennzeichnet, dass es bei Fehlererkennung hinreichend schnell in einen sicheren Zustand überführt wird. Weiterführende Informationen zum Fail-Safe-Architekturprinzip und verwandten Architekturprinzipien sind in Abschnitt 2.1.5.3 zu finden.

Systems zum Nachteil der Zuverlässigkeit [Dou09, S. 7]. Als Beispiel sei ein Elektronen-Linearbeschleuniger genannt, der für therapeutische Strahlung in der Krebstherapie eingesetzt wird. Kommt es zu einem Fehler in der Informationsverarbeitung des Geräts, kann es zu einer erhöhten Strahlenbelastung führen, was tragische Folgen für die Patienten haben kann (von einer Verbrennung bis hin zu einer Überdosis). [16] Im Falle der Erkennung eines Fehlers, muss dieses Gerät in einen sicheren Zustand (hier: Aus) gebracht werden, auch wenn dabei die Zuverlässigkeit sinkt.

Für viele Systeme ist eine Fail-Safe-Architektur nicht geeignet. Beispiel – Fly-by-Wire-Flugzeuge [Rei04]. Hier gilt es Fehler zu tolerieren: „Während eines Flugs mit 600 Knoten (ca. 1111 km/h) in der Höhe von 10 000 km ist es nicht sicher ein Triebwerk aufgrund eines Einzelfehlers auszuschalten“ [Dou09, S. 7]. Bei solchen Systemen kommen Redundanz/Fehlertoleranz (redundante Kanäle, redundante Subsysteme etc.) verstärkt zum Einsatz (vgl. auch Abschnitt 2.1.3). Durch derartige Maßnahmen geht die Erhöhung der Sicherheit mit der Erhöhung der Zuverlässigkeit einher [Dou09, S. 7].

2.1.5.2 Zuverlässigkeitskenngrößen

Hier wird auf die wesentlichen Kenngrößen der Zuverlässigkeit eingegangen.

Die **Lebensdauer** τ eines technischen Systems ist eine reelle Zufallsgröße mit der Verteilungsfunktion F(t) [MP10, S. 33]:

$$F(t) = P(\tau \leq t)$$

P(·): Wahrscheinlichkeit

F(t):Ausfallwahrscheinlichkeit

τ: Lebensdauer der Einheit

Gleichung 2-2: Berechnung der Ausfallwahrscheinlichkeit

Diese Verteilungsfunktion F(t) wird als **Ausfallwahrscheinlichkeit** (bzw. Lebensdauerverteilung) (engl. failure probability) bezeichnet. Sie ist die Wahrscheinlichkeit, dass eine Einheit zum Zeitpunkt t einen Ausfall aufweist, d.h. ihre Funktion nicht erfüllt [Rei12, S. 267], [LPP10, S. 283].

Dabei wird zum einen angenommen, dass eine neue Einheit funktionsfähig ist. Es gilt also [MP10, S. 33]:

$$F(t) = P(\tau \leq t) = 0 \text{ für } t \leq 0$$

---

[16] Das hier aufgeführte Beispiel eines Linearbeschleunigers zur Anwendung in der Strahlentherapie basiert auf einem tatsächlich aufgetretenen Fall. Es handelte sich hierbei um das Gerät Therac-25, dessen Funktionsfehler in den Jahren 1985-87 drei Patienten das Leben kostete, weitere Patienten erlitten schwere Verletzungen [Lev95].

Gleichung 2-3: Annahme der Funktionsfähigkeit einer neuen Einheit

Zum anderen wird unterstellt, dass diese Einheit zu einem bestimmten Zeitpunkt ausfällt [MP10, S. 33]:

$$\lim_{t \to \infty} F(t) = \lim_{t \to \infty} P(\tau \leq t) = 1$$

Gleichung 2-4: Annahme der Beendigung der Funktionsfähigkeit zu einem bestimmten Zeitpunkt

Das Komplement der Ausfallwahrscheinlichkeit wird als **Überlebenswahrscheinlichkeit** (Zuverlässigkeitsfunktion) R(t) (engl. reliability function) bezeichnet [MP10, S. 33]:

$$R(t) = P(\tau > t) = 1 - P(\tau \leq t) = 1 - F(t)$$

R(t): Überlebenswahrscheinlichkeit

Gleichung 2-5: Überlebenswahrscheinlichkeit als Komplement der Ausfallwahrscheinlichkeit

R(t) ist im Gegensatz zu F(t) eine monoton fallende Funktion [MP10, S.33]. Es gilt:

$$R(0) = 1 \text{ und } \lim_{t \to \infty} R(t) = 0$$

Gleichung 2-6: Annahmen in Bezug auf die Überlebenswahrscheinlichkeit

Die **Ausfalldichte** f(t) (engl. failure density function) beschreibt die Häufigkeit der Ausfälle und bildet „die Änderung der Wahrscheinlichkeit, ein System ausgefallen anzutreffen“ ab [Rei12, S. 267]. Sie lässt sich als erste Ableitung der Ausfallwahrscheinlichkeit berechnen [MP10, S. 34]:

$$f(t) = \frac{dF(t)}{dt} \text{ für alle } t$$

wobei

$$f(t) = 0 \text{ für } t < 0,$$

$$f(t) \geq 0 \text{ für } t \geq 0$$

und

$$\int_0^{\infty} f(t)dt = 1$$

f(t): Ausfalldichte

Gleichung 2-7: Berechnung der Ausfalldichte f(t)

Daraus ergeben sich die in Bild 2-7 graphisch dargestellten Gleichungen [MP10, S. 34]:

$$F(t) = \int_0^t f(\tau)d\tau$$

Gleichung 2-8: Zusammenhang zwischen der Ausfallwahrscheinlichkeit und der Ausfalldichte

und

$$R(t) = \int_t^\infty f(\tau)d\tau$$

Gleichung 2-9: Zusammenhang zwischen der Überlebenswahrscheinlichkeit und der Ausfalldichte

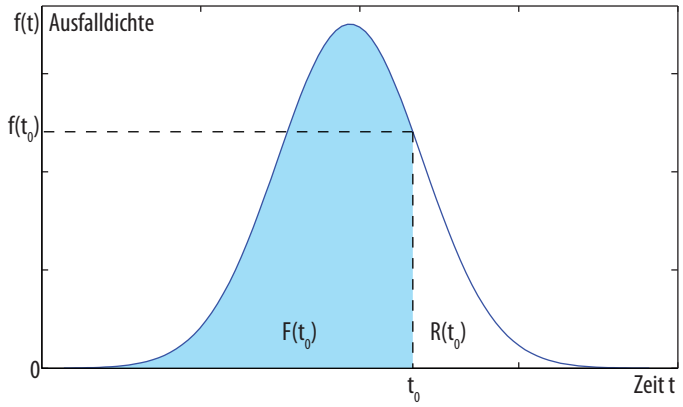


Bild 2-7: Überlebenswahrscheinlichkeit $R(t_0)$ als Komplement zur Ausfallwahrscheinlichkeit $F(t_0)$ [MP10, S. 35]

Die **Ausfallrate** λ(t) (engl. failure rate, hazard rate) zu einem Zeitpunkt t „lässt sich interpretieren als ein Maß für das Risiko eines [Systems bzw. Systemelements] auszufallen, unter der Voraussetzung, dass es bereits bis zu diesem Zeitpunkt t überlebt hat. Betrachtet man einen bestimmten Zeitpunkt t, so gibt die Ausfallrate an, wie viele von den insgesamt noch vorhandenen [Systemelementen] in der nächsten Zeiteinheit ausfallen werden“ [BL04, S. 23]. Daraus ergibt sich die folgende Gleichung [BL04, S. 22]:

$$\lambda(t) = \frac{\text{Ausfälle (zum Zeitpunkt t)}}{\text{Summe der noch intakten Einheiten (zum Zeitpunkt t)}}$$

λ(t):Ausfallrate

Gleichung 2-10: Definition der Ausfallrate

Da die **Dichtefunktion** f(t) die Anzahl der Ausfälle zum Zeitpunkt t und die Überlebenswahrscheinlichkeit R(t) die Summe der intakten Einheiten abbilden, kann die Ausfallrate λ(t) als Quotient der beiden Größen berechnet werden [BL04, S. 22], [MP10, S. 35]:

$$\lambda(t) = \frac{f(t)}{R(t)}$$

Gleichung 2-11: Zusammenhang Ausfallrate, -dichte und Überlebenswahrscheinlichkeit

Die Einheit der Ausfallrate ist 1/h. Die Ausfallrate wird oft mit der Einheit FIT (Failure-In-Time) dargestellt (1 FIT = 10^{-9}/h). 1 FIT entspricht „einem Ausfall eines Bauteils in 10^9 Stunden, also einmal in ca. 114 000 Jahren, bei konstanter Ausfallrate“ [LPP10, S. 332]. Für Beispiele von Ausfallraten typischer Systemelemente siehe Abschnitt 2.2.4.

Eine weitere relevante Kenngröße ist die **mittlere Lebensdauer bis zum Ausfall** (engl. Mean Time To Failure, MTTF). MTTF ist der Erwartungswert der Lebensdauer τ. Sie wird in Stunden gemessen und wie folgt berechnet [DIN61703, S. 19]:

$$\mathrm{MTTF} = \mathrm{E}(\tau) = \int_0^\infty \mathrm{R}(t)\mathrm{d}t$$

$\mathrm{E}(\tau)$: Erwartungswert der Lebensdauer τ

$\mathrm{R}(t)$: Überlebenswahrscheinlichkeit zum Zeitpunkt t

Gleichung 2-12: Berechnung der MTTF

Bei einer konstanten Ausfallrate ($\lambda(t) = \lambda = \text{const.}$) ist die MTTF der Kehrwert der Ausfallrate [LPP10, S. 284]. Es gilt [DIN61703, S. 19]:

$$\mathrm{MTTF} = \frac{1}{\lambda}$$

Gleichung 2-13: Berechnung der MTTF bei konstanter Ausfallrate

Zusammenfassend stellt Tabelle 2-1 den formelmäßigen Zusammenhang zwischen den wichtigsten Zuverlässigkeitskenngrößen.

Tabelle 2-1: Zusammenhang zwischen den Zuverlässigkeitskenngrößen [MP10, S. 38]

	Ausfallwahrscheinlichkeit F(t)	**Überlebenswahrscheinlichkeit R(t)**	**Ausfalldichte f(t)**	**Ausfallrate λ(t)**
F(t)		$1 - \mathrm{R}(t)$	$\int_0^t \mathrm{f}(\tau)\mathrm{d}\tau$	$1 - \mathrm{e}^{-\int_0^t \lambda(\tau)\mathrm{d}\tau}$
R(t)	$1 - \mathrm{F}(t)$		$\int_t^\infty \mathrm{f}(\tau)\mathrm{d}\tau$	$\mathrm{e}^{-\int_0^t \lambda(\tau)\mathrm{d}\tau}$
f(t)	$\frac{\mathrm{dF}(t)}{\mathrm{d}t}$	$-\frac{\mathrm{dR}(t)}{\mathrm{d}t}$		$\lambda(t)\cdot\mathrm{e}^{-\int_0^t \lambda(\tau)\mathrm{d}\tau}$
λ(t)	$\frac{1}{1 - \mathrm{F}(t)} \cdot \frac{\mathrm{dF}(t)}{\mathrm{d}t}$	$-\frac{1}{\mathrm{R}(t)} \cdot \frac{\mathrm{dR}(t)}{\mathrm{d}t}$	$\frac{\mathrm{f}(t)}{\int_t^\infty \mathrm{f}(\tau)\mathrm{d}\tau}$	

Zuverlässigkeitskenngrößen für zusammengesetzte Systeme

Typischerweise besteht ein System aus mehreren Subsystemen. Im Folgenden wird kurz darauf eingegangen, wie sich die Zuverlässigkeitskenngrößen Überlebenswahrscheinlichkeit R(t) und Ausfallrate λ(t) für das Gesamtsystem auf Basis der Kenngrößen der Subsysteme bestimmen lassen [Rei12, S. 265].

Allgemein wird zwischen zwei elementaren Strukturen von Systemen unterschieden: einer logischen Serienanordnung und einer logischen Parallelanordnung. Eine logische Serienanordnung liegt dann vor, wenn für die Funktionsfähigkeit des Gesamtsystems die Funktionsfähigkeit aller Subsysteme vorausgesetzt wird (Bild 2-8 a)). Eine derartige Anordnung wirkt sich ungünstig auf die Zuverlässigkeit und Sicherheit des Gesamtsystems aus [Rei12, S. 266]. „Eine Kette ist immer nur so stark wie ihr schwächstes Glied“. Eine Parallelanordnung ist vorhanden, wenn für die Funktionsfähigkeit des Gesamtsystems die Funktionsfähigkeit von nur einem der Subsysteme ausreicht (Bild 2-8 b)). Eine derartige Anordnung erhöht die Zuverlässigkeit und die Sicherheit des Gesamtsystems. Hier ist auch das Prinzip der Redundanz erkennbar, auf das bereits in Abschnitt 2.1.3 eingegangen wurde. Tabelle 2-2 stellt dar, wie die Kenngrößen Überlebenswahrscheinlichkeit und Ausfallrate für die beiden elementaren Strukturen zu berechnen sind.

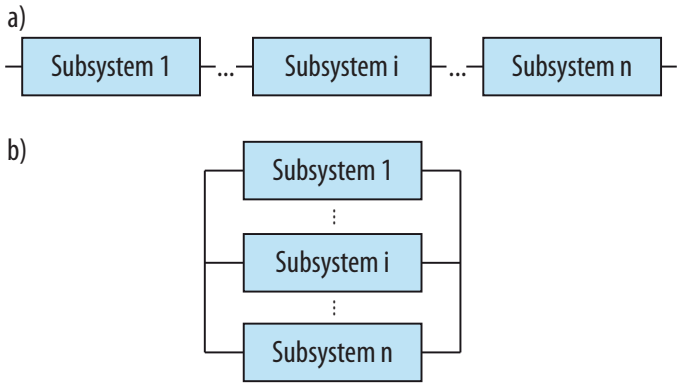


Bild 2-8: Elementare Strukturen von Systemen, die sich aus mehreren Subsystemen zusammensetzen: a) logische Serienanordnung, b) logische Parallelanordnung

Tabelle 2-2: Berechnung der Überlebenswahrscheinlichkeit und Ausfallrate für logische Serienanordnung und logische Parallelanordnung [Rei12, S. 275], [MP10, S. 172 ff.]

Art der Anordnung	Überlebens-wahrscheinlichkeit R(t)	Ausfallrate λ(t)
Logische Serienanordnung	$R(t) = \prod_{i=1}^{n} R_i(t)$	$\lambda(t) = \sum_{i=1}^{n} \lambda_i(t)$
Logische Parallelanordnung	$R(t) = 1 - \prod_{i=1}^{n} \left(1 - R_i(t)\right)$	$\lambda(t) = \frac{\sum_{i=1}^{n} (f_i(t) \cdot \prod_{k=1,k\neq i}^{n} F_i(t))}{1 - \prod_{i=1}^{n} F_i(t)}$

Technische Systeme lassen sich oft als Kombinationen von Serien- und Parallelstrukturen darstellen. Um die Überlebenswahrscheinlichkeit und Ausfallrate solcher Systeme zu berechnen, werden diese zuerst in die elementaren Strukturen dekomponiert. Danach erfolgt die Anwendung der mathematischen Formeln aus Tabelle 2-2. Bild 2-9 stellt dies für ein beispielhaftes System S schematisch dar. In einem ersten Schritt werden Subsysteme identifiziert, die eine parallele Anordnung aufweisen. Im dargestellten Beispiel lassen sich die drei Subsysteme A, B und C identifizieren. Das Subsystem A besteht aus den Subsystemen 1, 2 und 3. Das Subsystem B aus den Subsystemen 4 und 5. Das Subsystem C aus den Subsystemen 6, 7 und 8. Für die Subsysteme A, B und C wird nun jeweils die Überlebenswahrscheinlichkeit berechnet ($R_A(t)$, $R_B(t)$ und $R_C(t)$). Da das Gesamtsystem S eine serielle Anordnung der Subsysteme A, B und C darstellt, ergibt sich dessen Überlebenswahrscheinlichkeit aus der Multiplikation der einzelnen Überlebenswahrscheinlichkeiten der Subsysteme ($R(t) = R_A(t) \cdot R_B(t) \cdot R_C(t)$).

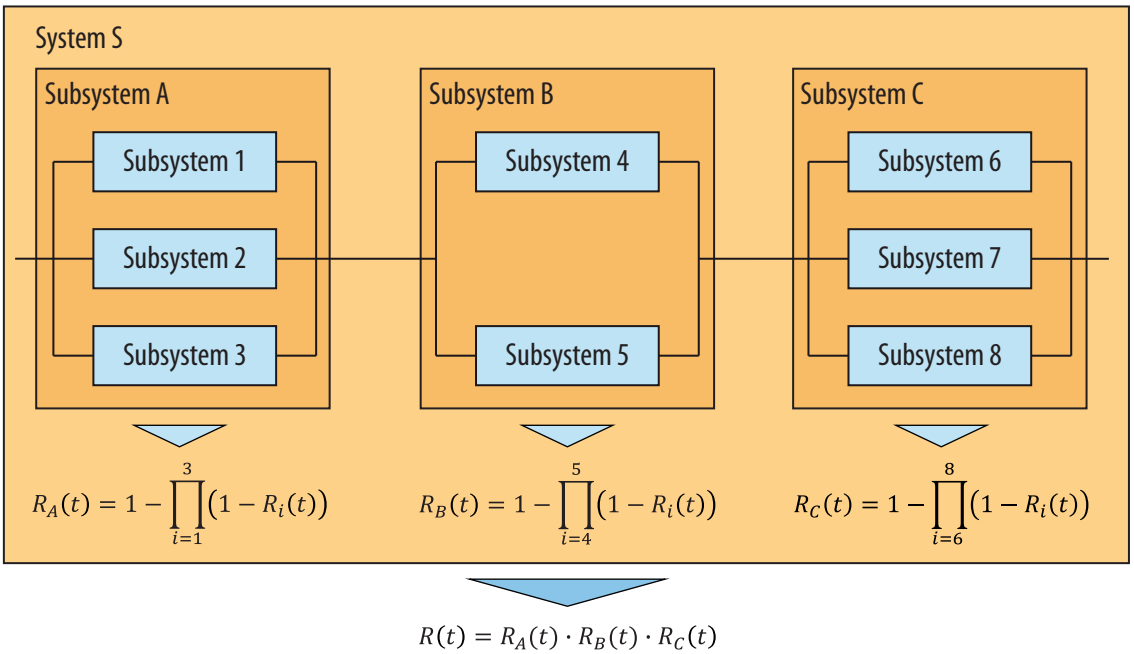


Bild 2-9: Berechnung der Überlebenswahrscheinlichkeit eines zusammengesetzten Systems

Nicht alle technischen Systeme lassen sich als eine Kombination der beiden vorgestellten elementaren Strukturen darstellen. Ein Beispiel einer nichtelementaren Struktur ist die in Bild 2-10 dargestellte Brückenanordnung. Für die Ermittlung der Überlebenswahrscheinlichkeit bzw. Ausfallrate einer derartigen Struktur kann die vorhin vorgestellte Vorgehensweise nicht angewandt werden. Stattdessen kommen Methoden wie die Methode der minimalen Ausfallschnitte (engl. minimal cut sets) und die Methode der minimalen Erfolgspfade (engl. minimal path sets) infrage [BL04, S. 175 ff.]. Eine kurze Darstellung der beiden Methoden ist in Anhang A1.2 zu finden.

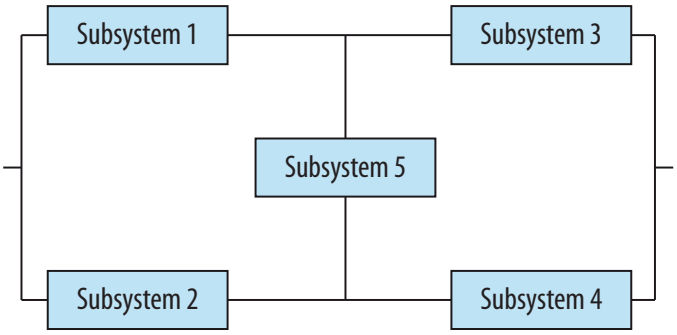


Bild 2-10: Beispiel einer nichtelementaren Struktur: die Brückenanordnung

2.1.5.3 Sicherheitskenngrößen

In Abschnitt 2.1.5.1 wurden die Begriffe Zuverlässigkeit und Sicherheit gegenübergestellt und deren Ähnlichkeiten und Unterschiede erklärt. Insbesondere wurde erklärt, dass bei Zuverlässigkeitsbetrachtungen alle Ausfällmöglichkeiten einer Betrachtungseinheit von Bedeutung sind und im Falle von Sicherheitsbetrachtungen nur die Ausfallmöglichkeiten von Interesse sind, die potentiell zu einer Gefahr führen können. Auch in Bezug auf Kenngrößen gibt es dementsprechend gewisse Analogien. Der Zuverlässigkeitskenngröße der Ausfallwahrscheinlichkeit entspricht in der Sicherheitstechnik die Sicherheitskenngröße der Gefahrenwahrscheinlichkeit. Die Gefahrenwahrscheinlichkeit bzw. die sicherheitsbezogene Ausfallwahrscheinlichkeit ist die Ausfallwahrscheinlichkeit, die sich auf einen Ausfall bezieht, der zu einer gefahrenbringenden Fehlfunktion führen kann [VDI/VDE3542-2, S. 5], [MP10, S. 55]. In ähnlicher Art werden die Begriffe der sicherheitsbezogenen Überlebenswahrscheinlichkeit (bzw. Sicherheitswahrscheinlichkeit), der sicherheitsbezogenen Ausfallrate (bzw. Gefahrenrate) etc. definiert [VDI/VDE3542-2, S. 4 ff.], [MP10, S. 55]. Tabelle 2-3 gibt einen Überblick über die Sicherheitskenngrößen. Insbesondere wird die Analogie-Beziehung zu den in Abschnitt 2.1.5.2 erläuterten Kenngrößen der Zuverlässigkeit dargestellt.

Tabelle 2-3: Zusammenhang der Nomenklaturen von Zuverlässigkeits- und Sicherheitskenngrößen [MP10, S. 55]

Zuverlässigkeitskenngrößen		**Sicherheitskenngrößen**	
Kenngröße	**Formel-zeichen**	**Kenngröße**	**Formel-zeichen**
Ausfallwahrscheinlichkeit	F(t)	Gefahrenwahrscheinlichkeit	G(t)
Überlebenswahrscheinlichkeit	R(t)	Sicherheitswahrscheinlichkeit	S(t)
Ausfalldichte	f(t)	Gefahrendichte	g(t)
Ausfallrate	h(t)	Gefahrenrate	σ(t)

Das in den Sicherheitsnorm IEC 61508 und deren Derivaten beschriebene Vorgehen zur Absicherung der Systemsicherheit sieht folgendes prinzipielles Vorgehen vor: Zunächst wird das Sicherheitsrisiko des Systems ermittelt, und zwar ohne Berücksichtigung von Sicherheitsmaßnahmen [IEC61508], [ISO26262]. Hierzu wird eine Gefahren- und Risikoanalyse herangezogen. [17] Ergebnis sind Sicherheitsziele, welche jeweils mit einem Sicherheitsintegritätslevel (SIL in der IEC 61508 bzw. ASIL in der ISO 26262) versehen werden, der das ermittelte Risiko beschreibt. Darauf aufbauend wird ein Sicherheitskonzept zur Minimierung des Systemrisikos und Erfüllung der Sicherheitsziele erarbeitet. Hier kommt es darauf an, durch Auswahl und Umsetzung geeigneter technischer Sicherheitsmaßnahmen das Systemrisiko auf ein vertretbares Restrisiko zu minimieren (Bild 2-11) [PH13, S. 390f.].

Die Dokumentation der Wirksamkeit des Sicherheitskonzepts erfolgt im Rahmen eines Sicherheitsnachweises [PH13, S. 391f.], [ISO26262-10, S. 9]. Der Sicherheitsnachweis stellt eine klare und umfassende Argumentation dar, welche belegt, dass die Betrachtungseinheit frei von unvertretbarem Risiko während Betriebs unter vorgegebenen Bedingungen ist [ISO26262-10, S. 9], [SZ13, S. 96].

In diesem Zusammenhang ist der Begriff des sicheren Zustands von hoher Bedeutung. Der **sichere Zustand** (engl. safe state) einer Betrachtungseinheit wird wie folgt definiert:

> *„Zustand einer Betrachtungseinheit, bei dem aufgrund des festgestellten Nichtauftretens von sicherheitsbezogenen Fehlfunktionen oder aufgrund der getroffenen Schutzmaßnahmen gegen mögliche sicherheitsbezogene Fehlfunktionen das Risiko vertretbar gering ist“ [VDI/VDE3542-1, S. 13f.], [ISO26262-1, S. 14].*

Für jedes der festgelegten Sicherheitsziele wird, sofern möglich, ein sicherer Zustand definiert [ISO26262-3, S. 11]. Kommt es zu einem Fehler mit Sicherheitszielverletzungspotential, so muss in den sicheren Zustand übergegangen werden.

Beispiel – die Bremslichtfunktion im Kraftfahrzeug. Das zugehörige Sicherheitsziel ist „Der Bremsvorgang soll dem nachfolgenden Verkehr korrekt angezeigt werden“. Der sichere Zustand ist in diesem Fall „Bremslicht an“. In diesem Fall kann es zwar dazu kommen, dass das Bremslicht auch dann an ist wenn keine Bremsanforderung vorliegt. Dies ist allerdings als sicher einzustufen. Ein weiteres Beispiel: Im Falle eines sicherheitsrelevanten Ausfalls einer elektromechanischen Lenkunterstützung (Electric Power Steering, EPS) ist der mögliche sichere Zustand: EPS aus. Der Grund: die Lenkunterstützung darf nur im fehlerfreien Normalbetrieb generiert werden. Andernfalls kann es zu einer ungewollten Aktor-Betätigung und damit einhergehend zu einer unmotivierten Lenkung kommen, die insbesondere bei Fahrten mit hoher Geschwindigkeit als hoch sicherheitskritisch

---

[17] Vgl. auch Abschnitt 3.2.2.1 für eine Darstellung der Gefahrenanalyse und Risikoabschätzung nach der ISO 26262.

einzuschätzen ist und vermieden werden muss. Wird die Lenkunterstützung ausgeschaltet, so wird auf die mechanische Rückfallebene übergegangen. Diese muss eine Lenkfähigkeit entsprechend der ECE-Regelung R79 gewährleisten [ECE-R79].

Die Fehlererkennung durch ein geeignetes Sicherheitskonzept und eine hinreichend schnelle Überführung des Systems in einen sicheren Zustand stellt eine Stufe der Degradation (Reduzierung des Funktionsumfangs) dar, die als **Fail-Safe**-Prinzip bezeichnet wird [PH13, S. 390], [Ise07a, S. 175]. Weitere Arten von Degradationsstufen sind Fail-Silent, Fail-Reduced und Fail-Operational [Rei12, S. 275f.], [Ise07a, S. 175]. Ein **Fail-Silent**-System verhält sich im Falle eines Fehlers passiv. Passiv heißt, dass es auf keine Signale von außen mehr reagiert, seine Funktion nicht erfüllt und andere Systeme nicht beeinflusst [Rei12, S. 276], [Ise07a, S. 175]. Ein Beispiel stellt das ABS-System dar: Im Fehlerfall wird dieses abgeschaltet, die konventionelle Bremsfunktion ohne ABS bleibt dabei erhalten [Rei12, S. 276]. Ein **Fail-Reduced**-System erbringt in einem Fehlerfall nur einen Teil seiner Funktionalität; dieser Zustand wird oft als Notlauf bezeichnet [Rei12, S. 276]. Zum Beispiel besitzen Automatikbetriebe oft einen mechanischen Notlauf [Rei12, S. 276]. Ein **Fail-Operational**-System erfüllt auch trotz eines aufgetretenen Fehlers seine Funktion ohne Einschränkung [Rei12, S. 276], [Ise07a, S. 175]. Dies ist insbesondere für X-by-Wire-Systeme ohne mechanische (bzw. hydraulische) Rückfallebene notwendig, z.B. für „reine“ Steer-by-Wire-Systeme [Rei12, S. 276], [PH13, S. 474], [WHW12, S. 309ff.] (vgl. auch Validierungsbeispiel in Abschnitt 5.1.2).

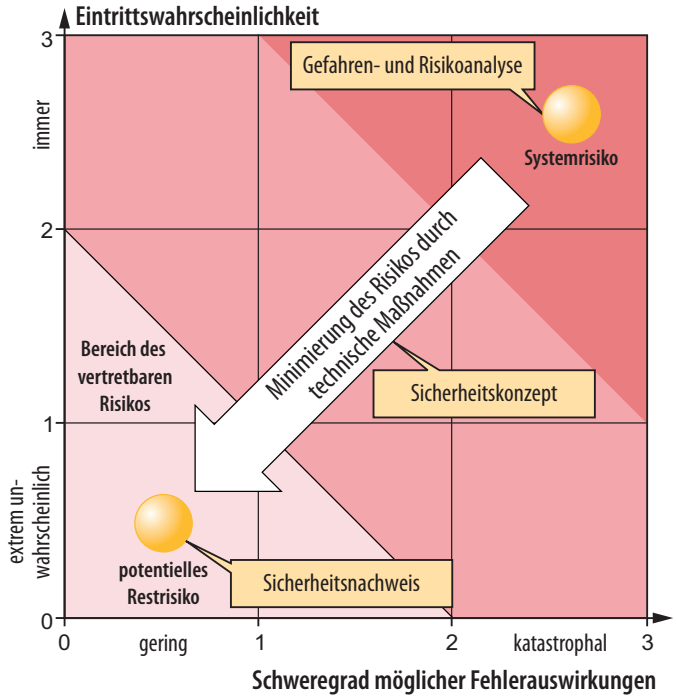


Bild 2-11: Sicherheitskonzept als Mittel zur Minimierung des Systemrisikos bis hin zu einem vertretbaren Niveau [PH13, S. 391]

2.1.5.4 Ausfallraten im zeitlichen Verlauf

Mechatronische Systeme bestehen überwiegend aus Serienschaltungen von mechanischen, elektromechanischen und elektronischen Systemelementen [Ise07a]. Mechanische, elektromechanische und elektronische Systemelemente weisen eine Ausfallrate auf. Diese ist über die Lebensdauer des Systemelements nicht konstant. Bild 2-12 stellt eine typische Entwicklung der Ausfallrate der Systemelemente über die Lebensdauer dar. Ihrem Verlauf entsprechend wird die Kurve als Badewannenkurve bezeichnet [MP10, S. 111], [LPP10, S. 284], [BL04, S. 23]. Es werden drei Bereiche der Badewannenkurve unterschieden.

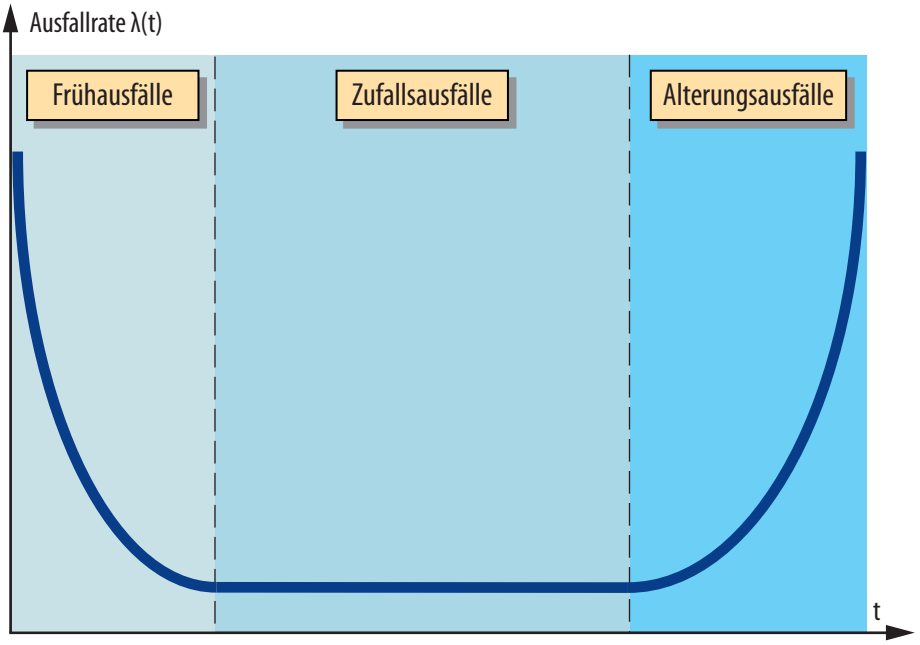


Bild 2-12: Die Badewannenkurve (in Anlehnung an [MP10, S. 111], [LPP10, S. 284])

Der Bereich 1 bildet **Frühausfälle** ab. Die Ausfallrate nimmt hier mit zunehmender Zeit ab. Ursachen für derartige Frühausfälle können Montage-, Fertigungs- und Werkstofffehler etc. sein [BL04, S. 23]. Der Bereich 2 beschreibt **Zufallsausfälle**; die Ausfallrate ist konstant. Die Ausfallursachen sind hier typischerweise Bedienungsfehler, Wartungsfehler, störende Wirkung von Schmutzpartikeln etc. [BL04, S. 24]. Im Bereich 3 (**Alterungsausfälle**) steigt die Ausfallrate mit zunehmender Zeit deutlich an. Verschleiß, Dauerbruch, Alterung etc. sind hier die typischen Ausfallursachen [BL04, S. 24]. In der Praxis muss ein Hersteller eines sicherheitskritischen Systemelements basierend auf der Badewannenkurve des Systemelements seine Lebensdauer angeben. Diese endet an dem Punkt, an dem die Badewannenkurve zu steigen beginnt. Wird die spezifizierte Lebensdauer überschritten, so gilt das Systemelement bzw. das System als nicht mehr sicher. Daher wird in der Praxis den Zuverlässigkeits- und Sicherheitsuntersuchungen vordergründig der Zeitraum der konstanten Ausfallrate zugrunde gelegt. Hinzu kommt, dass in Bezug auf Frühausfälle und Alterungsausfälle meistens keine quantitativen Daten zur

Verfügung stehen [LPP10, S. 283f.]. Dementsprechend ist es den Herstellern von Systemelementen sehr daran gelegen, diese Phase möglichst lang zu halten [MP10, S. 111]. Die Dauer der Phasen variiert in der Praxis ganz stark und hängt von der Charakteristika des betrachteten Systemelements stark ab [MP10, S. 112].

Jedem der oben erwähnten drei Bereiche der Badewannenkurve liegen verschiedene Ausfallursachen zugrunde. Damit einhergehend sind für jeden Bereich unterschiedliche Maßnahmen zur Absicherung der Zuverlässigkeit bzw. Sicherheit erforderlich. Für den Bereich 1 (Frühausfälle) gilt, dass das Systemelement vor dem Inverkehrsetzen einem End-of-Line-Test unterzogen werden sollte (z.B. Tests mit erhöhter Betriebsspannung, Tests unter extremen Temperaturbedingungen, Schnellalterungstests (HALT) etc.) [LPP10, S. 283f]. Das Ziel besteht dabei darin, möglichst viele Frühausfälle erkennen und beseitigen zu können. Ebenfalls gilt es, die Fertigung derartiger Systemelemente mit Sorgfalt abzusichern und zu kontrollieren [BL04, S. 24f]. Im Bereich 2 der Zufallsausfälle kommt es auf die korrekte Bedienung und Wartung an. Insbesondere ist der richtige Einsatz des Produkts unter korrekten Einsatzbedingungen sicherzustellen [BL04, S. 25]. Ein Beispiel einer geeigneten Maßnahme in Bezug auf Bereich 3 (Alterungsausfälle) ist das rechtzeitige Ersetzen des Systemelements. Im Fokus der Sicherheitsnormen IEC 61508 und ISO 26262 stehen die Zufallsausfälle (Bereich 2) [LPP10, S. 283].

Die Annahme einer konstanten Ausfallrate ($\lambda(t) = \lambda = \text{const.}$) impliziert, dass die Lebensdauer einer Exponentialverteilung folgt [MP10, S. 117]. Ein mit der Exponentialverteilung beschriebenes Ausfallverhalten beginnt mit einer großen Ausfallhäufigkeit, welche danach ständig abnimmt. Ein derartiges Ausfallverhalten weisen elektronische Komponenten auf. Daher wird in der Elektrotechnik meist mit einer Exponentialverteilung und damit einhergehend einer konstanten Ausfallrate gearbeitet [MP10, S. 117], [BL04, S. 41]. Im Maschinenbau lässt sich das mit der Exponentialverteilung beschriebene Ausfallverhalten nur sehr selten beobachten [BL04, S. 41]. Für die Beschreibung des Ausfallverhaltens maschinenbaulicher Erzeugnisse wird meist eine andere Lebensdauerverteilung, die Weibullverteilung, herangezogen [BL04, S. 37 und 41ff.]. Die Beschreibung des Ausfallverhaltens mit Hilfe der beiden Wahrscheinlichkeitsverteilungen ist in Anhang A1.3 genauer beschrieben; er gibt einen Überblick über die zugehörigen Formeln und Verläufe von Zuverlässigkeits- und Sicherheitskenngrößen sowie weiterführende Beispiele.

Quellen für Ausfallraten sind Feldbeobachtungen und statistische Analysen. Ferner können Ausfallraten den Datenblättern der Hersteller sowie den Standardquellen wie der Siemens SN Norm 29500, IEC TR 62380, MIL HDBK 217, MIL HDBK 338 entnommen werden [SN29500], [IEC-TR-62380], [Bir07], [MIL-HDBK-217], [MIL-HDBK-338].

2.2 Fortschrittliche mechatronische Systeme

Mechatronik – ein Kunstwort aus Mechanik und Elektronik – bezeichnet das symbiotische Zusammenwirken von Mechanik, Elektrik/Elektronik, Regelungstechnik und Softwaretechnik. Die Erzeugnisse des modernen Maschinenbaus und verwandter Branchen

wie der Automobilindustrie, Bahntechnik und Medizintechnik sind heute zunehmend mechatronische Systeme. Mechatronik ermöglicht eine Erweiterung der Funktionalität und die Verbesserung des Betriebsverhaltens, und zwar bei niedrigeren Kosten, geringerem Gewicht, Volumen und Bauraum. [VDI2206]

Die fortschreitende, dynamische Entwicklung der Informations- und Kommunikationstechnik eröffnet neue faszinierende Perspektiven für technische Erzeugnisse von morgen: mechatronische Systeme mit inhärenter Teilintelligenz, die im Verbund miteinander kommunizieren können. Diese Perspektive wird durch Begriffe wie „Intelligente Objekte“, „Cyber-Physical Systems“, „Industrie 4.0“ und „Selbstoptimierung“ bezeichnet [ADG+09], [aca09], [aca11], [Fa13]. Derartige Erzeugnisse werden in der Lage sein, sich selbstständig und flexibel an die sich verändernden Betriebs- bzw. Umgebungsbedingungen anzupassen. Sie werden meist aus einer Vielzahl von untereinander über Kommunikationsschnittstellen vernetzten, in sich komplexen Teilsystemen bestehen, wobei globale Netzwerke wie das Internet eine große Rolle spielen werden. Die Gesamtfunktionalität derartiger Systeme wird sich erst aus dem Zusammenspiel der einzelnen Teilsysteme ergeben. Hierbei werden weder die Vernetzung noch die Rolle und Funktion der Teilsysteme statisch sein. Vielmehr werden diese im Laufe des Produktlebenszyklus veränderbar und anpassbar sein. Bild 2-13 verdeutlicht diese fortschreitende Entwicklung mechatronischer Systeme bis hin zu intelligenten technischen Systemen von morgen.

Bild 2-13: Auf dem Weg zu intelligenten technischen Systemen von morgen [GRS14]

Derartige intelligente technische Systeme bedeuten neue Möglichkeiten für erfolgsversprechende Produktinnovationen. Neue Systemfunktionen werden möglich, die zur Erhöhung der Ressourcen- und Energieeffizienz, Verlässlichkeit, Benutzungsfreundlichkeit und Komfort bedeutend beitragen können [Möh04, S. 6ff.], [Ise08, S. 21f.], [aca12, S. 200ff], [Fa13, S. 28ff.].

Im Folgenden werden die Historie, der Aufbau sowie die Klassen mechatronischer Systeme erläutert (Abschnitt 2.2.1). Ferner wird auf die Entwicklung von klassischen mechatronischen Systemen (Abschnitt 2.2.1) über adaptive (Abschnitt 2.2.2) bis hin zu selbstoptimierenden Systemen (Abschnitt 2.2.3) eingegangen.

2.2.1 Mechatronische Systeme

Das Wort „Mechatronics“ wurde durch den japanischen Ingenieur K. KIKUCHI 1969 geprägt und durch eine japanische Firma als Warenzeichen bis 1972 gehalten [BB12, S. 366], [HTF96], [Möh04, S. 3]. Zunächst ging es um die Erweiterung mechanischer Erzeugnisse um elektrische Funktionen. Mit der zunehmenden Entwicklung der Mikroelektronik kam die Informationstechnik als weiterer wesentlicher Bestandteil der Mechatronik dazu [Möh04, S. 3]. Heute existieren verschiedene Definitionen der Mechatronik; ein Überblick ist zu finden in [VDI2206, S. 10ff.] und [Ise08, S. 3f.]. Die VDI-Richtlinie 2206 „Entwicklungsmethodik für mechatronische Systeme“ baut auf der Definition von HARASHIMA/TOMIZUKA/FUKUDA auf [HTF96]. Sie bietet die folgende Übersetzung der im Original englischen Definition:

> *„Mechatronik bezeichnet das synergetische Zusammenwirken der Fachdisziplinen Maschinenbau, Elektrotechnik und Informationstechnik beim Entwurf und der Herstellung industrieller Erzeugnisse sowie bei der Prozessgestaltung“ [VDI2206, S. 14].*

Die Erzeugnisse des modernen Maschinenbaus und verwandter Branchen sind heute zunehmend mechatronische Systeme. Beispiel Automobilindustrie. Der Einzug von mechatronischen Systemen in das Fahrwerk begann etwa 1979 mit dem ABS-Bremssystem und der mikroelektrisch gesteuerten Zündung und Einspritzung (Verbrennungsmotor) [BB12, S. 380]. Diese Entwicklung setzte sich mit der Antriebsschlupfregelung, der elektronischen Stabilitätsregelung und der elektromechanischen Servolenkung fort [BB12, S. 380]. Heute durchdringen mechatronische Systeme praktisch das gesamte Fahrzeug [Rei11, S. 162].

2.2.1.1 Klassen mechatronischer Systeme

Die Bandbreite der mechatronischen Systeme und deren Anwendungen ist groß. Nach GAUSEMEIER lassen sich zwei grundsätzliche Klassen mechatronischer Systeme unterscheiden: der Klasse 1 gehören die auf der räumlichen Integration von Mechanik und Elektronik beruhenden Systeme an, die Klasse 2 umfasst Mehrkörpersysteme mit kontrolliertem Bewegungsverhalten. Bild 2-14 stellt diese Unterteilung in zwei Klassen schematisch dar und visualisiert einige Beispiele der beiden Klassen.

Fokus der **Klasse 1** liegt auf einer hohen Integration von Mechanik und Elektronik auf kleinem Bauraum. Wesentliche Erfolgspotentiale bestehen in der Miniaturisierung und Verringerung der Herstellerkosten [Gau10, S. 15]. Im Mittelpunkt steht hier die Aufbau-

und Verbindungstechnik (AVT), z.B. auf Basis der Technologie MID (Molded Interconnect Devices, spritzgegossene Schaltungsträger). Die Entwicklung derartiger Systeme ist durch starke wechselseitige Abhängigkeiten zwischen Produkt und Produktionssystem gekennzeichnet [GF06, S. 18f.]. Denn die Restriktionen der Fertigungstechnologien determinieren in hohem Maße die Produktkonzeption. Umgekehrt wird die Auswahl der einsetzbaren Fertigungstechnologien stark von der Anforderungen an die Produktkonzeption beeinflusst.

Bei der **Klasse 2** geht es um die Verbesserung des kontrollierten Bewegungserhaltens von Mehrkörpersystemen. Hierzu werden Informationen über die Umgebung und das System über Sensoren erfasst und anschließend verarbeitet, woraufhin entsprechende Reaktionen mit Hilfe von Aktoren ausgelöst werden. Derartige Systeme sind in der Lage, auf Veränderungen der Umgebung zu reagieren, kritische Betriebszustände selbständig zu erkennen und Abläufe durch Einsatz von Regelungstechnik zu verbessern [Gau10, S. 18].

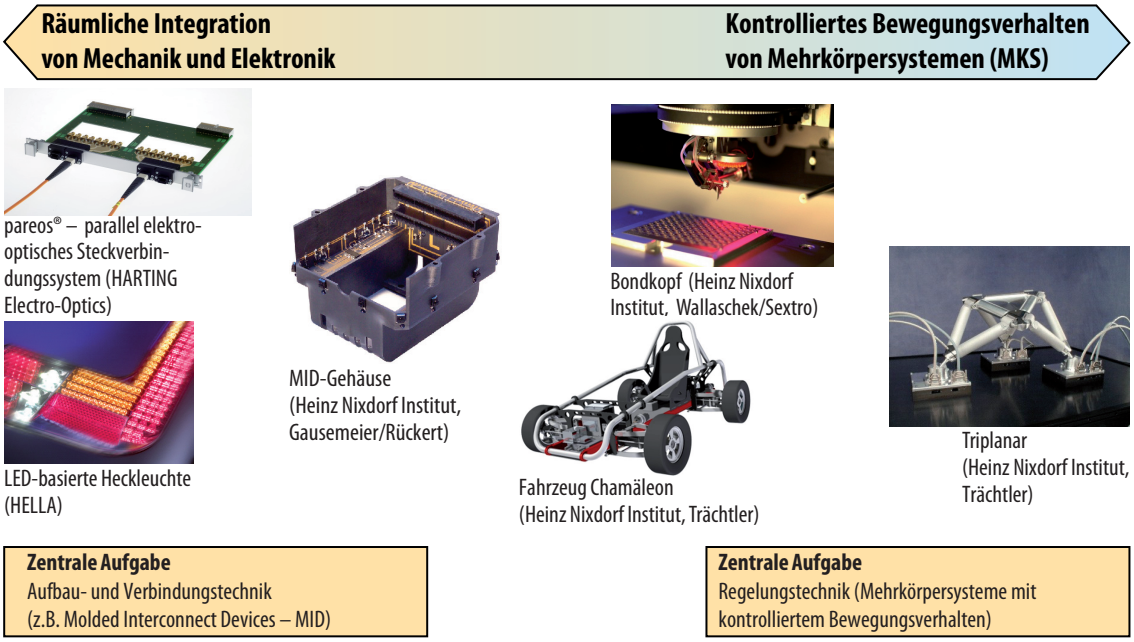


Bild 2-14: Klassen mechatronischer Systeme [Gau10, S. 15]

Beide Klassen mechatronischer Systeme treten oftmals in Kombination auf. Integrierte Systeme der ersten Klasse sind oftmals Bestandteil der Systeme der zweiten Klasse, z.B. in Form von fehlertoleranten Sensoren und Aktoren [Ise07a, S. 177f.]. Den Schwerpunkt der vorliegenden Arbeit stellen Systeme der Klasse 2 dar. Daher werden im Folgenden unter mechatronischen Systemen stets Systeme der Klasse 2 verstanden.

2.2.1.2 Grundsätzlicher Aufbau mechatronischer Systeme

Bild 2-15 stellt den grundsätzlichen Aufbau eines mechatronischen Systems in Anlehnung an die VDI-Richtlinie 2206 schematisch dar [VDI2206, S. 14]. Demnach besteht

ein mechatronisches System typischerweise aus einem Grundsystem, einer Sensorik, einer Aktorik sowie einer Informationsverarbeitung. Diese vier Systembestandteile bilden einen systeminternen Regelkreis[18]. Von Bedeutung ist außerdem die Umgebung, in der das System betrieben wird. Grundsätzlich stehen zwei Schnittstellen nach außen zur Verfügung: Das Kommunikationssystem dient zum Informationsaustausch mit anderen technischen Systemen (z.B. Kommunikationsbusse in einem Kraftfahrzeug über CAN, LIN, MOST etc.). Die Kommunikation mit dem Menschen (Systemanwender) erfolgt über die Mensch-Maschine-Schnittstelle (z.B. Lichtdrehschalter, Head-Up-Display, Bordcomputer in einem Kraftfahrzeug). Die Leistungsversorgung kann extern oder intern (z.B. über eine Lithium-Ionen-Batterie) erfolgen.

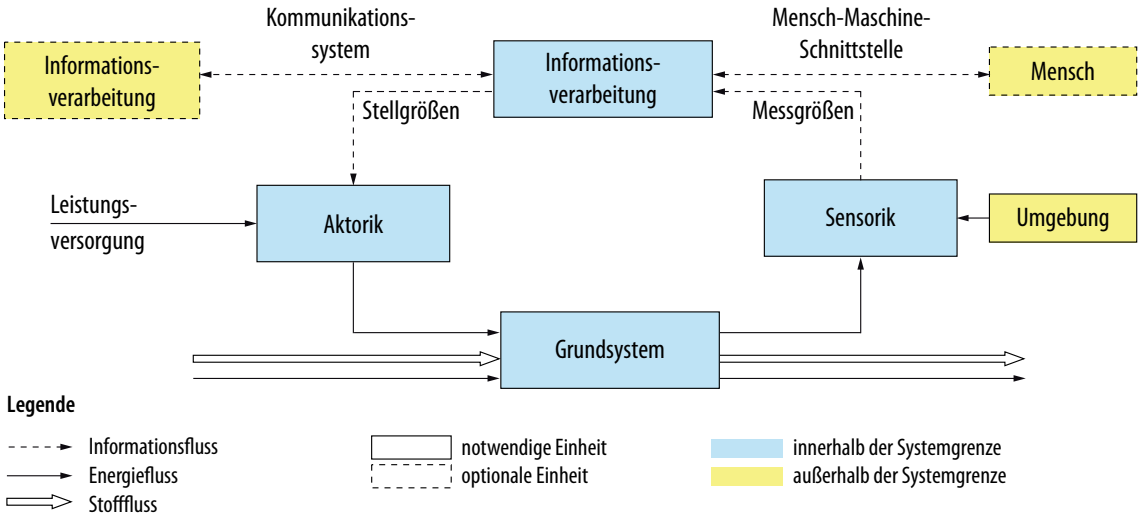


Bild 2-15: Grundstruktur eines mechatronischen Systems [VDI2206, S. 14]

Grundsystem: Das Grundsystem bildet die Grundstruktur eines mechatronischen Systems. Hierbei kann es sich um eine mechanische, hydraulische, pneumatische, elektronische, elektromechanische, magnetische, optische Struktur bzw. deren Kombination handeln [Czi08, S. 1], [VDI2206, S. 10].

Sensorik: Die Sensoren dienen dazu, ausgewählte Zustandsgrößen[19] des Systems sowie äußere Einflüsse aus der Umgebung zu erfassen. Eingang eines Sensors sind nichtelektrische Größen, die als elektrische Größen auf der Ausgangsseite des Sensors ausgegeben werden [Czi08, S. 61 ff.]. Die ermittelten Messwerte werden an die Informationsverarbeitung weitergegeben.

---

[18] Ausgewählte Grundlagen der Regelungstechnik sind in Anhang A1.4 kurz erklärt.

[19] Im Kontext eines technischen Systems sind Zustandsgrößen diejenigen physikalischen Größen, aus denen zu einem gegebenen Zeitpunkt t_0 der Ablauf des Systems für $t > t_0$ eindeutig bestimmt werden kann, sofern die Eingangsgrößen des Systems für $t > t_0$ bekannt sind [DIN60500-341, S. 7ff.].

Aktorik: Die Aufgabe von Aktoren besteht darin, beruhend auf steuerungs- und regelungstechnischen Funktionsprinzipien Bewegungen zu erzeugen, Kräfte auszuüben bzw. mechanische Arbeit zu leisten [Czi08, S. 119 ff.].

Informationsverarbeitung: Die Informationsverarbeitung stellt ein zentrales Element des mechatronischen Regelkreises dar. Sie bestimmt die notwendigen Einwirkungen mit dem Ziel, die Zustandsgrößen des Grundsystems in gewünschter Weise zu beeinflussen [VDI2206, S. 15]. Die Umsetzung dieser Einwirkungen geschieht durch Aktoren direkt am Grundsystem [VDI2206, S. 15]. Neben systemintern ermittelten Informationen werden hierbei auch die systemextern ermittelten Informationen (von anderen technischen Systemen und vom Benutzer) ins Kalkül gezogen.

Die Informationsverarbeitung wird heute in den meisten Fällen mit Hilfe eines Mikroprozessors realisiert [VDI2206, S. 15]. Alle Größen, die als Eingangsgrößen in einem auf einem Mikroprozessor ausgeführten Programm verarbeitet werden, sind zeit- und wertdiskrete (digitale) Signale[20] [SZ13, S. 43]. Im Allgemeinen ist aber auch die Realisierung der Informationsverarbeitung mit Hilfe rein analoger bzw. gemischt analog/digitaler Elektronik möglich [VDI2206, S. 15].

Die Einheiten der in Bild 2-15 dargestellten Grundstruktur eines mechatronischen Systems sind über Flüsse miteinander verbunden. Es werden nach PAHL/BEITZ folgende Flussarten unterschieden [PBF+07, S. 43]:

- **Stoffflüsse:** Diese beschreiben das Fließen von Stoffen wie Gase, Flüssigkeiten, feste Körper, Staub, Material, Behandlungsobjekt, Bauteil etc. [PBF+07, S. 43], [HSM+02]. Stoffflüsse werden oft als Materialflüsse bezeichnet.
- **Energieflüsse:** Es handelt sich um die Beschreibung des Energieumsatzes. Gemeint sind dabei unterschiedliche Energieformen wie mechanische, thermische, elektrische, chemische Energie etc. sowie Kraft, Strom, Wärme [PBF+07, S. 43], [HSM+02].
- **Informationsflüsse:** Diese beschreiben das Fließen von Messgrößen, Statussignalen, Steuerimpulsen, Daten, Informationen etc. [PBF+07, S. 43]. Informationsflüsse können unterschiedlicher Art sein (z.B. haptisch, optisch, akustisch etc.) und auf unterschiedliche Weise übertragen werden (analog bzw. digital). Informationsflüsse werden oft auch als Signalflüsse bezeichnet.

Die in Bild 2-15 dargestellte Grundstruktur eines mechatronischen Systems kann zum Aufbau fraktaler Strukturen herangezogen werden, wodurch sich eine Hierarchisierung

[20] Im Allgemeinen kann zwischen zeit- und wertkontinuierlichen Signalen, zeitdiskreten und wertkontinuierlichen Signalen, zeitkontinuierlichen und wertdiskreten sowie zeit- und wertdiskreten Signalen unterschieden werden. Zeit- und wertdiskrete Signale werden als digitale Signale bezeichnet. Einen detaillierten Überblick hierzu findet der Leser in [SZ13, S. 40 ff.].

ergibt [GEK01, S. 28f.]. So kann zum Beispiel ein Aktor ebenfalls die Grundstruktur eines mechatronischen Systems aufweisen [GEK01, S. 29].

2.2.2 Adaptive Systeme

Die Regelungstechnik nimmt im Kontext mechatronischer Systeme eine zentrale Stellung ein. Bei der Auslegung klassischer Regler wird von exakten Informationen über das Grundsystem ausgegangen [Lun13a, S. 584], [Sch08, S. 323]. Die so entworfenen Regler weisen typischerweise ein zufriedenstellendes Regelverhalten auf, sofern sich die Parameter des Grundsystems nicht ändern [Sch08, S. 323]. In vielen praktischen Anwendungen kann diese Voraussetzung nicht erfüllt werden [Lun13a, S. 584]. Dies trifft zum Beispiel dann zu, wenn der Regler vor Inbetriebnahme des Grundsystems entworfen werden muss oder wenn das Grundsystem keiner genauen theoretischen oder experimentellen Prozessanalyse zugänglich ist [Lun13a, S. 584]. Sobald sich allerdings im Betrieb ein Parameter des Grundsystems ändert, so verschlechtert sich das Regelverhalten, in manchen Fällen sogar bis zur Instabilität[21] des Regelkreises. In diesem Fall ist es notwendig, die Reglerparameter im jeweiligen Betriebszustand (Arbeitspunkt) an die sich verändernden Parameter des Grundsystems anzupassen [Sch08, S. 323].

Beispiel – Lageregelung eines Flugzeugs [Sch08, S. 323]: Die Parameter Flugzeuglängs- und Seitenbewegung des Grundsystems hängen von seinem jeweiligen Betriebszustand ab, der durch die zwei Größen Flughöhe h(t) und Geschwindigkeit v(t) charakterisiert ist. Für einen Flug mit Autopilot gilt, dass die Reglerparameter jeweils an den jeweiligen Betriebszustand (h(t) und v(t)) adaptiv anzupassen sind, damit ein gutes Regelverhalten erreicht werden kann.

Eine derartige Parameteranpassung kann mit sogenannten adaptiven Reglern erreicht werden, welche über klassische Regler hinausgehen. Bei adaptiven Reglern wird für den Entwurf kein möglichst genaues Modell des Grundsystems und dessen Parameter vorausgesetzt [Lun13b, 544]. Vielmehr ist der Regler in der Lage, das Regelverhalten an die Änderungen der Prozessdynamik und der Störgrößen anzupassen [AW95, S. 1]. Nach ÅSTRÖM/WITTENMARK ist ein adaptiver Regler „ein Regler mit verstellbaren Parametern und einem Mechanismus für Verstellung dieser Parameter“ [AW95, S. 1].

Bild 2-16 stellt die Grundstruktur einer adaptiven Regelung dar. Demnach besteht eine adaptive Regelung aus zwei Schleifen. Neben der bereits aus klassischen Regelungen bekannten Rückführschleife lässt sich eine weitere Schleife zur Anpassung der Reglerparameter erkennen [Sch08, S. 324]. Adaptive Regler werden in einer Vielzahl von Publikationen behandelt, siehe z.B. [Lun13a], [Sch08], [Ise08].

---

[21] Ein Regelkreis ist stabil, wenn jede beschränkte Eingangsgröße (Führungsgröße w(t) bzw. Störgröße z(t)) zu einer beschränkten Regelgröße x(t) führt. Es gilt $|w(t)| < \infty \; bzw. |z(t)| < \infty \Rightarrow |x(t)| < \infty$ [Trö05,S. 291].

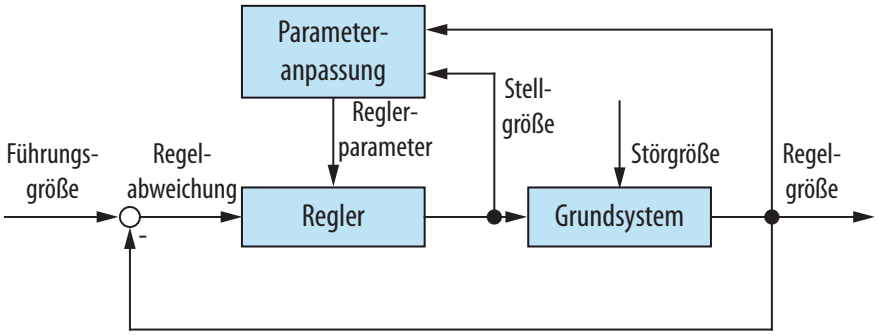


Bild 2-16: Grundstruktur einer adaptiven Regelung [AW95, S. 2], [Sch08, S. 324]

Zusammenfassend lässt sich die prinzipielle Wirkungsweise einer adaptiven Regelung als ein Prozess mit folgenden drei wesentlichen Phasen beschreiben [Lun13a, S. 584f.]:

1) **Identifikation:** Hier wird das gegenwärtige dynamische Verhalten des Grundsystems ermittelt.

2) **Festlegung der Reglerparameter:** Hier wird die Festlegung der Reglerparameter in Abhängigkeit von der ermittelten Änderung im dynamischen Verhalten des Grundsystems vorgenommen.

3) **Anpassung der Reglerparameter:** Die Reglerparameter werden den sich zeitlich verändernden Eigenschaften des Grundsystems nachgeführt.

Zusammenfassend lässt sich festhalten, dass adaptive Systeme eine Erweiterung klassischer geregelter mechatronischer Systeme sind. Kern der Erweiterung besteht in einer übergeordneten adaptiven Regelung, die eine Anpassung und Verbesserung des Regelverhaltens an die Änderungen der Prozessdynamik und der Störgrößen ermöglicht. Dadurch können die Funktionalität, Sicherheit und Zuverlässigkeit verbessert werden. Die Festlegung der zugrunde liegenden Zielgrößen erfolgt bereits beim Reglerentwurf; eine Änderung dieser durch das System im Betrieb ist nicht vorgesehen.

2.2.3 Selbstoptimierende Systeme

Der anhaltende rasche Fortschritt der Informations- und Kommunikationstechnik und die damit einhergehende Zunahme an Rechen-, Erfassungs-, Übertragungs- und Speicherkapazität ermöglichen bereits heute fortschrittliche mechatronische Systeme, die mit inhärenter Teilintelligenz ausgestattet sind. Im Sonderforschungsbereich (SFB) 614 werden derartige Systeme als selbstoptimierende (s.o.) Systeme bezeichnet. Der in diesem Zusammenhang zentrale Begriff der Selbstoptimierung wird dabei wie folgt definiert:

> *„Unter **Selbstoptimierung** (self-optimization) eines technischen Systems wird die endogene Anpassung der Ziele des Systems auf veränderte Einflüsse und die daraus resultierende zielkonforme autonome Anpassung der Parameter und ggf. der Struktur und somit des Verhaltens dieser Systeme verstanden. Damit geht Selbstoptimierung über die*

bekannten Regel- und Adaptionsstrategien wesentlich hinaus; Selbstoptimierung ermöglicht handlungsfähige Systeme mit inhärenter „Teilintelligenz", die in der Lage sind, selbständig und flexibel auf veränderte Betriebsbedingungen zu reagieren" [ADG+09, S. 5].

S.o. Systeme verfügen also über die Fähigkeit, ihr Systemverhalten während des Betriebs an veränderte Betriebsbedingungen autonom und flexibel anzupassen. Dazu müssen diese Systeme in der Lage sein, ihre Ziele während des Betriebs selbständig zu verändern und darauf folgend eine zielkonforme Verhaltensanpassung zu vollziehen. Die hierfür wesentlichen Aspekte eines s.o. Systems sowie deren Zusammenwirken zeigt Bild 2-17.

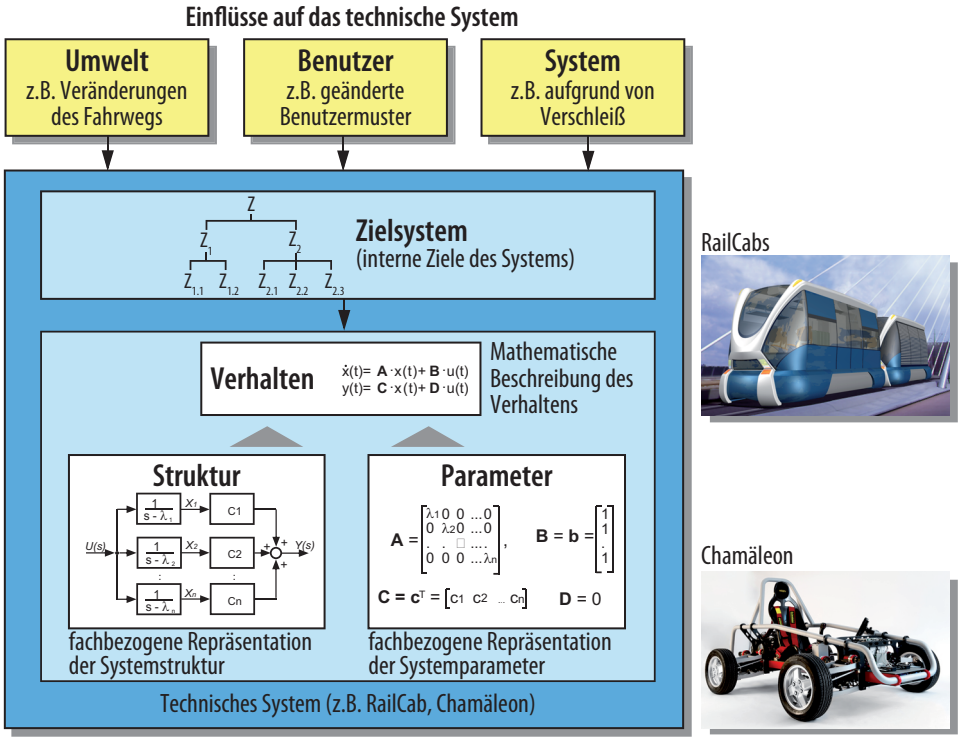


Bild 2-17: Aspekte eines s.o. Systems: Einflüsse auf das System bewirken eine Veränderung der Ziele und eine entsprechende Anpassung des Systemverhaltens (in Anlehnung an [GFD+08, S. 61])

S.o. Systeme beruhen auf der Mechatronik und sind somit technische Systeme. Auf ein s.o. System wirken verschiedene Einflüsse. Quellen dieser Einflüsse sind in der Regel die Umwelt, der Benutzer, andere technische Systeme sowie das System selbst.

Im Kontext eines s.o. Systems ist der Begriff eines Ziels von herausragender Bedeutung. **Ziele** beschreiben die geforderten, gewünschten sowie die zu vermeidenden Systemeigenschaften. Sie werden bereits im Zuge der Entwicklung definiert und in der Anforderungsliste abgebildet [PGD12]. Die Auswahl und Priorisierung der zu verfolgenden Ziele erfolgt durch das s.o. System während seines Betriebs. Es wird zwischen internen, inhärenten und externen Zielen unterschieden. **Externe Ziele** haben ihren Ursprung außerhalb

der Systemgrenze; sie werden an das System durch andere Systeme bzw. durch den Benutzer herangetragen (z.B. „Benutzerzufriedenheit maximieren“). **Inhärente Ziele** beschreiben Forderungen an Eigenschaften und Verhalten des Systems, die bereits während der Entwicklung bestehen und durch das s.o. System zu erreichen und zu verbessern sind. Beispiele inhärenter Ziele eines innovativen Schienenfahrzeugs sind „Verlässlichkeit maximieren“ und „Energiebedarf minimieren“. Ziele weisen typischerweise eine hierarchische Struktur auf. Sie werden durch untergeordnete Ziele verfeinert. Zum Beispiel ist „Sicherheit maximieren” ein potentielles Unterziel des Ziels „Verlässlichkeit maximieren”. Mögliche Unterziele des Ziels „Benutzerzufriedenheit maximieren“ sind „Fahrkomfort maximieren“ und „Reisezeit minimieren“. Im Betrieb wählt das s.o. System in Abhängigkeit von der vorherrschenden Situation die zu verfolgenden (inhärenten und externen) Ziele kontinuierlich aus und priorisiert diese. Die zu einem bestimmten Zeitpunkt durch das s.o. System verfolgten Ziele werden als **interne Ziele** bezeichnet. “Fahrkomfort maximieren” und “Sicherheit maximieren” sind Beispiele derartiger interner Ziele. Interne Ziele sind Basis für die Selbstoptimierung.

Die durch das System ausgewählten, zu verfolgenden Ziele können gegenläufig sein. Dies bedeutet, dass die jeweiligen Ziele in gewissen Situationen nicht alle gleichzeitig in vollem Umfang verfolgt werden können. Es wird in diesem Zusammenhang von einem **Zielkonflikt** gesprochen. Beispiel: im Zuge der Anpassung der Fahrgeschwindigkeit sind die Ziele „Fahrgeschwindigkeit maximieren“ und „Energiebedarf minimieren“ gegenläufig, da der Energiebedarf typischerweise mit steigender Fahrgeschwindigkeit ebenfalls zunimmt. Im Falle eines derartigen Zielkonflikts muss eine Priorisierung der Ziele vorgenommen werden. Das Vorhandensein von Zielkonflikten ist ein wesentliches Indiz für die Notwendigkeit des Einsatzes der Selbstoptimierung.

Die Auswahl und Priorisierung von Zielen führt zu einer zielkonformen Anpassung des Verhaltens des s.o. Systems. Diese Verhaltensanpassung kann, wie in Bild 2-18 dargestellt, auf folgende zwei Arten erfolgen [GFD+08, S. 61]:

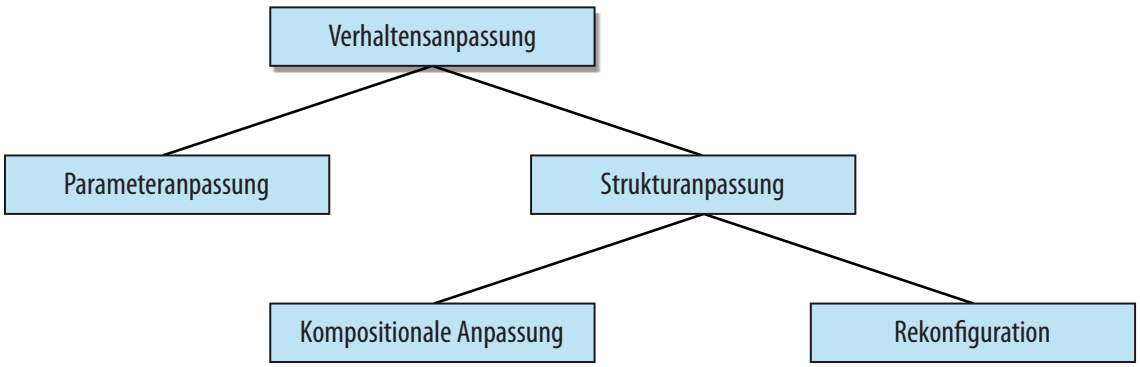


Bild 2-18: Möglichkeiten von Verhaltensanpassungen [ADG+09, S. 7]

- **Parameteranpassung:** Es handelt sich um die Anpassung eines Systemparameters (z.B. Änderung eines Reglerparameters).

- **Strukturanpassung:** Gemeint ist eine Änderung der Anordnung und der Beziehungen zwischen den Elementen eines Systems. Hierbei wird zwischen einer Rekonfiguration und einer kompositionalen Anpassung unterschieden. Bei der **Rekonfiguration** werden „die Beziehungen einer festen Menge von verfügbaren Elementen verändert“ [GFD+08, S. 61]. Bei der **kompositionalen Anpassung** werden „neue Elemente in die bisherige Struktur integriert bzw. Elemente aus der Struktur herausgenommen“ [GFD+08, S. 61].

Aus der vorhergehenden Beschreibung lässt sich ein grundsätzlicher Ablauf erkennen, der dem Anpassungsverhalten eines s.o. Systems zugrunde liegt. Dieser als **Selbstoptimierungsprozess** bezeichnete Ablauf umfasst folgende drei aufeinander folgende Phasen [ADG+09, S. 6], [GFD+08, S. 61]:

1) **Analyse der Ist-Situation (Situationsanalyse):** Hier werden der Zustand des Systems (Gesamtheit der Zustandsgrößen des Systems und deren gegenwärtigen Werte) sowie alle durchgeführten Beobachtungen über seine Umgebung analysiert. Diese Beobachtungen können sowohl direkt über Sensoren als auch indirekt über Kommunikation mit anderen Systemen gewonnen werden. Weiterhin kann auf eventuell vorliegende Aufzeichnungen zurückliegender Systemzustände und Umgebungsbeobachtungen zurückgegriffen werden, was eine intelligente und lernende Verhaltensanpassung fördert. Ein wesentlicher Aspekt der Situationsanalyse besteht in der Prüfung, ob die zum Zeitpunkt der Situationsanalyse verfolgten Ziele für die gegenwärtige Situation nach wie vor angebracht sind.

2) **Bestimmung der Systemziele (Zielbestimmung):** Bei der Bestimmung der zu verfolgenden Ziele wird auf den aus der Situationsanalyse gewonnenen Erkenntnissen aufgebaut. Die Zielbestimmung kann hierbei durch Auswahl, Anpassung oder Generierung von Zielen erfolgen [GFD+08, S. 61]. Bei der Auswahl wird eine Alternative aus einer fest vorgegebenen, endlichen Menge von möglichen Zielen ausgewählt. Unter einer Anpassung ist „die graduelle Veränderung bestehender Ziele“ zu verstehen [GFD+08, S. 61]. Bei einer Generierung werden die neuen Ziele unabhängig von den bisher bekannten neu erzeugt.

3) **Anpassung des Systemverhaltens (Verhaltensanpassung):** Die Bestimmung der neuen zu verfolgenden Ziele erfordert eine zielkonforme Anpassung des Systemverhaltens. Wie zuvor beschrieben, kann dies durch Parameteranpassung und, wo dies nicht hinreichend ist, durch Strukturanpassung geschehen. Die Umsetzung der Verhaltensanpassung erfolgt über die Aktorik am Grundsystem, was den Selbstoptimierungskreislauf schließt.

Kern der Selbstoptimierung besteht also in der endogenen Anpassung der Systemziele an veränderte Einflüsse und die damit einhergehende zielkonforme Verhaltensanpassung, womit die Selbstoptimierung wesentlich über die klassischen Regel- und Adaptionsstrategien hinaus geht [GFD+08, S. 61]. Gemäß Bild 2-19 ist die Selbstoptimierung als eine

Erweiterung der klassischen und der adaptiven Regelung zu verstehen. Die klassische Regelung ermöglicht ein in Bezug auf bekannte Einflüsse robustes System. Eine Verbesserung des Systemverhaltens bei sich ändernden Einflüssen, aber festen Zielen kann mittels einer adaptiven Regelung erreicht werden. Sind Veränderungen der Ziele während des Systembetriebs ins Kalkül zu ziehen, so bietet sich die Umsetzung einer selbstoptimierenden Regelung an [ADG+09, S. 27f.].

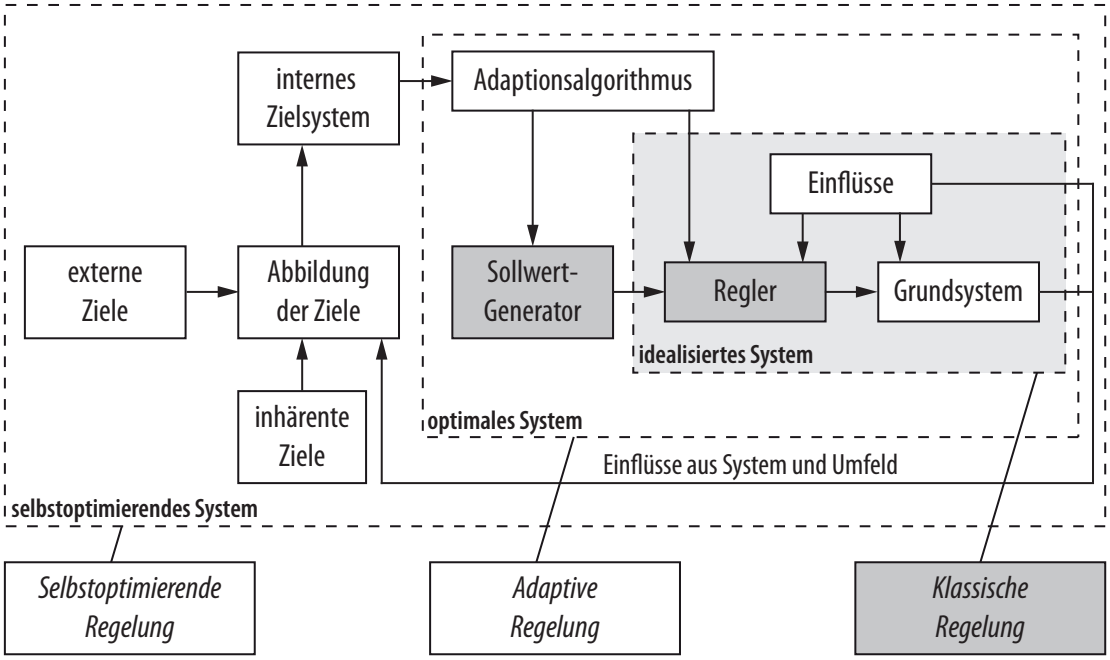


Bild 2-19: Erweiterung klassischer und adaptiver Regelungen zur selbstoptimierenden Regelung [ADG+09, S. 27], [BSK+06]

Für die Realisierung des Wirkparadigmas der Selbstoptimierung in der Informationsverarbeitung ist ein geeignetes **Architekturkonzept für die Informationsverarbeitung** essentiell. Für diesen Zweck wurde die OCM-Architektur (Operator-Controller-Modul) entwickelt [Nau00], [ADG+09, S. 13ff.]. Diese gliedert sich entsprechend Bild 2-20 in folgende drei Ebenen:

- **Controller:** Es handelt sich um die unterste Ebene der OCM-Architektur. Hier werden die regelungstechnischen Anteile der Informationsverarbeitung umgesetzt: das dynamische Verhalten des Grundsystems wird derart beeinflusst, dass die gewünschte Dynamik erreicht wird. Für diesen Zweck verarbeitet der Controller in direkter Wirkkette die Messsignale, ermittelt die Stellsignale und gibt diese aus. Daher wird er als motorischer Kreis bezeichnet. Die Software auf dieser Ebene arbeitet quasi-kontinuierlich und muss harten Echtzeitbedingungen genügen. Ähnlich wie im mechatronischen Regelkreis stellen die Sensorik und die Aktorik hier die Schnittstellen zum Grundsystem dar.

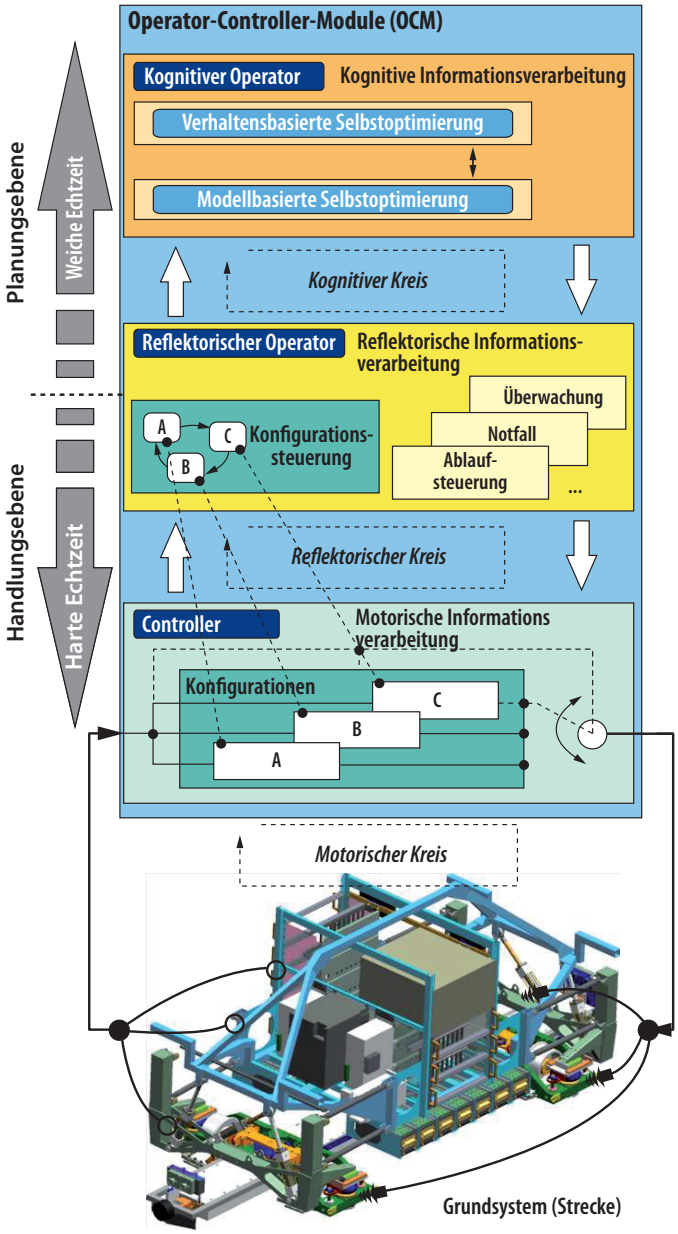


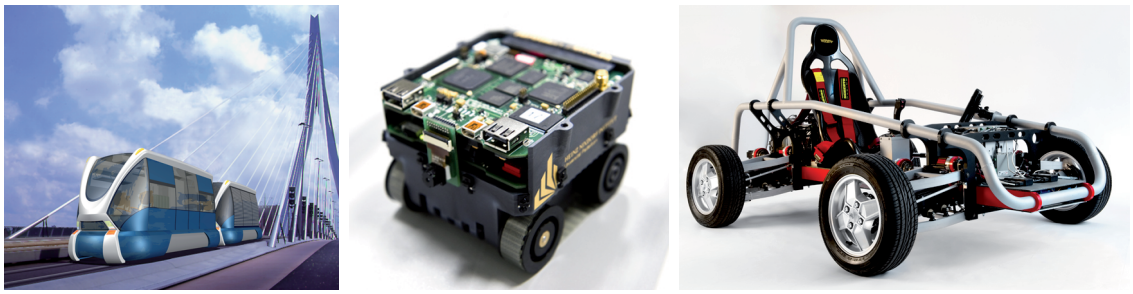
Bild 2-20: Die Operator-Controller-Modul-(OCM)-Architektur [ADG+09, S. 14]

- **Reflektorischer Operator:** Die Aufgabe dieser Ebene besteht in der Überwachung und Steuerung des Controllers. Zur Anpassung des Systemverhaltens greift der reflektorische Operator nicht direkt auf die Aktorik des Systems zu, sondern modifiziert hierzu den Controller. Die Modifikation des Controllers erfolgt, indem Parameter- oder Strukturänderungen initiiert werden. Kern der Strukturänderung bildet dabei die Konfigurationssteuerung des reflektorischen Operators, die zwischen Konfigurationen im Controller umschalten kann. Darüber hinaus erbringt die reflektorische Ebene Hilfsfunktionen wie Ablaufsteuerung, Überwachungs- und Notfallprozesse. Der reflektorische Operator arbeitet überwiegend ereignisorientiert. Aufgrund der engen Verknüpfung mit dem Controller muss der reflektorische Operator ebenso harten Echtzeitbedingungen genügen. Als Verbindungselement zur kognitiven Ebene des OCM bildet der reflektorische Operator ferner eine Schnittstelle zwischen den nicht

echtzeitfähigen bzw. in weicher Echtzeit arbeitenden Elementen der Informationsverarbeitung und dem Controller.

- **Kognitiver Operator:** Es handelt sich um die oberste Ebene des OCM. Der kognitive Operator sammelt und nutzt das Wissen über das System und dessen Umgebung zur Verbesserung des Systemverhaltens. Für diesen Zweck werden Methoden wie Lernverfahren, modellbasierte Optimierungsverfahren und wissensbasierte Systeme verwendet. Im Mittelpunkt stehen hier kognitive Fähigkeiten zur Realisierung der Selbstoptimierung entlang des Selbstoptimierungsprozesses. Der kognitive Operator arbeitet dabei in weicher Echtzeit.

Im SFB 614 wurden drei Demonstratoren zur Erprobung der darin entwickelten Methoden, Vorgehensmodelle und Werkzeuge entwickelt. Diese in Bild 2-21 dargestellten Demonstratoren sind: das autonome Schienenfahrzeug RailCab, der autonome Miniaturroboter BeBot und das vollelektrische X-by-Wire-Versuchsfahrzeug Chamäleon:



Schienenfahrzeug RailCab Miniaturroboter BeBot X-by-Wire-Versuchsfahrzeug Chamäleon

Bild 2-21: Demonstratoren des SFB 614

Im SFB 614 wird das Vorhaben „Neue Bahntechnik Paderborn/RailCab“ als Demonstrator verwendet. Kern sind autonome Schienenfahrzeuge (**RailCab**s) für den Personen- und Gütertransport, die nach Bedarf und nicht nach Fahrplan fahren [ADG+09, S. 29ff.], [NBP14-ol]. Sie handeln proaktiv. Beispielsweise bilden sie Konvois, um den Energiebedarf zu reduzieren. Der Antrieb erfolgt berührungslos mit Hilfe eines doppelt gespeisten elektromagnetischen Linearantriebs. Das Tragen und Führen erfolgt über einen Rad-Schiene-Kontakt; bestehende Trassen können genutzt werden. Dank einer aktiven Spurführung erfolgt die Richtungswahl der Fahrzeuge beim Überfahren von Weichen fahrzeugseitig. Eine aktive Federungs- und Neigetechnik führt zu einem hohen Fahrkomfort. Die wesentliche Technik der Fahrzeuge ist in der flach bauenden Bodengruppe untergebracht, auf der die Nutzlastzellen für den Personen- und Gütertransport aufsetzen.

Der autonome Miniaturroboter **BeBot** dient als Basissystem für die Forschung in den Bereichen dynamisch rekonfigurierbarer Systeme, Multi-Agenten-Systeme sowie Schwarmintelligenz [ADG+09, S. 108f.]. Basis für die Umsetzung der Selbstoptimierung sind insbesondere die im BeBot zum Einsatz kommenden leistungsstarken Mikrocontroller [ADG+09, S. 108]. Ferner werden verschiedene Funkstandards zur Kommunikation unterstützt, wodurch insbesondere Vernetzungsfähigkeit mit anderen Miniaturrobotern und

damit einhergehend Multiroboterszenarien ermöglicht werden [ADG+09, S. 109]. Eines der realisierten Szenarien ist ein robustes, mobiles Ad-hoc-Kommunikationsnetzwerk, das aus mehreren BeBots besteht. Die Gruppe der BeBots agiert hier gemeinsam [ADG+09, S. 108]. Ein weiteres Szenario ist die Kooperation in einem heterogenen Roboterteam, das sich aus BeBots und anderen Robotern zusammensetzt [ADG+09, S. 108]. Der Miniaturroboter BeBot ist ferner Versuchsträger für die Technologie MID, mit der hohe Funktionsintegration auf kleinem Raum realisiert wird [ADG+09, S. 109].

Das **Chamäleon** ist ein vollaktives mechatronisches Versuchsfahrzeug. Es wird komplett by-wire gesteuert: die wesentlichen Funktionen wie das Antreiben, Bremsen, Lenken und Federn und Dämpfen werden ausschließlich elektrisch aktuiert. Eine mechanische Rückfallebene im Sinne einer mechanischen Kopplung zwischen dem Bedienelement und der Aktorik ist nicht vorhanden. Ziel im Kontext des SFB 614 ist eine selbstoptimierende Fahrzeugregelung hinsichtlich der Vertikal- und Längsdynamik, des Energiemanagements sowie der Rekonfiguration der Fahrwerksaktorik [SFB11, S. 4]. In diesem Zusammenhang werden neuartige Lenk-, Brems- sowie Rekonfigurationsstrategien entwickelt, simuliert und validiert [RNJ+09], [NJT08], [ADG+09], [GRS14].

Die im Rahmen der vorliegenden Arbeit zu erstellende Systematik wird am Chamäleon (vgl. Kapitel 5) sowie an Teilsystemen des RailCabs validiert (vgl. Kapitel 4).

2.2.4 Zuverlässigkeit und Sicherheit mechatronischer Systeme

Mechatronische Systeme ersetzen bzw. ergänzen häufig rein mechanische, hydraulische, pneumatische und elektrische Systeme, welche für sich alleine ein gutes Ausfallverhalten haben [Ise07a, S. 171]. Dies gilt insbesondere für mechanische Systemelemente: aus heutiger Sicht kann eine hohe Zuverlässigkeit der Mechanik durch geeignete Werkstoffauswahl, Auswahl von Fertigungsverfahren, Überdimensionierung etc. erreicht werden [Ise07a, S. 171]. Die Hinzunahme von Sensoren, Aktoren, elektronischer Hardware und Informationsverarbeitung führt zum veränderten Ausfallverhalten. In hohem Maße herausfordernd ist insbesondere die Absicherung der Zuverlässigkeit und Sicherheit von elektronischen und elektromechanischen Systemelementen. Denn diese bestehen aus vielen Einzelkomponenten, die unerwartet und plötzlich ausfallen können [Ise07a, S. 171]. Erschwerend kommt hinzu, dass derartige Systemelemente einem großen Einfluss der Umweltfaktoren wie etwa Temperatur, Korrosion und EMV unterliegen [Ise07a, S. 172].

Im Folgenden wird in Anlehnung an ISERMANN [Ise07a, S. 171 f.] auf das für die Systemelemente der Fachdisziplinen der Mechatronik typische Ausfallverhalten eingegangen: **Elektronische Hardware** kann systematisches oder zufälliges Ausfallverhalten aufweisen. Systematische Fehler lassen sich auf Spezifikations- bzw. Entwurfsfehler zurückführen. Zufälliges Ausfallverhalten elektronischer Hardware tritt im Betrieb in Erscheinung, und zwar mit allen Arten von zeitlichem Verhalten (dauernd, transient, zufällig, driftförmig etc.). Ausfälle der **Software** sind systematisch und haben ihre Ursache in falscher

Spezifikation, fehlerhaftem Entwurf, Programmierfehlern, Zahlenüberläufen, Typkonversionsfehlern etc. Ausfälle eines **mechanischen Systemelements** lassen sich in die Kategorien Überlastung, Ermüdung, Abnutzung oder Korrosion klassifizieren [Ise07a, S. 171]. Diese treten als Drift (z.B. Änderungen – Abnutzung, Korrosion) oder abrupt (z.B. Bruch) zu einem zufälligen Zeitpunkt bzw. nach einer hohen Beanspruchung auf. **Elektrische Systemelemente** wie Widerstände, Transistoren, Kondensatoren etc. können unterschiedliche Fehlzustände einnehmen wie z.B. Kurzschluss, lose oder gebrochene Verbindungen, Eigenschaftsänderungen (Drift) [Bir07, S. 100]. Mögliche Quellen von Fehlzuständen sind Verschmutzung, Korrosion, Probleme in Bezug auf elektromagnetische Verträglichkeit (EMV) etc. Generell sind elektrische Fehler mehr zufällig als mechanische [Ise07a, S. 171]. Tabelle 2-4 zeigt die typischen Ausfallraten mechatronischer Systemelemente.

Tabelle 2-4: Typische Ausfallraten mechatronischer Systemelemente [Ise07a, S. 172]

mechanisch	λ [h^{-1}]	elektromechanisch	λ [h^{-1}]	elektronisch	λ [h^{-1}]
Kugellager	$1{,}6 \cdot 10^{-6}$	Aktor	$26 \cdot 10^{-6}$	Transistor	$1 - 70 \cdot 10^{-6}$
Getriebe	$4{,}7 \cdot 10^{-6}$	Elektromotor	$9 \cdot 10^{-6}$	Operationsverstärker	$0{,}5 \cdot 10^{-6}$
Pumpe	$4{,}4 \cdot 10^{-6}$	Kabel	10^{-6}	Analoger Schalter	$20 \cdot 10^{-6}$
Ventil, hydraulisch	$8{,}8 \cdot 10^{-6}$	Regler	$13 \cdot 10^{-6}$	CPU / 8 bit	$5 \cdot 10^{-6}$

Vermeidung des Ausfalls eines mechatronischen Systemelements kann prinzipiell auf zwei Weisen erreicht werden. Eine Möglichkeit zur Verbesserung des Ausfallverhaltens stellt die Perfektion dar (z.B. Überdimensionierung, sorgfältige Prüfung). Derartige Maßnahmen sind jedoch nur in einem begrenzten Umfang möglich und wirtschaftlich sinnvoll. Eine weitere Möglichkeit stellt die Fehlertoleranz bzw. Redundanz dar (vgl. auch Abschnitt 2.1.3). Bei sicherheitsrelevanten X-by-Wire-Systemen wie z.B. Flugzeuge ist der Einsatz der Fehlertoleranz unerlässlich [Ise07a, S. 171].

Ausgewählte Maßnahmen zur Verbesserung der Zuverlässigkeit der Systemelemente aus verschiedenen mechatronischen Fachdisziplinen sind in Tabelle 2-5 zusammengefasst. Demnach lassen sich mechanische, hydraulische und einige elektrische Systemelemente durch Überdimensionierung, Wartung, Schutzmaßnahmen und Verschleißreduzierung hinsichtlich ihrer Zuverlässigkeit verbessern. Für elektronische Hardware sowie einige elektrische Systemelemente wird eine Verbesserung der Zuverlässigkeit durch Überdimensionierung, Schutzmaßnahmen und Redundanz erzielt, für Software durch Pflege (Wartung) sowie diversitäre Redundanz [Ise07a].

2.3 Mögliche Negativfolgen für Unternehmen bei Nichterreichung von Zuverlässigkeit bzw. Sicherheit

Die Nichterreichung der Zuverlässigkeits- bzw. Sicherheitsziele kann für ein Unternehmen weitgreifende Verluste zur Folge haben. Wie in Bild 2-22 dargestellt, können diese

Folgen wirtschaftlicher sowie rechtlicher Natur sein. Im Folgenden werden beide Arten detaillierter erklärt. Insbesondere erfolgt eine Darstellung einschlägiger Beispiele.

Tabelle 2-5: Maßnahmen zur Verbesserung der Zuverlässigkeit und Sicherheit von Systemelementen [Ise07a, S. 173] (in Anlehnung an [SAE ARP926])

Maßnahme	Systemelemente				
	mechanisch	hydraulisch	elektrisch	elektron. HW	Software
Überdimensionierung	⊕⊕	⊕	⊕	⊕	○
Wartung	⊕⊕	⊕⊕	⊕	○	⊕
Schutzmaßnahmen	⊕⊕	⊕⊕	⊕	⊕⊕	○
Verschleißreduzierung	⊕⊕	⊕	⊕	○	○
Redundanz	○	⊕	⊕	⊕⊕	⊕
• statisch	○	⊕	⊕	⊕⊕	○
• dynamisch	○	○	⊕	⊕⊕	⊕
• diversitär	○	○	○	⊕⊕	⊕⊕

Legende ⊕⊕ sehr großes Potential ⊕ großes Potential ○ kleines Potential bzw. nicht anwendbar

2.3.1 Wirtschaftliche Folgen

Das Nichterreichen der Zuverlässigkeits- bzw. Sicherheitsziele kann wirtschaftliche Verluste nach sich ziehen. Dies betrifft insbesondere den Fall, wenn ein Produkt aufgrund der Zuverlässigkeits- bzw. Sicherheitsprobleme zurückgerufen werden muss. Rückrufe werden von Herstellern durchgeführt, um Produktmängel zu beseitigen. Dabei ist Rückruf nicht gleich Rückruf, da Produktmängel zu ganz unterschiedlichen Gefährdungen führen können [KBA13-ol]. Handelt es sich um Produktmängel, die gravierende Folgen haben können, bzw. ist die Anzahl betroffener Produkte groß, so haben derartige Produktrückrufe typischerweise Einbußen am Umsatz, Marktstellung sowie Imageschäden zur Folge. Beispiel – Toyota: Ende 2009 gab es eine Massenrückrufaktion wegen ungewollter Beschleunigung in den USA, die auf ein Verhaken des Gaspedals mit der nicht ausreichend befestigten Fußmatte zurückzuführen war [Spi09-ol]. Insgesamt rief Toyota zu dieser Zeit weltweit fast neun Millionen Autos in die Werkstätten [Spi12b-ol]. In der Folgezeit stieg die Zahl der zurückgerufenen Fahrzeuge sogar auf 12 Millionen [Spi12b-ol]. Der Rechtsstreit endete Ende 2012 mit einem Vergleich: US-Kunden erhielten in diesem Zusammenhang insgesamt 1,1 Milliarden Dollar Entschädigung [Spi12b-ol]. Kurz danach folgte Anfang 2010 ein Toyota-Rückruf in Europa. Es ging darum, dass unter bestimmten Umständen das Gaspedal nicht mit gewohnter Geschwindigkeit in seine Ausgangslage zurückkehrte bzw. gar in der getretenen Position verblieb, was aber nicht im Zusammenhang mit dem Fußmatten-Problem stand [Toy10-ol]. Dem Ansehen von

Toyota schadeten die Rückrufe massiv [Spi12b-ol]. Seither ist Toyota sehr sensibel bei Fehlern, es wurden bereits mehrfach freiwillig Rückrufe gestartet [Spi12b-ol], [Spi12a-ol].

Selbstredend ist in der Automobilbranche nicht nur Toyota betroffen, sondern auch weitere Automobilhersteller wie Honda, Volkswagen und GM – um nur einige zu nennen [Spi10-ol], [Han13-ol]. 2013 musste Volkswagen wegen Problemen bei seinen Doppelkupplungsgetriebe eine halbe Million Fahrzeuge in die Werkstätten zurückordern: Im Frühling 2013 wurden in China 384 000 Fahrzeuge für Reparaturen zurückgeordert, Anfang Mai 2013 folgte Japan mit 91 000 Autos und im Juni Australien mit weiteren 26 000 Wagen [Han13-ol], [Süd13-ol]. Auslöser der Probleme: „Kombination aus feucht-heißem Klima und häufiger Belastung im kriechenden Verkehr, etwa im Stop-and-Go verstopfter Innenstädte“ [Süd13-ol].

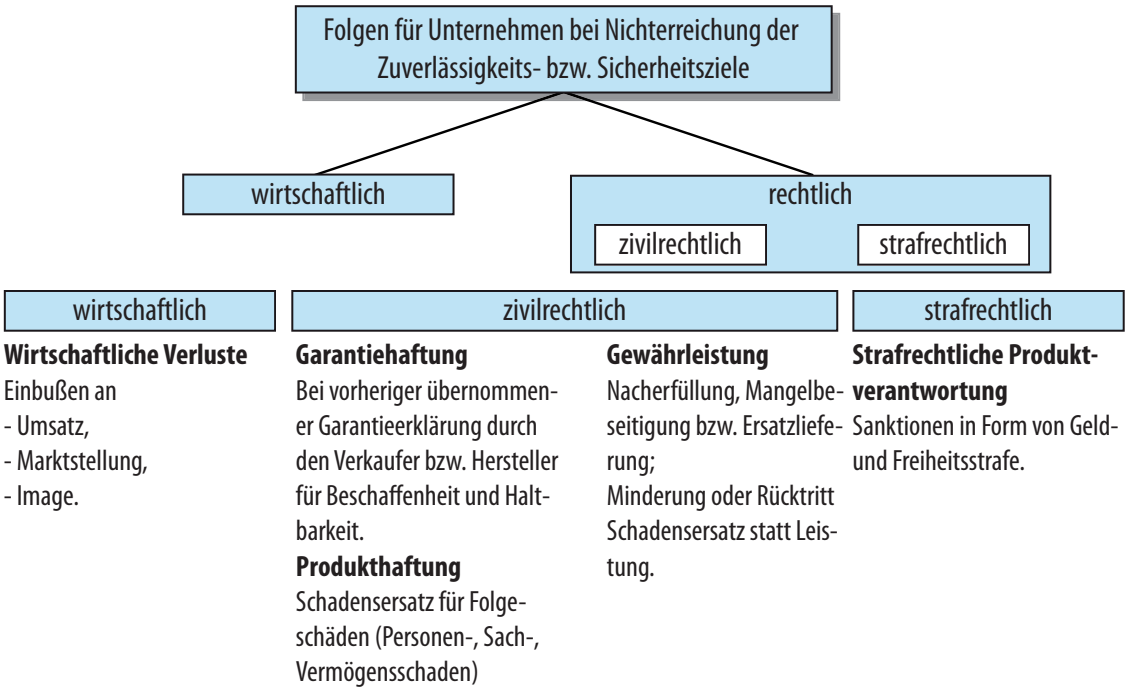


Bild 2-22: Mögliche Negativfolgen der Nichterreichung der Zuverlässigkeits- bzw. Sicherheitsziele für ein Unternehmen (in Anlehnung an [RLH96])

Weitere Beispiele aus der jüngsten Zeit: Toyota-Massenrückruf (Airbag löst falsch aus, Okt. 2013), Toyota – Rückruf von Minivans in Nordamerika (Autos können wegrollen, September 2013), Toyota – Rückruf für Toyota Prius (Materialermüdung an den Bremsen, Juni 2013), Nissan-Massenrückruf (Loses Lenkrad, Mai 2013), Nissan-Massenrückruf (Fehlerhafte Sensoren am Gaspedal, September 2013), Massenrückrufe durch GM (ab März 2014) [Aut13b-ol], [Foc13-ol], [Aut13a-ol], [Spi13a-ol], [Spi13b-ol], [Tag14].

Die Entwicklung der Anzahl der durch das Kraftfahrt-Bundesamt eingeleiteten Rückrufaktionen in den Jahren 1998 bis 2012 wurde bereits in Abschnitt 1.1 erläutert (vgl. auch

Bild 1-1). Insgesamt hat sich seit 1998 die Anzahl der Rückrufe mehr als verdreifacht und bleibt seit 2010 auf einem hohen Niveau.

2.3.2 Rechtliche Folgen

Die rechtlichen Folgen können zivilrechtlicher und strafrechtlicher Natur sein. Bei zivilrechtlichen Folgen kann zwischen Garantiehaftung, Gewährleistung und Produkthaftung unterschieden werden.

Im Zusammenhang mit Absicherung der Zuverlässigkeit und Sicherheit technischer Systeme ist die gesetzliche Produkthaftung von herausragender Bedeutung. Die gesetzliche Produkthaftung ist „die Haftung gegenüber Dritten“ [Mey11, S. 41]: Wer ein Produkt herstellt bzw. importiert und es in den Verkehr bringt ist dazu verpflichtet, die mit dem Produkt einhergehenden potentiellen Gefahren so gering wie möglich zu halten [Mey11, S. 41]. Nach der BGB-Produkthaftung haftet der Hersteller ausschließlich im Falle des Auftretens eines Schadens, und zwar für Konstruktions-, Fabrikations- und Instruktionsfehler, für die unterlassene Produktbeobachtung sowie – bei entsprechender Gefahrenlage – für einen unterlassenen Rückruf [Mey11, S. 42].

Treten Körper- und Gesundheitsschäden oder Sachschäden am privaten Eigentum auf, so wird die Haftung durch das Produkthaftungsgesetz noch verschärft [Mey11, S 43]. Beispiel – das sogenannte Mineralwasserflasche-Urteil [BGH-VI-ZR-158/94]: Die beklagte Organisation vertrieb kohlensäurehaltiges Mineralwasser, das sie in Mehrweg-Glasflaschen abfüllte. Als die Klägerin eine Sprudelflasche ergriff, explodierte die Flasche und ein Glassplitter verletzte ihr linkes Auge. Die Verteidigung der Organisation beruhte auf dem angeblich ausreichenden Prüfverfahren: Ein Haarriss – der vermutete Fehler der Flasche – ließe sich bei Ausgangskontrolle auch nach dem damaligen Stand der Wissenschaft und Technik nicht erkennen. Die beklagte Organisation konnte jedoch nicht beweisen, dass der Haarriss nicht vorhanden war, als sie die wiederbefüllte Flasche in den Verkehr wieder gebracht hatte [Mey11, S. 43]. Nach § 1 Abs. 1 ProdHaftG wird das Risiko, dass die Ware beim Inverkehrbringen frei von Produktfehlern ist durch den Hersteller und nicht durch den geschädigten Verbraucher getragen [Mey11, S. 43]. Folglich haftete der Hersteller, wenngleich er den Produktfehler nicht hätte vermeiden können [Mey11, S. 43].

Einen Meilenstein in der Rechtsprechung in Bezug auf die Produkthaftung in der Automobilindustrie stellt das sogenannte Airbag-Urteil des Bundesgerichtshofs (BGH) dar. Hintergrund war eine „Klage, in der der Kläger behauptet, der Thorax- und der Kopfairbag seines drei Jahre alten BMW 330d seien beim Durchfahren eines Schlaglochs bzw. beim Ausweichen auf das unbefestigte Fahrbahnbankett ausgelöst worden und hätten ihn an der Halsschlagader verletzt, so dass er in der Folge einen Hirninfarkt erlitten habe“ [Rec09-ol]. Der BGH stellte klar, dass für jedes Produkt bereits in der Konzeptions- und Planungsphase Absicherungsmaßnahmen zu treffen sind, „die zur Vermeidung einer Gefahr objektiv erforderlich und nach objektiven Maßstäben zumutbar sind“ [BGH-VI-ZR-

107/08]. Diese Absicherungsmaßnahmen müssen „dem im Zeitpunkt des Inverkehrbringens des Produkts vorhandenen neuesten Stand der Wissenschaft und Technik“ entsprechen [BGH-VI-ZR-107/08]. Der BGH stellte ferner klar, dass der maßgebliche Stand der Wissenschaft und Technik dabei nicht mit Brancheüblichkeit gleichgesetzt werden kann. Denn „die in der jeweiligen Branche tatsächlich praktizierten Sicherheitsvorkehrungen können durchaus hinter der technischen Entwicklung und damit hinter den rechtlich gebotenen Maßnahmen zurückbleiben“ [BGH-VI-ZR-107/08], [Hel09a, S. 190]. Darüber hinaus formulierte der BGH, dass „den Verwendern des Produkts […] eine eigenverantwortliche Entscheidung darüber ermöglicht werden muss, ob sie sich in Anbetracht der mit dem Produkt verbundenen Vorteile den mit seiner Verwendung verbundenen Gefahren aussetzen wollen […] Sie müssen darüber hinaus in die Lage versetzt werden, den Gefahren soweit wie möglich entgegenzuwirken“ [BGH-VI-ZR-107/08]. Wird also ein Produkt trotz des verbleibenden Restrisikos in Verkehr gebracht, so trifft den Hersteller eine umfassende Informationspflicht [Hel09b, S. 691].

Eine Organisation, die nicht in der Lage ist, die vereinbarten Kundenvorgaben einzuhalten, muss mit Gewährleistungsansprüchen rechnen, und zwar unabhängig davon, ob ein Schaden entstanden ist [Mey11, S. 44]. Es handelt sich zunächst um Nachbesserungs- und Neulieferungsansprüche, ggf. ist auch Preisminderung und Rücktritt vom Vertrag möglich [Mey11, S. 44]. Ist ein Schaden entstanden, „kommt bei Verschulden der Organisation Schadenersatz hinzu“ [Mey11, S. 44]. Unter Umständen ist der Hersteller auch noch strafrechtlich verantwortlich [Mey11, S 44]. Das Lederspray-Urteil des BGH vom 6. Juli 1990 stellt hierbei einen Meilenstein dar [BGH-2-StR-549/89]. Es handelte sich um die strafrechtliche Verantwortlichkeit der Geschäftsführer des Herstellers eines gesundheitsschädlichen Imprägniersprays. Obwohl sich die gesundheitlichen Beschwerden der Verbraucher häuften und bei der Geschäftsführung des Herstellers eingingen, wurde der Vertrieb des Produkts nicht eingestellt und das Produkt nicht zurückgerufen. Da dies schuldhaft unterlassen wurde, wurden die angeklagten Geschäftsführer wegen vorsätzlicher Körperverletzung zu 18-monatigen „Freiheitsstrafen auf Bewährung verurteilt“. [Mey11, S. 44f.]

2.4 Problemabgrenzung

Die Absicherung der Zuverlässigkeit und Sicherheit der durch das enge Zusammenwirken mehrerer Fachdisziplinen gekennzeichneten mechatronischen Systeme ist heute ein noch unzureichend gelöstes Problem. Indikatoren hierfür sind die vielen Rückrufaktionen der letzten Jahre (vgl. Abschnitt 2.3.1). Diese Rückrufaktionen sind meist mit sehr hohen Kosten sowie Imageschäden verbunden [Süd13-ol], [Spi12b-ol]. Führen Zuverlässigkeits- und Sicherheitsprobleme zu schweren Verletzungen von Menschen oder gar Todesfällen, wie die Bahnkatastrophe von Eschede aus dem Jahre 1998, so ist die Grenze des tolerierbaren Restrisikos weit überschritten [Spi10-ol]. Das Erreichen der Zuverlässigkeits- und Sicherheitsziele ist ferner zum großen Teil gesetzlich vorgeschrieben (vgl. Abschnitt 2.3.2) und normativ geregelt [IEC61508], [ISO26262]. Das Nichterreichen der

Zuverlässigkeits- und Sicherheitsziele kann für ein Unternehmen wirtschaftliche sowie rechtliche Folgen haben (vgl. auch Abschnitt 2.3).

Einen Lösungsansatz zum Umgang mit den skizzierten Herausforderungen stellt die **frühzeitige Absicherung der Zuverlässigkeit und Sicherheit auf Basis der Spezifikation der Produktkonzeption** dar. Hierbei findet eine angemessene, entwicklungsbegleitende Absicherung der Zuverlässigkeit und Sicherheit bereits in der frühen Entwicklungsphase der Konzipierung statt. Die Grundlage für die Analyse und Verbesserung der Zuverlässigkeit und Sicherheit bildet dabei eine ganzheitliche, fachdisziplinübergreifende Spezifikation der Produktkonzeption, die zuverlässigkeits- und sicherheitsbezogene Informationen berücksichtigt. Insgesamt ergeben sich folgende **Nutzenpotentiale**:

- **Frühzeitige Fehlervermeidung:** Schwachstellen können bereits früh im Produktentwicklungsprozess entdeckt werden und entsprechende Abstellmaßnahmen eingeleitet werden.
- **Berücksichtigung disziplinübergreifender Zusammenhänge:** Da die Absicherung auf Basis einer ganzheitlichen, fachdisziplinübergreifenden Spezifikation der Produktkonzeption erfolgt, ist es möglich, auch disziplinübergreifende Zusammenhänge und Ausfallfortpflanzungspfade angemessen zu berücksichtigen.
- **Reduzierung von Iterationsschleifen:** Dadurch, dass mögliche Schwachstellen bereits früh aufgedeckt und behoben werden, werden viele der potentiellen nachträglichen Iterationsschleifen und Produktänderungen vermieden, die zeitraubend und kostenintensiv sind. Zeit und Geld werden gespart.

Auf dem Weg zu der angestrebten frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit eines fortschrittlichen mechatronischen Systems gilt es, folgenden **Herausforderungen** zu begegnen:

- **Zunehmende Systemkomplexität:** Mit der Zunahme der Leistungsfähigkeit mechatronischer Systeme (Stichworte: Selbstoptimierung, Cyber-Physical Systems, Industrie 4.0) geht eine steigende Komplexität dieser Systeme einher. Der Entwurf derartiger Systeme ist daher mehr denn je herausfordernd. Dies gilt insbesondere für das Erreichen der Zuverlässigkeit und Sicherheit [BGJ+09]. Eine wesentliche Voraussetzung für das sichere und zuverlässige Funktionieren der Systeme im späteren Betrieb ist die Beherrschung der entstehenden Komplexität.
- **Verstärkte Interdisziplinarität:** Zurückführen lässt sich der Großteil von Fehlern auf eine unzureichende Abstimmung der beteiligten Fachdisziplinen [Gau10, S. 197]. Insbesondere werden die disziplinübergreifenden Ausfallausbreitungspfade unzureichend bzw. zu spät ins Kalkül gezogen [STP+12, S. 138]. Zuverlässigkeits- und Sicherheitsprobleme werden oft erst bei der Integration der Beiträge der Fachdisziplinen oder gar erst im Systembetrieb erkannt [Gau10, S. 39]. Die Folge sind aufwändige Iterationsschleifen im Entwicklungsprozess [Gau10, S. 138]. Notwendig sind

Methoden, Vorgehensmodelle und Werkzeuge, welche die Absicherung der Zuverlässigkeit und Sicherheit von Beginn der Entwicklung an in einer Weise unterstützen, die disziplinübergreifenden Wechselwirkungen und Abhängigkeiten adäquat berücksichtigt.

- **Unzureichende Entwicklungsmethodik:** Die heute etablierten Entwicklungsmethoden und -prozesse tragen der zunehmenden Interdisziplinarität und der steigenden Komplexität der Systeme nur unzureichend Rechnung, weil sie typischerweise die jeweilige Fachdisziplin im Fokus haben. Eine ganzheitliche disziplinübergreifende Systembetrachtung findet – wenn überhaupt – nur ansatzweise statt. Die von den einzelnen Fachdisziplinen erarbeiteten und zu integrierenden Lösungen sind aus Sicht der jeweiligen Fachdisziplin hinsichtlich Zuverlässigkeit und Sicherheit oft optimal. Dies heißt aber noch lange nicht, dass die Summe der optimalen Teillösungen die bestgeeignete Gesamtlösung bildet: „Das Ganze ist mehr als die Summe seiner Teile“. Bis heute fehlt eine Entwicklungsmethodik – im Sinne von Beschreibungsmitteln, Vorgehensmodellen, Methoden und Werkzeugen – die das Gesamtsystem in den Mittelpunkt stellt, die disziplinübergreifende Wechselwirkungen und Abhängigkeiten angemessen ins Kalkül zieht und damit einhergehend eine ganzheitliche, disziplinübergreifende Absicherung der Zuverlässigkeit und Sicherheit effizient unterstützt.
- **Auswahl von geeigneten Methoden:** Den Entwicklern steht im Allgemeinen eine Fülle von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit zur Verfügung. Welche Methode, wann, wie und in welchem Fall am effektivsten einzusetzen ist, wird nicht vermittelt. Hilfsmittel sind notwendig, welche die Entwickler dabei unterstützen, die für ihre jeweilige Entwicklungsaufgabe adäquaten Methoden effizient auszuwählen.
- **Zu später Einsatz von Absicherungsmethoden:** Die klassischen Methoden zur Absicherung der Zuverlässigkeit und Sicherheit wie FMEA und FTA werden typischerweise relativ spät im Entwicklungsprozess eingesetzt, und zwar erst dann, wenn detaillierte Systementwürfe vorliegen. Hinzu kommt, dass diese heute sehr oft durch Vorgehensweisen und Anforderungen der jeweiligen Fachdisziplin geprägt sind [Gau10, S. 39]. Es gilt die Methoden zur Absicherung der Zuverlässigkeit und Sicherheit so aufzubereiten, dass diese möglichst frühzeitig, bereits in der frühen Entwicklungsphase der fachdisziplinübergreifenden Konzipierung verwendet werden können.

Daraus resultiert ein grundlegender **Bedarf** für eine *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit mechatronischer Systeme* auf Basis der Produktkonzeption. Die Systematik soll zum einen erste grundlegende Aussagen zur Zuverlässigkeit und Sicherheit des Produkts in der Konzipierung ermöglichen sowie die Identifikation von Schwachstellen unterstützen. Zum anderen ermöglicht die Systematik, die Implementierung von Abstellmaßnahmen und damit einhergehend die Verbesserung der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit.

Vor diesem Hintergrund sollte die Systematik folgende Bestandteile umfassen:

- **Strukturiertes Vorgehensmodell:** Kern der Systematik muss ein Vorgehensmodell sein, welches die frühzeitige Absicherung der Zuverlässigkeit und Sicherheit eines mechatronischen Systems systematisiert. Es soll die durchzuführenden Tätigkeiten, deren Reihenfolge und Zusammenhänge untereinander sowie die zugehörigen Hilfsmittel beschreiben. Eine idealtypische Darstellung ist hierbei ausreichend.
- **Hilfsmittel zur Auswahl und Kombination von Methoden:** Notwendig sind Hilfsmittel zur Auswahl von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit in der Konzipierung. Diese sollen den Entwickler bei einer effektiven Auswahl und Kombination der für seine Entwicklungsaufgabe adäquaten Methoden unterstützen.
- **Sprache zur Systembeschreibung:** Analysierbare Modelle der Produktkonzeption sind eine wesentliche Voraussetzung für den frühzeitigen Einsatz von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit. Es bedarf einer modellbasierten Spezifikation der Produktkonzeption, welche den grundsätzlichen Aufbau, die Wirkungsweise und das gewünschte Verhalten des Produkts unter besonderer Berücksichtigung der Zuverlässigkeit und Sicherheit disziplinübergreifend beschreibt. Eine derartige Spezifikation der Produktkonzeption ermöglicht eine frühzeitige Absicherung der Produktkonzeption, wodurch die Anzahl der späten, nachträglichen Iterationsschleifen reduziert wird. Insbesondere wird mit der Spezifikation der Produktkonzeption eine Basis für die wirksame Kooperation und Kommunikation von Fachexperten aus den involvierten Fachdisziplinen geschaffen. Hierbei gilt es, auf etablierten Beschreibungsmitteln des modellbasierten Systems Engineerings (MBSE) aufzubauen und diese entsprechend zu erweitern.
- **Methoden zur Analyse und Verbesserung:** Notwendig sind Methoden zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit eines mechatronischen Produkts. Diese sollen auf Basis der Produktkonzeption im Rahmen der Konzipierung durchführbar sein. Die Methoden müssen so gestaltet sein, dass sie 1) erste grundlegende Aussagen bzgl. der Zuverlässigkeit und Sicherheit des betrachteten Produkts, 2) die Identifikation von Schwachstellen, 3) das Ableiten von Gegenmaßnahmen und 4) die Verbesserung der Produktkonzeption ermöglichen. Dabei soll auf etablierten Methoden der Zuverlässigkeits- und Sicherheitstechnik aus der einschlägigen Literatur und Normen wie z.B. FTA, FMEA aufgebaut werden, die es für die frühe Phase der Konzipierung verfügbar zu machen gilt.
- **Konzept einer IT-Unterstützung:** Für eine effiziente Absicherung der Zuverlässigkeit und Sicherheit eines mechatronischen Systems in der Konzipierung ist eine IT-Unterstützung essentiell. Diese soll die Modellierung des Produkts unter besonderer Berücksichtigung von Zuverlässigkeit und Sicherheit ermöglichen sowie dessen Analyse und Verbesserung unter Verwendung entsprechender Methoden. Ferner soll sie die Hilfsmittel zur Auswahl und Kombination von Methoden unterstützen.

2.5 Anforderungen an die Systematik

Aus der Problemanalyse ergeben sich folgende Anforderungen an eine *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme*:

A1) Interdisziplinarität: Im Fokus der Systematik steht nicht eine Fachdisziplin. Vielmehr soll sie es ermöglichen, disziplinübergreifende Zusammenhänge zu erfassen und zu untersuchen. Dadurch wird den Gegebenheiten der mechatronischen Systeme von heute und morgen Rechnung getragen, die durch das symbiotische Ineinandergreifen von Fachdisziplinen wie Mechanik, Hydraulik, Regelungstechnik, Elektronik aber auch Mathematik und künstliche Intelligenz zunehmend geprägt sind.

A2) Fokus auf die Konzipierung: Im Fokus der Systematik soll die Absicherung des Produkts in der frühen Entwicklungsphase der Konzipierung stehen. Durch eine derartige frühzeitige Absicherung können Zeit und Geld gespart werden, da die Anzahl zeitraubender und kostenintensiver, nachträglicher Iterationsschleifen reduziert wird.

A3) Zukunftsrobustheit und Erweiterbarkeit: Die Systematik soll sowohl für klassische als auch für fortschrittliche mechatronische Systeme anwendbar sein. Die Auswahl der einzusetzenden Methoden sowie der zu untersuchenden Aspekte, Informationen und Beziehungen muss bei der Anwendung der Systematik vom Entwickler im Einzelfall eingeschränkt oder erweitert werden können. Ferner muss sich die Systematik um weitere Methoden aufwandsarm erweitern lassen und Hilfsmittel wie Handlungsanweisungen und Leitfäden für die Durchführung derartiger Erweiterungen bereitstellen. Dies trifft insbesondere für den Fall zu, dass weitere über die klassischen Fachdisziplinen der Mechatronik hinausgehende Disziplinen (z.B. Mathematik und künstliche Intelligenz) an der Entwicklung beteiligt sind.

A4) Suche, Auswahl und Kombination von Methoden: Die Entwicklung zuverlässiger und sicherer mechatronischer Systeme erfordert einen entwicklungsbegleitenden Einsatz von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit. Obwohl dem Entwicklern eine Fülle von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit zur Verfügung steht, wird es nicht vermittelt, welche von diesen wie anwendungsfallspezifisch auszuwählen und einzusetzen sind. Notwendig sind Hilfsmittel zur Suche, Auswahl und Kombination von Methoden ausgehend von der zugrunde liegenden Aufgabenstellung. Hierzu gilt es, die Methoden zur Absicherung der Zuverlässigkeit und Sicherheit anhand festzulegender Klassifizierungsmerkmale zu charakterisieren, welche die effiziente Suche, Auswahl und Kombination von Methoden unterstützen.

A5) Ganzheitliche Spezifikation: Im Zentrum der Systematik steht die Spezifikation der Produktkonzeption. Diese muss ganzheitlich sein. Gemeint ist die Abbildung aller relevanten Aspekte und damit einhergehend aller relevanten Informationen und Beziehungen. Abhängig von der zugrunde liegenden Aufgabenstellung sollen darin insbesondere alle

Informationen abgebildet werden, die für die frühzeitige Analyse der Zuverlässigkeit und Sicherheit von Relevanz sind.

A6) Produktmodellzentrierte Analyse und Verbesserung: Die angestrebte Systematik soll zum einen Aussagen bzgl. der Zuverlässigkeit und Sicherheit des Produkts auf Basis der Beschreibung der Produktkonzeption ermöglichen. Zum anderen soll sie die Ableitung von Verbesserungsmaßnahmen und damit einhergehend die Verbesserung der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit unterstützen.

A7) Problemunabhängigkeit: Die angestrebte Systematik soll unabhängig von der Art des zu entwickelnden Systems bzw. der Klasse der Entwicklungsaufgabe anwendbar sein. Insbesondere darf sie in keiner direkten Abhängigkeitsbeziehung zu einer oder mehreren bestimmten Normen der Sicherheits- und Zuverlässigkeitstechnik stehen. Vielmehr sollen die Bestandteile der Systematik auf die allgemeinen Eigenschaften mechatronischer Systeme ausgerichtet sein und eine Integration von branchen-, problemklassen- bzw. normenspezifischen Informationen unterstützen.

A8) Anwenderakzeptanz: Für die erfolgreiche frühzeitige Absicherung der Zuverlässigkeit und Sicherheit eines fortschrittlichen mechatronischen Produkts ist die Akzeptanz der Anwender essentiell. Die Systematik muss daher durch eine hohe Gebrauchstauglichkeit[22] und Aufgabenangemessenheit[23] gekennzeichnet sein. Die Systematik soll hierbei auf etablierten Beschreibungsmitteln, Methoden und Verfahren der Produktmodellierung und der Zuverlässigkeits- und Sicherheitstechnik aufbauen. Denn diese tragen zu einer hohen Anwenderakzeptanz in besonderem Maße bei.

A9) Rechnerunterstützung: Damit die Absicherung der Zuverlässigkeit und der Sicherheit eines fortschrittlichen mechatronischen Produkts effizient erfolgen kann, ist eine Rechnerunterstützung unabdingbar. Diese soll den Entwickler bei der Durchführung aller Phasen der Systematik unterstützen. Insbesondere soll sie eine effiziente Suche nach adäquaten Methoden, das Ablegen von Methoden sowie die Spezifikation und Analyse der Produktkonzeption unter Berücksichtigung von Zuverlässigkeit und Sicherheit unterstützen. Die Rechnerunterstützung gilt es prototypisch umzusetzen. Dabei kann auf bestehenden Werkzeugen, z.B. zur Spezifikation der Produktkonzeption, aufgebaut werden.

---

[22] Die Gebrauchstauglichkeit ist „das Ausmaß, in dem ein Produkt durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“ [DIN9241-11, S. 4]. Der Nutzungskontext ist wie folgt definiert: „Die Benutzer, Arbeitsaufgaben, Arbeitsmittel (Hardware, Software und Materialien) sowie die physische und soziale Umgebung, in der das Produkt genutzt wird“ [DIN9241-11, S. 4].

[23] Definition der Aufgabenangemessenheit nach DIN 9241-110: „Ein interaktives System ist aufgabenangemessen, wenn es den Benutzer unterstützt, seine Arbeitsaufgabe zu erledigen, d.h., wenn Funktionalität und Dialog auf den charakteristischen Eigenschaften der Arbeitsaufgabe basieren, anstatt auf der zu Aufgabenerledigung eingesetzten Technologie“ [DIN9241-110, S. 8].

3 Stand der Technik

In diesem Kapitel werden bestehende Methoden, Vorgehensmodelle und Werkzeuge mit Relevanz für eine *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* vorgestellt und im Hinblick auf die in Abschnitt 2.5 aufgestellten Anforderungen untersucht. Zuerst werden in Abschnitt 3.1 Vorgehensmodelle zur Entwicklung zuverlässiger und sicherer mechatronischer Systeme erklärt. Abschnitt 3.2 gibt dann einen Überblick über etablierte Methoden der Zuverlässigkeits- und Sicherheitsanalyse wie die Vorläufige Gefahrenanalyse (PHA), Fehlzustandsart- und -auswirkungsanalyse (FMEA), Fehlzustandsbaumanalyse (FTA), Ereignisbaumanalyse (ETA) etc. Abschnitt 3.3 widmet sich der Problematik der Auswahl von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit technischer Systeme ausgehend von einer konkreten Entwicklungsaufgabe. Abschnitt 3.4 befasst sich mit Modellierungssprachen zur Beschreibung des Produktmodells. Darauf aufbauend werden in Abschnitt 3.5 bestehende Ansätze zur Durchführung etablierter Methoden der Zuverlässigkeits- und Sicherheitsanalyse auf Basis der Spezifikation des Produktmodells vorgestellt. Danach findet in Abschnitt 3.6 die Vorstellung von Software-Werkzeugen zur rechnerunterstützten Modellierung und Analyse der Zuverlässigkeit und Sicherheit technischer Systeme statt. Abschließend wird in Abschnitt 3.7 der Stand der Technik auf die Erfüllung der Anforderungen aus der Problemanalyse beurteilt, woraus der Handlungsbedarf für diese Arbeit deutlich wird.

3.1 Vorgehensmodelle zur Entwicklung zuverlässiger und sicherer mechatronischer Systeme

Eine wesentliche Voraussetzung für die erfolgreiche und effiziente Entwicklung zuverlässiger und sicherer mechatronischer Systeme ist ein systematisches und klar strukturiertes Vorgehensmodell. Dieses beschreibt, welche Tätigkeiten in welcher Reihenfolge idealtypisch durchzuführen sind, welche Arbeitsprodukte hierbei als Inputs und Outputs dienen und welche Methoden die Durchführung der einzelnen Tätigkeiten unterstützen. Für die Entwicklung zuverlässiger und sicherer mechatronischer Systeme existiert eine Reihe von Vorgehensmodellen, die zum Teil aus der Normungsarbeit und zum Teil aus der Forschung kommen. Vor allem auf dem Gebiet der Sicherheitstechnik sind etablierte Sicherheitsnormen vorhanden. Nachfolgend werden vier Vorgehensmodelle zur Entwicklung zuverlässiger und sicherer mechatronischer Systeme vorgestellt, welche als Basis für die in dieser Arbeit angestrebte Systematik dienen könnten.

3.1.1 Die Grundsicherheitsnorm IEC 61508 und der zugehörige Sicherheitslebenszyklus

Die internationale Norm IEC 61508 wurde im Jahr 1998 verabschiedet und im Jahr 2011 als deutsche Norm DIN EN 61508 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ übernommen [LPP10, S. 8], [IEC61508-1, S. 5]. Im Jahr 2010 erschien die zweite Edition der Norm IEC 61508, welche die erste Edition ersetzt [IEC61508-1, S. 5]. Sie stellt eine Grundnorm für die funktionale Sicherheit dar und definiert die allgemeingültigen Anforderungen an die funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer (E/E/PE) Systeme [LPP10, S. 10]. Aus dieser Grundnorm wurden branchenspezifische Normen (Derivate) z.B. für die Bahntechnik, Medizintechnik, Automobiltechnik etc. abgeleitet. Bild 3-30 gibt hierzu einen Überblick.

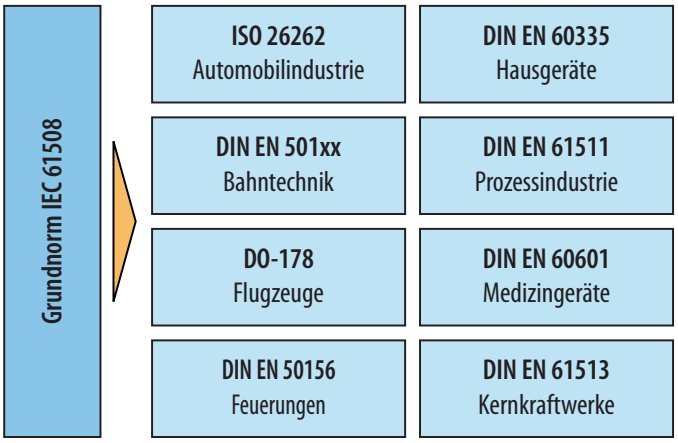


Bild 3-1: Die Grundnorm IEC 61508 und ihre branchenspezifischen Derivate (in Anlehnung an [LPP10, S. 9])

Die Anforderungen an sicherheitsbezogene E/E/PE Systeme werden von der Norm mit dem Ziel gestellt, definierte Sicherheitsziele zu erreichen, indem das vom System ausgehende Risiko auf ein vertretbares Restrisiko vermindert wird. Dieser Grundsatz der IEC 61508 und deren Derivate wurde bereits zusammen mit den zugehörigen Begriffen in Abschnitt 2.1.5.3 erklärt (siehe auch Bild 2-11).

Für diesen Zweck definiert die Norm einen Sicherheitslebenszyklus [IEC61508-1, S. 17ff.]. Wie in Bild 3-2 gezeigt, erstreckt sich dieser von der Konzeptdefinition bis zur Außerbetriebnahme. Ausgangspunkt stellt die Ermittlung des Sicherheitsrisikos des Systems ohne Betrachtung von üblichen, geplanten bzw. bereits umgesetzten Sicherheitsmaßnahmen. Hierzu erfolgt eine grundlegende Beschreibung des zu betrachtenden Systems und dessen Umwelt sowie der zugehörigen Gefahren (Konzept und Anwendungsbereich). Auf dieser Basis findet eine Gefahren- und Risikoanalyse statt. Resultat sind

Sicherheitsziele, welche jeweils mit einem Sicherheitsintegritätslevel (safety integrity level, SIL) versehen werden, der jeweils das ermittelte Risiko beschreibt.[24] Die Sicherheitsziele dienen als Basis für alle folgenden Absicherungsaktivitäten, die im Sicherheitszyklus als Phasen abgebildet sind [LPP10, S. 53]. Die IEC61508 stellt eine Menge von Anforderungen an jede der Phasen mit dem Ziel der Absicherung der funktionalen Sicherheit.

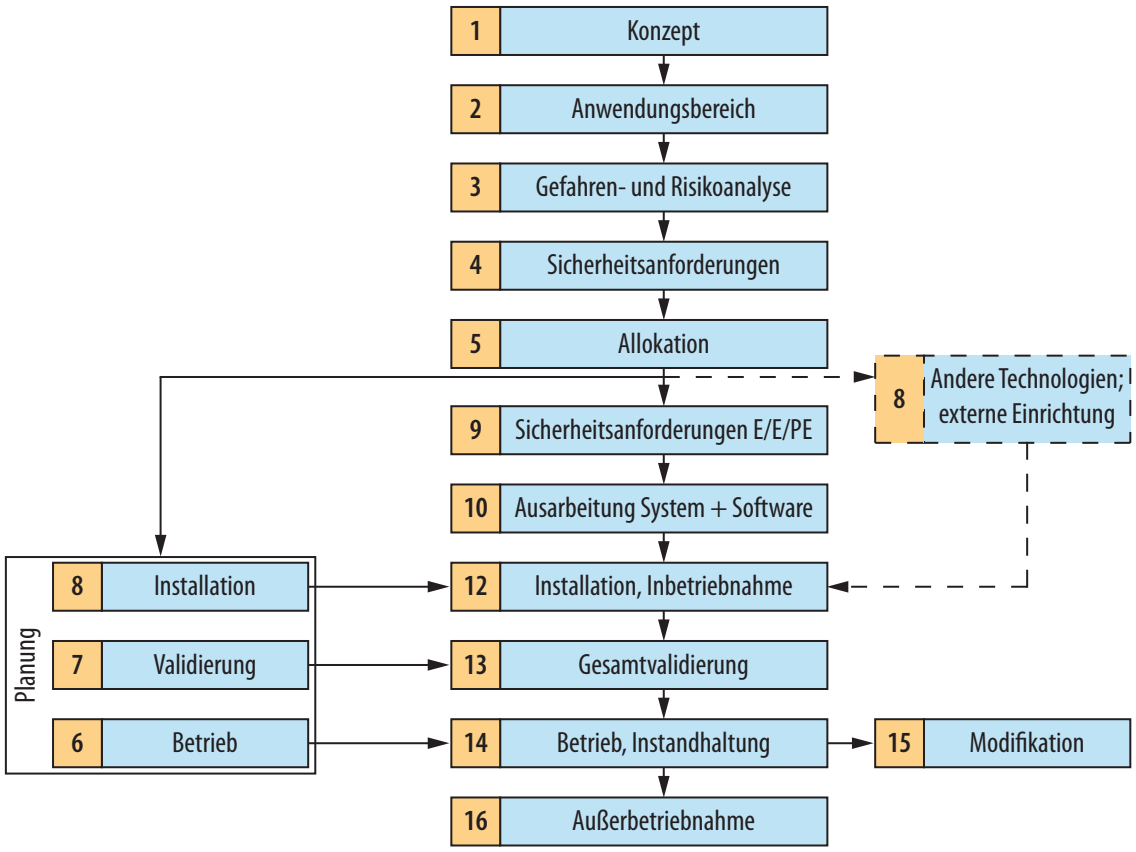


Bild 3-2: Sicherheitslebenszyklus nach IEC 61508; Iterationsschleifen sind nicht dargestellt [IEC61508-1, S. 18], [LPP10, S. 54]

Insgesamt fordert die IEC 61508 eine auf dem Sicherheitslebenszyklus und den zugehörigen Normanforderungen aufbauende systematische Vorgehensweise zur nachweisbaren Erreichung der ermittelten Sicherheitsziele und der zugehörigen Risikominderung. Diese systematische Vorgehensweise soll folgende Punkte umsetzen [LPP10, S. 9f.]:

- Spezifikation der Sicherheitsanforderungen, die ausgehend von den Sicherheitszielen erfolgt. Die so festgelegten Sicherheitsanforderungen beschreiben die erforderliche

[24] Die IEC61508 sieht vier unterschiedliche SIL-Einstufungen vor. Diese sind – in Reihenfolge der aufsteigenden Sicherheitskritikalität – SIL 1, SIL 2, SIL 3 und SIL 4.

Risikominderung [LPP10, S. 9]. Sie werden weiter verfeinert und den Systemelementen zugeordnet, wodurch sich ein Sicherheitskonzept ergibt [ISO26262-1].

- Management der Aktivitäten im Sicherheitslebenszyklus mit dem Ziel der Sicherstellung einer vollständigen und nachweisbaren Realisierung der Sicherheitsanforderungen und des Sicherheitskonzepts.
- Entwurf von elektronischen Hardware und der zugehörigen eingebetteten Software unter Verwendung von Maßnahmen zur Fehlerverhinderung (z.B. Nutzung etablierter Entwurfsmuster, statische Code-Analyse etc.), Fehlerbeseitigung (z.B. Inspektionen, Fehlerinjektions-Tests etc.), Fehlertoleranz (z.B. Plausibilitätsprüfungen, Redundanz mit Mehrheitsentscheidung etc.) und Fehlervorhersage (z.B. FMEA, FTA), die in Abschnitt 2.1.3 detailliert beschrieben wurden. Diese finden zum einen Eingang in die Spezifikation des Sicherheitskonzepts (z.B. redundante Auslegung von Systemelementen). Zum anderen kommt es darauf an, den zugehörigen Entwicklungsprozess zu verbessern. Zum Beispiel werden für Software ab einem gewissen Sicherheitsintegritätslevel die Definition und Verwendung von Entwurfs- und Codierungsrichtlinien, eingeschränkte Nutzung von Pointern, statische Code-Analyse, Inspektionen etc. gefordert. Diese Punkte müssen Eingang in die Definition des zugrunde liegenden Entwicklungsprozesses sowie der zugehörigen Leitfäden, Prozesshandbücher und -manuals finden und in den Projekten so nachweisbar gelebt werden.
- Planbare und nachvollziehbare Umsetzung über definierte unterstützende Prozesse (z.B. für Projektmanagement, Change Management, Konfigurationsmanagement, Entwurf, Test etc.) [LPP10, S. 10].

Wie bereits in Abschnitt 2.1.5.3 dargelegt, erfolgt die Dokumentation der Wirksamkeit des Sicherheitskonzepts im Rahmen eines Sicherheitsnachweises [PH13, S. 391f.].

Bei dem Sicherheitslebenszyklus handelt es sich um ein generisches Modell, welches es bei einer Anwendung in spezifischen Branchen und Unternehmen entsprechend zu interpretieren und zu übertragen gilt [LPP10, S. 54]. Im Allgemeinen folgen die abgeleiteten, branchenspezifischen Derivate dieser von der Grundnorm vorgegebenen Vorgehensweise [LPP10, S. 10]. Es ist zu empfehlen die branchenspezifische Norm, soweit vorhanden, zu verwenden, da diese auf die spezifischen Gegebenheiten der jeweiligen Branche zugeschnitten ist [LPP10, S. 10]. Die Auswahl von Methoden für die Phasen des Sicherheitslebenszyklus nach IEC 61508 wird separat in Abschnitt 3.3.3 adressiert.

Bewertung: Die IEC 61508 schreibt vor, wie die funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer (E/E/PE) Systeme abzusichern ist. Andere Fachdisziplinen wie die Mechanik stehen nicht im Fokus. Als Grundnorm ist die IEC 61508 weitgehend branchenunabhängig. Der durch die Norm definierte Sicherheitslebenszyklus lässt sich in den Entwicklungsprozess des jeweiligen Unternehmens integrieren. Existiert eine branchenspezifische Ableitung, ist diese für die

jeweilige Branche typischerweise vorzuziehen. Der Sicherheitslebenszyklus sieht explizit Phasen zur Produktkonzipierung vor; dies umfasst eine Spezifikation auf Systemebene.

3.1.2 Die Sicherheitsnorm ISO 26262 und der zugehörige Sicherheitslebenszyklus

Die ISO Norm 26262 ist eine branchenspezifische Ableitung der Grundnorm IEC 61508, die im November 2011 verabschiedet wurde [ISO26262-1]. Sie gilt für Serienfahrzeuge bis 3,5 Tonnen zulässiges Gesamtgewicht. Die ISO 26262 liegt nicht in deutscher Sprache vor. Daher werden einzelne Begriffe auch im englischen Original angegeben, damit deutlich und eindeutig ist, was gemeint ist. Der Aufbau der ISO 26262 ist im Anhang A1.5 kurz erklärt, siehe auch [LPP10, S. 119].

Bild 3-3 stellt den Sicherheitslebenszyklus nach ISO 26262 dar [ISO26262-2, S. 3f.], [LPP10, S. 118ff.]. Die Nummerierung der einzelnen Phasen stimmt mit der Gliederung der Norm überein: so bedeutet die Nummerierung 3-8 ein Verweis auf Kapitel 8 im Teil 3.

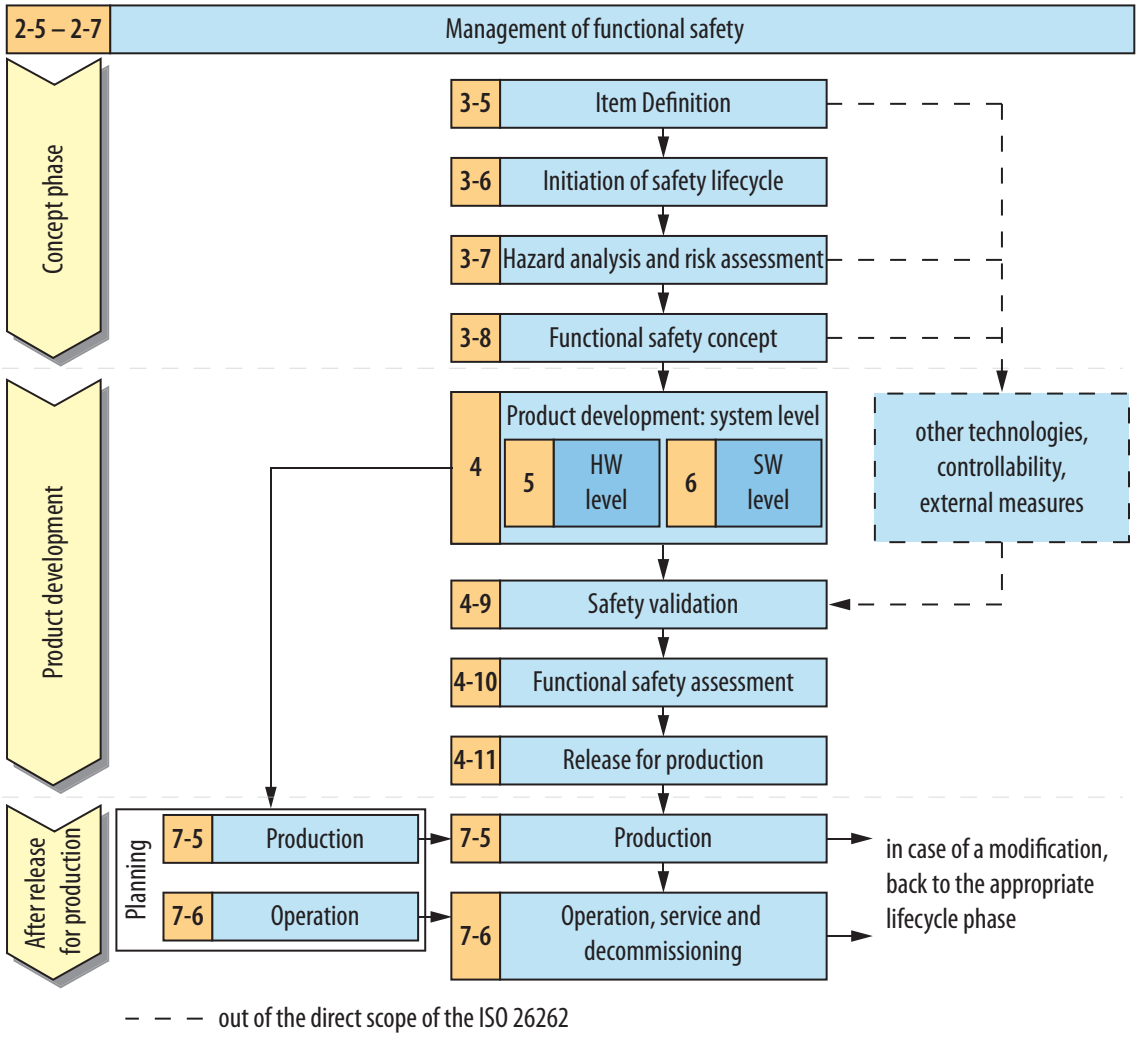


Bild 3-3: Sicherheitslebenszyklus nach ISO 26262; Iterationsschleifen sind nicht dargestellt [ISO26262-2, S. 4], [LPP10, S. 118]

Die ISO 26262 trägt den speziellen Gegebenheiten der Automobilindustrie Rechnung. Insbesondere ist die ISO26262 im Vergleich zur Grundnorm IEC 61508 stärker auf die Entwicklung und Produktion von Serienprodukten im Automobilbereich zugeschnitten [LPP10, S. 119]. Dies zeigt insbesondere der Vergleich mit dem Sicherheitslebenszyklus der Grundnorm: der für eine Großanlage typischen Inbetriebnahme und Gesamtvalidierung stehen im Automobilbereich die Produktfreigabe nach der Entwicklung sowie die darauf folgende Serienproduktion gegenüber [LPP10, S. 119]. Im Sicherheitslebenszyklus nach ISO 26262 ist darüber hinaus die Phase der Produktentwicklung klarer strukturiert [LPP10, S. 119]. Es wird die Produktentwicklung auf Systemebene hervorgehoben, in welche die Phasen der Hardware- und der Software-Entwicklung eingebettet sind. Eine besondere Rolle spielen hierbei die Spezifikation der Hardware-Software-Schnittstelle und der Integrationstest. Für eine detailliertere Vorstellung des Sicherheitslebenszyklus nach ISO 26262 und einen tiefergehenden Vergleich der ISO 26262 mit der Grundnorm IEC 61508 sei auf die Buchpublikation von LÖW ET AL. verwiesen [LPP10, S. 118ff.]. In Abschnitt 3.3.4 wird die Auswahl von Methoden nach ISO 26262 behandelt.

Bewertung: Im Vergleich zur IEC 61508 sind der durch die ISO 26262 definierte Sicherheitslebenszyklus und die zugehörigen Anforderungen stärker auf die speziellen Gegebenheiten der Automobilindustrie ausgelegt. Dies betrifft insbesondere die Entwicklung und Produktion von Serienprodukten, die Zusammenarbeit mit Lieferanten sowie die vernetzte Produktentwicklung. Ferner werden die Themen funktionale Architektur und Systems Engineering stärker adressiert. Insbesondere wird die Produktentwicklung auf Systemebene als Phase des Sicherheitslebenszyklus stärker hervorgehoben.

3.1.3 Methodik zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen

Eines der wesentlichen Ergebnisse der DFG-Forschergruppe 460 „Entwicklung von Konzepten und Methoden zur Ermittlung der Zuverlässigkeit mechatronischer Systeme in frühen Entwicklungsphasen“ (Laufzeit 2002-2008; Leitung Prof. Bertsche) ist eine Methodik zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen [BGJ+09, S. 47ff.]. Diese Methodik ist auch für Sicherheitsuntersuchungen anwendbar. Im Mittelpunkt der Methodik steht die Phase „Systementwurf“ des V-Modells für die Entwicklung mechatronischer Systeme nach der VDI Richtlinie 2206 [VDI2206, S. 29f.]. Die Methodik unterstützt die Integration etablierter Entwicklungsmethoden (Beschreibungsmittel, Analysemethoden etc.) [BGJ+09, S. 47]. Als Modellierungssprache verwendete die Forschergruppe vordergründig die Beschreibungssprache SQMA, die in Abschnitt 3.4.1 detailliert vorgestellt wird. Kern der Methodik bildet das in Bild 3-4 dargestellte Vorgehensmodell, welches folgende 6 Phasen umfasst [BGJ+09, S. 48ff]:

Phase 1 – Identifikation Topfunktion/Topfehlfunktion: Ziel ist die Bestimmung von Topfunktionen und der zugehörigen Topfehlfunktionen. Die Topfunktionen ergeben sich im Zuge des Untergliederns der Gesamtfunktion des Systems in Teilfunktionen [FG13,

S. 244]. Für die identifizierten Topfunktionen werden die zugehörigen Topfehlfunktionen bestimmt. Einer Topfunktion können eine oder mehrere Topfehlfunktionen zugeordnet werden. Eine der möglichen Topfehlfunktionen ergibt sich typischerweise durch Negation der Topfunktion. Weitere Topfehlfunktionen können z.B. unter Verwendung von Checklisten wie die nach FENELON ET AL. ermittelt werden (vgl. Abschnitt 3.2.2.2 und Bild 3-18) [FMN+94]. Für jede Topfehlfunktion wird ihr Schweregrad ermittelt. Ein mögliches Klassierungsverfahren bestehend aus vier Schweregraden „niedrig“, „mittel“, „hoch“ und „kritisch“ ist beschrieben in [BGJ+09, S. 35], [VDA3-1]. Diesen Schweregraden und damit einhergehend den zugehörigen Topfehlfunktionen und Topfunktionen werden Zuverlässigkeits- bzw. Sicherheitsziele zugeordnet [BGJ+09, S. 49]. Hilfestellung hierbei geben z.B. die VDI Richtlinie 4007 für die Zuverlässigkeitsziele und die Norm IEC 61508 für die Sicherheitsziele (vgl. auch Abschnitt 3.1.1) [VDI4007], [Bra11], [IEC61508]. Diese Sicherheits- bzw. Zuverlässigkeitsziele dienen als Messlatte bei der späteren Sicherheits- bzw. Zuverlässigkeitsbewertung [BGJ+09, S. 49].

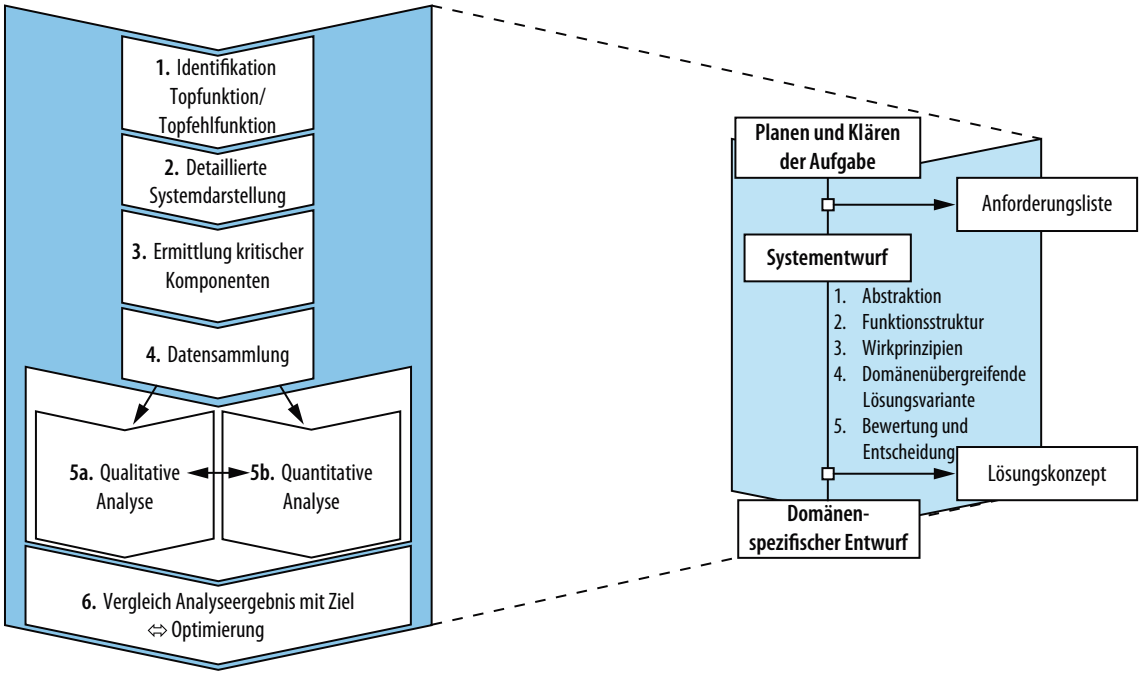


Bild 3-4: Methodik zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen [BGJ+09, S. 47], [VDI2006, S. 29]

Phase 2 – Detaillierte Systemdarstellung: Ausgehend von der Spezifikation der Topfunktionen und Topfehlfunktionen wird hier eine detaillierte Darstellung des Systems erarbeitet. Aufgebaut wird hierbei auf vorliegenden Informationen über das zu entwickelnde System (z.B. auf Blockschaltbildern, Prinzipskizzen, verbalen Beschreibungen, Anforderungslisten etc.) [BGJ+09, S. 49]. Die Methodik sieht vor, die für die Systemdarstellung wesentlichen Beschreibungsaspekte wie z.B. Anwendungsfälle des Systems mit

etablierten Beschreibungsmitteln wie der UML[25] zu beschreiben [BGJ+09, S. 50f.]. Gemäß der Empfehlungen der Methodik lässt sich aus einer derartigen Anwendungsfallbeschreibung und den dabei gewonnenen Erkenntnissen „ein erstes physikalisches Modell aufbauen, in dem die aus den Anwendungsfällen identifizierten mechanischen und elektro-mechanischen Komponenten enthalten sind“ [BGJ+09, S. 51]. Dieses erste physikalische Modell gilt es im Laufe des Entwicklungsprozesses weiter zu verfeinern [BGJ+09, S. 52]. Als Ergebnis der Phase 2 soll letztendlich ein Modell vorliegen, welches die „Strukturen und das Verhalten des mechatronischen Systems beschreiben kann“ [BGJ+09, S. 52]. In der Forschergruppe wurde die SQMA als Methode zur Modellbildung und -analyse ausgewählt, die in Abschnitt 3.4.1 genauer vorgestellt wird [BGJ+09, S. 54].

Phase 3 – Ermittlung kritischer Komponenten: Hier wird ermittelt, welche Systemelemente hinsichtlich Sicherheit bzw. Zuverlässigkeit am kritischsten sind. Gemeint sind Systemelemente, die im Vergleich zu anderen Systemelementen in der Sicherheits- bzw. Zuverlässigkeitsstruktur ein größeres Risiko (Schadensausmaß und Auftretenswahrscheinlichkeit; vgl. Abschnitt 2.1.1) aufweisen. Derartige kritische Systemelemente gilt es detaillierter zu betrachten.

Ausgangspunkt für die Ermittlung der kritischen Systemelemente ist die auf Systemebene festgestellte unerwünschte globale Auswirkung, welche durch Zuweisung von Schweregraden und Sicherheits- bzw. Zuverlässigkeitszielen zu Topfunktionen und Topfehlfunktionen in Phase 1 abgebildet wurde. Diese unerwünschte globale Auswirkung wird auf Basis der Systemdarstellung auf die einzelnen Systemelemente zurückverfolgt, wodurch kritische Systemelemente identifiziert werden [BGJ+09, S. 56]. Hierzu kann z.B. ein mit der SQMA spezifiziertes Systemmodell verwendet werden [BGJ+09, S. 56].

Phase 4 – Datensammlung: Ist eine quantitative Betrachtung angestrebt, so sind quantitative Daten wie Lebensdauerdaten erforderlich. Mögliche Quellen dieser Daten sind nach IEEE 1413 gesichertes Wissen aus firmeneigenen und allgemeinen Datenbanken und aus physikalischen Vorhersagen, empirisch bzw. experimentell ermittelte Ergebnisse (Tests und Feldeinsätze) sowie Wissen aus nichtdokumentierten Quellen [BGJ+09, S. 56], [IEEE1413-1]. Gerade in frühen Entwicklungsphasen fehlen für die Bestimmung genauer Zuverlässigkeits- bzw. Sicherheitswerte detaillierte Informationen z.B. über das zugehörige Temperaturprofil [BGJ+09, S. 56]. Für den Umgang mit daraus resultierenden unsicheren Daten definiert die Methodik einen Programmablaufplan, welcher die folgenden 5 Analysearten einbettet [BGJ+09, S. 56f.]: 1) Verwendung von Versuchsdaten, 2) Nutzung von Netzstrukturen, 3) Nutzung von quantitativem Expertenwissen, 4) Nutzung

[25] Die Unified Modeling Language (UML) in eine durch die Object Management Group (OMG) standardisierte Modellierungssprache zur Beschreibung von Software [OMG11], [MH06, S. 245 ff.], [Wei07]. Sie baut zum Teil auf bewährten Modellierungsnotationen wie Zustandsmaschinen auf.

von qualitativem Expertenwissen, 5) Verwendung von Ausfallratenkatalogen (vgl. hierzu auch Abschnitt 2.1.5.4).

Phase 5 – Qualitative und quantitative Analyse: Hier findet eine qualitative Analyse statt, die in Abhängigkeit von der zugrunde liegenden Entwicklungsaufgabe um eine quantitative Analyse ergänzt werden kann (vgl. Abschnitt 2.1.3 für Definitionen der Begriffe der qualitativen und quantitativen Analyse). Bei qualitativen Analysen kommen vordergründig FMEA und FTA zum Einsatz. Weitere mögliche qualitative Analysemethoden sind z.B. ETA und HAZOP. Die FMEA, die FTA und die ETA können auch für eine quantitative Betrachtung eingesetzt werden. Weitere quantitative Analysemethoden sind z.B. die Markoff-Analyse, die Bayesschen Netze, die in Abschnitt 3.2 vorgestellt werden, sowie die FMEDA [ISO26262-5, Annex E]. Die meisten qualitativen und quantitativen Analysemethoden können auf Basis der Spezifikation des Systemmodells durchgeführt werden (vgl. auch Abschnitt 3.5).

Phase 6 – Vergleich Analyseergebnis mit Ziel – Optimierung: Die im Rahmen der qualitativen und quantitativen Analyse ermittelten Ergebnisse werden hier mit den in Phase 1 festgelegten Sicherheits- bzw. Zuverlässigkeitszielen verglichen. Im Falle einer nicht akzeptablen Abweichung des Ist- von dem Soll-Zustand gilt es, Verbesserungsmaßnahmen zu definierten und in das Systemmodell zu integrieren. Das überarbeitete Systemmodell wird erneut einer Analyse unterzogen, und zwar solange, bis die angestrebten Ziele erreicht werden.

Bewertung: Die Methodik zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen fokussiert die frühen Phasen der Produktentwicklung. Durch die Integration der Methode SQMA ist eine disziplinübergreifende Spezifikation der Struktur und des zustandsübergangsbasierten Verhaltens des Produkts und deren Zusammenhangs möglich. Jedoch kommen die Rückverfolgbarkeit von Anforderungen, funktionale Dekomposition und die Beschreibung des Ablaufverhaltens zu kurz. Die Methodik sieht ferner eine Integration von bewährten Methoden wie FMEA, FTA, Use-Case-Diagramme der UML etc. vor. Hierfür wurde ein Vorgehen auf Makro-Ebene festgelegt. Jedoch ist das Vorgehen auf Mikro-Ebene an vielen Stellen unzureichend definiert. Dies betrifft insbesondere die Fragestellung, welche Methoden wann konkret einzusetzen sind und wie deren Verzahnung zu gestalten ist.

3.1.4 Referenzprozess für die Konzipierung selbstoptimierender mechatronischer Systeme des SFB 614

Im SFB 614 entstand ein Referenzprozess für die Konzipierung selbstoptimierender mechatronischer Systeme, welcher auch für klassische mechatronische Systeme anwendbar ist [GRS14], [ADG+09, S. 167ff.]. Aufgebaut wurde dabei auf etablierten Entwicklungsmethodiken für mechatronische Systeme wie beispielsweise der VDI-Richtlinie 2206, der VDI Richtlinie 2221, dem Entwicklungsvorgehen nach ISERMANN, dem 3-Ebenen-Vorgehensmodell nach BENDER etc. [VDI2206], [VDI2221], [Ise08], [Ben05].

Die Entwicklung s.o. Systeme gliedert sich in zwei Phasen: die fachdisziplinübergreifende Konzipierung und den fachdisziplinspezifischen Entwurf und Ausarbeitung. In der Konzipierung erarbeiten Entwickler der Disziplinen Maschinenbau, Elektrotechnik, Regelungs- und Softwaretechnik gemeinsam die Produktkonzeption. Diese legt den grundsätzlichen Aufbau und die Wirkungsweise des Systems fest. In der anschließenden Phase Entwurf und Ausarbeitung arbeiten sie die ihre Fachdisziplin betreffenden Aspekte parallel zueinander aus. Diese Entwicklungsphase ist durch einen hohen Abstimmungs- und Koordinationsaufwand geprägt. Das Vorgehensmodell für die Konzipierung wird nachfolgend detailliert erläutert.

Wie in Bild 3-5 zu sehen, gliedert sich das grundsätzliche Vorgehen in der domänenübergreifenden Konzipierung in die vier Phasen „Planen und Klären der Aufgabe“, „Konzipierung auf Systemebene“, „Konzipierung auf Subsystemebene“ und „Konzeptintegration“ [GRS14], [GFD+08, S. 167f.], [ADG+09, S. 96ff.].

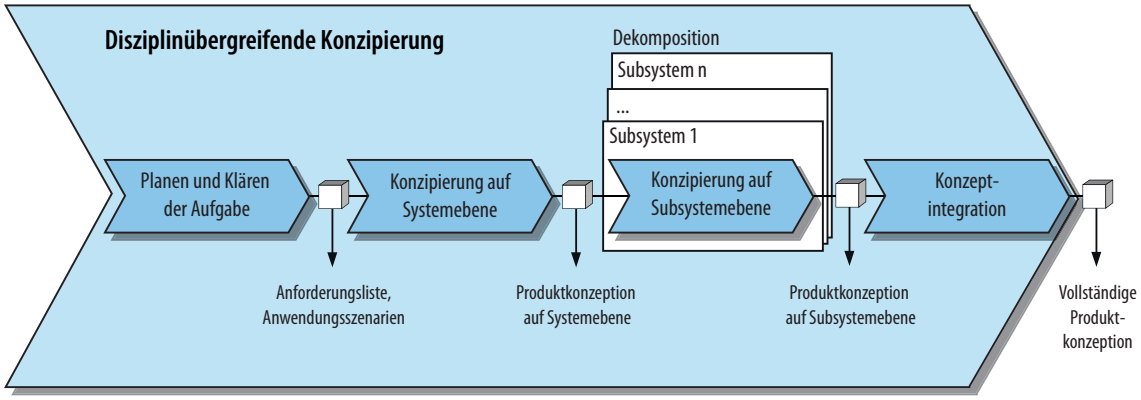


Bild 3-5: Vorgehen bei der Konzipierung selbstoptimierender mechatronischer Systeme [GRS14], [GFD+08, S. 96]

Planen und Klären der Aufgabe: Bild 3-6 stellt das grundsätzliche Vorgehen für diese Phase dar. Zuerst wird der Entwicklungsauftrag abstrahiert und dessen Kern identifiziert. Anschließend wird eine Umfeldanalyse durchgeführt, in welcher die relevanten Einflussbereiche (z.B. Witterung, mechanische Belastungen etc.) und Einflüsse (z.B. Wärmestrahlung, Windlast etc.) identifiziert werden; diese schließen die den Systemzweck störenden Einflüsse ein (z.B. Verschleiß, Temperatur, Regen, Schnee, Laub etc.). Daneben zeichnen sich in der Umfeldanalyse erste externe Ziele des Systems ab (z.B. „Komfort maximieren“, „Verschleiß minimieren“, „Wartungsaufwand minimieren“ etc.). Darauf aufbauend werden Anwendungsszenarien, die eine situationsspezifische Sicht auf das System und dessen Verhalten darstellen. Sie beschreiben jeweils einen Ausschnitt der Gesamtfunktionalität des zu entwickelnden Systems und ermöglichen eine erste Abschätzung der erschließbaren Nutzenpotentiale. Die Ergebnisse dieser ersten Phase werden in Form von Forderungen und Wünschen in der Anforderungsliste dokumentiert.

Konzipierung auf Systemebene: Bild 3-7 zeigt die Schritte der Konzipierung auf Systemebene: Ausgehend von den zuvor festgelegten Anforderungen an das System werden

zunächst dessen Funktionen in einer Funktionshierarchie dargestellt. Für die in der Funktionshierarchie dokumentierten Funktionen wird anschließend nach Lösungsmustern[26] gesucht. Die am besten geeigneten Lösungsmuster werden ausgewählt und unter Verwendung des morphologischen Kastens miteinander zu Lösungsvarianten kombiniert. Die sich daraus ergebenden Lösungsvarianten werden gegenübergestellt. Hierzu kann z.B. die Nutzwertanalyse verwendet werden [GID+13]. Nur die vielversprechendsten Lösungsvarianten werden weiterverfolgt. Für diese werden die Struktur-, Verhaltens- und Gestaltmodelle auf Basis der Beschreibungen der jeweiligen Lösungsmuster synthetisiert und zur Produktkonzeption auf Systemebene zusammengeführt [DAG+13], [Dum11].

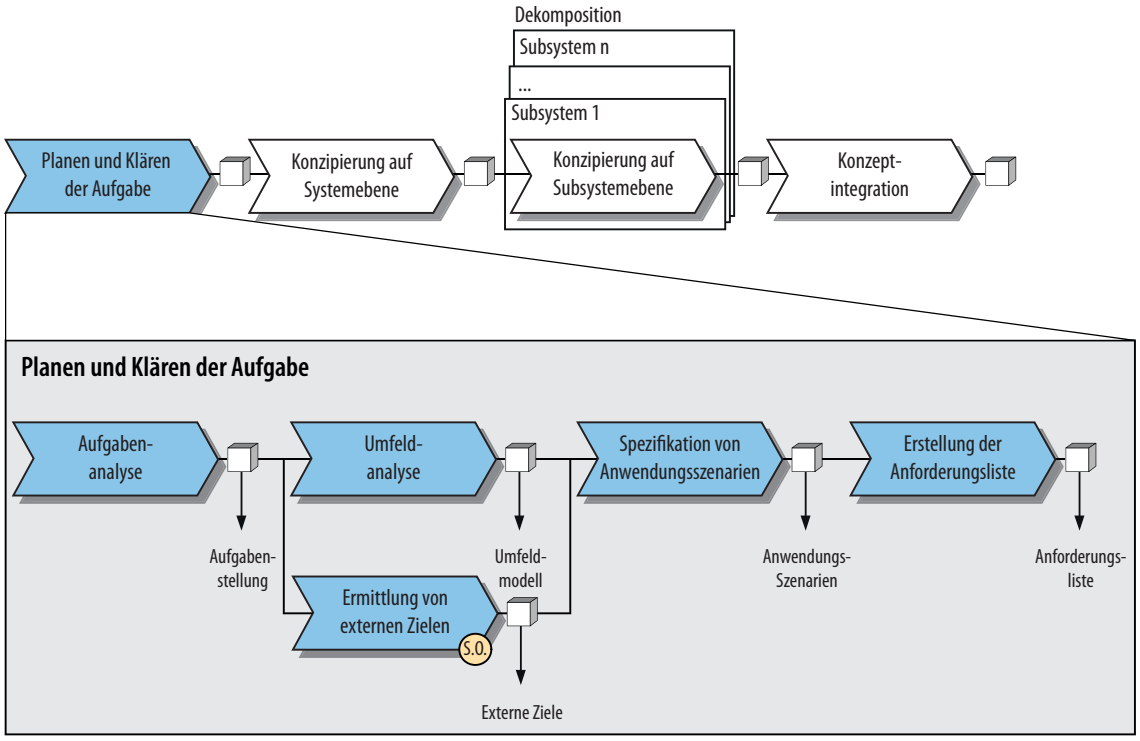


Bild 3-6: Konzipierungsphase "Planen und Klären der Aufgabe" [GRS14], [GFD+08]

Anschließend erfolgt die Beurteilung der Produktkonzeption auf das Vorhandensein von potentiell gegenläufigen Zielen, wodurch auf das Vorhandensein von Selbstoptimierungs-Potential geschlossen werden kann. Werden derartige Ziele gefunden, so wird die vorliegende Spezifikation der Produktkonzeption um die Beschreibung des Zielsystems ergänzt (vgl. Abschnitt 2.2.3). Hierzu kann die Methode zur Beschreibung des Zielsystems nach POOK verwendet werden [PGD12], [Poo11]. Entlang der drei Phasen des Selbstoptimierungsprozesses ergeben sich zusätzliche Anforderungen an das System hinsichtlich der Erfassung der Ist-Situation, Bestimmung und Priorisierung der Systemziele und der Verhaltensanpassung. Diese zusätzlichen Anforderungen werden in die Anforderungsliste aufgenommen.

26 Lösungsmuster beschreiben den Kern einer Lösung für ein wiederkehrendes Problem [ADG+09].

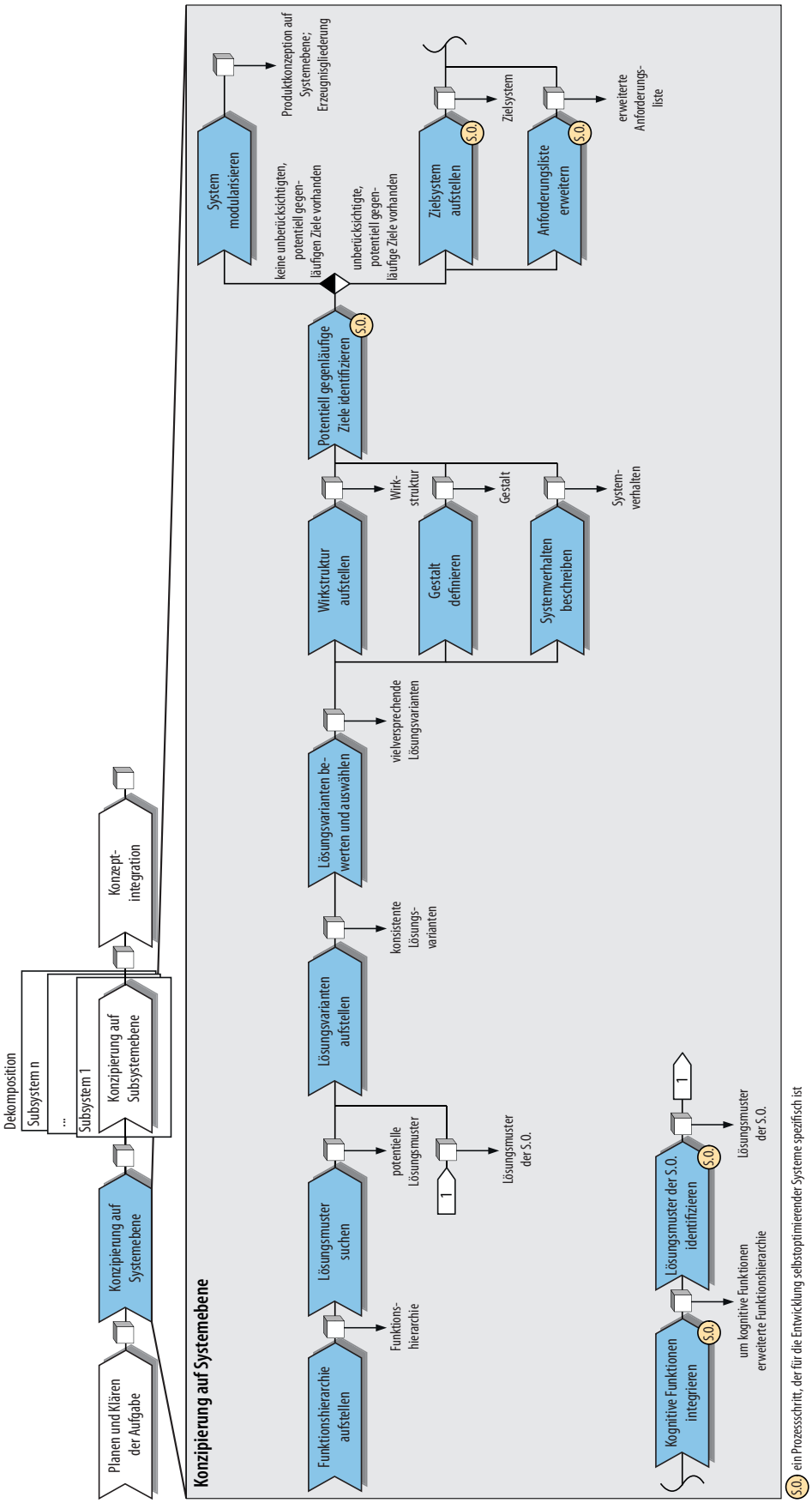


Bild 3-7: Konzipierungsphase "Konzipierung auf Systemebene" [GRS14]

Die Produktkonzeption auf Systemebene beschreibt das Gesamtsystem. Um entscheidungsrelevante Aussagen über die technische und wirtschaftliche Realisierbarkeit der gefundenen Lösung treffen zu können, ist es jedoch notwendig, die Lösung detaillierter zu betrachten. Hierfür wird eine Modularisierung vorgenommen [Ste07]. Das Ergebnis ist eine entwicklungsorientierte Erzeugnisgliederung. Diese fasst die Systemelemente nach unterschiedlichen Beziehungsaspekten zu Subsystemen zusammen.

Konzipierung auf Subsystemebene: In dieser Phase werden für jedes der im Rahmen der Modularisierung identifizierten Subsysteme Produktkonzeptionen erarbeitet. Insbesondere wird für jedes Subsystem das Zielsystem und die damit einhergehende Verhaltensanpassungsfähigkeit und Kommunikationstopologie spezifiziert. Die Ansätze zur Steigerung der Verlässlichkeit finden ebenfalls Anwendung. Die Vorgehensweise entspricht dabei im Allgemeinen der Konzipierung auf Systemebene. Das Ergebnis dieser Phase sind die Produktkonzeptionen auf Modulebene.

Konzeptintegration: Bild 3-8 zeigt die im Rahmen dieser Phase durchzulaufenden Schritte. In einem ersten Schritt werden die Produktkonzeptionen der Subsysteme zu einer vollständigen Produktkonzeption des Gesamtsystems integriert. In diesem Zusammenhang werden die Lösungen auf Widersprüche analysiert (z.B. Widersprüche zwischen Anwendungsszenarien, zwischen den Verhaltensmodellen der Subsysteme etc.) und es wird geprüft, welche dieser Widersprüche durch Selbstoptimierung gelöst werden können.

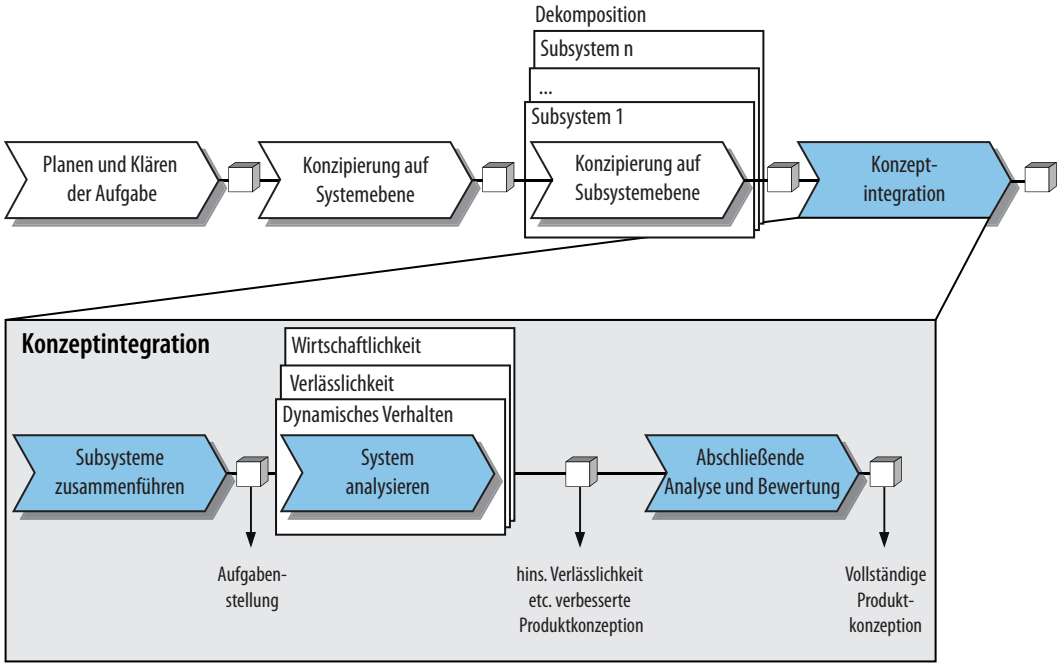


Bild 3-8: Konzipierungsphase "Konzeptintegration" [GRS14]

Ferner werden Zielkonflikte zwischen den Zielen unterschiedlicher Subsysteme ermittelt (z.B. zwischen dem Ziel des Fahrwerks „Spurkranzanläufe minimieren“ und dem Ziel des Feder-Neigesystems eines RailCabs „Aufbaubeschleunigung minimieren“) und die

damit verbundene Verhaltensanpassungsfähigkeit integriert [PGD12], [Poo11, S. 155]. Die so zusammengeführte Produktkonzeption wird anschließend einer Analyse im Hinblick auf Verlässlichkeit, Wirtschaftlichkeit etc. unterzogen. Danach findet eine abschließende technisch-wirtschaftliche Bewertung der Produktkonzeption statt. Das Ergebnis dieser Konzipierungsphase ist die vollständige Produktkonzeption, welche als Ausgangspunkt und Basis für die weitere Entwicklungsphase Entwurf und Ausarbeitung dient, die in den einzelnen involvierten Fachdisziplinen (Mechanik, Elektronik, Regelungstechnik, Softwaretechnik) parallel erfolgt.

Der zugrunde liegende Ablauf ist nicht als eine stringente Folge von Prozessschritten zu sehen. Vielmehr ist dieser durch zahlreiche Iterationen gekennzeichnet. Als Beschreibungssprache kann zum Beispiel die Spezifikationstechnik CONSENS bzw. die SysML verwendet werden (beide werden in Abschnitt 3.4 vorgestellt).

Bewertung: Der Referenzprozess definiert die fachdisziplinübergreifende Konzipierung von mechatronischen und selbstoptimierenden Systemen. Im Mittelpunkt steht eine ganzheitliche Spezifikation der Produktkonzeption, die konzipierungsbegleitend geschieht und alle wesentlichen Aspekte einer Produktbeschreibung (Umfeldmodell, Anwendungsszenarien, Anforderungen, Funktionen, Systemstruktur, Systemverhalten, Gestalt etc.) berücksichtigt. Die Analyse und Verbesserung des Produkts hinsichtlich ausgewählter Analyseaspekte wie der Sicherheit und Zuverlässigkeit greift nicht weit genug. Sie erstreckt sich zwar in einer impliziten Weise durch die gesamte Konzipierung, kommt jedoch explizit nur im Rahmen der Konzeptintegration vor.

3.2 Methoden der Zuverlässigkeits- und Sicherheitsanalyse

In der einschlägigen Literatur und den einschlägigen Normen ist eine Menge von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit zu finden. In der industriellen Praxis sind insbesondere Methoden wie die FMEA, FTA und HAZOP branchenübergreifend stark verbreitet. Dieser Abschnitt widmet sich derartigen etablierten Methoden der Zuverlässigkeits- und Sicherheitsanalyse.

Eine im Rahmen der vorliegenden Arbeit durchgeführte Gegenüberstellung von etablierten Methoden der Zuverlässigkeits- und Sicherheitsanalyse hat ergeben, dass allen hier betrachteten Methoden das in Bild 3-9 dargestellte generische Vorgehensmodell zugrunde liegt. Dieses generische Vorgehensmodell beruht auf dem allgemeinen Problemlösungsprozess [HNB+02, S. 47ff]. Es umfasst folgende sieben Phasen:

Phase 1 – Systemdefinition: In dieser Phase geht es um die Spezifikation des Produktmodells. Welche Aspekte hierbei beschrieben werden müssen (Anforderungen, Anwendungsszenarien, Funktionen, Systemstruktur, Verhalten etc.), hängt stark von der jeweiligen Methode ab. Zum Beispiel ist für die Durchführung einer FMEA die Beschreibung von Funktionen und Struktur des Produkts essentiell. Für eine Markoff-Analyse ist die Beschreibung des Systemverhaltens in Form von Zustandsdiagrammen erforderlich.

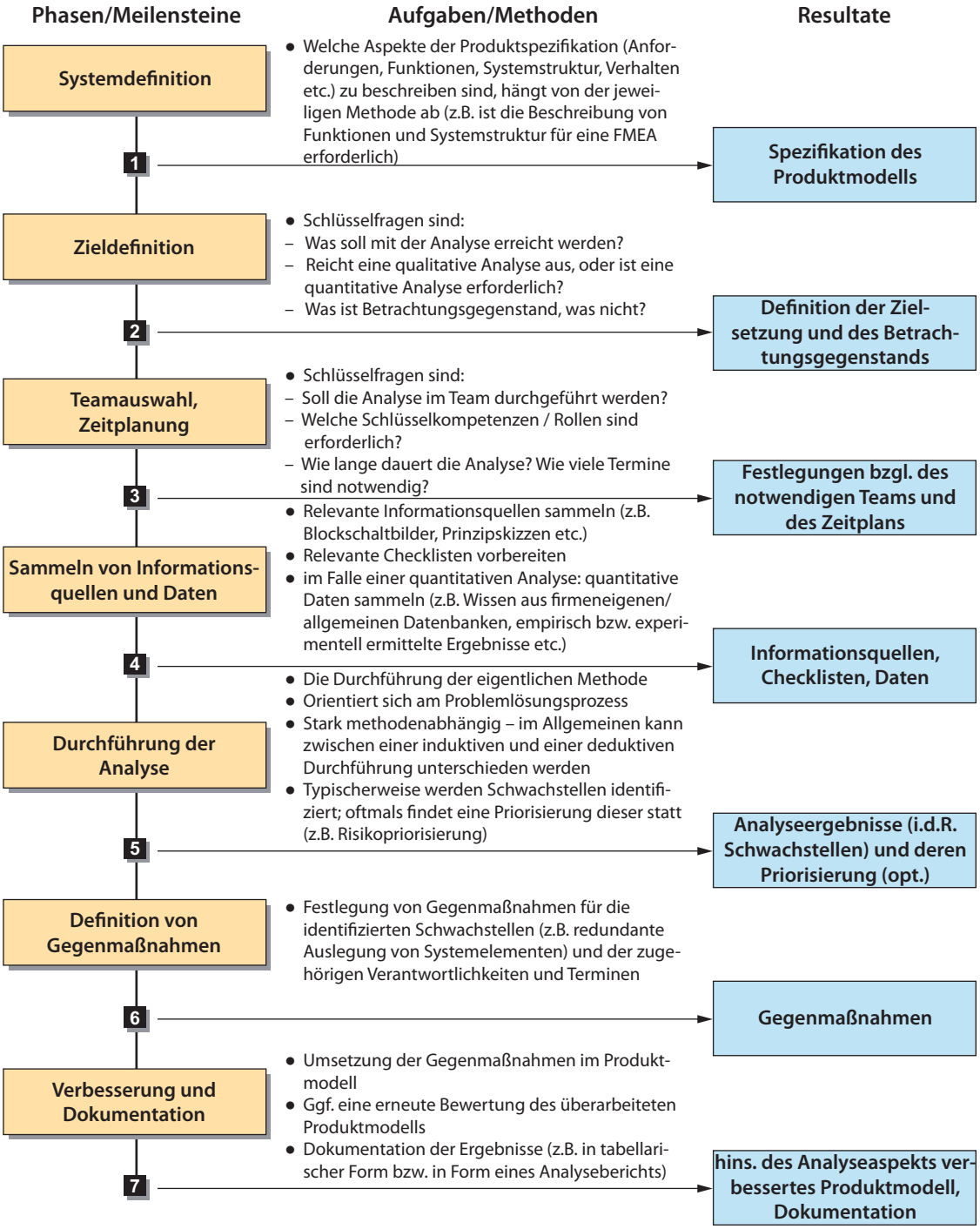


Bild 3-9: Generisches Vorgehen bei der Anwendung von Methoden der Zuverlässigkeits- und Sicherheitsanalyse

Phase 2 – Zieldefinition: Hier werden die Zielsetzung und der Betrachtungsgegenstand definiert. Dabei wird insbesondere festgelegt, welches Ziel mit der Analyse verfolgt wird, ob eine quantitative Analyse erforderlich ist und was zum Betrachtungsgegenstand gehört und was nicht.

Phase 3 – Teamauswahl, Zeitplanung: In dieser Phase erfolgt zum einen die Festlegung des für die Durchführung der Analyse erforderlichen Teams im Sinne von Schlüsselkompetenzen bzw. Rollen. Zum anderen wird die zugehörige Zeitplanung definiert.

Phase 4 – Sammeln von Informationsquellen und Daten: Es werden die relevanten Informationsquellen gesammelt (z.B. vorliegende Blockschaltbilder, Analyseresultate aus älteren Produktgenerationen bzw. in Bezug auf artverwandte Produkte, Prinzipskizzen etc.). Ebenso werden relevante Checklisten vorbereitet. Handelt es sich um eine quantitative Analyse, so ist darüber hinaus die Sammlung quantitativer Daten erforderlich (z.B.: Wissen aus firmeneigenen bzw. allgemeinen Datenbanken, empirisch bzw. experimentell bestimmte Daten etwa aus Tests, Feldeinsatz etc.).

Phase 5 – Durchführung der Analyse: Hier wird die eigentliche Analyse durchgeführt. Diese orientiert sich am Problemlösungsprozess und liefert typischerweise Schwachstellen hinsichtlich Sicherheit bzw. Zuverlässigkeit als Ergebnis. Üblicherweise erfolgt zusätzlich eine Priorisierung der Schwachstellen statt (z.B. eine qualitative Risikopriorisierung mit Hilfe einer Risikoprioritätszahl bei einer FMEA etc.)

Phase 6 – Definition von Gegenmaßnahmen: Für die in Phase 5 identifizierten Schwachstellen werden Gegenmaßnahmen definiert. Gemeint sind Maßnahmen zur Steigerung der Zuverlässigkeit bzw. Sicherheit (z.B. redundante Auslegung, Signalplausibilisierung etc.). Ebenso werden die zugehörigen Verantwortlichkeiten und Termine festgelegt.

Phase 7 – Verbesserung und Dokumentation: Hier erfolgt die Umsetzung der definierten Gegenmaßnahmen. In diesem Zusammenhang wird das Produktmodell überarbeitet und ggf. einer erneuten Bewertung unterzogen. Resultat ist ein hins. Zuverlässigkeit bzw. Sicherheit verbessertes Produktmodell. Die Analyseergebnisse werden dokumentiert. Dies kann z.B. in tabellarischer Form oder in Form eines Analyseberichts erfolgen.

Aus dem dargestellten generischen Vorgehensmodell ist Folgendes ersichtlich: Die wesentlichen Unterscheidungsmerkmale zwischen den Methoden bestehen in den erforderlichen Inputs (welche Aspekte und Informationen müssen in der als Ausgangspunkt für die Analyse dienenden Spezifikation des Produktmodells vorliegen), der Zielsetzung der Methode, der Durchführung der Methode und den Resultaten.

Nachfolgend werden ausgewählte etablierte Methoden der Zuverlässigkeits- und Sicherheitsanalyse vorgestellt. Dabei wird auf die oben genannten Unterscheidungsmerkmale eingegangen. Insbesondere werden für jede Methode Input-Output-Diagramme, welche die notwendigen Eingangsinformationen und Resultate darstellen, sowie Vorlagen vorgestellt. Aus der Darstellung der Methoden wird deutlich, dass die meisten der Methoden ein hohes Potential für einen frühzeitigen Einsatz in der Konzipierung auf Basis der Spezifikation einer Produktkonzeption aufweisen.

3.2.1 Methoden zur Gefahrenanalyse nach MIL-STD-882

Der MIL-STD-882 ist ein technischer Militärstandard des US-amerikanischen Verteidigungsministeriums (Department of Defense, DoD) für Absicherung der funktionalen Systemsicherheit [MIL-STD-882]. Er liegt derzeit in der Version E vor. Der Standard beschreibt eine Menge von Methoden zur Gefahrenanalyse. Sie ermöglichen die Identifikation von Gefahren, deren Ursachen und Auswirkungen sowie die Definition von Gegenmaßnahmen. Ausgewählte Methoden werden nachfolgend vorgestellt. Diese sind konkret die vorläufige Gefahrenliste (PHL), die vorläufige Gefahrenanalyse (PHA), die Gefahrenanalyse auf Subsystemebene (SSHA), die Gefahrenanalyse auf Systemebene (SHA) und die Operating and Support Hazard Analysis (O&SHA) [Eri05, S. 45ff.].

Alle dieser Methoden werden typischerweise in moderierten Workshops unter Verwendung von Kreativitätstechniken wie Brainstorming und Heranziehung von Checklisten (z.B. Gefahren-Checklisten) durchgeführt. Die erarbeiteten Ergebnisse werden typischerweise in tabellarischer Form dokumentiert. Die Methoden können aufeinander aufbauen. Zum Beispiel ist es zu empfehlen, die Ergebnisse der vorläufigen Gefahrenanalyse im Rahmen der Gefahrenanalyse auf Subsystemebene weiter zu verwenden und ggf. zu verfeinern. Ferner können sie im Zusammenspiel mit weiteren etablierten Methoden wie der FTA und der FMEA eingesetzt werden [Eri05].

Ein wesentlicher Bestandteil der meisten dieser Methoden ist eine Risikoeinschätzung. Hierzu erfolgt eine qualitative Bewertung der zwei Bewertungsdimensionen Schwere und Auftretenswahrscheinlichkeit. Für diesen Zweck kann die durch den MIL-STD-882 vorgeschlagene, in Tabelle 3-1 dargestellte Risikoeinschätzungsmatrix[27] verwendet werden [MIL-STD-882, S. 10ff.], [Eri05, S. 80]. Eine derartige Risikoeinschätzung gibt Aufschluss darüber, welche der gefahrbringenden Ausfällmöglichkeiten am kritischsten sind und an erster Stelle angegangen werden sollten.

Tabelle 3-1: Risikoeinschätzungsmatrix nach MIL-STD-882 [MIL-STD-882, S. 12]

Risikoeinschätzungsmatrix				
Schwere / Auftretensws.	katastrophal (1)	kritisch (2)	marginal (3)	vernachlässigbar (4)
häufig (A)	sehr hoch	sehr hoch	hoch	mittel
wahrscheinlich (B)	sehr hoch	sehr hoch	hoch	mittel
gelegentlich (C)	sehr hoch	hoch	mittel	niedrig
selten (D)	hoch	mittel	mittel	niedrig
unwahrscheinlich (E)	mittel	mittel	mittel	niedrig
beseitigt (F)	beseitigt			

[27] Eine ähnliche Risikomatrix mit ähnlichen qualitativen Ausprägungen der beiden Bewertungsdimensionen wird auch in der Bahntechnik nach DIN EN 51026 verwendet [Bra07, S. 668ff.], [CENELEC50126].

Nachfolgend erfolgt die Darstellung der einzelnen Methoden der Gefahrenanalyse nach MIL-STD-882. Abschließend findet eine zusammenfassende Bewertung hinsichtlich der Anforderungen aus der Problemanalyse statt.

3.2.1.1 Vorläufige Gefahrenliste (PHL)

Mit der vorläufigen Gefahrenliste (Preliminary Hazard List, PHL) wird eine erste grundlegende Aussage zu den potentiell aus dem System ausgehenden Gefahren und deren möglichen Auswirkungen auf Gesamtsystemebene getroffen [MIL-STD-882, S. 44ff.], [Eri05, S. 55ff.]. Die PHL kommt typischerweise bereits während der Konzipierungsphase „Planen und Klären der Aufgabe“ zum Einsatz. Die mit der PHL ermittelten Gefahren stellen einen Ausgangspunkt für weiterführende Gefahrenanalysen, die in den nachfolgenden Abschnitten beschrieben werden. Die Inputs und Outputs der PHL sind in Bild 3-10 dargestellt. Auf Basis einer vorläufigen Beschreibung der Produktkonzeption (Anwendungsszenarien, Umfeld) werden die möglichen Gefahren und deren Auswirkungen ermittelt.

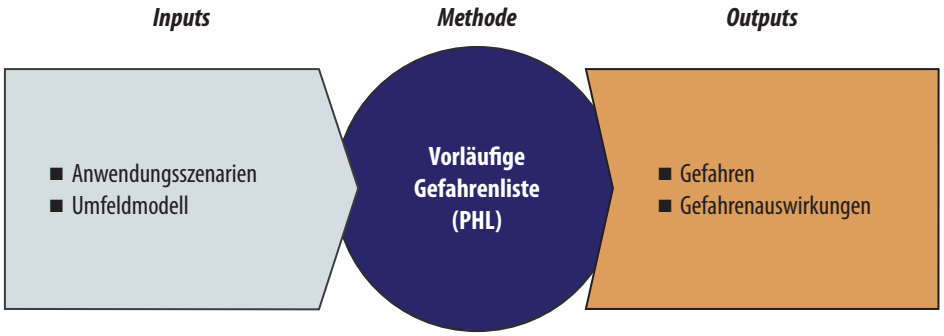


Bild 3-10: Inputs und Outputs der vorläufigen Gefahrenliste PHL

Die Ergebnisse der PHL werden in einer Tabelle schriftlich festgehalten. Tabelle 3-2 zeigt eine Vorlage für eine PHL-Tabelle. Eine verwandte Analyse ist die funktionale Gefahrenanalyse (FHA); mit dieser werden auf Basis der Funktionsbeschreibung die potentiellen Fehlfunktionen bzw. Gefahren ermittelt [Eri05, S. 271ff.].

Preliminary Hazard List (PHL)			
System: ... Blatt: .. Bearbeiter: ... Stand: ...			
Nr.	Betrachtungseinheit	Gefahr	Gefahrenauswirkung
...	...	...	...

Tabelle 3-2: Vorlage für eine vorläufige Gefahrenliste PHL (in Anlehnung an [Eri05, S. 61])

3.2.1.2 Vorläufige Gefahrenanalyse (PHA)

Die vorläufige Gefahrenanalyse (Perliminary Hazard Analysis, PHA) kommt in der Konzipierungsphase „Konzipierung auf Systemebene“ zum Einsatz [MIL-STD-882, S. 46ff.],

[Eri05, S. 73ff.]. Sie ist detaillierter als eine PHL und kann aufbauend auf einer PHL oder als eine eigenständige Analyse durchgeführt werden.

Bild 3-11 zeigt die Eingangs- und Ausgangsgrößen der PHA: Untersucht wird das Gesamtsystem, dessen Einbettung in das Umfeld sowie die vorläufigen Annahmen bzgl. der Systemarchitektur. Hierbei finden Beschreibungen von Anwendungsszenarien und Funktionen ebenfalls Berücksichtigung. Für jede Betrachtungseinheit werden die potentiellen Gefahren, deren Ursachen und Auswirkungen untersucht und auf deren Risiko hin qualitativ bewertet (z.B. mit der Risikoeinschätzungsmatrix). Ebenso werden Verbesserungsmaßnahmen vorgeschlagen. Die Ergebnisse der PHA werden in PHA-Tabellen dokumentiert. Tabelle 3-3 stellt eine Vorlage für eine PHA-Tabelle dar. Je Analyseeinheit entsteht eine PHA-Tabelle [Eri05, S. 84]. Das Ergebnis ist eine hinsichtlich Sicherheit verbesserte Produktkonzeption.

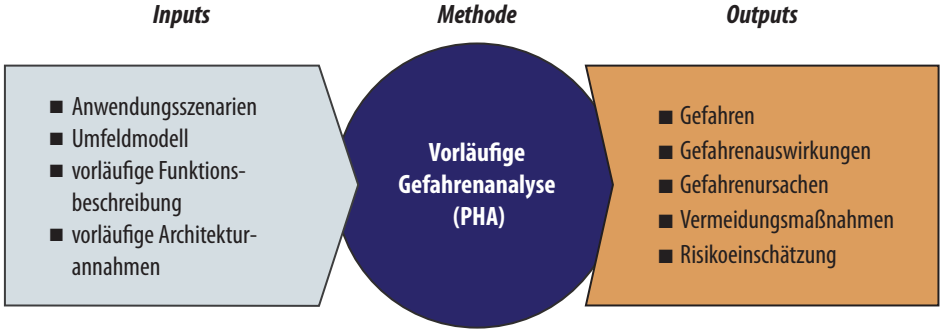


Bild 3-11: Inputs und Outputs der vorläufigen Gefahrenanalyse (PHA)

Die Ergebnisse der PHA stellen einen Ausgangspunkt für weitere Gefahrenanalysemethoden dar, welche zu einem späteren Zeitpunkt im Produktentwicklungsprozess mit der zunehmenden Konkretisierung des Produktmodells durchgeführt werden. Insbesondere wird jede mit der PHA ermittelte Gefahr durch die weiterführenden Gefahrenanalysen detaillierter betrachtet.

Tabelle 3-3: Vorlage für eine PHA (in Anlehnung an [Eri05, S. 79])

Preliminary Hazard Analysis (PHA) für Analyseeinheit ...						
System: ... Blatt: .. Bearbeiter: ... Stand: ...						
Nr.	Gefahr	Ursache(n)	Auswirkung(en)	Anwendungsszenario	Risikoeinschätzung	Verbesserungsmaßnahme(n)
...	...	...	...			

3.2.1.3 Gefahrenanalyse auf Subsystemebene (SSHA)

Die Gefahrenanalyse auf Subsystemebene (Subsystem Hazard Analysis, SSHA) wird auf Basis von Produktbeschreibungen durchgeführt, die einen gewissen Konkretisierungsgrad aufweisen [MIL-STD-882, S. 51ff.], [Eri05, S. 94ff.]. Im Mittelpunkt der Analyse stehen die untergeordneten Subsysteme. Diese Subsysteme werden jeweils in Isolation

voneinander tiefergehend untersucht, eine Betrachtung der subsystemübergreifenden Beziehungen findet im Rahmen der SSHA nicht statt. Eine Voraussetzung für die Durchführung der SSHA ist das Vorhandensein von Spezifikationen auf Subsystemebene. Demnach wird die SSHA typischerweise erst im Rahmen der „Konzipierung auf Subsystemebene“ durchgeführt. Folglich stellt die SSHA eine tiefergehende Gefahrenanalyse als die vorhergehenden PHL und PHA dar: Mit der SSHA werden die mit der PHL und der PHA identifizierten Gefahren detailliert betrachtet und verfeinert, da der Informationsgehalt der Spezifikation der Produktkonzeption höher ist. Auch neue, in den bisherigen Analysen nicht berücksichtigte Gefahren können mit der SSHA gefunden werden.

Folgendes Beispiel verdeutlicht den Zusammenhang zwischen der PHA und der SSHA: Sei das zu analysierende System zum Beispiel eine adaptive Geschwindigkeitsregelung (Adaptive Cruise Control, ACC). So werden im Rahmen der PHA die Subsysteme des ACC wie z.B. der Radarsensor als Black-Box betrachtet, eine Betrachtung der inneren Struktur des Radarsensors findet im Rahmen der PHA nicht statt. Eine SSHA geht ein Schritt weiter: es werden auch die Subsysteme des Radarsensors wie Antennen, Steuergerät etc. ins Kalkül gezogen.

Bild 3-11 stellt die wesentlichen Eingangsinformationen und Ergebnisse der vorläufigen Gefahrenanalyse dar. Als Eingangsdokumente dienen hierbei die Spezifikation der Systemstruktur auf Subsystemebene sowie die Beschreibung der zugehörigen Funktionen.

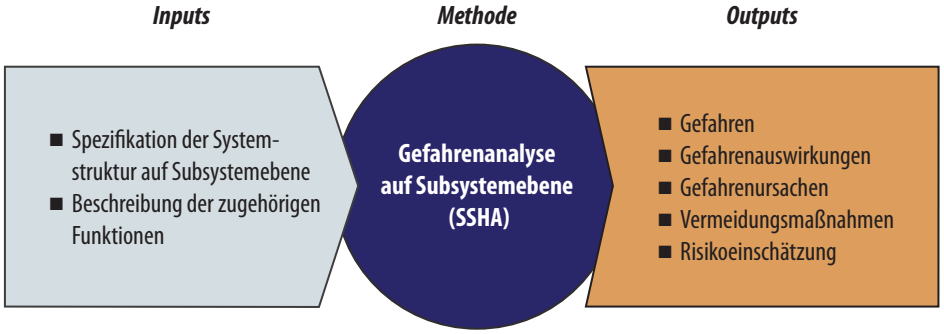


Bild 3-12: Inputs und Outputs der Gefahrenanalyse auf Subsystemebene (SSHA)

Auch die Ergebnisse der SSHA werden in tabellarischer Form dokumentiert. Tabelle 3-4 zeigt eine Vorlage für eine SSHA-Tabelle.

Tabelle 3-4: Vorlage für die Gefahrenanalyse auf Subsystemebene SSHA (in Anlehnung an [Eri05, S. 108])

Subsystem Hazard Analysis (SSHA) für Subsystem ...							
System: ... Blatt: .. Bearbeiter: ... Stand: ...							
Nr.	**Gefahr**	**Ursache(n)**	**Auswirkung(en)**	**Anwendungs-szenario**	**Risikoeinschät-zung (davor)**	**Verbesserungs-maßnahme(n)**	**Risikoeinschät-zung (danach)**
...	...	...	...				

3.2.1.4 Gefahrenanalyse auf Systemebene (SHA)

Die Gefahrenanalyse auf Systemebene (System Hazard Analysis, SHA) ist eine Analysemethode zur Evaluierung der Sicherheit auf Gesamtsystemebene mit Fokus auf die Schnittstellen und Flüsse zwischen den Subsystemen und die Interaktion des Systems mit dem Umfeld [MIL-STD-882, S. 54ff.], [Eri05, S. 115ff.]. Ebenso findet eine Berücksichtigung möglicher Ausfälle infolge gemeinsamer Ursache statt (vgl. Abschnitt 2.1.2 für eine Definition) [Eri05, S. 122]. Demnach eignet sich die SHA besonders gut für einen Einsatz in der Konzipierungsphase „Konzeptintegration".

Bild 3-13 zeigt die wesentlichen Inputs und Outputs der SHA. Als wesentliche Inputs dienen die Beschreibung der Schnittstellen zum Umfeld sowie die Spezifikation der Zusammenhänge zwischen den Subsystemen (Flüsse und Schnittstellen). Demnach ist die SHA eine ideale Ergänzung zur SSHA, welche die einzelnen Subsysteme an sich fokussiert und deren Interaktion mit anderen Subsystemen nicht in den Mittelpunkt stellt.

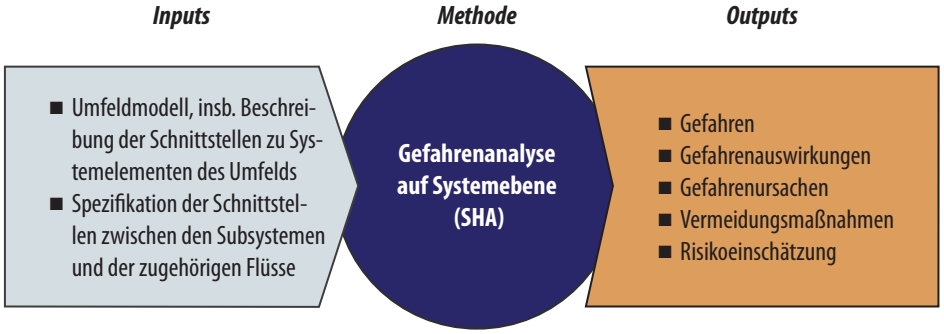


Bild 3-13: Inputs und Outputs der Gefahrenanalyse auf Systemebene SHA

Die SHA wird typischerweise erst dann durchgeführt, wenn die SSHA vollständig abgeschlossen wurde [Eri05, S. 118]. Darüber hinaus baut die SHA auf den Ergebnissen der PHL, PHA – soweit vorhanden – auf und verfeinert diese. Empfehlenswert ist die Durchführung der SHA im Wechselspiel mit der Operating and Support Hazard Analysis (O&SHA), die in Abschnitt 3.2.1.5 vorgestellt wird und die Betrachtung des Systemverhaltens in den Mittelpunkt stellt. Ferner kann die SHA in Kombination mit weiteren Methoden wie der FTA durchgeführt werden, damit die Auswirkung ausgewählter Gefahren auf der Gesamtsystemebene detaillierter betrachtet werden kann. Dies ist insbesondere dann zu empfehlen, wenn im Rahmen einer SHA Gefahren gefunden werden, die auf Ausfälle infolge gemeinsamer Ursache zurückzuführen sind. Denn diese können mit einer FTA umfassender untersucht werden.

Die Ergebnisse der SHA werden in einer SHA-Tabelle dokumentiert. Eine Vorlage für eine SHA-Tabelle ist in Tabelle 3-5 zu sehen. Die Spalte „Sicherheitsrelevante Funktion aus Gesamtsystemebene" verdeutlicht, dass der Fokus der SHA auf der Untersuchung von Gefahren auf Gesamtsystemebene liegt.

Tabelle 3-5: Vorlage für die Gefahrenanalyse auf Systemebene SHA (in Anlehnung an [Eri05, S. 126])

System Hazard Analysis (SHA)						
System: ... Blatt: .. Bearbeiter: ... Stand: ...						
Nr.	Sicherheitsrelevante Funktion auf Gesamtsystemebene	Gefahr	Ursache(n)	Auswirkung(en)	Risikoein-schätzung	Verbesserungs-maßnahme(n)
...	...		...	...		

3.2.1.5 Operating and Support Hazard Analysis (O&SHA)

Operating and Support Hazard Analysis (O&SHA, auch bekannt als Operating Hazard Analysis) ist eine Gefahrenanalyse, die das Ablaufverhalten des Systems im normalen Betrieb, während Test, Installation, Instandhaltung, Reparatur, Ausbildung, Lagerung, Transport sowie in Notfall- und Rettungssituationen etc. fokussiert [MIL-STD-882, S. 57ff.], [Eri05, S. 131ff.].

Für die Erläuterung der O&SHA sind die Begriffe einer Aktivität und einer Aktion von zentraler Bedeutung. In dieser Arbeit werden die Definitionen aus der Sprachspezifikation der UML verwendet [OMG11, S. 319]: Eine Aktivität beschreibt das für die Erreichung eines Ziels vorgegebene Ablaufverhalten in Form eines Flusses von sogenannten Aktionen. Eine Aktion stellt hierbei eine innerhalb der jeweiligen Aktivität durchzuführende Aufgabe dar. Ein Beispiel einer Aktivität ist „Batterie austauschen“. Die zugehörigen Aktionen sind z.B. „alte Batterie entfernen“, „Ersatzbatterie einsetzen“ etc.

Bild 3-14 zeigt die wesentlichen Inputs und Outputs der O&SHA. Eine wesentliche Voraussetzung für die Durchführung ist das Vorliegen von Beschreibungen des Ablaufverhaltens des Systems. Diese können z.B. in Form von Aktivitätsdiagrammen vorliegen. In diesem Zusammenhang kommen ebenso die Beschreibungen von Anwendungsszenarien zur Verwendung. Im Rahmen der O&SHA werden auch die im Rahmen der Herstellung, des Betriebs, der Instandhaltung des Systems etc. zum Einsatz kommenden Chemikalien, Werkstoffe etc. und die damit verbundenen Gefahren ins Kalkül gezogen.

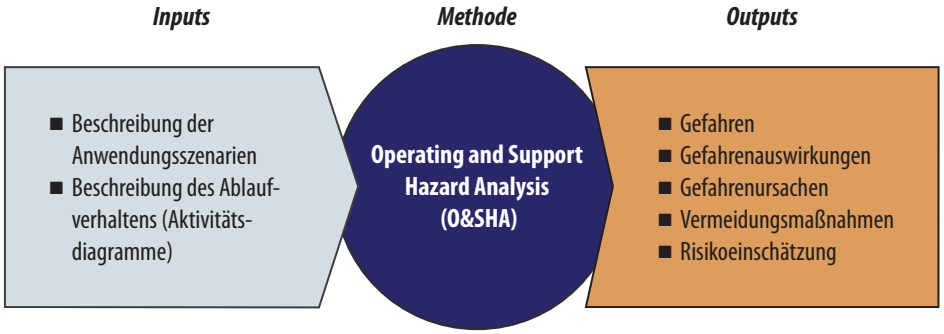


Bild 3-14: Inputs und Outputs der Operating and Support Hazard Analysis (O&SHA)

Die Ergebnisse der O&SHA werden in einer O&SHA-Tabelle beschrieben. Dabei entsteht eine Tabelle je Betrachtungseinheit und Aktivität. Tabelle 3-6 zeigt eine Vorlage für eine solche Tabelle. Für jede Aktion innerhalb der betrachteten Aktivität werden Gefahren identifiziert, welche mit den mit System im Zusammenhang stehenden Abläufen verbunden sind. Ebenfalls werden deren Ursachen (Prozesse, Fehler im Systementwurf, menschliches Versagen, Werkstoffeigenschaften etc.) und potentielle Auswirkungen ermittelt und auf deren Risiko hin bewertet. Darauf aufbauend erfolgt die Festlegung von sicherheitsbezogenen Anforderungen zum Abstellen der Gefahr. Dies umfasst insbesondere Anforderungen in Bezug auf Bedienungs- und Warnungshinweise etc., welches es in den Handbüchern, Bedienungseinleitungen etc. zu unterbringen gilt.

Tabelle 3-6: Vorlage für die Operating and Support Hazard Analysis O&SHA (in Anlehnung an [Eri05, S. 138])

Operating and Support Hazard Analysis (O&SHA) für Betrachtungseinheit ...						
System: ... Aktivität: ... Blatt: .. Bearbeiter: ... Stand: ...						
Nr.	**Aktion**	**Gefahr**	**Ursache(n)**	**Auswirkung(en)**	**Risikoeinschätzung**	**Verbesserungsmaßnahme(n)**
...	...		...	...		

3.2.1.6 Bewertung

Auch wenn die Methoden der Gefahrenanalyse nach MIL-STD-882 aus dem Militärbereich kommen, lassen sich diese sehr gut auf andere Branchen übertragen. Sehr gut geeignet sind die Methoden zum Einsatz in der Konzipierung. Unterstrichen wird dies durch die Tatsache, dass die Methoden an unterschiedlichen Stellen der Konzipierung nach dem Referenzprozessmodell aus Abschnitt 3.1.4 eingesetzt werden können. So kann in der Konzipierungsphase „Planen und Klären der Aufgabe“ die PHL zum Einsatz kommen, die PHA in der „Konzipierung auf Systemebene“, die SSHA eignet sich sehr gut für die „Konzipierung auf Subsystemebene“ und die SHA unterstützt die Absicherung der Sicherheit im Rahmen der „Konzeptintegration“. Die Gefahrenanalysemethoden sind intuitiv anwendbar und problemunabhängig. Sie weisen ferner ein hohes Potential für eine Durchführung auf Basis der Spezifikation der Produktkonzeption auf.

3.2.2 Weitere ausgewählte Methoden der Sicherheits- und Zuverlässigkeitstechnik

Neben den Gefahrenanalysen nach MIL-STD-882 existiert eine Menge von weiteren etablierten Methoden der Sicherheits- und Zuverlässigkeitstechnik. Nachfolgend wird eine Auswahl derartiger Methoden vorgestellt. Abschließend findet eine zusammenfassende Bewertung der Methoden im Hinblick auf die in der Problemanalyse aufgestellten Anforderungen.

3.2.2.1 Gefahrenanalyse und Risikoeinschätzung nach ISO 26262

Mit der durch die ISO 26262 vorgeschriebenen Methode der Gefahrenanalyse und Risikoeinschätzung[28] (engl. hazard analysis and risk assessment) werden zum einen die aus dem Produkt ausgehenden Gefahren identifiziert und bewertet [ISO26262-3, S. 6ff. und 18ff.], [LPP10, S. 122ff.]. Zum anderen werden die durch das Produkt zu erreichenden Sicherheitsziele formuliert und mit einem Automotive Sicherheitsintegritäts-Level (ASIL) versehen. Bild 3-15 zeigt das zugehörige Vorgehen, welches folgende fünf Phasen umfasst [LPP10, S. 122ff.]:

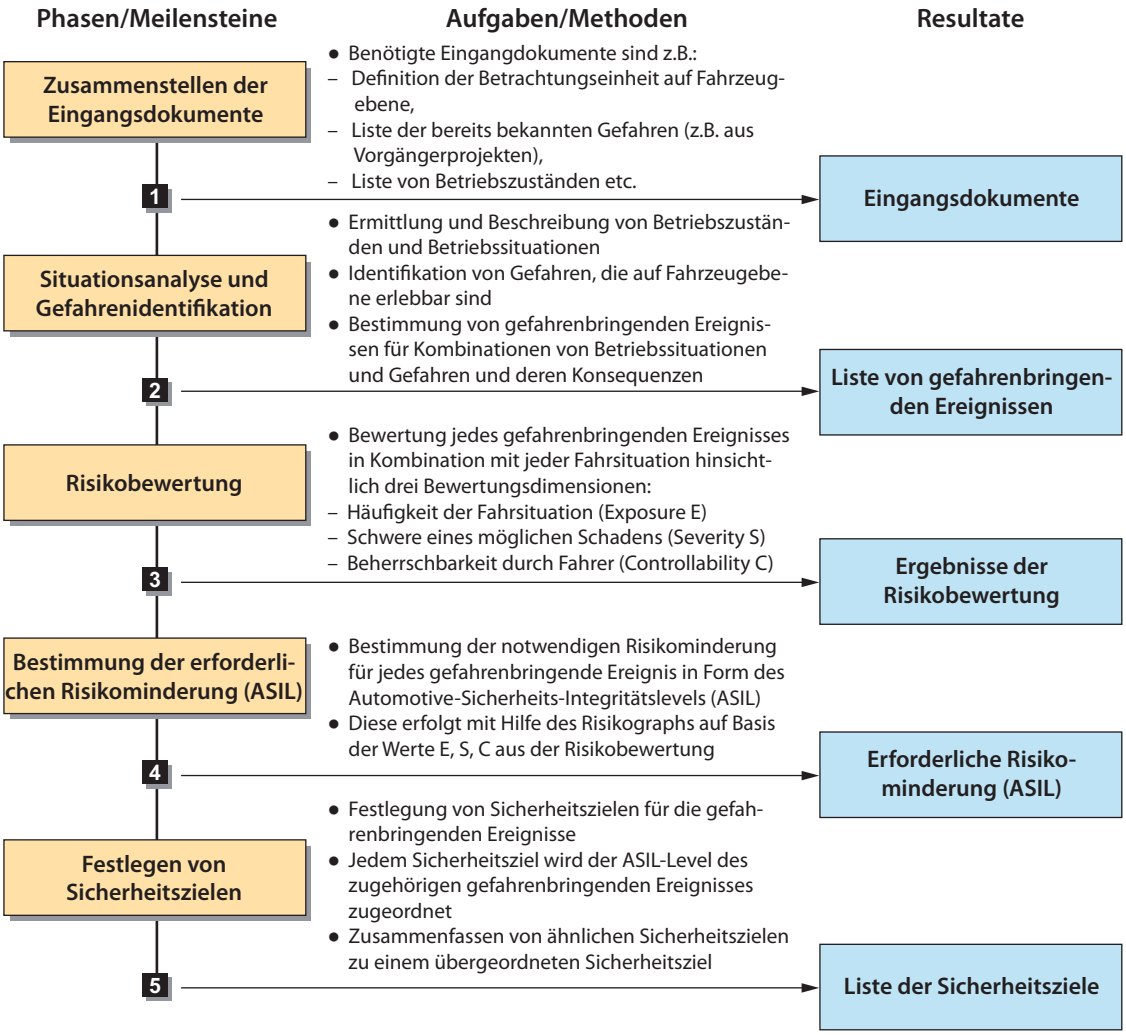


Bild 3-15: Vorgehen zur Gefahrenanalyse und Risikoeinschätzung [LPP10, S. 123]

[28] Bzgl. der Bestimmung der Sicherheitsziele und der ASIL-Level gibt die ISO 26262 konkrete Vorgaben und mit der Gefahrenanalyse und Risikoeinschätzung eine konkrete Methode vor. Die Grundnorm für funktionale Sicherheit IEC61508 geht hier aufgrund ihrer Anwendbarkeit für unterschiedliche Branchen und Anwendungen anders vor. Sie stellt eine Menge von Methoden zur Bestimmung der Sicherheitsintegritätslevel vor. Welche Methode verwendet wird, hängt von der konkreten Problemstellung ab. Für detailliertere Informationen hierzu sei auf [SS11b, S. 22ff.], [IEC61508-5, S. 21ff.] verwiesen.

Phase 1 – Zusammenstellung der Eingangsdokumente: Hier werden die relevanten Eingangsdokumente zusammengestellt. Gemeint sind z.B. die Definition der Betrachtungseinheit auf Fahrzeugebene (insb. Umfeldmodell und Funktionen; engl. Item Definition), eine Liste bereits bekannter Gefahren (z.B. auf Basis von Vorgängerprojekten), Liste von Betriebszuständen (z.B. Initialisierung, Normalbetrieb, Shutdown und Wartungsbetrieb) und Einsatzbedingungen (z.B. Witterung, Fahrbedingungen), Liste möglicher Fehlbedienungen etc. [LPP10, S. 123], [ISO26262-3, S. 7].

Phase 2 – Situationsanalyse und Gefahrenidentifikation: Hier erfolgt zum einen die Identifikation und Beschreibung von Betriebszuständen (engl. operating modes) und Betriebssituationen (engl. operational situations), in denen eine Abweichung von gewünschtem Verhalten zu einer Gefahr führen kann [ISO26262-3, S. 7]. Dabei wird sowohl die korrekte Nutzung als auch die vorhersehbare Fehlanwendung betrachtet. Beispiele von zu berücksichtigenden Betriebssituationen sind „Autobahn mit freier Fahrt“, „Autobahn mit Stop & Go“, „Landstraße“, „Spurwechsel im Stadtverkehr“, „Tunnelfahrt“, „Parkieren“, „Fahrzeug auf Hegebühne“ etc. [LPP10, S. 123], [ISO26262-1, S. 11]. Zum anderen werden die auf Fahrzeugebene erlebbaren Gefahren ermittelt. Für die relevanten Kombinationen von Betriebssituationen und Gefahren werden die gefahrenbringenden Ereignisse identifiziert [ISO26262-3, S. 8]. Dabei wird in dieser Phase noch keine Ursachenanalyse durchgeführt. Beispiele für gefahrenbringende Ereignisse sind „Fahrlicht schaltet unmotiviert ab“, „Fahrlicht schaltet auf Anforderung nicht ein“, „Lenkunterstützung bewirkt einen ungewollten Lenkeingriff“ etc. [LPP10, S. 124].

Phase 3 – Risikobewertung: Hier wird jedes der ermittelten gefahrenbringenden Ereignisse (Phase 3) in Kombination mit jeder Fahrsituation (Phase 2) auf sein Risiko hin bewertet. Die Bewertung erfolgt entlang der drei in Bild 3-16 a) dargestellten Kenngrößen:

a)
E – Häufigkeit der Fahrsituation (Exposure E)
E0: Unvorstellbar
E1: Sehr niedrige Wahrscheinlichkeit
E2: Niedrige Wahrscheinlichkeit
E3: Mittlere Wahrscheinlichkeit
E4: Hohe Wahrscheinlichkeit

S – Schwere eines möglichen Schadens (Severity S)
S0: Keine Verletzungen
S1: Leichte und mittlere Verletzungen
S2: Schwere Verletzungen – Überleben wahrscheinlich
S3: Lebensgefährliche Verletzungen – Überleben unwahrscheinlich

C – Beherrschbarkeit durch den Fahrer (Controllability C)
C0: Im Allgemeinen beherrschbar
C1: Einfach beherrschbar
C2: Normalerweise beherrschbar
C3: Schwierig oder nicht beherrschbar

b)

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Bild 3-16: Risikograph nach ISO 26262: a) Kenngrößen der Risikobewertung und deren Ausprägungen, b) Bestimmung des ASIL-Levels anhand der Werte der Kenngrößen [ISO26262-4, S. 10]

- **Häufigkeit der Fahrsituation (Exposure, E):** von E0 (unvorstellbar) bis E4 (hohe Wahrscheinlichkeit). E4 bedeutet bei jeder Fahrt, z.B. beim Schalten, Beschleunigen. E2 heißt typischerweise mehrmals im Jahr, z.B. Anhängerfahrt [LPP10, S. 125].
- **Schwere eines möglichen Schadens (Severity, S):** von S0 (keine Verletzungen) bis S3 (Lebensgefährliche Verletzungen – Überleben unwahrscheinlich). Ein Beispiel für die Bewertung mit S3 ist ein Seitenaufprall eines anderen Fahrzeugs mit Geschwindigkeit über 35 km/h [LPP10, S. 125].
- **Beherrschbarkeit durch den Fahrer (Controllability, C):** von C0 (Im Allgemeinen beherrschbar) bis C3 (schwierig oder nicht beherrschbar). Beispiel für C1: ein Fahrer kann i.d.R. Personenschäden durch Bremsen vermeiden, wenn die Lenksäule beim Anfahren blockiert [LPP10, S. 125].

Phase 5 – Bestimmung der erforderlichen Risikominderung (ASIL): Für jedes gefahrenbringende Ereignis wird die erforderliche Risikominderung in Form eines ASIL-Levels bestimmt. Die ISO 26262 sieht vier Ausprägungen eines ASIL-Levels vor. Diese sind in aufsteigender Reihenfolge: ASIL A, ASIL B, ASIL C und ASIL D. Liegt keine Sicherheitsrelevanz vor, so wird statt einer ASIL-Einstufung die Bezeichnung QM („Quality Management“) verwendet. Die Bestimmung des ASIL-Levels erfolgt unter Verwendung des in Bild 3-16 b) dargestellten Risikographs auf Basis der in Phase 4 durchgeführten Risikobewertung. So ergibt sich aus einer Risikobewertung S = S2, E = E3 und C = E3 ein ASIL B.

Phase 6 – Festlegen von Sicherheitszielen: Für die gefahrenbringenden Ereignisse werden die zu sicherstellenden Sicherheitsziele festgelegt. Jedem Sicherheitsziel wird dabei der ASIL-Level des zugrunde liegenden gefahrenbringenden Ereignisses zugeordnet [ISO26262-3, S. 11]. Ähnliche Sicherheitsziele können zu einem übergeordneten Sicherheitsziel zusammengefasst werden [ISO26262-3, S.11]. In diesem Fall ist der höchste ASIL-Level der ursprünglichen Sicherheitsziele zu übernehmen. Tabelle 3-7 zeigt Beispiele von Sicherheitszielen und typische ASIL-Einstufungen.

Tabelle 3-7: Beispiele von Sicherheitszielen [LPP10, S. 218], [PH13, S. 391]

System	Sicherheitsziel	Typischer ASIL
ESP (Elektronisches Stabilitätsprogramm)	Gefährlich falsche Eingriffe in die Fahrzeugstabilität verhindern	ASIL D
Elektromagnetische Lenkradverriegelung	Verhindern der Verriegelung während der Fahrt	ASIL D
Airbag	Verhindern des Auslösens, wenn nicht notwendig	ASIL D
EPS (Electric Power Steering, Elektromechanisches Lenksystem)	Unmotiviertes Lenken verhindern	ASIL D
	Plötzliches Einsetzen der Lenkunterstützung z.B. durch ungewolltes Wiedereinschalten verhindern	ASIL A
	Ausfall der Lenkunterstützung verhindern	QM

Bild 3-17 fasst die wesentlichen Eingangsinformationen und Resultate der Gefahrenanalyse und Risikoeinschätzung zusammen. Die Resultate der Gefahrenanalyse und Risikoeinschätzung stellen, wie in Abschnitt 3.1.2 beschrieben, eine wesentliche Grundlage für alle weiteren sicherheitsbezogenen Aktivitäten im Sicherheitslebenszyklus dar. Ein Beispiel für die Anwendung der Gefahrenanalyse und Risikoeinschätzung wird in Abschnitt 5.6 vorgestellt.

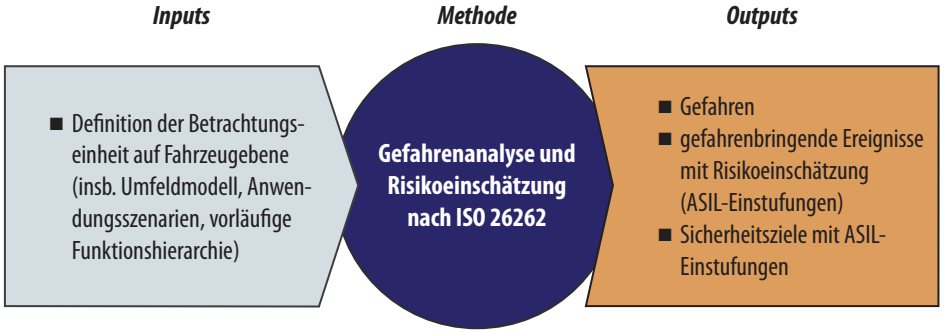


Bild 3-17: Inputs und Outputs der Gefahrenanalyse und Risikoeinschätzung nach ISO 26262 (in Anlehnung an [ISO26262-3, S. 17])

3.2.2.2 Hazard and Operability Study (HAZOP)

Hazard and Operability Study (HAZOP) ist eine auf einer Liste von Leitworten beruhende Methode zur Absicherung der Sicherheit und Zuverlässigkeit [Eri05, S. 365ff.], [OK12, S. 189ff.]. Die zu verwendenden Leitworte werden jeweils ausgehend von der zugrunde liegenden Problemstellung aufgestellt. Zum Beispiel kann die Klassifikation von Ausfällen nach FENELON ET AL. als Liste von Leitworten verwendet werden, welche die in Bild 3-18 dargestellten Ausfallarten vorsieht [FMN+94].

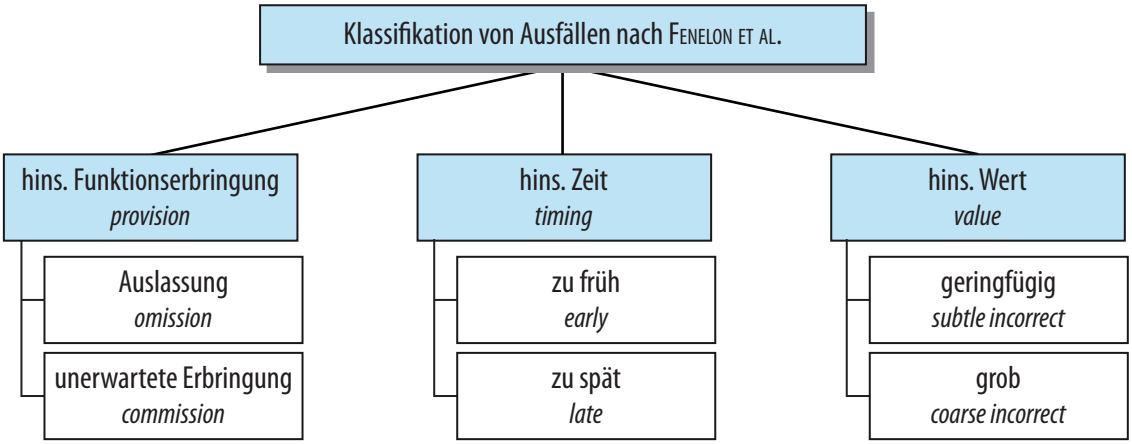


Bild 3-18: Klassifikation von Ausfällen nach FENELON ET AL. [FMN+94]

Bild 3-19 zeigt die wesentlichen Inputs und Outputs der HAZOP-Analyse. Demnach wird für jedes Systemelement unter Berücksichtigung dessen Schnittstellen und der zugrunde liegenden Funktionen entlang der Liste von Leitworten untersucht, ob und wie es zu einer Abweichung von der gewünschten Funktionalität kommen kann.

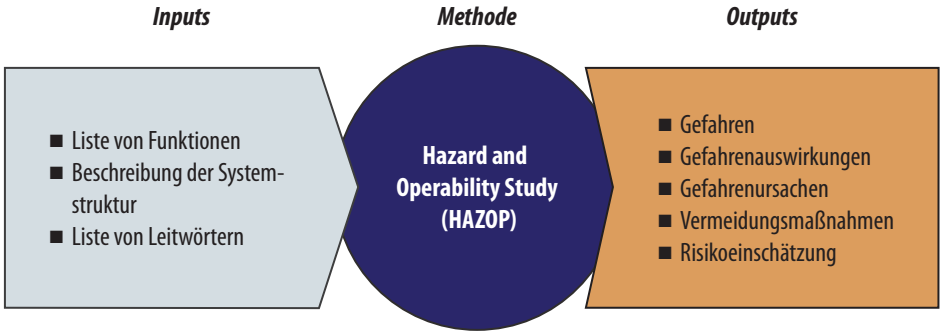


Bild 3-19: Inputs und Outputs der HAZOP-Analyse

Die Ergebnisse werden in tabellarischer Form dokumentiert. Eine beispielhafte Vorlage für die HAZOP-Analyse ist in Tabelle 3-8 zu sehen. Die HAZOP-Analyse lässt sich mit anderen Analysemethoden kombinieren (z.B. mit einer PHA, FMEA etc.).

Tabelle 3-8: Vorlage für eine HAZOP-Tabelle (in Anlehnung an [Eri05, S 374], [OK12, S. 192])

HAZOP Analyse								
System: ... Blatt: .. Bearbeiter: ... Stand: ...								
Nr.	System-element	Funktion	Leitwort	Auswirkung	Ursache(n)	Gefahr	Risikoeinschät-zung	Verbesserungs-maßnahme(n)
...	...	...	...	...	...	...	...	...

3.2.2.3 Fehlzustandsbaumanalyse (FTA)

Die Fehlzustandsbaumanalyse (Fault Tree Analysis, FTA) ist eine in der Praxis sehr etablierte, deduktive Analysemethode [DIN61025], [BL04, S. 160ff.], [Eri05, S. 183ff.], [MP10, S. 251ff.], [OK12, S. 157f.]. Bild 3-20 fasst ausgewählte, zur Beschreibung eines Fehlzustandsbaums verwendete Symbole zusammen und stellt eine kurze Beschreibung dieser bereit.

Ausgangspunkt ist die Festlegung der zu untersuchenden Ausfallmöglichkeit (Hauptereignis, engl. top event); diese stellt die Wurzel des Fehlzustandsbaums dar. Anschließend werden alle potentiellen Ursachen für das Hauptereignis ermittelt und als untergeordnete Knoten (Ereignisse) abgebildet. Diese untergeordneten Ereignisse werden jeweils mittels eines Gatters (typischerweise UND bzw. ODER Gatter) miteinander verknüpft. Die Verknüpfung mit Hilfe eines UND Gatters beschreibt, dass das übergeordnete Ereignis dann eintritt, wenn alle untergeordneten Ereignisse eingetreten sind. Im Falle einer ODER-Verknüpfung reicht das Eintreten von mindestens einem der untergeordneten Ereignisse aus. Die untergeordneten Ereignisse werden in analoger Weise ebenfalls untersucht und weiter verfeinert, wodurch sich eine Baumstruktur ergibt. In der graphischen Darstellung, wird die das Hauptergebnis repräsentierende Wurzel oben dargestellt, die Leserichtung ist von oben nach unten.

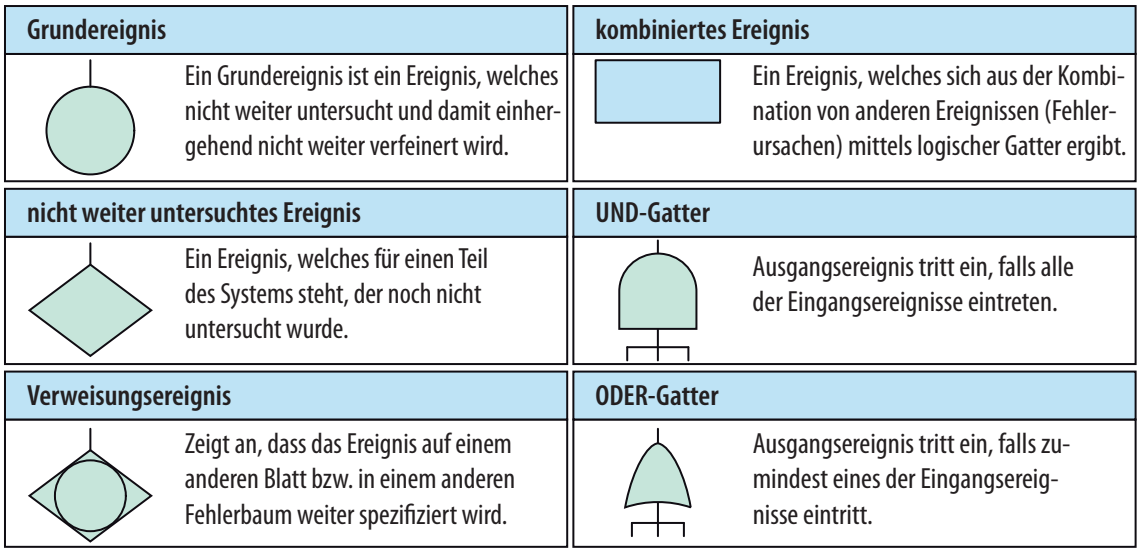


Bild 3-20: Ausgewählte Symbole zur Erstellung eines Fehlzustandsbaums und dessen Bedeutung (in Anlehnung an [DIN61025, S. 37ff.], [OK12, S. 158])

Bild 3-21 zeigt einen beispielhaften Fehlzustandsbaum für ein Getriebe. Das Hauptereignis ist hier „Ausfall Getriebe“. Die möglichen Fehlerursachen, die zu diesem Hauptereignis führen könnten, sind u.a. „Versagen der Lagerung“, „Ausfall Abrieb“ und „Versagen des Gehäuses“. Diese werden im Fehlzustandsbaum weiter untergliedert [BL04, S. 166].

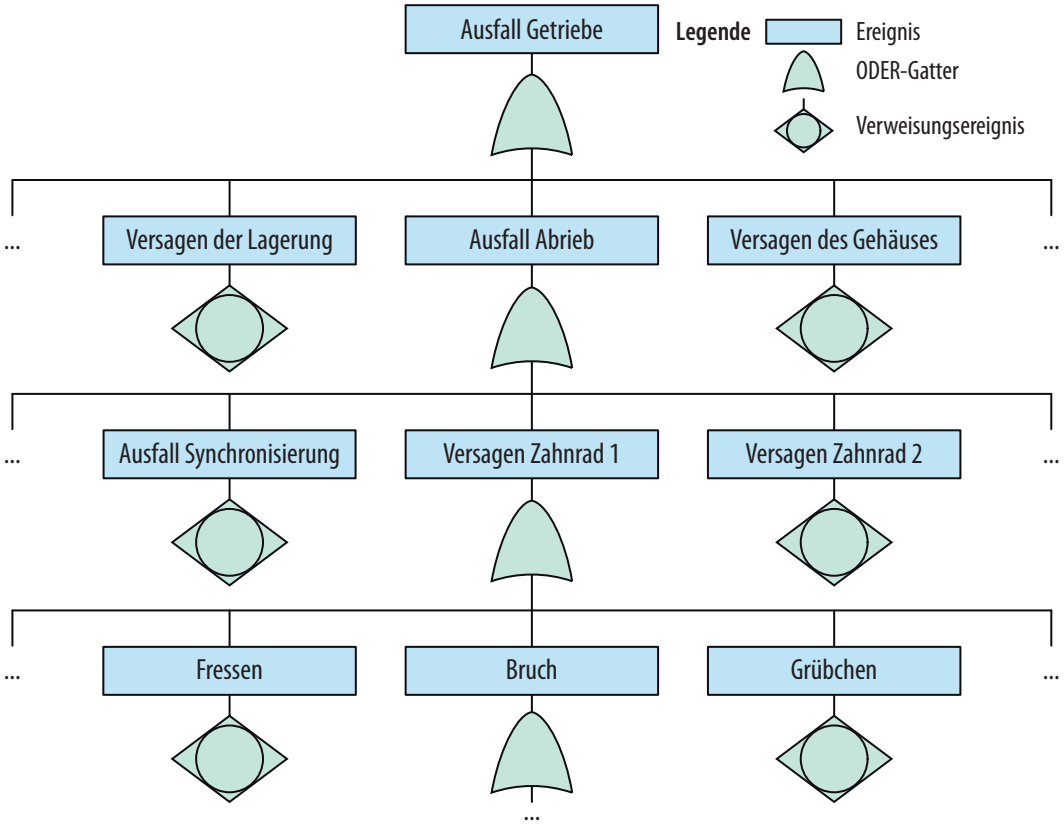


Bild 3-21: Beispiel eines Fehlzustandsbaums für das Hauptereignis „Ausfall Getriebe“; für Legende siehe Bild 3-20 [BL04, S. 166]

Für jedes der zu untersuchenden Hauptereignisse wird jeweils ein Fehlerbaum erstellt [OK12, S. 157]. Für sicherheitsrelevante Systeme, die nach der Sicherheitsnorm IEC 61508 bzw. den Derivaten wie der ISO 26262 entwickelt werden, werden typischerweise die zu den festgelegten Sicherheitszielen korrespondierenden gefahrenbringenden Ereignisse als Hauptergebnisse behandelt.

Das bisher gezeigte Beispiel stellt eine qualitative Untersuchung dar. Soweit die Eintrittswahrscheinlichkeiten der Grundereignisse bekannt sind, kann auch eine quantitative Untersuchung mit einem Fehlzustandsbaum durchgeführt werden [DIN61025, S. 9], [BL04, S. 168ff.], [MP10, S. 261ff.]. Im Rahmen der quantitativen Analyse können die Eintrittswahrscheinlichkeiten der Zwischenereignisse und des Hauptereignisses berechnet werden [DIN61025, S. 9]. Auf Basis eines Fehlzustandsbaums lassen sich Methoden wie die Methode der Minimalschnitte oder die Methode der minimalen Erfolgspfade (vgl. auch Anhang A1.2) durchführen und mit ihrer Hilfe die Kenngrößen der Zuverlässigkeit und Sicherheit wie Ausfallrate und Überlebenswahrscheinlichkeit bestimmen (vgl. auch Abschnitt 2.1.5).

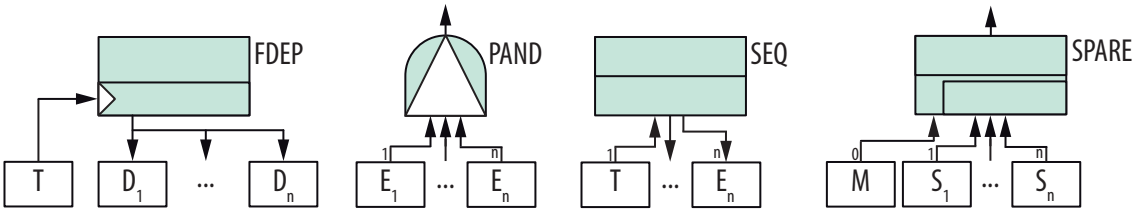
3.2.2.4 Dynamische Fehlzustandsbäume (DFT)

Dynamische Fehlzustandsbäume (engl. Dynamic Fault Tree, DFT) sind eine Erweiterung von klassischen Fehlzustandsbäumen [DBB92], [Cod11], [DIN61025]. Die Gatter der klassischen Fehlzustandsbäume sind statisch: das Ergebnis hängt nicht von der Reihenfolge des Eintritts der Eingangsereignisse ab [DIN61025, S. 16]. DFT führen neue Arten von Gattern ein, die sogenannten dynamischen Gatter. Bei den dynamischen Gattern ist das Ergebnis von der Reihenfolge des Eintritts der Eingangsereignisse abhängig [DIN61025, S. 16]. Folglich können in einem DFT Abhängigkeiten zwischen Fehlern abgebildet und analysiert werden (z.B. kann die Reihenfolge des Eintritts der Fehler spezifiziert werden). Insbesondere lassen sich abhängige Ausfälle modellieren (vgl. auch Abschnitt 2.1.2). Bild 3-22 gibt einen Überblick über die dynamischen Gatter.

Mit dem Ersatzgatter kann insbesondere die dynamische Redundanz („hot standby“ und „cold standby“ Konfiguration) abgebildet werden (vgl. auch Abschnitt 2.1.3).[29] Zur Ana-

[29] Hierzu sind die Ereignisse S_1, …, S_n als Ereignisse mit drei möglichen Zuständen standby, aktiv, ausgefallen abzubilden. Ein Ersatz-Systemelement ist anfangs im Standby-Zustand. Ein Übergang in den aktiven Zustand findet statt, soweit das zu ersetzende Systemelement ausgefallen ist. Die Ausfallrate der Ersatz-Systemelemente gestaltet sich wie folgt: Sei λ die Ausfallrate eines Ersatz-Systemelements in seinem aktiven Zustand. Die Ausfallrate dieses Ersatz-Systemelement in seinem Standby-Zustand beträgt $\alpha\lambda$, wobei α der sogenannte Standby-Faktor mit $0 \leq \alpha \leq 1$ ist. Beträgt der Standby-Faktor 0, so wird das Ersatz-Systemelement als ein Ersatz-Systemelement in der “cold standby” Konfiguration bezeichnet und kann in seinem Standby-Zustand nicht ausfallen. Beträgt der Standby-Faktor 1, so handelt es sich um ein Ersatz-Systemelement in der „hot standby“ Konfiguration. Die Ausfallrate eines derartigen Systemelements ist genauso hoch im aktiven Zustand wie im Standby-Zustand. Ist der Standby-Faktor größer 0 und kleiner 1, so handelt es sich um ein sogenanntes Ersatz-Systemelement in „warm standby“ Konfiguration.

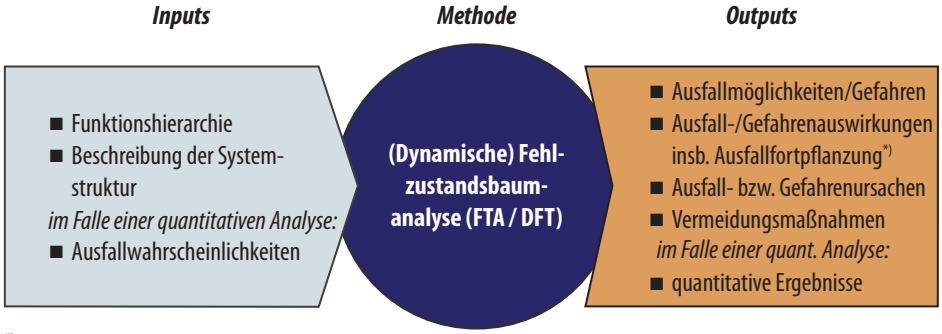
lyse von DFT werden typischerweise zeitkontinuierliche Markoff-Ketten bzw. Stochastische Petri Netze verwendet [MRL11], [Bir07, S. 271], [CSD00], [Cod05]. Die Definition der formalen Semantik von DFT ist zu finden in [BCS10].



Gattername	Beschreibung	Anzahl der Eingänge	Anzahl der Ausgänge
Funktionale Abhängigkeit (Functional Dependency; FDEP)	Das FDEP-Gatter dient zur Modellierung der funktionalen Abhängigkeit zwischen Ereignissen. Es bildet den Zusammenhang zwischen einem auslösenden Ereignis (Trigger T) und einer Menge der von dem auslösenden Ereignis abhängigen Ereignisse (E_1, .. E_n). Tritt das auslösende Ereignis ein, so treten alle der abhängigen Ereignisse ebenfalls ein.	1	≥ 1
Priority-AND (PAND)	Mit dem PAND-Gatter werden sequentielle Abhängigkeiten modelliert. Es bildet den Zusammenhang zwischen einer Menge von Eingangsereignissen (E_1, .. E_n), die mit dem Gatter über nummerierte Kanten verbunden sind, und einem Ausgangsereignis. Das Augangsereignis tritt nur dann ein, wenn die Eingangsereignisse in der durch die Nummerierung der Kanten vorgegebenen Reihenfolge eintreten.	≥ 2	1
Erzwungene Reihenfolge (Sequence Enforcing; SEQ)	Das SEQ-Gatter hat ein auslösendes Ereignis (Trigger T) als Eingang und ist mit einer Menge von abhängigen Ausgangsereignissen (E_1, .. E_n) über nummerierte Kanten verbunden. Tritt das auslösende Ereignis T ein, so hat dies das Eintreten der abhängigen Ausgangsereignisse zur Folge, und zwar in der durch die nummerierten Kanten vorgegebenen Reihenfolge.	1	≥ 2
Ersatzgatter (ERSATZ bzw. SPARE)	Mit dem SPARE-Gatter wird die Existenz und Allokation von Ersatzsystemelementen abgebildet. Es hat ein Ausgangsereignis und ist mit einer Menge von Eingangsereignissen (M, S_1, ..., S_n) über nummerierte Kanten verbunden. M repräsentiert hierbei das Haupt-Systemelement (M ist wahr, wenn das Haupt-Systemelement ausgefallen ist). Die zugehörige Kante ist mit der Nummer 0 versehen. S_1, ..., S_n stellen n Ersatz-Systemelemente dar, welche dazu dienen, das Hauptsystemelement M im Falle seines Ausfalls in seiner Funktion zu ersetzen (S_i ist wahr, wenn das Ersatzsystemelement i ausgefallen ist). Das Ersetzen erfolgt in der durch die nummerierten Kanten vorgegebenen Reihenfolge: M wird durch S_1 ersetzt, S_1 durch S_2 etc. Das Ausgangsereignis des SPARE-Gatters ist wahr, wenn M sowie S_1, ..., S_n alle wahr sind.	≥ 2	1

Bild 3-22: Dynamische Gatter eines dynamischen Fehlzustandsbaums und deren Beschreibung [Cod11, S. 537ff.]

Bild 3-23 zeigt die Inputs und Resultate der Fehlzustandsbaumanalyse. Diese gelten auch für eine auf dynamischen Fehlzustandsbäumen beruhende Analyse.



*) Im Rahmen von Analysemethoden wie die PHA, SHA, FMEA etc. werden lediglich kausale Zusammenhänge in Form von ODER-Beziehungen betrachtet. FTA und DFT gehen darüber hinaus und ermöglichen zusätzlich eine Betrachtung von UND-Beziehungen. Somit können die potentiellen Ausfallfortpflanzungspfade im System detaillierter beschrieben werden.

Bild 3-23: Inputs und Outputs der Fehlzustandsbaumanalyse und der auf dynamischen Fehlzustandsbäumen beruhenden Analyse

3.2.2.5 Fehlzustandsart- und -auswirkungsanalyse (FMEA)

Die Fehlzustandsart- und -auswirkungsanalyse (FMEA) ist eine induktive Analysemethode, die in der Praxis sehr verbreitet ist. Sie wird typischerweise in moderierten Workshops mit Fachexperten aus den involvierten Fachdisziplinen durchgeführt [DIN60812], [Eri05, S. 246ff.], [BL04, S. 106ff.]. Die wesentlichen Inputs und Outputs einer FMEA sind in Bild 3-24 dargestellt. Demnach werden für jedes Systemelement unter Berücksichtigung der zugrunde liegenden Funktion die Ausfallmöglichkeiten bzw. mögliche Gefahren, deren Ursachen und Auswirkungen ermittelt und auf deren Risiko hin beurteilt. Ebenso findet die Festlegung von Vermeidungsmaßnahmen statt.

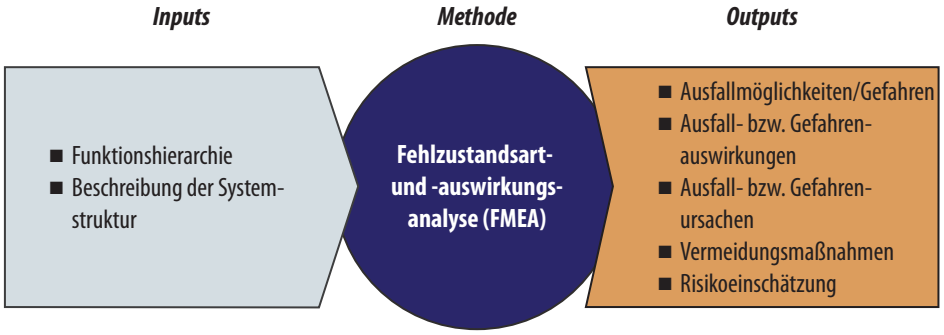


Bild 3-24: Inputs und Outputs der FMEA

Die Ergebnisse einer FMEA werden in tabellarischer Form dokumentiert. Tabelle 3-9 zeigt die Vorlage für eine FMEA-Tabelle.

Im Rahmen der Risikobewertung werden für jede Kombination bestehend aus Ausfallmöglichkeit, Ausfallursache und Ausfallauswirkung jeweils folgende Kennzahlen qualitativ festgelegt: die Schwere der Ausfallauswirkung (S), die Entdeckungswahrscheinlichkeit der Ausfallursache (E) und die Auftretenswahrscheinlichkeit der Ausfallursache (A). Aus den drei Kennzahlen wird durch Multiplikation von S, A und E die Risikoprioritäts-

zahl (RPZ) gebildet, die ein Maß für die Kritikalität darstellt. Die Wertskala zur Bewertung der drei Kennzahlen umfasst typischerweise die ganzzahligen Werte von 1 bis 10 [BL04, S. 114]. Der Wertebereich für die RPZ erstreckt sich folglich von 1 bis 1000. Für die Einschätzungen, die für ein zuverlässiges Produkt extrem negativ ausfallen, wird typischerweise eine 10 vergeben. Zum Beispiel wird die Bewertungszahl 10 für die Entdeckungswahrscheinlichkeit einer Ausfallursache vergeben, deren Entdeckung unwahrscheinlich ist. Kann die Ausfallursache mit hoher Wahrscheinlichkeit sicher und rechtzeitig entdeckt werden, so wird für die Kennzahl E die Bewertungszahl 1 vergeben. Die Schwere einer sicherheitsrelevanten Ausfallauswirkung wird typischerweise mit einer Bewertungszahl 9-10 bewertet.

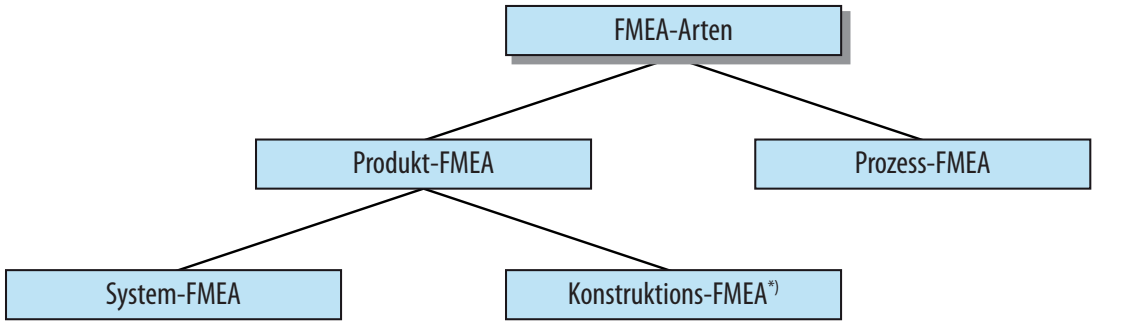
Tabelle 3-9: Vorlage für die FMEA (in Anlehnung an [Eri05, S 249], [BL04, S. 111])

Fehlzustandsart- und -auswirkungsanalyse (FMEA)										
System: ... Blatt: .. Bearbeiter: ... Stand: ...										
Nr.	System-element	Funktion(en)	Ausfall-möglichkeit	Ausfall-auswirkung(en)	S	Ausfall-ursache(n)	E	A	RPZ	Verbesserungs-maßnahme(n)
...	...	..								

S: Schwere der Ausfallauswirkung
E: Entdeckungswahrscheinlichkeit der Ausfallursache
A: Auftretenswahrscheinlichkeit der Ausfallursache
RPZ: Risikoprioritätszahl (RPZ = S × E × A)

Die so ermittelten Risikoprioritätszahlen stellen die Grundlage dafür dar, verschiedene Ausfallmöglichkeiten gegenüberzustellen und Gegenmaßnahmen abzuleiten. Die Ableitung von Gegenmaßnahmen beginnt in der Regel für die Ausfallursache mit der größten RPZ und erfolgt solange, bis eine gewisse Untergrenze der RPZ, z.B. 125, erreicht wird [BL04, S. 114f.]. In diesem Zusammenhang sind auch hohe Einzelbewertungen genauer zu betrachten (auch wenn die zugehörige RPZ kleiner als die festgelegte Untergrenze ist) [BL04, S. 114f.], [Bra07, S. 672f.].

Es gibt mehrere FMEA-Arten. Im Allgemeinen wird zwischen einer Produkt- und einer Prozess-FMEA unterschieden [BL04, S. 110], [DIN60812, S. 5], [LPP10, S. 264] (Bild 3-25). Die Produkt-FMEA fokussiert die Funktionsweise und den Aufbau des Produkts. Es wird zwischen einer System-FMEA und einer Konstruktions- bzw. Entwicklungs-FMEA unterschieden. Die System-FMEA wird auf Systemebene durchgeführt, es werden sowohl Mechanik- als auch Elektronikanteile betrachtet [LPP10, S. 264]. Die Konstruktions- bzw. Entwicklungs-FMEA wird jeweils für die Mechanik und für die Elektronik durchgeführt. Die Prozess-FMEA befasst sich mit den Abläufen zur Herstellung des Produkts. Im Fokus der vorliegenden Arbeit steht die System-FMEA. Die FMEA-Analysen, die auf verschiedenen Ebenen (System, Mechanik / Elektronik, Prozess) durchgeführt werden, überlappen sich [BL04, S. 135]: Mit der zunehmenden Konkretisierung können die Analyseergebnisse von einer FMEA-Art zur nächsten weitergegeben [LPP10, S. 265]. Die Ausfallmöglichkeit der oberen Ebene (z.B. System) kann z.B. als Ausfallauswirkung der FMEA der nächstunteren Ebene übernommen werden (z.B. Mechanik) [BL04, S. 135]. Für konkrete Beispiele siehe [BL04, S. 135f.], [LPP10, S. 265].



*) wird auch als „Entwicklungs-FMEA" bezeichnet. Wird als Methode i.d.R. für die Mechanik sowie die elektronische Hardware verwendet.

System-FMEA	Konstruktions-FMEA	Prozess-FMEA
Ziel: Aufdeckung von Entwicklungsrisiken in der Systemkonzeption.	**Ziel:** Aufdeckung von Entwicklungsrisiken in der Produktauslegung.	**Ziel:** Aufdeckung von Produktionsrisiken in der Prozessauslegung.
Zentrale Fragestellung: Erfüllt das Produkt die im Lastenheft festgelegten Anforderungen?	**Zentrale Fragestellung:** Gewährleistet die konstruktive Bauteilauslegung die Funktionsfähigkeit?	**Zentrale Fragestellung:** Lässt sich das Produkt prozesssicher herstellen?
Betrachtungsgegenstand: – Systemfunktionen – Systemschnittstellen – Umwelteinflüsse	**Betrachtungsgegenstand:** – Bauteilfunktionen – Bauteileigenschaften – Bauteilversagen	**Betrachtungsgegenstand:** – Prozessschritte – Prozessfehler – Prozesseinflüsse

Bild 3-25: FMEA-Arten [LPP10, S. 264], [BL04, S. 110], [DIN60812, S. 5]

3.2.2.6 Ereignisbaumanalyse (ETA)

Die Ereignisbaumanalyse (Event Fault Tree, ETA) ist eine induktive Analyse zur Beschreibung und Bewertung von Ereignisabläufen, mit der Ausfälle in technischen Systemen untersucht werden können [DIN60300-3-1, S. 20f.], [Eri05, S. 223ff.]. Ausgehend von einem Anfangsereignis (z.B. Komponentenausfall, Fehlbedienung) werden die Folgeereignisse bis zu den möglichen Endzuständen der Betrachtungseinheit ermittelt. Es geht vor allem darum, alle möglichen Pfade von Folgeereignissen und ihre Reihenfolge zu untersuchen [DIN60300-3-1, S. 20]. Diese qualitative Analyse kann zu einer quantitativen Analyse erweitert werden, mit der untersucht werden kann, welches der aus dem Anfangsereignis resultierenden Endzustände der Betrachtungseinheit am wahrscheinlichsten ist. Bild 3-26 fasst die Inputs und Outputs einer ETA zusammen. Bild 3-27 zeigt einen quantitativen Ereignisbaum für das Beispiel „Ausfall eines Fahrzeugreifens"; die Zahlen wurden hierbei beispielhaft gewählt [DIN60300-3-1, S. 21].

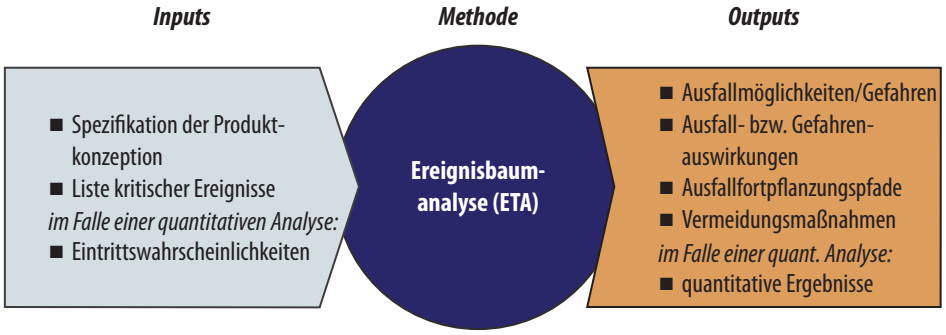


Bild 3-26: Inputs und Outputs einer ETA

Der Ereignisbaum lässt sich mit einem Fehlzustandsbaum kombinieren [DIN60300-3-1, S. 20]: die Wurzel eines Ereignisbaums kann als das Hauptereignis eines Fehlzustandsbaums angesehen und untersucht werden. Die Ereignisbaumanalyse wird dann zur Analyse der Folgen eines Anfangsereignisses verwendet; mit der Fehlzustandsbaumanalyse werden die Ursachen untersucht [DIN60300-3-1, S. 20], [Eri05, S. 234].

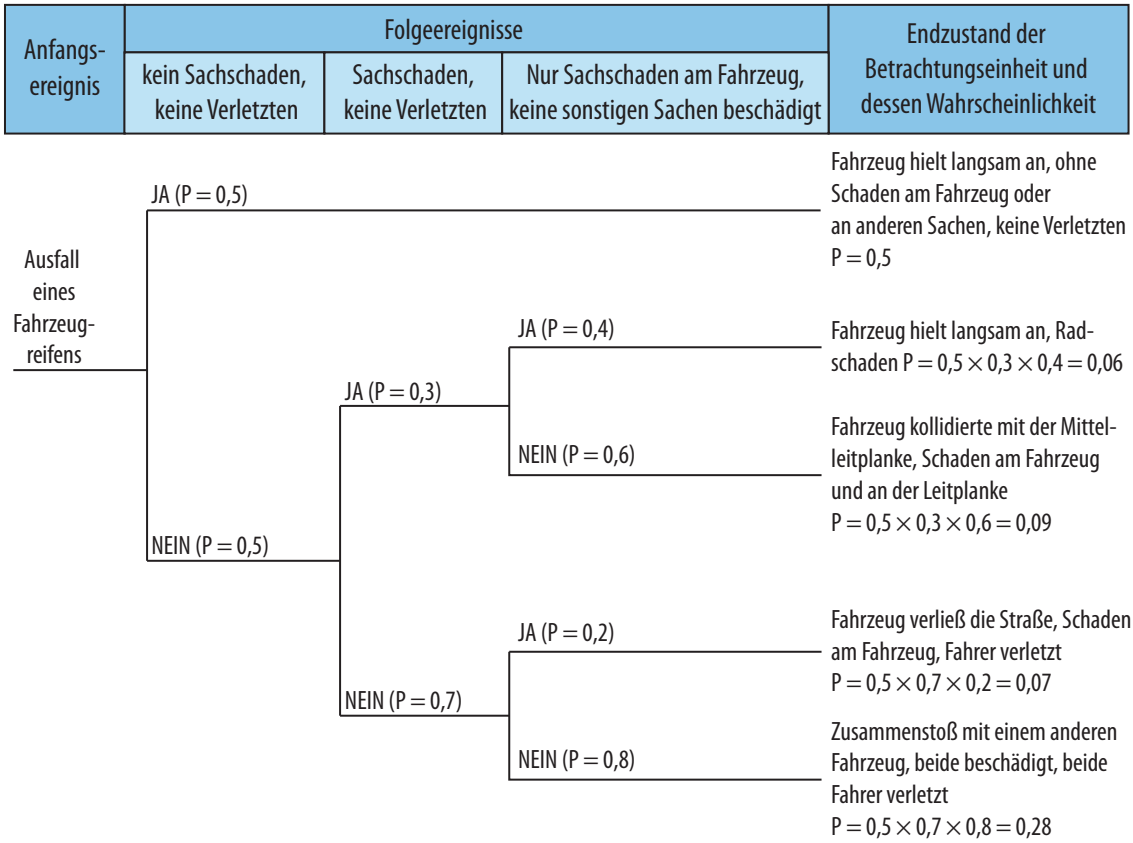


Bild 3-27: Beispiel einer quantitativen Ereignisbaumanalyse für das Anfangsereignis „Ausfall eines Fahrzeugreifens“; Zahlen beispielhaft [DIN60300-3-1, S. 21]

3.2.2.7 Markoff-Analyse

Die Markoff-Analyse dient zur zustandsübergangsbasierten Modellierung und Analyse des Systems mit Bezug auf Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit [DIN61165, S. 10]. Sie wird auf Basis eines Markoff-Modells durchgeführt.

Ein Markoff-Modell ist ein Zustandsdiagramm. Es bildet alle Systemzustände und mögliche Zustandsübergänge ab [DIN60300-3-1, S. 23]. Die Zustandsübergänge werden mit (konstanten) Übergangsraten (Ausfall- bzw. Reparaturraten) versehen [DIN60300-3-1, S. 23]. Das System befindet sich zu einem bestimmten Zeitpunkt in genau einem Zustand [VDI4003, S. 46]. Typischerweise ist das Ergebnis der Analyse die Wahrscheinlichkeit, dass sich das System in einer gegebenen Menge von Zuständen befindet, wodurch eine Voraussage der Verfügbarkeit und Zuverlässigkeit des Systems möglich wird [DIN60300-3-1, S. 23], [VDI4003, S. 46]. Bild 3-28 fasst die wesentlichen Inputs und Outputs zusammen.

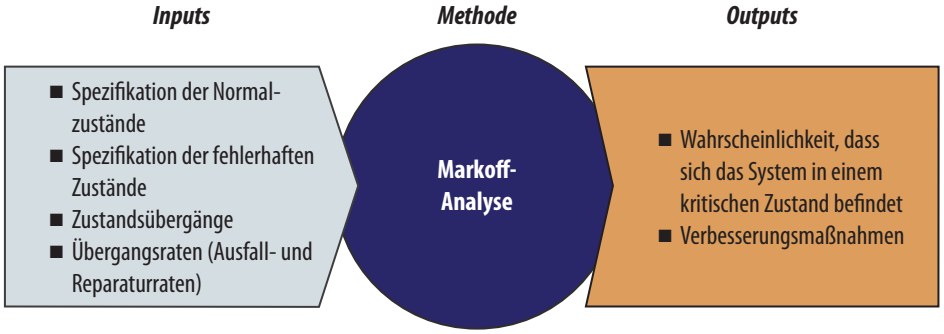


Bild 3-28: Inputs und Outputs einer Markoff-Analyse

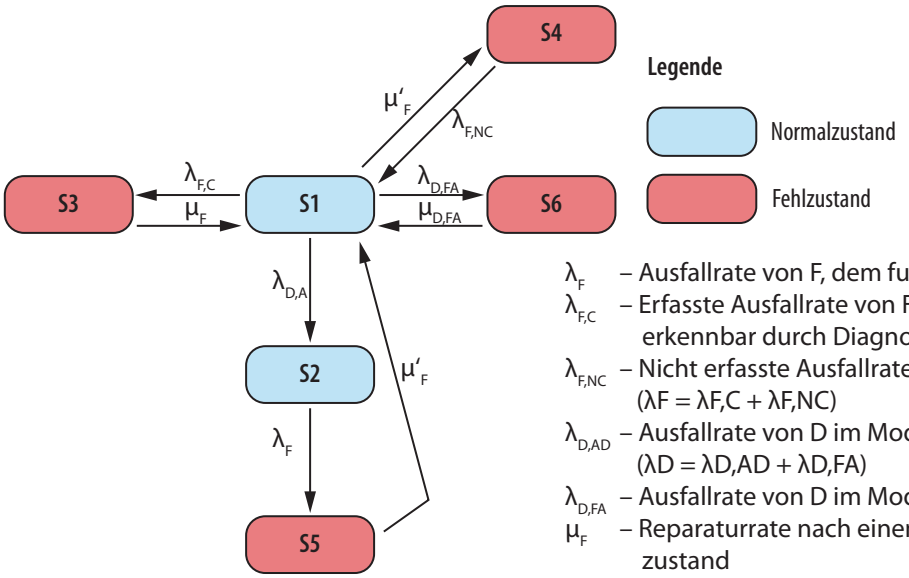
Bild 3-29 zeigt ein Beispiel eines Markoff-Modells [DIN60300-3-1, S. 23ff.]. Es handelt sich hierbei um ein elektronisches Gerät mit einem funktionalen Teil (F) und einer Diagnoseeinrichtung (D) [DIN60300-3-1, S. 23]. Die Diagnoseeinrichtung dient zur Überwachung des funktionalen Teils und Auslösung eines eventuellen Alarms. Bild 3-29 stellt das zugehörige Markoff-Modell dar [DIN60300-3-1, S. 26]. Insbesondere werden folgende Zustände ins Kalkül gezogen [DIN60300-3-1, S. 25]:

- Es erfolgt keine Erfassung des funktionalen Teils durch die Diagnoseeinrichtung. Der Ausfall des funktionalen Teils kann nicht erkannt werden (S4),
- Diagnoseeinrichtung löst kein Alarm aus, obwohl sie dies nicht tun sollte (S6) und
- Diagnoseeinrichtung löst kein Alarm aus, obwohl sie dies tun sollte (S2 und S5).

Mit den Markoff-Modellen können redundante Konfigurationen, komplexe Instandhaltungsstrategien, komplexe Ereignisabfolgen und komplexe Modelle zur Behandlung von Fehlzuständen (z.B. transiente Fehlzustände, latente Fehlzustände, Rekonfiguration) modelliert werden [DIN60300-3-1, S. 23f.]. Ebenso lassen sich Degradationsstufen und Ausfälle mit gemeinsamer Ursache abbilden. Darüber hinaus liefert die Markoff-Analyse probabilistische Lösungen für Bausteine, die sich in andere Methoden integrieren lassen

[DIN61165, S. 11ff.]. Zum Beispiel können Markoff-Modelle als Grundereignisse eines Fehlzustandsbaums verwendet werden [DIN60300-3-1, S. 18].

Mit zunehmender Anzahl von Systemelementen und deren Beziehungen steigt die Anzahl der Zustände und Zustandsübergänge exponentiell an, wodurch das Aufstellen der Modelle aufwändiger und fehleranfälliger wird [DIN60300-3-1, S. 24], [DIN61165, S. 10]. Insgesamt erfordern das Aufstellen und die Analyse der Markoff-Modelle hohe Methodenkenntnisse und den Einsatz von spezifischen Software-Werkzeugen [DIN60300-3-1, S. 24]. Die Modelle sind im Allgemeinen nur bei konstanten Übergangsraten numerisch auswertbar [DIN60300-3-1, S. 24]. Ab einer gewissen Komplexität des Systems lassen sich die Markoff-Modelle aufgrund des Zustandsraumexplosionsproblems nicht auswerten [RGD10, S. 219], [SO92].



λ_F – Ausfallrate von F, dem funktionalen Teil
$\lambda_{F,C}$ – Erfasste Ausfallrate von F (Ausfälle erkennbar durch Diagnoseeinrichtungen)
$\lambda_{F,NC}$ – Nicht erfasste Ausfallrate von F ($\lambda F = \lambda F,C + \lambda F,NC$)
$\lambda_{D,AD}$ – Ausfallrate von D im Modus Alarmfehler ($\lambda D = \lambda D,AD + \lambda D,FA$)
$\lambda_{D,FA}$ – Ausfallrate von D im Modus falscher Alarm
μ_F – Reparaturrate nach einem erfassten Fehlzustand
μ'_F – Reparaturrate nach einem nicht erfassten Fehlzustand

S1 – Korrekter Betrieb
S2 – Diagnostischer Fehlzustand im Alarmfehlermodus
S3 – Von der Diagnoseeinrichtung erkannter funktionaler Fehlzustand
S4 – Von der Diagnoseeinrichtung nicht erkannter funktionaler Fehlzustand (nicht erkennbar)
S5 – Von der Diagnoseeinrichtung nicht erkannter funktionaler Fehlzustand, da diese in den Alarmfehlermodus ausgefallen ist
S6 – Diagnostischer Fehlzustand in falschem Alarmmodus

Bild 3-29: Beispiel eines Markoff-Modells – Zustände und Zustandsübergänge mit den zugehörigen Ausfall- bzw. Reparaturraten [DIN60300-3-1, S. 25f.]

3.2.2.8 Bayessche Netze (BN)

Bayessche Netze (BN) dienen zur kompakten Darstellung einer multivariaten Wahrscheinlichkeitsverteilung und ermöglichen eine probabilistische Analyse eines Systems hinsichtlich Zuverlässigkeit und Sicherheit [LP07, S. 93], [JN07, S. 32ff.]. Die BN beruhen in ihrem Kern auf dem Satz von Bayes [FKP+07, S. 211ff.]:

Sei $A_1, \ldots, A_k$ eine disjunkte Zerlegung von Ω, wobei für mindestens ein i mit i = 1, …, k, $P(A_i) > 0$ und $P(B \mid A_i) > 0$ erfüllt ist. Dann gilt:

$$P(A_j|B) = \frac{P(B|A_j)P(A_j)}{\sum_{i=1}^{k} P(B|A_i)P(A_i)} = \frac{P(B|A_j)P(A_j)}{P(B)}, \; j=1,\ldots,k$$

Gleichung 3-1: Satz von Bayes [FKP+07, S. 213]

Die Wahrscheinlichkeit $P(A_i)$ wird als a-priori[30] Wahrscheinlichkeit und die Wahrscheinlichkeit $P(B \mid A_i)$ als a-posteriori[30] Wahrscheinlichkeit bezeichnet [FKP+07, S. 213].

Mathematisch ist ein BN ein Paar $(G, \{p_i\})$ mit i = 1, ..., N, wobei [JN07, S. 33f.]:

- G = (X, E) ist ein gerichteter azyklischer Graph. $X = \{X_1, \ldots, X_N\}$ ist die Menge der Knoten des Graphen, die N Zufallsvariablen darstellen. Jede Zufallsvariable besitzt eine endliche Menge von sich gegenseitig ausschließenden Zuständen. E ist die Menge der Kanten. Die Kanten beschreiben die kausalen Beziehungen zwischen den Knoten. Der Graph G stellt die qualitative Beschreibung eines BN dar.
- $\{p_i\}_{i=1,\ldots,N}$ ist eine Menge von bedingten Wahrscheinlichkeitsverteilungen (engl. Conditional Probability Distributions, CPDs). Diese Menge stellt die quantitative Beschreibung des BN dar [LP07, S. 93]. Typischerweise wird zur Beschreibung bedingter Wahrscheinlichkeitsverteilungen eine Tabelle bedingter Wahrscheinlichkeiten verwendet (engl. Conditional Probability Table, CPT).

Der Aufbau eines BN wird am Beispiel des Modells des vereinfachten Kraftfahrzeug-Startproblems erklärt [JN07, S. 24ff. und S. 35f.], [KM13, S. 11ff.]. Das zugehörige BN ist in Bild 3-30 dargestellt [JN07, S. 24f.]. Es umfasst drei binäre Knoten (mit zwei Zuständen) „Starten des Autos? (SA)“ „Benzin? (Be)“, „Saubere Zündkerzen? (SZ)“ und einen Knoten „Benzinstand? (BS)“ mit drei möglichen Zuständen. Die Kanten bilden die kausalen Zusammenhänge zwischen den Knoten ab. Zum Beispiel wird aus der BN-Darstellung deutlich, dass der Vorgang des Startens des Kraftfahrzeugs von dem Vorhandensein des Benzins sowie vom Zustand der Zündkerzen[31] abhängt. Ferner beeinflusst der Zustand des Knotens „Benzin? (Be)“ den Zustand des Knotens „Benzinstand? (BS)“.

Die elternlosen Knoten des BN wurden mit den Auftretenswahrscheinlichkeiten versehen. Gemäß dem Modell sind zum Bespiel die Zündkerzen mit einer Wahrscheinlichkeit von 95 % sauber: P(SZ = ja) = 0,95 = 95 %. Für die übrigen Knoten wurden Tabellen

---

[30] a priori: lat., von dem, was vorher kommt; a posteriori: lat., von dem, was nachher kommt

[31] Ein mögliches Szenario, das in unsauberen Zündkerzen resultieren kann: das Benzin wird dem kalten Motor vermehrt zugeführt. Da die Zündkerzen unter Umständen nicht alles zünden können, kann es vorkommen, dass nachdem der Motor abgestellt wurde, die Zündkerzen mit dem nicht verbrannten Benzin nässen. Folglich springt der Motor nicht an, da die Zündkerzen aufgrund der Feuchtigkeit nicht in der Lage sind zu zünden.

bedingter Wahrscheinlichkeiten spezifiziert. Diese beschreiben die bedingten Wahrscheinlichkeiten in Bezug auf die Kombination aller möglichen Zustände des jeweiligen Knoten und der Elternknoten. Es wird unter anderem spezifiziert, dass die Wahrscheinlichkeit eines gelungenen Starts des Kraftfahrzeugs im Falle des Vorhandenseins des Benzins und sauberen Zündkerzen 99 % beträgt: Pr(SA = ja | Be = ja, SZ = ja) = 99 %. Hierbei wird auch Raum für eventuelle Restfehler gelassen: der Startvorgang kann trotzdem mit einer Wahrscheinlichkeit von 1 % aufgrund anderer Ursachen nicht gelingen.

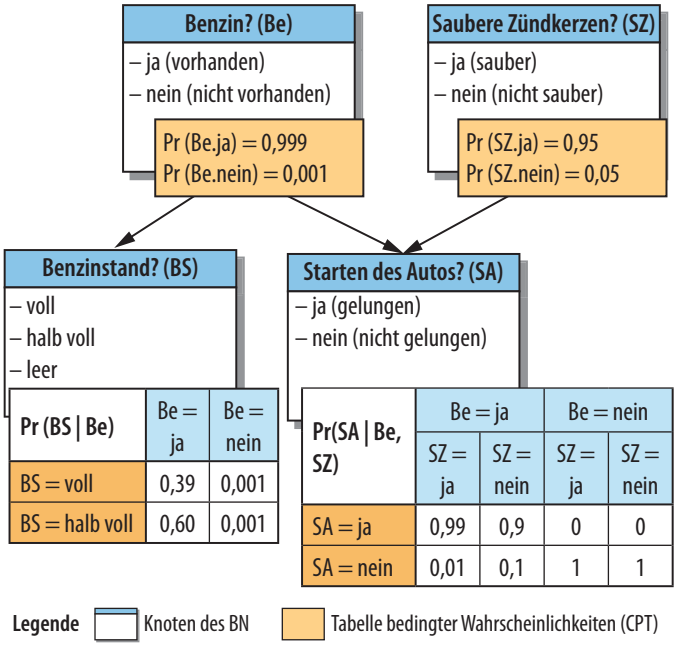


Bild 3-30: BN-Modell des vereinfachten Kraftfahrzeug-Startproblems (in Anlehnung an [KM13, S. 11f.], [JN07, S. 35f.])

Die BN beruhen auf der Aktualisierung von Wissen über Unbekanntes durch zusätzliche Daten [VDI4003, S. 52]. Mögliche Quellen für diese zusätzlichen Daten sind dabei statistische Tests, Auswertung der Betriebserfahrung, Experteneinschätzungen etc. [VDI4003, S. 52], [WMS+12, S. 673]. Zur Propagation und damit einhergehend Aktualisierung von Wissen (Observationen) werden Inferenzalgorithmen verwendet [LP07, S. 99ff.]. Dabei wird das Vorwissen durch a-priori-Wahrscheinlichkeitsverteilung beschrieben. Die Beschreibung des aktualisierten Wissens erfolgt mittels einer a-posteriori-Wahrscheinlichkeitsverteilung [VDI4003, S. 52]. Dadurch unterstützen BN folgende zwei grundsätzliche Analysearten [BPM+01, S. 249], [LP07, S. 102f.]:[32]

- **Vorwärtsgerichtete Analysen:** Gemeint ist das Berechnen der Auftretenswahrscheinlichkeit eines jeden Knotens des BN auf Basis der (a-priori) Auftretenswahrscheinlichkeiten der Elternknoten und der zugehörigen Tabellen bedingter Wahrscheinlichkeiten [BPM+01, S. 249]. Die Analyse ähnelt in ihrer Art der klassischen

[32] Die hier dargestellten Berechnungen und die daraus resultierenden Ergebnisse wurden mit dem Software-Werkzeug AgenaRisk in der Version 6.0 Rev. 1312 ermittelt [MNF10], [Age13-ol].

quantitativen Analyse, die im Rahmen einer FTA erfolgt. Die Eintrittswahrscheinlichkeit eines bestimmten Fehlers kann so berechnet werden. Bezogen auf das hier betrachtete Beispiel, kann die Wahrscheinlichkeit eines nicht gelungenen Autostarts berechnet werden. Diese beträgt $P(SA = nein) \approx 0{,}01549 \approx 1{,}549\ \%$.

- **Rückwärtsgerichtete Analyse:** Mit dieser kann ermittelt werden, mit welcher Wahrscheinlichkeit eine bestimmte Fehlerursache zu einem bestimmten Ausfall geführt hat (die sogenannte Fussel/Vesely-Importanzkenngröße) [LP07, S. 102]. Bezogen auf das hier betrachtete Beispiel kann so die Wahrscheinlichkeit berechnet werden, dass das Kraftfahrzeug aufgrund des Fehlens des Benzins nicht startet. Hierzu wird das BN-Modell um die Beobachtung ergänzt, dass das Auto nicht startet. Diese Beobachtung wird mittels Inferenzalgorithmen im BN-Modell fortgepflanzt, wodurch die zu ermittelnde Wahrscheinlichkeit berechnet wird: $P(Be = nein \mid SA = nein) \approx 6{,}458\ \%$ [KM13, S. 12]. Die Wahrscheinlichkeit, dass unsaubere Zündkerzen die Ursache sind, beträgt analog $P(SZ = nein \mid SA = nein) \approx 32{,}579\ \%$. Es ist also viel wahrscheinlicher, dass die Ursache in unsauberen Zündkerzen liegt. Ergänzt man das BN-Modell zusätzlich um die Observation, dass die Benzinstandanzeige auf „leer“ zeigt, so sind weiterführende Aussagen möglich. In der neuen Situation wird erwartungsgemäß das Fehlen des Benzins zur wahrscheinlichsten Ursache. Es gilt $P(Be = nein \mid SA = nein, BS = leer) \approx 87{,}325\ \%$ und $P(SZ = nein \mid SA = nein, BS = leer) \approx 8{,}737\ \%$.

Ferner ist eine rückwärtsgerichtete Analyse über eine Menge von Systemelementen unter Verwendung von BN möglich [LP07, S. 102f.]. Diese Analyse ist artverwandt mit der in Abschnitt 2.1.5.2 vorgestellten Methode der minimalen Ausfallschnitte. Kern ist die Berechnung der gemeinsamen a-posteriori-Wahrscheinlichkeit über alle Kombinationen von Systemelementen unter der Annahme eines Gesamtsystemausfalls [LP07, S. 102f.]. Ein BN lässt sich aus einem Fehlzustandsbaum automatisch erzeugen. Hierzu kann der durch BOBBIO ET AL. vorgeschlagene Algorithmus herangezogen werden, welches auf einem Katalog von Abbildungsvorschriften für die Abbildung von Gattern und Ereignissen des Fehlzustandsbaums auf ein Bayessches Netz beruht [BPM+01]. Weitere Informationen zum Einsatz von Bayesschen Netzen findet der Leser in Abschnitt 4.5.4.

Da BN gerichtete azyklische Graphen sind, sind sie zur Modellierung von Problemen mit Zyklen (Schleifen) nicht geeignet[Fri00, S. 9] [33]. Ferner können dynamische Änderungen des Systems im Zeitverlauf (z.B. Übergänge zwischen Betriebszuständen) mit klassischen BN nicht abgebildet werden [DBA+07], [KM13, S. 102].

[33] Der Grund: Im Allgemeinen ist das mathematische Entscheidungsproblem, welches der Berechnung von a-posteriori-Wahrscheinlichkeiten über ein beliebig komplexes Netz zugrunde liegt, ist NP schwer [BPM+01, S. 259]. Es lässt sich auf ein in Polynomialzeit lösbares Entscheidungsproblem reduzieren, unter der Annahme, dass der ungerichtete Graph des betrachteten Netzes keine Zyklen enthält [BPM+01, S. 259].

3.2.2.9 Dynamische Bayessche Netze (DBN)

Mit den klassischen BN können weder Zyklen noch dynamische Systemänderungen im Zeitverlauf abgebildet werden [KM13, S. 102]. Diese beiden Punkte können allerdings mit dynamischen Bayesschen Netzen (DBN) spezifiziert werden, die eine Erweiterung der klassischen BN darstellen [KM13, S. 102], [BD05], [Mur02]. Klassische BN sind statisch, da sie den Zustand des Systems zu einem bestimmten Zeitpunkt abbilden.

Kern der Erweiterung zu DBN besteht in der Aufteilung der Dynamik des Modells entlang einer gewünschten Anzahl von Zeitschritten. Bild 3-31 a) zeigt ein statisches Bayessches Netz, welches den Zustand eines zu untersuchenden Systems zu einem bestimmten Zeitpunkt abbildet. Im Laufe des Systembetriebs ändern sich mit zunehmender Zeit die Zustandsgrößen des Systems. Darüber werden Beobachtungen gemacht. Diese können in das Modell eingespeist werden und unter Verwendung der Inferenzalgorithmen propagiert werden, wodurch das Wissen über die übrigen Zustandsgrößen aktualisiert wird [KM13, S. 102].

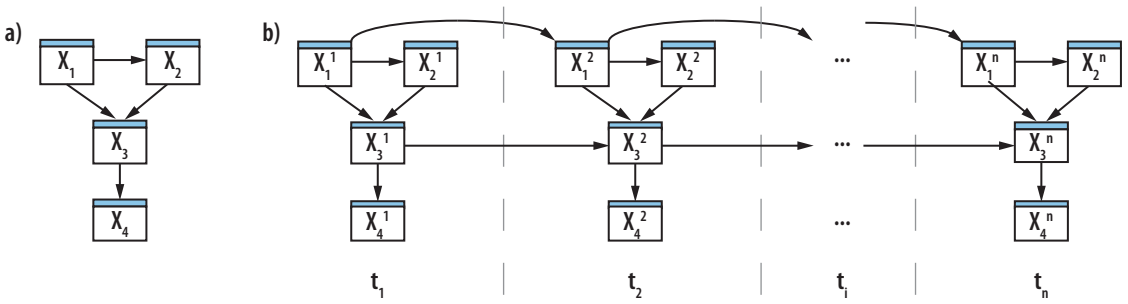


Bild 3-31: a) statisches BN; b) dynamisches BN mit n Zeitscheiben [KM13, S. 102f.]

Nicht nur der gegenwärtige Zustand des zu analysierenden Systems kann so untersucht werden. Vielmehr können auf diese Weise auch Aussagen über den Zustand des Systems zu früheren bzw. zu späteren Zeitpunkten getroffen werden [KM13, S. 102]. Damit dieser Zusammenhang zwischen dem gegenwärtigen Zustand und den vormaligen sowie zukünftigen Zuständen des Systems abgebildet werden kann, wird das in Bild 3-31 b) abgebildete DBN verwendet. Es werden n Zeitschritte abgebildet. Der Zustand des Systems in jedem der Zeitschritte wird durch ein klassisches BN abgebildet. Die Veränderung des Systems im Zeitverlauf wird in Form von Kanten zwischen den Knoten aus unterschiedlichen benachbarten Zeitschritten modelliert. Diese Kanten werden als temporale Kanten bezeichnet. Sie beschreiben die bedingte Wahrscheinlichkeitsverteilung für den Zeitschritt t_i unter den durch den Zeitschritt t_{i-1} beschriebenen Bedingungen. Die Analyse eines DBN beruht im Prinzip darauf, dass klassische Algorithmen für die einzelnen Zeitschritte angewendet werden [KM13, S. 102], [DBA+07]. Für die mathematische Definition des DBN siehe [DBA+07]. Die in Bild 3-23 für FTA und DFT dargestellten wesentlichen Inputs und Outputs gelten im Wesentlichen auch für BN und DBN.

Ein dynamischer Fehlzustandsbaum kann mit einem automatisierten Algorithmus in ein dynamisches Bayessches Netz übertragen werden [PCM10], [CBM+12a], [CBM+12b]. Kern des Algorithmus ist ein Katalog von Abbildungsvorschriften für die Abbildung von Gattern und Ereignissen des dynamischen Fehlzustandsbaums auf ein dynamisches Bayessches Netz (vgl. auch Abschnitt 4.5.4).

3.2.2.10 Zusammenfassende Bewertung

Die vorgestellten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit adressieren unterschiedliche Aspekte der Beschreibung eines Produktmodells. So wird zum Beispiel die Gefahrenanalyse und Risikoeinschätzung sehr früh im Produktentwicklungsprozess auf Basis der Beschreibungen von Anforderungsszenarien und einer Funktionsbeschreibung durchgeführt. Für die Durchführung einer FTA bzw. einer FMEA sind die Beschreibung von Funktionen und der Systemstruktur von wesentlicher Bedeutung. Die Markoff-Analyse dient zu einer Analyse des zustandsübergangsbasierten Systemverhaltens insbesondere in Bezug auf Ausfall- und Reparaturverhalten. Auch weiterführende Analyseaspekte wie Zeit- bzw. Abfolgeabhängigkeiten zwischen Ausfällen (z.B. ETA, Markoff-Analyse, DFT) können untersucht werden. Alle der vorgestellten Methoden lassen sich grundsätzlich auf Basis einer Spezifikation der Produktkonzeption bereits in der Konzipierung durchführen. Für die Markoff-Analyse und die (dynamischen) Bayesschen Netze gilt jedoch, dass die erforderlichen quantitativen Informationen (z.B. Ausfallraten) typischerweise in der Konzipierung nicht bzw. nur unzureichend vorliegen und mit Schätzungen bzw. qualitativen Werten gearbeitet werden muss.

3.3 Hilfsmittel zur Auswahl von Methoden

Den Entwicklern von mechatronischen und s.o. Systemen steht eine Fülle von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit zur Verfügung. Welche Methode wann und wie am effektivsten einzusetzen ist, entscheidet der Entwickler jedoch in den meisten Fällen alleine auf Basis seiner Erfahrung. Dieser Auswahlprozess ist meist suboptimal. Im Folgenden werden ausgewählte Ansätze vorgestellt, welche die Auswahl von Methoden unterstützen.

3.3.1 DIN EN 60300-3-1

Die DIN EN Norm 60300-3-1 „Zuverlässigkeitsmanagement – Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik“ ist Teil der Normreihe DIN EN 60300 „Zuverlässigkeitsmanagement“. Sie gibt einen allgemeinen Überblick über Methoden zur Absicherung der Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit. Die meisten dieser Methoden lassen sich ebenfalls für Sicherheitsuntersuchungen einsetzen. Betrachtet werden u.a. die FTA, die FMEA, die ETA, die Markoff-Analyse und die HAZOP. Im Anhang A der Norm erfolgt eine kurze Beschreibung

der Methoden. Außerdem findet darin die Erklärung der Methoden anhand von Beispielen statt. Darüber hinaus schlägt die DIN EN 60300-3-1 Kriterien zur Beurteilung und Auswahl von Methoden ausgehend von der zugrunde liegenden Aufgabestellung vor [DIN60300-3-1, S. 11ff.]. Diese Kriterien sind in Bild 3-32 dargestellt und kurz erklärt.

Systemkomplexität	„Komplexe Systeme, z. B. mit Redundanz oder diversitären Merkmalen, erfordern üblicherweise eine tiefergehendere Analyse als einfachere Systeme“ [DIN60300-3-1, S. 12]
Neuartigkeit des Systems	„Ein vollständig neuer Systementwurf kann eine intensivere Analyse als ein bewährter Entwurf erfordern“ [DIN60300-3-1, S. 12]
Quantitative Analyse	„Ist eine quantitative Analyse notwendig?“ [DIN60300-3-1, S. 12]
Mehrfach-Fehlzustände	„Wirken sich Kombinationen von Fehlzuständen aus oder können diese vernachlässigt werden?“ [DIN60300-3-1, S. 12]
Zeit- bzw. Abfolge-abhängigkeiten	„Spielt das Aufeinanderfolgen von Ereignissen eine Rolle in der Analyse? Zeigt das System zeitabhängiges Verhalten?“ [DIN60300-3-1, S. 12]
Abhängige Ereignisse	„Sind die Ausfall- oder Reparaturmerkmale einer einzelnen Einheit vom Zustand des Systems abhängig?“ [DIN60300-3-1, S. 12]
Induktiv oder deduktiv?	Ist eine deduktive Analyse ausreichend? Oder ist eine induktive Analyse erforderlich?
Verlässlichkeits-zuweisung	„Sollte [die Methode] fähig sein, Anforderungen an [den betrachteten Verlässlichkeitsaspekt] quantitativ aufzuteilen?“ [DIN60300-3-1, S. 12]
Erforderlicher Ausbildungsstand	„Welcher Ausbildungsgrad oder welche Erfahrung ist erforderlich, um [die Methode] sinnvoll und richtig anzuwenden?“ [DIN60300-3-1, S. 12]
Akzeptanz und Allgemeingültigkeit	„Ist [die Methode] allgemein anerkannt, z. B. von Behörden oder einem Kunden?“ [DIN60300-3-1, S. 12]
Werkzeugunter-stützung benötigt?	„Benötigt [die Methode] (rechnergestützte) Werkzeugunterstützung oder kann [sie] auch von Hand durchgeführt werden?“ [DIN60300-3-1, S. 12]
Plausibilitäts-prüfungen	„Kann man die Plausibilität der Ergebnisse leicht von Hand nachprüfen? Falls nicht, sind die verfügbaren Werkzeuge validiert?“ [DIN60300-3-1, S. 12]
Verfügbarkeit von Werkzeugen	„Sind Werkzeuge [...] verfügbar?“ Bestehen Schnittstellen zu anderen Analysewerkzeugen (Export und Wiederverwendung von Ergebnissen)? [DIN60300-3-1, S. 12]
Normung	„Gibt es eine Norm, die das Merkmal [der Methode] und die Darstellung der Ergebnisse (z. B. Symbole) beschreibt?“ [DIN60300-3-1, S. 12]

Bild 3-32: Kriterien zur Auswahl von Methoden zur Steigerung der Verlässlichkeit nach DIN EN 60300-3-1 [DIN60300-3-1, S. 12]

Für die in der DIN EN 60300-3-1 betrachteten Methoden erfolgt in der Norm eine Charakterisierung dieser hinsichtlich der aufgestellten Kriterien. Tabelle 3-10 stellt einen Ausschnitt dieser Charakterisierung für die im Rahmen der vorliegenden Arbeit betrachteten Methoden dar.

Tabelle 3-10: Charakterisierung ausgewählter Methoden hinsichtlich der in der DIN 60300-3-1 aufgestellten Kriterien (Ausschnitt) [DIN60300-3-1, S. 13]

Methoden	Kriterien													
	Systemkomplexität	Neuartigkeit des Systems	Quantitative Analyse	Mehrfach-Fehlerzustände	Zeit- bzw. Abfolgeabhängigkeiten	Abhängige Ereignisse	Induktiv oder deduktiv?	Verlässlichkeitszuweisung	Erforderlicher Ausbildungsstand	Akzeptanz und Allgemeingültigkeit	Braucht Werkzeugunterstützung?	Plausibilitätsprüfungen	Verfügbarkeit von Werkzeugen	Normung
Fehlzustandsbaum-analyse FTA	Ja	Ja	Ja	Ja	Nein	Nein	Ded.	Ja	Mit-tel	Hoch	Mit-tel	Ja	Hoch	DIN 61025
Ereignisbaumana-lyse ETA	NE	NE	Ja	NE	Ja	Ja	Ind.	NE	Hoch	Hoch	Mit-tel	Ja	Mit-tel	-
Markoff-Analyse	Ja	Ja	Ja	Ja	Ja	Ja	Ded.	Ja	Hoch	Mit-tel	Hoch	Nein	Mit-tel	DIN 61165
Fehlzustandsart- und -auswirkungs-analyse FMEA	NE	NE	Ja	Nein	Nein	Nein	Ind.	NE	Nied-rig	Hoch	Nied-rig	Ja	Hoch	DIN 60812
Hazard and Opera-bility Study HAZOP	Ja	Ja	Nein	Nein	Nein	Nein	Ind.	Nein	Nied-rig	Mit-tel	Nied-rig	Ja	Mit-tel	DIN 61882

Legende NE: nicht empfohlen; kann für einfache Systeme eingesetzt werden, sollte in Zusammenspiel mit weiteren Methoden verwendet werden
Ded.: deduktiv Ind.: induktiv
Bewertungskala (falls zutreffend): Niedrig, Mittel, Hoch

Wird z.B. nach einer Analysemethode gesucht, die für Systeme mit hoher Komplexität anwendbar ist, neben der qualitativen auch eine quantitative Untersuchung ermöglicht und einen deduktiven Charakter aufweist, so bietet sich beispielsweise die FTA an.

Bewertung: Die DIN EN 60300-3-1 definiert Kriterien zur Auswahl von Methoden der Sicherheit und Zuverlässigkeit. Ausgewählte etablierte Methoden werden darüber hinaus hinsichtlich dieser Kriterien in der Norm bewertet. Behandelt wird der Produktentwicklungsprozess in seiner Gesamtheit; eine Fokussierung auf die Konzipierung findet nicht statt. Die Bewertungskriterien sind branchen- und produktklassenunabhängig. Sie können für die Auswahl von Methoden in der Konzipierung sehr gut verwendet werden.

3.3.2 Auswahl von Methoden zur Risikobeurteilung nach IEC 31010

In der IEC Norm 31010 “Risk management – Risk assessment techniques” werden Methoden bzw. Techniken zur Risikobeurteilung erklärt (Anhang B der Norm) sowie Kriterien zur Auswahl von geeigneten Methoden ausgehend von der zugrunde liegenden Problemstellung vorgeschlagen [IEC31010]. Dabei wird der in der DIN ISO 31000 definierte Risikobeurteilungsprozess als Teil des Risikomanagements aufgegriffen [DIN31000].

Dieser Risikobeurteilungsprozess stellt eine Grundlage für die weitere Risikobewältigung (engl. risk treatment) dar und ist in Bild 3-33 dargestellt.

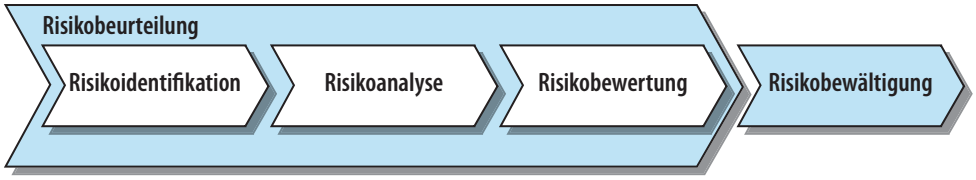


Bild 3-33: Der Risikobeurteilungsprozess nach DIN ISO 31000 und IEC 31010 und dessen Bestandteile; die Ergebnisse der Risikobeurteilung dienen als Basis für die weitere Risikobewältigung (Vereinfachte Darstellung) [DIN31000, S. 22], [IEC31010]

Ausgangspunkt ist die Festlegung von Risikokriterien, die bei der Bewertung der Bedeutung von Risiken angewandt werden. Auf dieser Basis wird die Risikobeurteilung durchgeführt. Der Risikobeurteilungsprozess (engl. risk assessment process) umfasst dabei die Phasen Risikoidentifikation (engl. risk identification), Risikoanalyse (engl. risk analysis) und Risikobewertung (engl. risk evaluation) [IEC31010]. Die Risikoidentifikation dient zur Ermittlung einer möglichst umfassenden Liste potentieller Risiken. Im Rahmen der Risikoanalyse werden die möglichen Ursachen und Quellen dieser Risiken untersucht. Ebenso findet eine Untersuchung der Auswirkungen der Risiken und deren Auftretenswahrscheinlichkeiten statt, welche eine Basis für die Abschätzung der zugehörigen Risikohöhe[34] bildet [IEC31010, S. 13]. Dabei wird die Wirksamkeit der eventuell vorhandenen Gegenmaßnahmen ins Kalkül gezogen. Die Risikoanalyse kann abhängig von der zugrunde liegenden Fragestellung qualitativer, quantitativer oder gemischter Natur sein [DIN31000, S. 27]. Basiert auf den Ergebnissen der Risikoanalyse erfolgt im Rahmen der Risikobewertung die Festlegung, welche der Risiken wie, in welchem Ausmaß und mit welcher Priorität behandelt werden sollen. Hierfür wird die in der Risikoanalyse ermittelte Risikohöhe den eingangs definierten Risikokriterien gegenübergestellt [DIN31000, S. 27]. In diesem Zusammenhang wird auch definiert, welche Maßnahmen zur Risikobewältigung für die jeweiligen Risiken am geeignetsten sind. Unter Heranziehung der festgelegten Maßnahmen findet dann die Risikobewältigung statt [DIN31000, S. 28].

Die IEC 31010 betrachtet u.a. die Methoden PHA, HAZOP, FMEA, FTA, ETA, Markoff-Analyse und Bayessche Netze. Diese werden in der Norm auf deren Beitrag zu den einzelnen Phasen der Risikobeurteilung hin bewertet (Tabelle 3-11). Eine FMEA adressiert alle Phasen der Risikobeurteilung gleichermaßen gut. Denn im Rahmen einer FMEA findet zum einen die Ermittlung von Risiken (z.B. von gefahrbringenden Ausfällen), deren

---

[34] Die Risikohöhe wird definiert als „Ausmaß eines Risikos oder einer Kombination von Risiken, das als bestimmte Kombination von Auswirkungen und ihrer Wahrscheinlichkeit zum Ausdruck gebracht wird“ [DIN31000, S. 13]. In einer FMEA kann die Risikohöhe z.B. durch die Kennzahl „Schwere der Ausfallmöglichkeit“ ausgedrückt werden [IEC31010, S. 48].

Ursachen und Auswirkungen statt. Zum anderen wird für die gefundenen Risiken die Risikoprioritätszahl berechnet, die als Entscheidungsgrundlage dafür gilt, welche Risiken weiterbetrachtet werden. Mit einer FTA geschieht die Risikoidentifikation nur im Zusammenhang mit den zu untersuchenden Hauptereignissen. Der Fokus liegt hierbei in der Ursachenermittlung; Auswirkungen von den ermittelten Ursachen werden nicht weiter betrachtet. In einer quantitativen FTA werden die Auftretenswahrscheinlichkeiten der Ursachen betrachtet. Darauf aufbauend wird die Auftretenswahrscheinlichkeit des Hauptereignisses ermittelt. Die Beurteilung der Risikohöhe kann im Rahmen einer FTA ins Kalkül gezogen werden, steht aber nicht im Fokus.

Tabelle 3-11: Beurteilung ausgewählter Methoden hinsichtlich deren Beitrags zu den einzelnen Phasen der Risikobeurteilung (Ausschnitt)[IEC31010]

Methode	Beitrag zur Risikobeurteilung				
	Risiko-identifikation	Risikoanalyse			Risikobewertung
		Analyse der Auswirkungen	Auftretens-wahrscheinlich-keit	Risikohöhe	
Vorläufige Gefahrenanalyse PHA	++	-	-	-	-
Hazard and Operability Study HAZOP	++	++	+	+	+
Fehlzustandsart- und -auswirkungsanalyse FMEA	++	++	++	++	++
Fehlzustandsbaumanalyse FTA	+	-	++	+	+
Ereignisbaumanalyse ETA	+	++	+	+	-
Markoff-Analyse	+	++	-	-	-
Bayessche Netze	-	++	-	-	++

Legende ++ sehr geeignet + geeignet - nicht anwendbar

Ähnlich wie es bei der DIN EN 60300-3-1 der Fall war, werden in der IEC 31010 Auswahlkriterien für die Methoden zur Risikobeurteilung aufgestellt (Bild 3-34).

Verfügbarkeit von ausgebildeten Ressourcen	Stehen auf dem adressierten Gebiet gut ausgebildete, erfahrene Ressourcen zur Verfügung? Kann für die Durchführung der Methoden eine gewisse Zeit eingeräumt werden? [IEC31010]
Grad der Unsicherheit	Ist der Grad der Unsicherheit von Informationen über den Betrachtungsgegenstand hoch? [IEC31010]
Komplexität	Ist die zugrunde liegende Problemstellung komplex? Bedarf die Problemstellung den Einsatz von Methoden, die komplexe Sachverhalte abbilden können? [IEC31010]
Quantitative Analyse	Kann unter Heranziehung der Methode eine quantitative Analyse durchgeführt werden? [IEC31010]

Bild 3-34: Kriterien zur Auswahl von Methoden zur Risikobeurteilung nach IEC 31010 [IEC31010]

Ebenso findet in der IEC31010 eine Beurteilung der Methoden hinsichtlich der Auswahlkriterien statt. Tabelle 3-12 fasst dies zusammen. Wie die darin abgebildete Beurteilung der Methoden zu interpretieren ist, wird am Beispiel des Auswahlkriteriums „Grad der Unsicherheit“ kurz erklärt: Die zugehörige Leitfrage ist „Ist der Grad der Unsicherheit von Informationen über den Betrachtungsgegenstand hoch?“. Wird diese Frage mit ja beantwortet, so sind die mit „hoch“ bewerteten Methoden für diese Problemstellung besser geeignet. Zum Beispiel eignen sich die Bayesschen Netze in diesem Zusammenhang weniger, da sie genaue Spezifikationen erfordern, um verwertbare Ergebnisse zu liefern.

Tabelle 3-12: Beurteilung der Eignung ausgewählter Methoden hinsichtlich der in der IEC 31010 aufgestellten Auswahlkriterien (Ausschnitt) [IEC31010]

Methode	Eignung bzgl. der Auswahlkriterien			
	Ressourcen und Ausbildungsstand	Grad der Unsicherheit	Komplexität	Quantitatives Ergebnis
Vorläufige Gefahrenanalyse PHA	hoch	hoch	medium	nein
Hazard and Operability Study HAZOP	mittel	hoch	hoch	nein
Fehlzustandsart- und -auswirkungsanalyse FMEA	mittel	mittel	mittel	ja
Fehlzustandsbaumanalyse FTA	niedrig	hoch	mittel	ja
Ereignisbaumanalyse ETA	mittel	mittel	mittel	ja
Markoff-Analyse	niedrig	niedrig	hoch	ja
Bayessche Netze	niedrig	niedrig	hoch	ja

Legende Bewertungskala (falls zutreffend): niedrig, mittel, hoch

Bewertung: Im Fokus der IEC 31010 steht die Risikobeurteilung, wodurch Überschneidungen mit dem in der vorliegenden Arbeit fokussierten Gebiet der Zuverlässigkeits- und Sicherheitstechnik bestehen. Ähnlich wie die DIN EN 60300-3-1 definiert die IEC 31010 Kriterien zur Auswahl von Methoden der Risikobeurteilung. Ebenfalls werden ausgewählte Methoden hinsichtlich dieser Kriterien bewertet. Die darin definierten Kriterien lassen sich grundsätzlich bei Auswahl von Methoden in der Konzipierung anwenden. Dies gilt vor allem für Sicherheitsuntersuchungen, da die Risikobeurteilung für diese eine zentrale Rolle spielt.

3.3.3 IEC 61508

Bezüglich der Auswahl von einzusetzenden Maßnahmen[35] zur Fehlerverhinderung, Fehlerbeseitigung, Fehlertoleranz und Fehlervorhersage lässt die IEC 61508 einen gewissen Interpretations- und Anpassungsspielraum zu. Im Allgemeinen werden keine konkreten Maßnahmen vorgeschrieben. Vielmehr werden durch die Norm grundlegende Leitlinien vorgegeben. Dies betrifft insbesondere die Auswahl von Methoden.

Diese Leitlinien werden in Form von Anforderungen innerhalb der Norm aufgefasst. Sehr oft kommen hierbei Tabellen als Hilfsmittel zum Einsatz. Tabelle 3-13 zeigt beispielhafte Maßnahmen für Software. Ähnliche Tabellen gibt es in der Norm ebenfalls für die elektronische Hardware.

Es gilt, eine adäquate Kombination von Maßnahmen ausgehend vom zugrunde liegenden Sicherheits-Integritätslevel (SIL) auszuwählen und im Projekt einzusetzen. In einigen Fällen stehen alternative Maßnahmen zur Verfügung. Diese sind neben der laufenden Nummer zusätzlich mit einem Buchstaben gekennzeichnet (z.B. 4a) und 4b) für die Entwicklungsphase „Modifikation“ sind als alternativ anzusehen). In diesem Fall genügt es, nur eine der alternativen Maßnahmen zu verwenden. Anstelle der in den Tabellen aufgeführten Maßnahmen dürfen auch andere nicht aufgeführte Maßnahmen zum Einsatz kommen, soweit die zugehörigen Anforderungen und Ziele erfüllt werden [IEC61508-3, S. 46].

Bewertung: In Bezug auf die Auswahl von Methoden stellt die IEC 61508 einige Maßnahmentabellen bereit. Diese geben eine grundsätzliche Richtung bei Auswahl von Methoden in den Phasen des Sicherheitslebenszyklus der Norm vor. Bis auf wenige Ausnahmen werden jedoch keine konkreten Methodenvorgaben gemacht, womit ein gewisser Interpretationsspielraum bei der Auswahl von Methoden existiert.

3.3.4 ISO 26262

Auch in der ISO 26262 werden Anforderungen in Bezug auf die zu verwendenden Maßnahmen in der Produktentwicklung auf System-, SW- und HW-Ebene sowie in den zugehörigen Tests gestellt. Dies umfasst insbesondere Maßnahmentabellen. Diese Maßnahmentabellen der ISO 26262 sind im Vergleich zur IEC 61508 übersichtlicher und praxisnäher [LPP10, S. 142].

---

[35] Wie in Abschnitt 2.1.3 erklärt, lässt sich die Verlässlichkeit eines technischen Systems durch eine Kombination von Maßnahmen zur Fehlerverhinderung, Fehlerbeseitigung, Fehlertoleranz und Fehlervorhersage verbessern. Dies umfasst insbesondere die im Mittelpunkt dieses Abschnitts stehenden Methoden zur Steigerung der Zuverlässigkeit und Sicherheit, die typischerweise als Maßnahmen zur Fehlervorhersage klassifiziert werden. Immer wenn hier von Maßnahmen gesprochen wird, sind also auch insbesondere Methoden gemeint.

Tabelle 3-13: Beispiele für Forderungen in Bezug auf die einzusetzenden Maßnahmen für verschiedene SIL-Level; Vereinfachte Darstellung; es wurden Auszüge aus mehreren Tabellen zusammengefasst [MHD+07], [IEC61508-3]

Entwicklungsphase	Maßnahme/Methode	SIL1	SIL2	SIL3	SIL4	Ursprung
Entwurf der SW-Architektur	Strukturierte Design-Methoden (z.B. Blockdiagramme, Zustandsmaschinen)	HR	HR	HR	HR	Tab. A.2, 11a) [IEC61508-3]
SW-Entwurf und SW-Entwicklung	Zertifizierter Compiler	R	HR	HR	HR	Tab. A.3, 4a) [IEC61508-3]
	Entwurfs- und Codierungsrichtlinien	R	HR	HR	HR	Tab. A.4, 5 [IEC61508-3]
Modifikation	Impact-Analyse	HR	HR	HR	HR	Tab. A.8, 1 [IEC61508-3]
	Neuverifikation geänderter SW-Module	HR	HR	HR	HR	Tab. A.8, 2 [IEC61508-3]
	Neuvalidierung betroffener SW-Module	R	HR	HR	HR	Tab. A.8, 3 [IEC61508-3]
	Neuvalidierung des gesamten Systems	---	R	HR	HR	Tab. A.8, 4a) [IEC61508-3]
SW-Verifikation	Formaler Beweis	---	R	R	HR	Tab. A.9, 1 [IEC61508-3]
	Statische Analyse	R	HR	HR	HR	Tab. A.9, 3 [IEC61508-3]

Legende HR: besonders empfohlen R: empfohlen ---: keine Empfehlung für oder gegen eine Verwendung
SW: Software SIL: Sicherheits-Integritätslevel (SIL1 < SIL2 < SIL3 < SIL4)

Tabelle 3-14 zeigt die Forderungen der ISO 26262 in Bezug auf Sicherheitsanalysen auf Systementwurfsebene. Tabelle 3-15 geht auf die Anforderungen der Norm in Bezug auf Notationen zur Beschreibung des Softwarearchitekturentwurfs. Die Tabellen aus der ISO 26262 sind wie folgt zu interpretieren:

4. Produktentwicklung auf Systemebene ► 4-7. Systementwurf ► Tabelle 1. Analyse des Systementwurfs

Nr.	Maßnahme/Methode	ASIL			
		A	B	C	D
1	Deduktive Analyse	o	+	++	++
2	Induktive Analyse	++	++	++	++

Legende ++: besonders empfohlen +: empfohlen
o: keine Empfehlung für oder gegen eine Verwendung
ASIL: Automotive Sicherheits-Integritätslevel (ASIL A < ... < ASIL D)

Tabelle 3-14: Forderungen der ISO 26262 bzgl. der Sicherheitsanalysen auf Systementwurfsebene, abgestuft nach dem ASIL-Level [ISO26262-4, S. 12]

Jede der in den Maßnahmentabellen der ISO 26262 aufgeführten Maßnahmen stellt entweder einen konsekutiven (gekennzeichnet mit einer laufenden Nummer wie 1, 2, 3…) oder einen alternativen Eintrag dar (gekennzeichnet mit einer Nummer gefolgt durch einen Buchstaben – z.B. 2a, 2b). Für konsekutive Einträge gilt: es sollen alle zugehörigen Maßnahmen angewendet werden, und zwar entsprechend der in der Maßnahmentabelle abgebildeten ASIL-bezogenen Empfehlung. Sollen andere, nicht aufgeführte Maßnahmen zum Einsatz kommen, so gilt es zu begründen, dass diese die zugehörigen Anforderungen im erforderlichen Ausmaß erfüllen [ISO26262-4, S. 3].

Wie bereits bei der Vorstellung der Grundnorm IEC 61508 erklärt, lässt sich auch hier feststellen, dass die IEC Norm 61508 und ihre Derivate nur in wenigsten Fällen konkrete Maßnahmen vorschreiben. Für Analyse des Systementwurfs hinsichtlich Sicherheit ist für jeden ASIL-Level gemäß Tabelle 3-14 eine induktive Analyse vorgeschrieben. Induktive Analysen sind z.B. die bereits vorgestellten Analysen FMEA, ETA und Markoff-Analyse. Welche Analysen konkret einzusetzen sind, schreibt die Norm nicht vor.

6. Produktentwicklung auf Software-Ebene ► 7-7. SW-Entwurf ► Tabelle 2. Notationen zur Beschreibung des Softwarearchitekturentwurfs

Nr.	Maßnahme/Methode	ASIL			
		A	B	C	D
1a	Informale Notationen	++	++	+	+
1b	Semiformale Notationen	+	++	++	++
1c	Formale Notationen	+	+	+	+

Legende ++: besonders empfohlen +: empfohlen
o: keine Empfehlung für oder gegen eine Verwendung
SW: Software
ASIL: Automotive Sicherheits-Integritätslevel (ASIL A < ... < ASIL D)

Tabelle 3-15: Anforderungen in Bezug auf Notationen zur Beschreibung des Softwarearchitekturentwurfs, abgestuft nach dem ASIL-Level [ISO26262-4, S. 12]

Für alternative Einträge gilt: zu verwenden ist eine geeignete Kombination von Maßnahmen nach Maßgabe des vorliegenden ASIL-Levels. Dabei sind Maßnahmen vorzuziehen, die einen höheren Empfehlungsgrad gemäß der jeweiligen Maßnahmentabelle aufweisen. Es ist stets zu begründen, dass die getroffene Maßnahmenauswahl der zugrunde liegenden Normanforderung genügt [ISO26262-4, S. 3].

Gemäß Tabelle 3-15 ist für die Spezifikation des Softwarearchitekturentwurfs ab ASIL C eine semiformale Notation[36] erforderlich. Ob hierbei die Unified Modeling Language (UML), die System Analysis and Design Techniques (SADT) oder andere semiformale Notationen zu verwenden sind, gibt die Norm nicht vor [ISO26262-1, S. 16]. Für ASIL B ist sowohl die Verwendung einer informalen als auch einer semiformalen Notation besonders empfohlen. In diesem Fall gilt es, eine geeignete Kombination auszuwählen und zu begründen. Zum Beispiel kann begründet werden, dass bei der Spezifikation des Softwarearchitekturentwurfs durchgängig eine semiformale Notation verwendet wird, womit sich die Verwendung einer informalen Notation erübrigt. Ein Verzicht auf die Verwendung einer semiformalen Notation bedarf in Fall einer ASIL B Entwicklung hingegen einer sehr guten, nachvollziehbaren Begründung.

Bewertung: Ähnlich wie ihre Mutternorm IEC 61508 gibt auch die ISO 26262 eine Hilfestellung bei Auswahl von Methoden in Form von Maßnahmentabellen. Bis auf wenige

[36] Für eine Definition des Begriffs einer semiformalen Notation siehe Abschnitt 2.1.4.

Ausnahmen (z.B. die Gefahrenanalyse und Risikoabschätzung) werden jedoch keine konkreten Methodenvorgaben gemacht. Auch im Falle der ISO 26262 ist dementsprechend ein Interpretationsspielraum bei der Auswahl von Methoden vorhanden.

3.3.5 Methodik zur Auswahl von Methoden des SFB 614

Im SFB 614 entstand eine Methodik zur Auswahl von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit [DGG+13], [GRS+14]. Sie unterstützt den Entwickler dabei, die für seine Aufgabenstellung adäquaten Methoden auszuwählen. Betrachtet wurden dabei die Phasen Konzipierung, Entwurf und Ausarbeitung sowie Betrieb. Eine detaillierte Betrachtung der einzelnen Phasen fand nicht statt.

Wesentliche Bestandteile der Methodik sind: 1) eine Methodendatenbank, 2) ein Leitfaden zur Auswahl von Methoden sowie 3) eine prototypische werkzeugtechnische Umsetzung. Die Methodendatenbank umfasst die Beschreibungen der Methoden zur Absicherung der Zuverlässigkeit und Sicherheit. Es handelt sich dabei vordergründig um Methoden, die im Rahmen des SFB 614 entwickelt wurden wie z.B. die Methode zur Konzipierung eines fortschrittlichen Condition Monitorings für s.o. Systeme [SMD+12]. Jede Methode wird durch Klassifikationsmerkmale charakterisiert (z.B. adressierter Verlässlichkeitsaspekt, Relevanz bzgl. Branche und bzgl. Fachdisziplin etc.). Das Vorgehen zur Auswahl von Methoden mittels der beschriebenen Methodik ist in Bild 3-35 dargestellt:

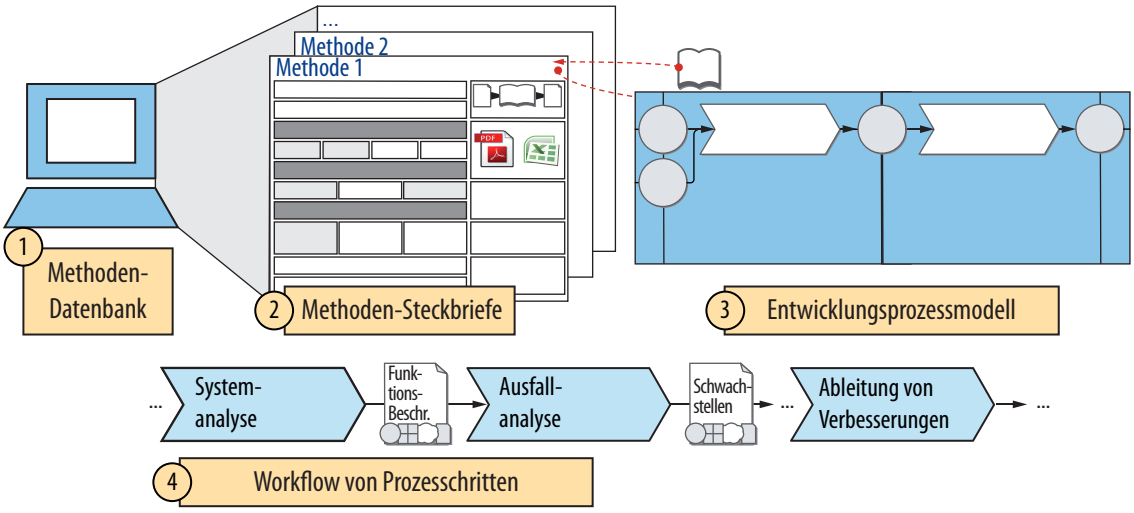


Bild 3-35: Vorgehen zur Auswahl und Kombination von Methoden zur Steigerung der Verlässlichkeit [DGG+13, S. 60]

Phase 1: Hier wird mit Hilfe der Methodendatenbank nach adäquaten Methoden gesucht. Die prototypische werkzeugtechnische Umsetzung der Methodik stellt hierfür eine Suchmaske bereit. Mit dieser kann nach Methoden gesucht werden, welche spezifischen Ausprägungen von Klassifikationsmerkmalen entsprechen. Zum Beispiel kann eine Suche nach Methoden vorgenommen werden, welche den Verlässlichkeitsaspekt Sicherheit adressieren und in der Entwicklungsphase Entwurf und Ausarbeitung für die Fachdisziplin

Software anwendbar sind. Als Ergebnis erhält der Entwickler eine Liste von Methoden, die seinen Suchkriterien entsprechen und ihn im Rahmen seiner Entwicklungstätigkeit unterstützen können.

Phase 2: Die werkzeugtechnische Umsetzung ermöglicht für jede Methode die Anzeige des zugehörigen Methoden-Steckbriefes. Anhand dessen kann der Entwickler alle in der Methoden-Datenbank abgelegten Informationen über die Methode sowie deren Einsatz abrufen. Gemeint sind u.a. die Eingangs- und Ausgangsinformationen der Methode, die Abhängigkeitsbeziehungen zu anderen Methoden (z.B. kann abgebildet werden, dass die Ergebnisse einer Methode als Input für eine andere Methode dienen), Vorlagen und Leitfäden für die Durchführung der Methode, Beispiele für einen erfolgreichen Einsatz in anderen Projekten etc.

Phase 3: Ein Modul der werkzeugtechnischen Umsetzung ermöglicht die Abbildung und Visualisierung des Entwicklungsprozesses [KGD10]. Das darin abgebildete Entwicklungsprozessmodell wird mit der Methode OMEGA (Objektorientierte Methode zur Geschäftsprozessmodellierung und -analyse) beschrieben. Die Beschreibung umfasst die Prozessschritte, deren Ablaufzusammenhang, die zugehörigen Methoden und Ressourcen etc. [GP14, S. 254ff.]. Wird dieses Modul eingesetzt, so kann der Entwickler von dem Methoden-Steckbrief aus zu dem Prozessschritt navigieren, in dem die Methode eingesetzt wird. Ebenfalls können Methodenbeschreibungen aus dem Prozessmodell heraus aufgerufen werden.

Phase 4: Falls der Entwickler sich für den Methodeneinsatz entscheidet, wird er durch die Methodik in die Lage versetzt, auf Basis von für die Methoden hinterlegten Informationen und Abhängigkeitsbeziehungen einen Workflow von Prozessschritten manuell zu erarbeiten. Dadurch wird er bei einem ordnungsgemäßen Verwenden der vorgeschlagenen Auswahl von Methoden unterstützt.

Bewertung: Die Methodik zur Auswahl von Methoden des SFB 614 adressiert die zwei Entwicklungsphasen „Konzipierung“ und „Entwurf und Ausarbeitung“ sowie den Systembetrieb. Eine detaillierte Betrachtung der einzelnen Phasen – insbesondere der Konzipierung – findet jedoch nicht statt. Entsprechend sind die gleichzeitig als Suchkriterien dienenden Klassifizierungsmerkmale der Methoden gar nicht auf die Konzipierung ausgelegt. Die Methodik fokussiert in besonderem Maße Methoden zur Absicherung der Zuverlässigkeit und Sicherheit selbstoptimierender Systeme, die im Rahmen des SFB 614 entwickelt wurden.[37] Die werkzeugtechnische Umsetzung unterstützt eine effiziente Suche und Auswahl von Methoden.

---

[37] Die zugehörige Methoden-Datenbank umfasst insgesamt 17 Methoden, von denen 2 Methoden der Konzipierung zuordenbar sind. Siehe dazu auch [GRS+14].

3.4 Modellierungssprachen zur Beschreibung des Produktmodells

Für die angestrebte Systematik ist die Absicherung der Zuverlässigkeit und Sicherheit auf Basis einer Spezifikation des Produktmodells bzw. der Produktkonzeption von zentraler Bedeutung. Nachfolgend werden ausgewählte Modellierungssprachen zur Beschreibung des Produktmodells vorgestellt.

3.4.1 Situationsbasierte Qualitative Modellbildung und Analyse (SQMA)

Die Situationsbasierte Qualitative Modellbildung und Analyse (SQMA) wurde am Institut für Automatisierungs- und Softwaretechnik der Universität Stuttgart für Gefahrenanalyse von technischen Systemen entwickelt [Bie03], [BGJ+09, S. 54ff. und S. 348ff.]. Kern der Methode besteht in der Erstellung eines Systemmodells, welches als Basis für qualitative Analysen verwendet werden kann. Dabei werden die Struktur und das Verhalten des Systems abgebildet.

Bild 3-36 stellt das zugehörige Vorgehen zur Modellierung und Gefahrenanalyse eines technischen Systems mit der SQMA dar. Die wesentlichen Arbeitsprodukte werden am Beispiel eines Mehr-Tank-Systems in Bild 3-37 dargestellt [Man99].

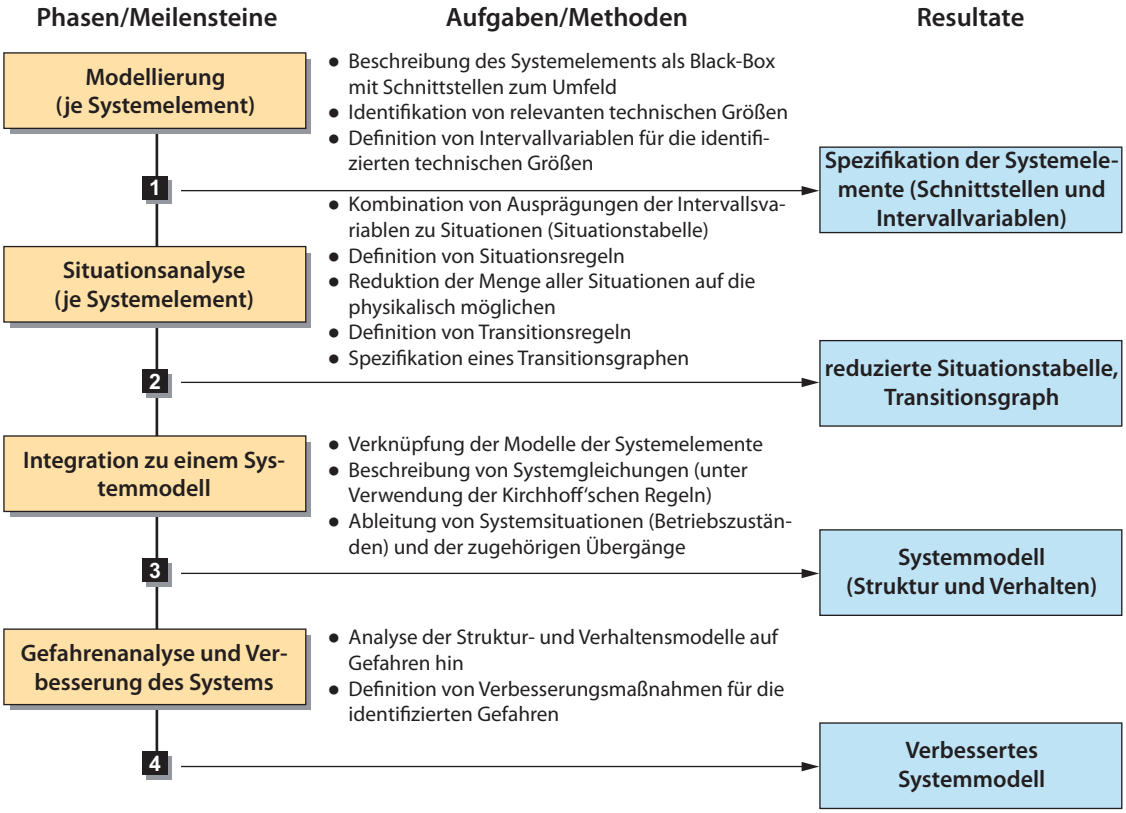


Bild 3-36: Vorgehen zur Modellierung und Gefahrenanalyse mit der SQMA

Phase 1 – Modellierung (je Systemelement): In Phase 1 erfolgt die Modellierung eines jeden Systemelements mit der SQMA. Jedes Systemelement wird zunächst separat im

Sinne eines wiederverwendbaren Bausteins mit klar definierten Schnittstellen modelliert [Bie03, S. 22]. In dem Mehr-Tank-Beispiel wird u.a. das Systemelement Tank spezifiziert (Bild 3-37). Für jedes Systemelement erfolgt die Identifikation der relevanten technischen Größen. Gemeint sind alle Größen, die für das Verhalten und die Wechselwirkungen des Systemelements mit seinem Umfeld von Relevanz sind [Man99]. Dies betrifft insbesondere die an einer Schnittstelle in Erscheinung tretenden physikalischen Systemgrößen [Bie03, S. 39]. Für das Systemelement Tank im Mehr-Tank-Beispiel sind die relevanten technischen Größen Zufluss Q_{Zu}, Abfluss Q_{Ab}, Füllstand h und der an der Abflussschnittstelle auftretende Druck P_{Ab}. Für jede technische Größe werden qualitative Intervallvariablen definiert. Für den Füllstand werden zum Beispiel die qualitativen Intervalle „leer", „halb voll", „voll" und „Überlauf" festgelegt (Bild 3-37).

Phase 2 – Situationsanalyse (je Systemelement): Gegenstand der Phase 2 ist die Situationsanalyse. Diese erfolgt zunächst separat für jedes Systemelement. Eine Situation ist dabei eine bestimmte Kombination der Intervalle aller technischen Größen des jeweiligen Systemelements. Situationen dienen zur Beschreibung des Verhaltens des Systemelements. Durch Kombination von Ausprägungen (Intervalle) der Intervallvariablen aller identifizierten technischen Größen wird der vollständige Situationsraum aufgestellt und in einer Situationstabelle dokumentiert. Da manche Kombinationen und damit einhergehend Situationen physikalisch nicht möglich sind, werden diese mit Hilfe von sogenannten Situationsregeln ausgeschlossen. Situationsregeln beschreiben das reale Verhalten der jeweiligen Systemelemente. Sie werden in Form von Gleichungen bzw. in Form von logischen Aussagen formuliert, die für alle Situationen erfüllt werden müssen [Man99]. Eine Situation wird als gültig bezeichnet, wenn sie alle Situationsbedingungen erfüllt. Ein Beispiel stellt die Situationsregel „aus einem leeren Tank kann nichts herausfließen" dar (Bild 3-37) [Man99]. Die zugehörige Gleichung ist: $h = \text{leer} \Rightarrow Q_{Ab} \leq 0$ [Man99]. Mit Hilfe der so aufgestellten Situationsregeln wird die Menge aller Situationen auf die physikalisch möglichen reduziert. Diese werden in einer reduzierten Situationstabelle dokumentiert (Bild 3-37). Mit sogenannten Kommentarregeln kann in der SQMA eine Situation bzw. eine Gruppe von Situationen mit einer Beschreibung und zusätzlichen Attributen versehen werden [Bie03, S. 39f.]. Diese Kommentare dienen zur Veranschaulichung der Erkenntnisse aus der Modellierung und Analyse. Ein Beispiel des Einsatzes von Kommentarregeln ist in der in Bild 3-37 dargestellten, reduzierten Situationstabelle zu sehen. Die Situation Nr. 10 (Tank-Überlauf) wurde farblich hervorgehoben, da diese eine gefährliche Situation darstellt (getroffene Annahme: der Inhalt des Tanks ist gefährlich) [Man99].

Ferner werden Übergange zwischen Situationen aus der Situationstabelle (sogenannte Transitionen) betrachtet. Für die Definition dieser können Transitionsregeln definiert werden, die ähnlich wie die Situationsregeln aufgebaut sind. Die Menge aller möglichen Transitionen wird in Form einer Transitionsmatrix bzw. eines Transitionsgraphen abgebildet [Man99]. In Bild 3-37 ist ein Beispiel eines derartigen Transitionsgraphen zu sehen

[Man99]: Spezifiziert wurden die einzelnen Transitionen von einem leeren Tank (Situation Nr. 3) über einen gefüllten Tank mit Zufluss (Situation Nr. 6) sowie die anschließende Entleerung des Tanks (Situationen Nr. 12 und Nr. 9).

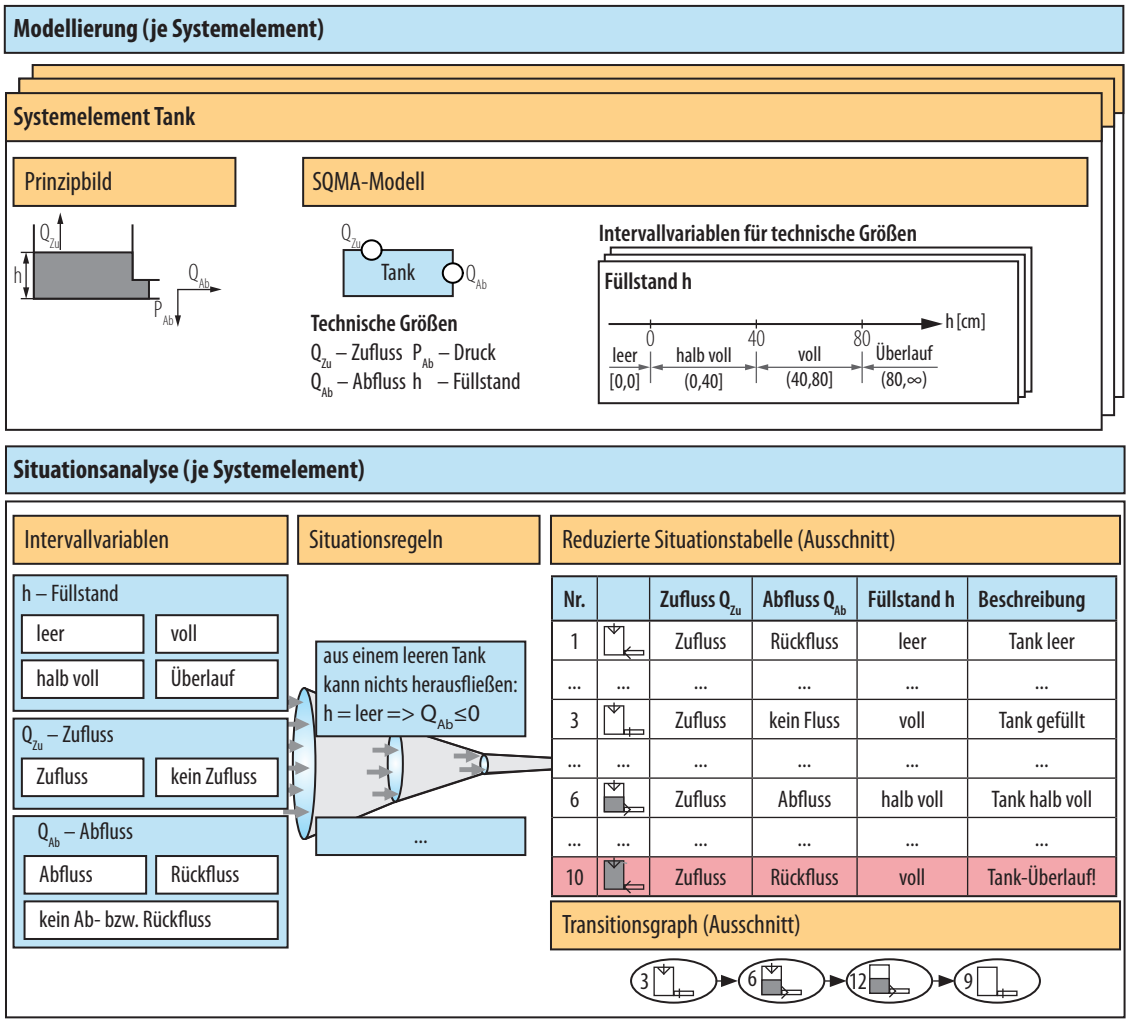


Bild 3-37: Prinzipielles Vorgehen für Modellierung und Situationsanalyse in Bezug auf ein Systemelement mit der SQMA-Methode am Beispiel eines Mehr-Tank-Systems (Beispiele entnommen aus [Man99], [Bie03])

Phase 3 – Integration zu einem Systemmodell: In Phase 3 werden die so spezifizierten Systemelemente entsprechend der physikalischen Struktur zu einem Systemmodell miteinander verknüpft [Bie03, S. 42f.]. Entsprechend der Kirchoffschen Regeln werden ferner Systemgleichungen aufgestellt. Dies erfolgt durch Verknüpfung der an den Schnittstellen der Systemelemente auftretenden Größen. Die Systemgleichungen repräsentieren somit die Wechselwirkungen zwischen den einzelnen Systemelementen. Ferner werden Systemsituationen bzw. Betriebszustände beschrieben. Diese werden aus der im Systemmodell abgebildeten Systemstruktur und den in Modellen der Systemelemente abgebildeten Informationen abgeleitet [Bie03, S. 42]. Eine Systemsituation ist dabei eine Menge

von Situationen der einzelnen Systemelemente, die alle Systemgleichungen erfüllt. Analog werden Transitionen auf Systemebene ermittelt. Das mögliche Verhalten des betrachteten technischen Systems wird durch die Menge aller Systemsituationen und der zugehörigen Transitionen beschrieben.

Phase 4 – Gefahrenanalyse und Verbesserung des Systems: Die SQMA-Methode sieht in Phase 4 eine Gefahrenanalyse und eine auf den Ergebnissen der Gefahrenanalyse aufbauende Verbesserung des Systems vor. Hierzu wird das spezifizierte Systemmodell auf sicherheitskritische Situationen hin untersucht. Für die eventuell identifizierten sicherheitskritischen Situationen findet eine Risikopriorisierung statt [Bie03, S. 50]. Hierzu kann zum Beispiel die Risikoprioritätszahl verwendet werden. Zur Bewältigung der sicherheitskritischen Situationen werden Sicherheitsmaßnahmen definiert [Bie03, S. 50]. Die Spezifikation des Systemmodells wird um die Beschreibung der Sicherheitsmaßnahmen und deren Einbettung in das System ergänzt.

Auch Software-Bausteine und menschliche Bedieneingriffe können mit der SQMA modelliert werden [BGJ+09, S. 348ff.]. Für Beispiele sei auf [Bie03, S. 60ff.] verwiesen. Ferner wurde eine prototypische werkzeugtechnische Unterstützung in Form eines Eclipse-Plugins realisiert [BGJ+09, S. 359ff.].

Bewertung: Die SQMA weist ein Vorgehensmodell auf, welches systematische Modellierung und Analyse eines technischen Systems unterstützt. Die SQMA beschränkt sich auf die Beschreibung der Systemstruktur und des zustandsübergangsorientierten Systemverhaltens. Zwar ermöglichen die Kommentarregeln die Erweiterung des Verhaltensmodells um zusätzliche Informationen, die für eine Gefahrenanalyse verwendet werden können. Jedoch lassen sich derartige Informationen in der Beschreibung der Struktur nur unzureichend modellieren. Weitere wichtige Beschreibungsaspekte wie Ablaufverhalten und Anforderungen kommen bei der SQMA zu kurz. Ferner ist die Beschreibung von disziplinübergreifenden strukturellen Zusammenhängen nur unzureichend möglich. Dies betrifft insbesondere die Hardware-Software-Schnittstelle. Die SQMA kann in der Konzipierung eingesetzt werden, da die Beschreibung der technischen Größen qualitativ über Intervallvariablen erfolgt, so dass keine detaillierten Informationen über diese Größen vorliegen müssen.

3.4.2 Systems Modeling Language (SysML)

Die Systems Modeling Language (SysML) ist eine durch die Object Management Group (OMG) und INCOSE (International Council on Systems Engineering) entwickelte und standardisierte Modellierungssprache für das Systems Engineering. Sie baut auf der UML 2.0 – einer etablierten Modellierungssprache für Software – auf und ergänzt diese um einige Aspekte wie das Anforderungs- oder das Zusicherungsdiagramm. Für das Systems Engineering nicht benötigte Elemente der UML wurden weggelassen.

Die SysML sieht eine Reihe von Diagrammen vor, die in Bild 3-38 dargestellt sind. Definiert werden dabei zwei Strukturdiagrammarten, vier Diagrammarten für die Beschreibung des Systemverhaltens sowie drei weitere Diagrammarten (Anforderungs-, Paket- und Zusicherungsdiagramm) [FMS12, S. 29ff]:

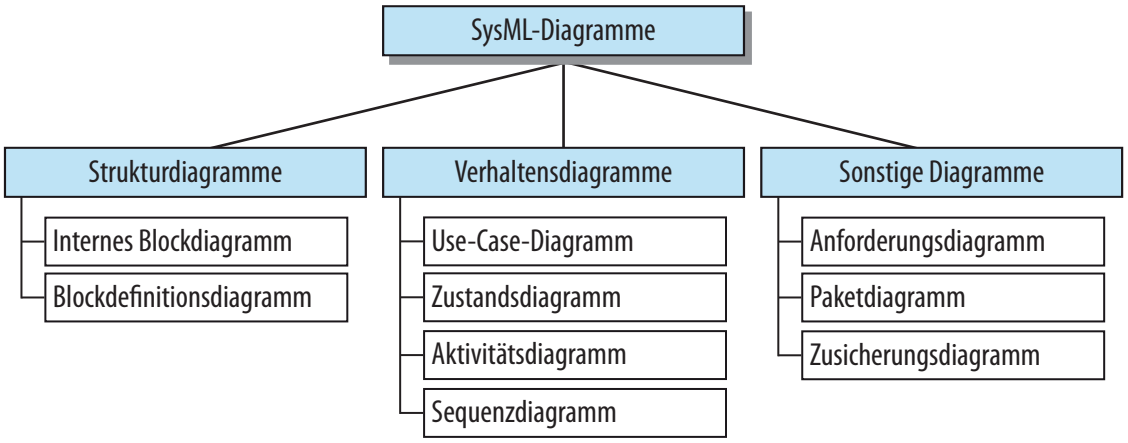


Bild 3-38: Überblick über die SysML-Diagramme [FMS12, S. 30]

Anforderungsdiagramm: dient zur Beschreibung von Anforderungen und deren Beziehungen untereinander sowie zu anderen Modelelementen wie Systemelemente und Testfälle mit dem Ziel, die Rückverfolgbarkeit von Anforderungen zu unterstützen.

Use-Case-Diagramm: stellt die Funktionalität des Systems prinzipiell dar. Es wird insbesondere beschrieben, welche Funktionen das System für die Interaktion mit anderen Entitäten (z.B. Anwender, andere Systeme) bereitstellt.

Blockdefinitionsdiagramm: beschreibt strukturelle Elemente der Betrachtungseinheit auf Typebene (sogenannte Blöcke).[38] Ebenso wird die Komposition der Systemelemente abgebildet.

Internes Blockdiagramm: bildet strukturelle Elemente der Betrachtungseinheit auf Instanzebene ab (Instanzen der Blöcke). Instanzen eines in einem Blockdefinitionsdiagramm definierten Blocks „Antrieb“ können z.B. „Antrieb links“ und „Antrieb rechts“ sein. Ebenso werden die Flüsse zwischen den Systemelementen modelliert.

Zustandsdiagramm: stellt das reaktive Verhalten der Betrachtungseinheit dar. Beschrieben werden Zustände und Zustandsübergänge, die durch Ereignisse ausgelöst werden können.

---

[38] Technische Systeme umfassen oft Bauteile, Baugruppen oder Softwarekomponenten, die mehrfach in einem System eingesetzt werden (z.B. Antrieb, Bremseinheit, etc.). Diese werden in der SysML nur einmal als Block abgebildet und können in der Systemspezifikation als sogenannte Instanzen mehrfach verwendet werden (z.B. Antrieb links, Antrieb rechts). Die Schnittstellen des Systemelements, seine innere Struktur und sein Verhalten werden im Rahmen der Spezifikation des Blocks nur einmal abgebildet (Typebene) und durch alle Instanzen übernommen.

Aktivitätsdiagramm: dient zur Beschreibung des Ablaufverhaltens der Betrachtungseinheit. Beschrieben wird die Ablaufabfolge von Aktionen im Zusammenhang mit der Verfügbarkeit der zugehörigen Eingangsgrößen, Ausgangsgrößen und dem Kontrollfluss. Ebenfalls wird beschrieben, wie durch Aktionen die Eingangsgrößen auf die Ausgangsgrößen abgebildet werden.

Sequenzdiagramm: beschreibt, welche Informationen bzw. Nachrichten zwischen Systemen bzw. Subsystemen ausgetauscht werden und in welcher Reihenfolge dies geschieht.

Zusicherungsdiagramm: ermöglicht die Beschreibung von Systemgrößen und deren Zusammenhangs. Zum Beispiel können damit physikalische Zusammenhänge wie $F = m \cdot a$ spezifiziert werden.

Paketdiagramm: dient zur Beschreibung der Struktur des SysML-Modells.

Die SysML ist mit dem Anspruch entwickelt worden, eine möglichst allgemeine Sprache für Systems Engineering zu sein, die weitgehend branchen- und anwendungsgebietsübergreifend ist. Sie kann jedoch für branchen- bzw. firmenspezifische Zwecke angepasst werden. Der hierfür zum Einsatz kommende Erweiterungsmechanismus der SysML wird als Profilmechanismus bezeichnet.[39] Zum Beispiel kann festgelegt werden, dass drei Arten von Flüssen zur Verfügung stehen: Material-, Informations- und Energieflüsse, was über die SysML-Spezifikation hinausgeht. Ebenso kann definiert werden, dass bestimmte Modellelemente mit einem SIL- bzw. ASIL-Attribut versehen werden können (vgl. auch Abschnitte 3.3.3 und 3.3.4).

Die SysML gibt kein Vorgehensmodell vor [Alt12, S. XI]. Bevor ein Unternehmen SysML einführen kann, muss ein entsprechendes Vorgehensmodell konzipiert, in Pilotprojekten evaluiert und implementiert werden [BC10]. Es entstand eine Menge von unternehmens- bzw. toolherstellerspezifischen Vorgehensmodellen wie Harmony-SE und RUP/SE [Est08]. Mit OOSEM (Object Oriented Systems Engineering Method) der INCOSE [FMS12, S. 431ff.] und dem SYSMOD von Weilkiens [Wei07] wurde versucht, ein allgemeines Vorgehensmodell zu etablieren.

Die bekanntesten Software-Werkzeuge für die SysML sind IBM Rational Rhapsody, MagicDraw der Firma NoMagic und Enterprise Architect der Sparx Systems. Es handelt sich jeweils um Erweiterung eines gleichnamigen UML-Werkzeugs.

---

[39] SysML ist selbst als ein UML-Profil umgesetzt. Das UML-Metamodell wurde einerseits um neue Stereotypen und Attribute derart erweitert. Andererseits verwendet SysML nicht die gesamte UML, sondern lässt auch Teile der UML weg, die sehr softwarespezifisch sind [Alt12, S. 32]. Dieses Ausblenden von Teilen des UML-Metamodells stellt eine Besonderheit dar. Standardmäßig sieht die UML- bzw. SysML-Spezifikation nur das Erweitern der zugrunde liegenden Sprache vor. Das Ausblenden von Teilen der Sprache mit dem Profilmechanismus sieht die Spezifikation nicht vor, wenngleich dies durch einige der SysML-Werkzeuge bereits heute ermöglicht wird [Alt12, S. 32].

Bewertung: Ein wesentlicher Vorteil der SysML ist ihre Erweiterbarkeit (Profilmechanismus). Der Profilmechanismus der SysML ist durch die meisten SysML-Werkzeuge umgesetzt, wodurch es möglich ist, die anwendungsgebietsspezifischen SysML-Profile in diesen Werkzeugen einzusetzen. Auf Basis eines mit einem entsprechenden SysML-Profil erstellten Produktmodells lassen sich prinzipiell Analysen zur Absicherung der Sicherheit und Zuverlässigkeit durchführen. SysML baut auf der UML auf und übernimmt die wesentlichen Konzepte. Die Vorteile der SysML sind insbesondere der breite Bekanntheitsgrad der SysML-Spezifikation sowie die Verfügbarkeit sehr ausgereifter Diagramme, die sich im Bereich Softwareentwicklung bewährt haben. Auf der anderen Seite ist die SysML aufgrund der starken Verwandtschaft mit der UML nach wie vor sehr softwarezentriert, eine ingenieurgerechte Aufbereitung fehlt [BC10]. Ein etabliertes Vorgehensmodell fehlt, welches die Verwendung der verschiedenartigen SysML-Diagramme systematisieren würde. Die für die Entwicklung technischer Systeme wesentlichen Aspekte wie z.B. Gestalt, Bauzusammenhang, kinematisches und dynamisches Verhalten etc. können nicht ohne weiteres in der SysML abgebildet werden. Die Diagramme der SysML eignen sich nur bedingt als Grundlage zur Kommunikation und Kooperation der Fachleute aus den involvierten Fachdisziplinen und verursachen teils erhebliche Akzeptanzprobleme. Für die Darstellung unterschiedlicher Sachverhalte werden sehr ähnliche Symbole genutzt, wodurch die Unterscheidung zwischen diesen schwer fällt. Zum anderen kommt es nicht selten vor, dass ein und derselbe Sachverhalt mit der SysML auf mehrere unterschiedliche Weisen abgebildet werden kann [AHJ+10], z.B. die Allokation von SW- zu HW-Komponenten. Dies erschwert das Verstehen der Modelle, das (teil-)automatisierte Vergleichen von Modellen sowie Modelltransformationen. Etablierte Modellierungsregeln für die SysML, mit denen sichergestellt werden kann, dass mehrere Anwender bei der Modellierung mit SysML zu gleichen Diagrammen kommen, sind nicht bekannt.

Folgendes lässt sich festhalten: Wenngleich die UML in der Softwaretechnik aus heutiger Sicht in der Praxis sehr oft zum Einsatz kommt, hat sich die SysML trotz ihres hohen Bekanntheitsgrads im industriellen Systems Engineering bislang nicht in erwartetem Maße durchgesetzt [Taz11]. Eine der wesentlichen Gründe hierfür sind die oben beschriebenen Akzeptanzprobleme. Dies wird durch die Tatsache unterstrichen, dass selbst innerhalb der SysML-Community Aktivitäten installiert wurden, mit dem Ziel der Erhöhung der Anwenderakzeptanz und Gebrauchstauglichkeit der SysML (z.B. das durch die INCOSE ins Leben gerufene MBSE Usability Team). In der jüngsten Zeit veröffentlichte Ergebnisse sind die SysML Lite und die Minimal SysML, welche jeweils eine vereinfachte Version der SysML darstellen [FMS12], [Dou13-ol].

3.4.3 Spezifikationstechnik CONSENS

Im SFB 614 entstand die Spezifikationstechnik CONSENS[40] zur fachdisziplinübergreifenden Beschreibung der Produktkonzeption eines selbstoptimierenden mechatronischen Systems [GFD+08]. Die Beschreibung der Produktkonzeption mit der Spezifikationstechnik CONSENS umfasst acht Aspekte. Diese Aspekte sind gemäß Bild 3-39: Umfeld, Anwendungsszenarien, Anforderungen, Funktionen, Wirkstruktur, Gestalt, Verhalten und Zielsystem. Rechnerintern werden alle genannten Aspekte durch Partialmodelle repräsentiert. Da die Aspekte zueinander in Beziehung stehen und ein konsistentes Ganzes ergeben, besteht die Produktkonzeption aus einem kohärenten System von Partialmodellen [GFD+08, S. 92]:

Umfeld: Hier werden das Umfeld des zu entwickelnden Systems und die Einbettung des Systems darin abgebildet. Das System wird dabei als ein „Black-Box“ behandelt. Es werden andere Systeme aus dem Umfeld und deren Interaktion mit dem zu entwickelnden System beschrieben. Ebenfalls werden relevante Einflüsse des Umfelds wie Wetterverhältnisse, Temperatur, Feuchtigkeit, Staub etc. beschrieben. Einflüsse, die eine störende Wirkung auf das System haben können, werden als solche gekennzeichnet. Die zu einem Zustandsübergang innerhalb des Systems führenden Einflüsse werden als Ereignisse abgebildet. Die Ermittlung relevanter Einflüsse wird durch entsprechende Kataloge und Checklisten unterstützt [GFD+08, S. 92].

Anwendungsszenarien: Anwendungsszenarien stellen eine erste Konkretisierung des Systemverhaltens dar. Sie beschreiben die typischen Betriebsmodi des Systems und das zugehörige Verhalten. Beispiele von Anwendungsszenarien eines Kraftfahrzeugs sind „Spurwechsel“, „Wenden bei langsamer Fahrt mit kleinstmöglichem Wendekreis“ etc.

Anforderungen: Ausgehend von den bei der Erstellung des Umfeldmodells und der Beschreibung der Anwendungsszenarien gewonnenen Erkenntnissen wird eine Anforderungsliste aufgestellt. Gemeint ist eine strukturierte Sammlung von Anforderungen, die durch das System zu erfüllen sind (z.B. hinsichtlich der Abmaße, Funktion, Performance, Qualität, Sicherheit). Es kann zwischen Fest- und Wunschanforderungen unterschieden werden [FG13, S. 334]. Jede Anforderung wird textuell beschrieben. Soweit zutreffend erfolgt ebenfalls die Beschreibung der zugehörigen Parameter (z.B. Temperatur, Länge, Geschwindigkeit). Die Ermittlung von Anforderungen wird durch Checklisten unterstützt [FG13, S. 324ff.], [Rot00], [Ehr03].

Funktionen: Dieser Aspekt beschreibt die hierarchische Aufteilung der angestrebten Systemfunktionalität. Eine Funktion ist der gewollte Zusammenhang zwischen Eingangs- und Ausgangsgrößen des Systems mit dem Ziel der Erfüllung einer Aufgabe [FG13, S. 242]. Ausgehend von der Gesamtfunktion des Systems erfolgt eine Unterteilung in Subfunktionen. Diese Unterteilung erfolgt solange, bis für die Funktionen Lösungsmuster

[40] CONSENS – CONceptual design Specification technique for the ENgineering of mechatronic Systems

gefunden werden [ADG+09]. Die Beschreibung der Funktionshierarchie wird durch Funktionskataloge unterstützt [GFD+08, S. 93].

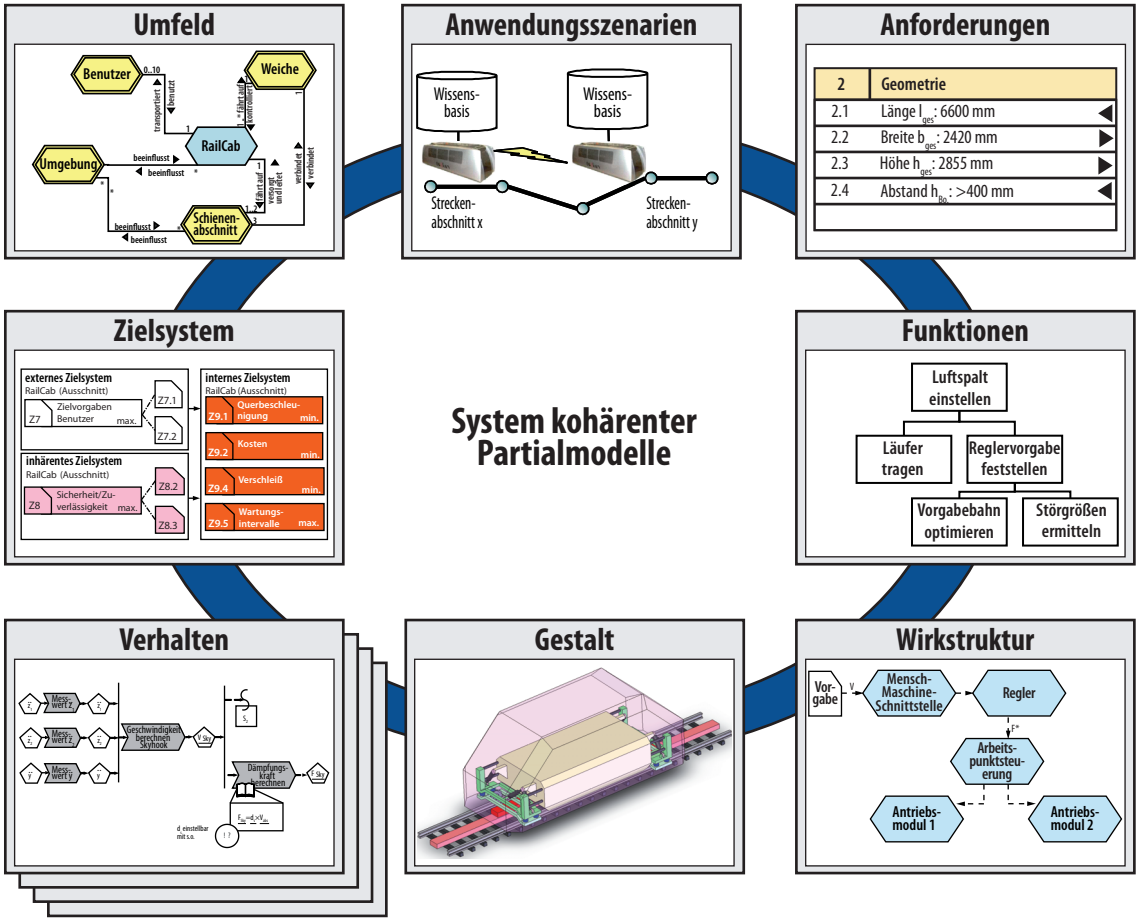


Bild 3-39: Aspekte bzw. Partialmodelle zur fachdisziplinübergreifenden Beschreibung der Produktkonzeption eines selbstoptimierenden mechatronischen Systems [GFD+08, S. 92]

Wirkstruktur: Die Wirkstruktur stellt den zentralen Aspekt der mit Spezifikationstechnik CONSENS beschriebenen Produktkonzeption. Die Beschreibung der Wirkstruktur umfasst die Systemelemente, deren Attribute sowie die Beziehungen der Systemelemente zueinander. Die Beschreibung der Beziehungen zwischen den Systemelementen erfolgt in Form von Material-, Energie- und Informationsflüssen sowie logischen Beziehungen (z.B. kann mit der „läuft auf“-Beziehung beschrieben werden, dass eine Softwarekomponente auf einem Hardwarebaustein ausgeführt wird).

Gestalt: Hier werden erste Festlegungen in Bezug auf die Gestalt des Systems abgebildet. Gemeint ist insbesondere die Beschreibung von Wirkflächen, Wirkorten, Hüllflächen und Stützstrukturen [GFD+08, S. 94]. Die rechnerunterstützte Spezifikation der Gestalt erfolgt mit Hilfe von 3D-CAD-Systemen.

Verhalten: Diese Gruppe von Aspekten umfasst mehrere Arten von Verhalten. Der Aspekt Verhalten – Zustände bildet das zustandsübergangsbasierte Verhalten ab. Insbesondere werden hier die möglichen Zustände und Zustandsübergänge sowie die diese Zustandsübergänge auslösenden Ereignisse beschrieben. Das Ablaufverhalten des Systems wird mit Hilfe des Aspekts Verhalten – Aktivitäten beschrieben. Der Aspekt Verhalten – Sequenzen dient dazu, die Interaktionen zwischen den Systemelementen abzubilden.

Zielsystem: Dieser Aspekt dient zur Beschreibung der externen, inhärenten und internen Ziele sowie deren Beziehungen (vgl. Abschnitt 2.2.3). Insbesondere wird die hierarchische Beziehung zwischen den Zielen beschrieben. Ebenso werden im Zielsystem potentielle Zielkonflikte abgebildet.

Die mit der Spezifikationstechnik CONSENS spezifizierte Produktkonzeption fördert das gemeinsame Systemverständnis für alle Beteiligten und ist die Grundlage für die effiziente Kommunikation und Kooperation der Entwickler im Zuge des weiteren disziplinspezifischen Entwurfs und Ausarbeitung. Ferner lassen sich auf Basis der Spezifikation der Produktkonzeption bereits frühzeitig verschiedenartige Analysen durchführen. Zum Beispiel lassen sich Zuverlässigkeit, Rückverfolgbarkeit von Anforderungen sowie das dynamische Verhalten des zu entwickelnden Systems frühzeitig analysieren und verbessern [Gau10], [GDP+10], [DG12], [BAG+11]. Außerdem existieren für CONSENS Modellierungsregeln [Kai14]. Die werkzeugtechnische Umsetzung der Spezifikationstechnik, der Mechatronic Modeller, wird in Abschnitt 3.6.3 vorgestellt. Sie beruht auf einem Metamodell für die Spezifikationstechnik CONSENS, welches über 110 Modellelemente umfasst [GDK10], [GLL12, S. 104ff.], [HNI11].

Die Spezifikationstechnik CONSENS wurde im SFB 614 Hand in Hand mit dem in Abschnitt 3.1.4 vorgestellten Referenzprozess für die Konzipierung selbstoptimierender mechatronischer Systeme entwickelt. Damit einhergehend ist sie auf diesen Referenzprozess sehr stark ausgerichtet. Im Rahmen des SFB 614 wurde ferner in einem durch den Verfasser geleiteten Projekt ein SysML-Profil für die Spezifikationstechnik CONSENS definiert, welches eine Abbildung der Spezifikationstechnik CONSENS auf die SysML beschreibt. Mit dem SysML-Profil ist es insbesondere möglich, mit einem SysML-Werkzeug CONSENS-konforme Spezifikationen der Produktkonzeption zu erstellen. Die Ergebnisse wurden publiziert und werden am Heinz Nixdorf Institut weiterentwickelt und in praktischen Projekten eingesetzt [IKD+13].

Bewertung: Die Spezifikationstechnik CONSENS realisiert einen systematischen Ansatz zur ganzheitlichen Beschreibung einer disziplinübergreifenden Produktkonzeption durch eine Menge von problemangepassten und miteinander konsistenten Partialmodellen. Sie bildet eine gute Basis für die Absicherung der Zuverlässigkeit und Sicherheit auf Basis der Spezifikation der Produktkonzeption unter Verwendung von etablierten Methoden. Die Spezifikationstechnik CONSENS ist sehr stark auf die Konzipierung mechatronischer Systeme ausgerichtet. Die Anzahl der zur Verfügung stehenden Partialmodelle ist auf das Notwendigste beschränkt; die bei der Beschreibung der einzelnen Partialmodelle

verwendeten Symbole sind klar voneinander unterscheidbar. Aus den genannten Gründen weist CONSENS eine hohe Aufgabenangemessenheit und Gebrauchstauglichkeit auf und ist zudem ingenieurgerecht aufbereitet und erweiterbar. Die Kompatibilität mit der SysML-Welt ist durch das Vorhandensein des SysML-Profils für CONSENS gegeben.

3.5 Methoden zur Absicherung der Zuverlässigkeit und Sicherheit auf Basis einer Beschreibung des Produktmodells

Es existieren einige Ansätze zur Durchführung von etablierten Methoden zur Absicherung der Sicherheit und Zuverlässigkeit auf Basis einer Beschreibung des Produktmodells. Ausgewählte Ansätze dieser Art werden nachfolgend kurz vorgestellt.

3.5.1 Functional Failure Identification and Propagation (FFIP)

Die FFIP (Functional Failure Identification and Propagation) dient zur Analyse der Sicherheit und Zuverlässigkeit mechatronischer Systeme [STP+12], [KTJ10]. Sie kann bereits in der Konzipierung eingesetzt werden. Die FFIP ermöglicht die Untersuchung von disziplinübergreifenden Ausfallausbreitungspfaden. In diesem Zusammenhang kann insbesondere die kombinierte Auswirkung mehrerer Fehlzustände von softwarebasierten, elektrischen sowie mechanischen Subsystemen untersucht werden [STP+12, S. 137]. Bild 3-40 stellt die drei Kernbestandteile der Methode dar: 1) ein Systemmodell, 2) eine Verhaltenssimulation und 3) eine Beurteilung des Zustands der Systemfunktionen mit dem sogenannten FFL-Reasoner (Functional-Failure Logic). Das zugehörige Vorgehen ist in Bild 3-41 dargestellt. Es umfasst folgende vier Phasen [KTJ10, S. 213ff.]:

Phase 1 – Spezifikation des Produkts: Die Spezifikation des Produkts umfasst die Aspekte Funktionen, Systemstruktur und zustandsübergangsbasiertes Verhalten sowie deren Zusammenspiel. Für die Beschreibung von Funktionen wird eine Funktionsstruktur verwendet. Die Systemstruktur wird als ein Systemflussdiagramm beschrieben. Zur Modellierung des Verhaltens werden Zustandsdiagramme herangezogen (siehe Bild 3-42 für Beispiele). Im Zuge der weiteren Analyse erfolgt zudem die Beschreibung von sicherheits- bzw. zuverlässigkeitsrelevanten Anwendungsszenarien.

Phase 2 – Beurteilung der Bedeutung der Funktionen: Hier wird jede Funktion des Systems auf ihre Bedeutung beurteilt. Die Bedeutung der Funktion wird mittels einer FCR-Bedeutungskennzahl (Functional Criticality Rating) ausgedrückt. Es wird ermittelt, wie wichtig eine bestimmte Funktion für den Betrieb des Systems ist. Grundlage bildet hierbei die im Modell der Funktionsstruktur abgebildete Beschreibung der hierarchischen Beziehung zwischen den Funktionen (Funktionshierarchie).

Die Bedeutung der Gesamtfunktion wird mit 1 bewertet. Entlang der Funktionshierarchie wird dieser Wert entsprechend aufgeteilt und den Unterfunktionen zugewiesen (eine mögliche Aufteilung im Falle von vier Unterfunktionen könnte z.B. 0.25, 0.25, 0.3 und 0.2 sein). Diese Aufteilung wird in Abstimmung mit den Experten aus den involvierten

Fachdisziplinen bestimmt. Sie erfolgt so lange, bis für jede Funktion der Funktionsstruktur eine Beurteilung der Bedeutung vorliegt. Je höher die mit der FCR-Kennzahl ausgedrückte Bedeutung einer Funktion ist, desto wichtiger ist es, die Funktionsfähigkeit dieser Funktion während des Betriebs zu erhalten [KTJ10, S. 214f.].

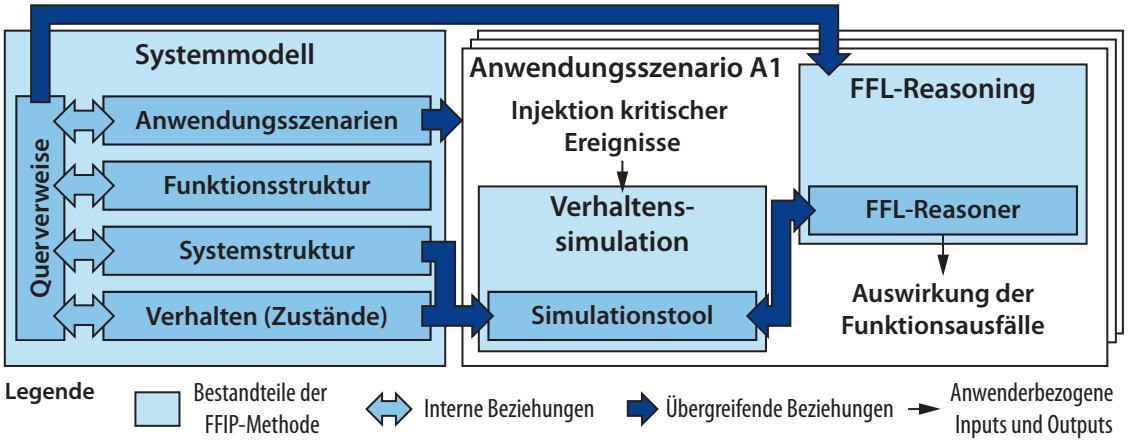


Bild 3-40: Grundlegende Bestandteile der FFIP-Methode und deren Zusammenspiel (in Anlehnung an [STP+12, S. 139])

Phase 3 – Analyse der Auswirkung von Funktionsausfällen: Ziel ist die Beurteilung der Auswirkung von Funktionsausfällen. Hierbei werden drei untergeordnete Phasen durchlaufen**.** Zuerst erfolgt die Spezifikation von zuverlässigkeits- und sicherheitskritischen Anwendungsszenarien des Systems **(Phase 3.1)**. Für die spezifizierten Anwendungsszenarien werden ferner die zu untersuchenden Funktionsausfälle festgelegt. Beispiel für ein kritisches Szenario und den zugehörigen Funktionsausfall: ein Relais schließt nicht, da es den sogenannten „stuck at open“ Ausfall aufweist.

Jedes der spezifizierten kritischen Anwendungsszenarien wird einer ereignisbasierten Verhaltenssimulation unterzogen **(Phase 3.2)**. Hierzu kommt das FFIP-Verhaltenssimulationstool zum Einsatz. Konkret wird untersucht, wie das System auf die Injektion von bestimmten Ereignissen in einer vorgegebenen Reihenfolge (welche den kritischen Anwendungsszenarien entsprechen) reagiert und sein Verhalten durch Zustandsübergänge ändert. Hierbei werden weitere in der Produktspezifikation abgebildete Informationen (z.B. zugrunde liegende Funktionen und zugehörige Systemelemente) ebenfalls ins Kalkül gezogen. Als kritische Ereignisse werden insbesondere die in Phase 3.1 für das jeweilige Anwendungsszenario spezifizierten Funktionsausfälle betrachtet. Zum Beispiel kann untersucht werden, wie sich das System verhält, wenn ein Relais nicht in der Lage ist zu schließen [KTJ10, S. 221]. Da in der Konzipierung konkrete Werte für Zustandsgrößen üblicherweise nicht vorliegen, werden diese kontinuierlichen Werte qualitativ diskretisiert. Zum Beispiel wird festgelegt, dass die Zustandsgröße elektrischer Strom einen der diskreten Werte Null, niedrig, nominal oder hoch einnehmen kann [KTJ10, S. 215]. Die Verhaltenssimulation erfolgt über eine vorgegebene Anzahl von Iterationsschritten bzw. bis ein vorgegebener Zustand erreicht wird [KTJ10, S. 222].

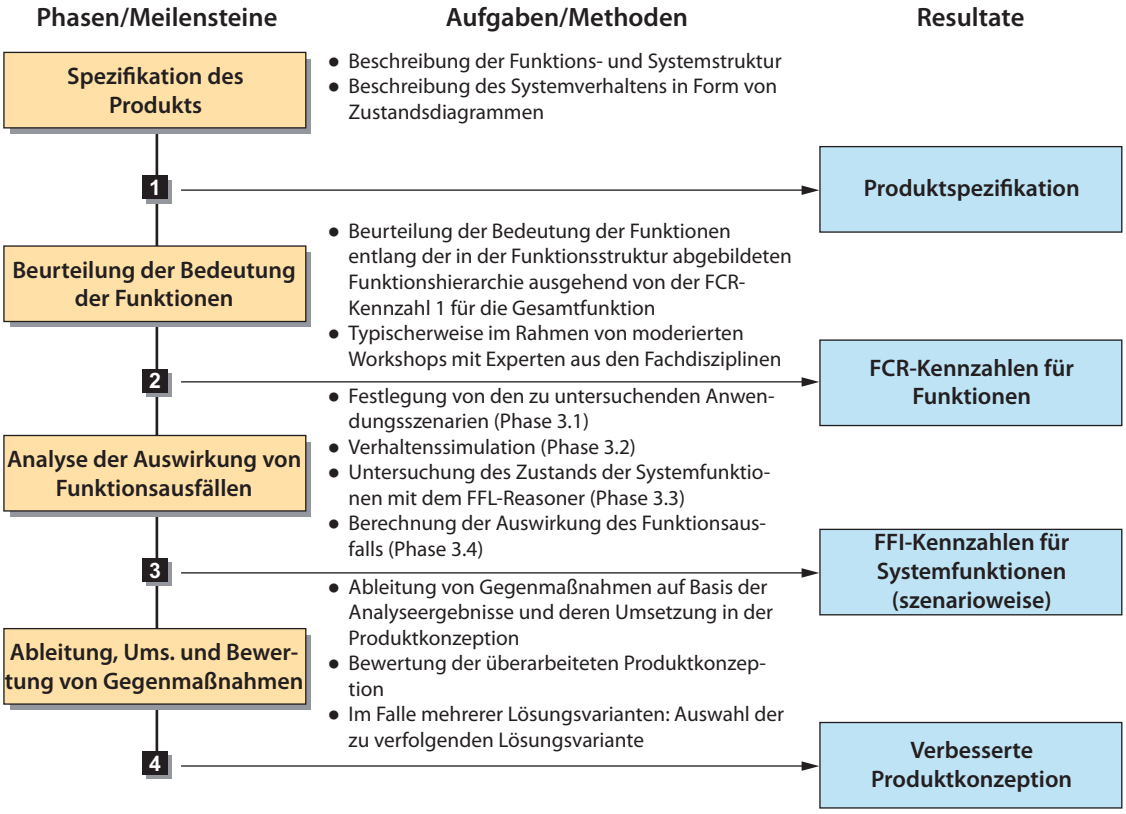


Bild 3-41: Das der FFIP-Methode zugrunde liegende Vorgehen

Im Wechselspiel mit der Verhaltenssimulation findet eine Untersuchung des Zustands der Systemfunktionen mit dem FFL-Reasoner statt (Function-Failure Logic) **(Phase 3.3)** [KTJ10, S. 215f.]. Die Verhaltenssimulation gibt den Systemzustand zum Ende eines jeden Simulationsschritts an den FFL-Reasoner weiter. An diesen diskreten Zeitpunkten ermittelt der FFL-Reasoner den Zustand der Systemfunktionen (funktionsfähig, degradiert, ausgefallen wiederherstellbar, ausgefallen nicht wiederherstellbar) [KTJ10, S. 215]. Die Ermittlung beruht auf sogenannten Modellen der Funktionsausfalllogik. Diese beschreiben den Zustand einer Systemfunktion in Abhängigkeit von den Werten der Eingangs-, Ausgangs- und Zustandsgrößen der Systemelemente, welche die betrachtete Funktion konkretisieren (diese Information liegt in der Produktspezifikation als ein Querverweis vor).

Dies wird am Beispiel eines elektrischen Antriebssystems aus dem Luftfahrtbereich kurz erklärt [KTJ10, S. 210 und 216ff.]. Kern der Funktionalität des Antriebssystems ist die Versorgung von ausgewählten Verbrauchern (z.B. Bordelektronik, Antrieb, Lebenserhaltungssystem) mit Strom. Als Energiequelle besitzt das System ein oder mehrere Batteriemodule. Eine der Teilfunktionen des Systems ist „Energie beim vorliegenden Bereitstellungswunsch bereitstellen“, um die Leistung von der Energiequelle an die ausgewählten Verbraucher weiterzuleiten. Es muss dabei möglich sein, eine Zustandsänderung einzuleiten, welche das Vorhandensein bzw. Nichtvorhandensein des Bereitstellungswunsches abbildet. Ferner ist die Information über den Zustand der Funktion auszugeben.

Diese Funktion wird durch ein Relais realisiert, mit dem der entsprechende Laststromkreis für die entsprechenden Verbraucher geschaltet werden kann. Ein extern angeschlossener Positionssensor kann die Schaltstellung des Relais über translatorische Energie erfassen. Ein Relais kann aufgrund eines Fehlers seinen nominalen Zustand „Nominal geöffnet“ bzw. „Nominal geschlossen“ verlassen und einen fehlerhaften Zustand einnehmen („Fehlerhaft geöffnet“ bzw. „Fehlerhaft geschlossen“). Dies kann an der Veränderung der Eingangs-, Ausgangs- und Zustandsgrößen des Relais erkannt werden. Dies wird in Bild 3-42 in Form von Verhaltensregeln sowie im Modell der Funktionsausfalllogik abgebildet. Die Funktionsausfalllogik besagt, dass es Abweichungen von der gewünschten Funktion gibt, wenn: 1) keine Leistung am Ausgang des Relais fließt, obwohl seine Schließung angestoßen wurde, 2) eine Leistung am Ausgang des Relais fließt, obwohl seine Öffnung angeordnet wurde. Anhand der Beobachtung dieser Größen kann der Zustand der Funktion ermittelt werden (Variable „RelState“ im Funktionsausfalllogikmodell).

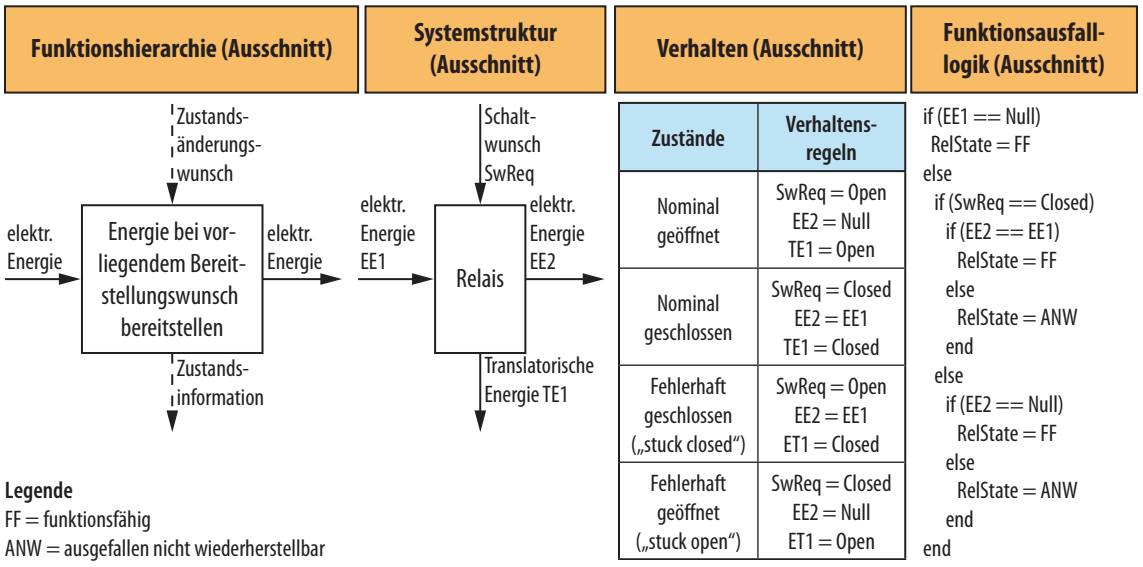


Bild 3-42: Modell der Funktionsausfalllogik sowie die zugehörige Produktspezifikation für eine durch ein Relais konkretisierte Funktion (Vereinfachte Darstellung in Anlehnung an [KTJ10, S. 219])

Auf Basis der Ergebnisse wird für jedes kritische Szenario eine FFI-Kennzahl (Functional Failure Impact) berechnet **(Phase 3.4)**. Für jede Funktion wird die in Phase 2 festgelegte FCR-Bedeutungskennzahl mit einem Gewichtungsfaktor multipliziert, das von dem in Phase 3.3 ermittelten Funktionszustand abhängt. Das Gewichtungsfaktor könnte wie folgt definiert werden: ist der Funktionszustand „funktionsfähig“, dann gilt $C_i = 0$, für „ausgefallen wiederherstellbar“ gilt $C_i = 1$, für „degradiert“ gilt $C_i = 2$ und für „ausgefallen nicht wiederherstellbar“ $C_i = 4$ [KTJ10, S. 216]. Ein Ausfall einer Funktion mit hohem Bedeutungsfaktor resultiert in einer schwerwiegenderen Auswirkung für das Gesamtsystem. Liegen mehrere Lösungsvarianten vor, welche die spezifizierte Funktionsstruktur und die zugehörigen Anforderungen erfüllen, so erfolgt die Analyse für alle diese Varianten. Die

Abschätzung der Auswirkung eines Funktionsausfalls stellt hierbei eine wesentliche Information für die Gegenüberstellung der Lösungsvarianten und für die darauf aufbauende Auswahl der weiter zu verfolgenden Variante [KTJ10, S. 216].

Phase 4 – Ableitung, Umsetzung und Bewertung von Gegenmaßnahmen: Abschließend werden Abstellmaßnahmen festgelegt und quantifiziert. Ein Beispiel ist eine redundante Auslegung eines Subsystems, z.B. eines Sensors. FFIP sieht die Gegenüberstellung der ursprünglichen und der überarbeiteten Produktkonzeption mit umgesetzten Verbesserungsmaßnahmen vor. Hierfür wird die komplette FFIP-Analyse für die überarbeitete Produktkonzeption für die festgestellten kritischen Szenarien durchgeführt. Aus den FFI-Kennzahlen der ursprünglichen und der überarbeiteten Produktkonzeption wird die RIR-Kennzahl (Reduction in Risk, RIR) berechnet, die die erreichte Risikominderung quantitativ ausdrückt. Sie dient als Grundlage für die Priorisierung von potentiellen Abstellmaßnahmen. Dies kommt insbesondere dann zum Tragen, wenn mehrere alternative Produktkonzeptionen gegenübergestellt werden. Für zuverlässigkeits- und sicherheitskritische Systeme sollte die RIR-Kennzahl jedoch nicht die alleinige Entscheidungsgrundlage darstellen, da sie ähnlich wie eine RPZ der FMEA stark subjektiv ist [KTJ10, S. 224].

Beurteilung: Mit der FFIP-Methode kann die Produktkonzeption modelliert und analysiert werden. Die Beschreibung der Produktkonzeption beschränkt sich auf die Aspekte Anwendungsszenarien, Funktionen, Systemstruktur und zustandsübergangsbasiertes Verhalten. Für die Beschreibung der Systemgrößen kommen qualitative Intervallvariablen zum Einsatz. Ein integraler Bestandteil ist die Simulation und Verbesserung der Produktkonzeption, wobei in besonderem Maße disziplinübergreifende Ausfallfortpflanzungspfade berücksichtigt werden. Der Einsatz von qualitativen Kennzahlen unterstützt eine Gegenüberstellung von mehreren Lösungsvarianten. Die FFIP-Methode sieht keine Erweiterungspunkte vor.

3.5.2 Ein UML-Profil zur FTA-basierten Absicherung der Sicherheit eines technischen Systems nach DOUGLASS

DOUGLASS schlägt ein UML-Profil[41] zur Spezifikation und Absicherung der Sicherheit eines Systems vor, welches die Durchführung einer FTA auf Basis eines mit dem Profil erstellten Modells ermöglicht [Dou09]. Dieser Ansatz lässt sich auch mit der SysML realisieren. Kern des UML-Profils bildet das in Bild 3-43 dargestellte Metamodell[42].

---

[41] Ein UML-Profil stellt eine problemspezifische Erweiterung der UML dar. Dieses wird mit einem auf Stereotypen und Tagged Values beruhenden Erweiterungsmechanismus (Profilmechanismus) erstellt (vgl. auch Abschnitt 3.4.2) [OMG11], [MH06, S. 245 ff.], [Wei07].

[42] Für eine Definition des Begriffs eines Metamodells siehe Abschnitt 2.1.4.

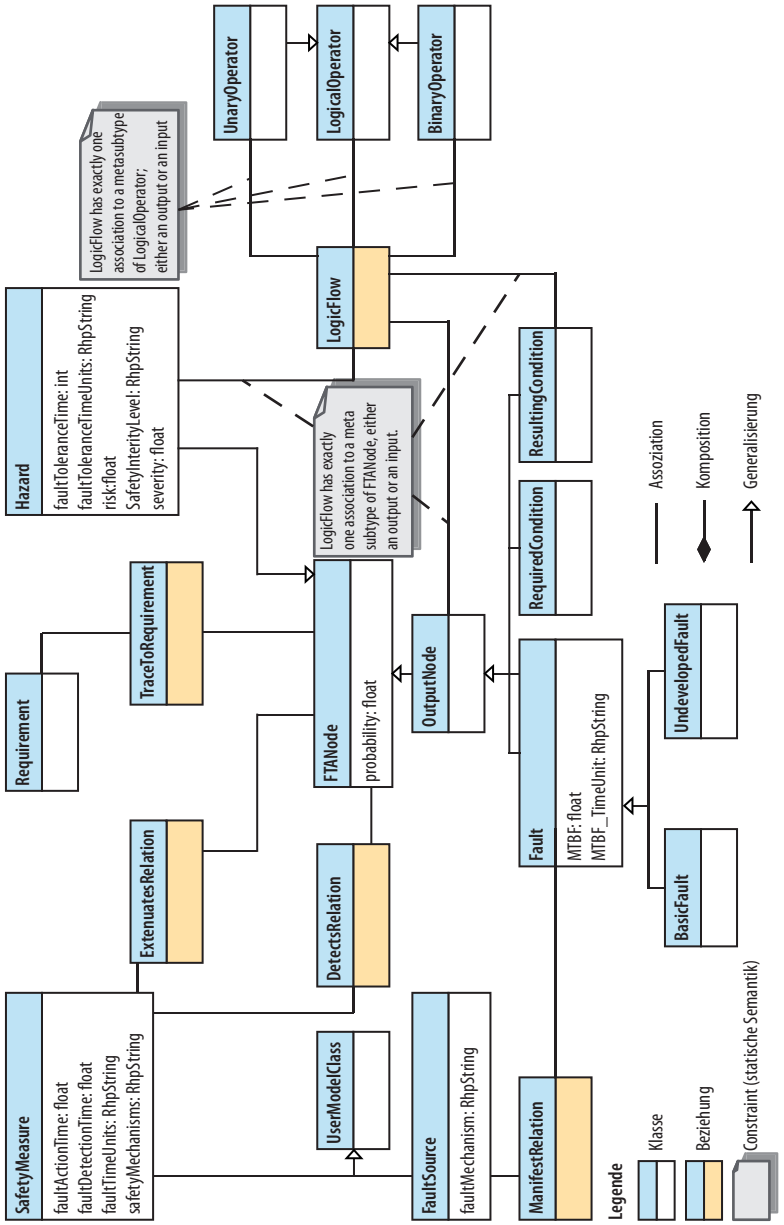


Bild 3-43: Metamodell des UML-Profils für FTA-basierte Sicherheitsanalysen nach DOUGLASS (vereinfachte Darstellung in Anlehnung an [Dou09, S. 17])

Bewertung: Das UML-Profil nach DOUGLASS zeigt eindrucksvoll, dass etablierte Methoden wie die Fehlzustandsbaumanalyse auf Basis eines Produktmodells durchführbar sind und zu einer frühen Verbesserung des Produktmodells hinsichtlich Zuverlässigkeit und Sicherheit führen können. Das Profil ist stark auf die Fehlzustandsbaumanalyse ausgerichtet. Hilfestellung für Integration weiterer Methoden ist nicht gegeben.

3.5.3 Analysen auf Basis einer mit der Spezifikationstechnik CONSENS beschriebenen Produktkonzeption

Am Heinz Nixdorf Institut entstanden zwei Ansätze zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit auf Basis einer mit der Spezifikationstechnik CONSENS

erstellten Beschreibung der Produktkonzeption. Aufgegriffen wurden hierbei die FTA und die FMEA.

Frühzeitige FMEA nach GAUSEMEIER ET AL.: GAUSEMEIER ET AL. schlagen einen Ansatz zur Durchführung einer FMEA auf Basis einer mit der Spezifikationstechnik CONSENS spezifizierten Produktkonzeption [GKP09]. Die Systemstruktur und die Funktionen des zu untersuchenden Systems werden aus der Spezifikation der Produktkonzeption ausgeleitet und in die FMEA-Tabelle übertragen. Danach folgen die übrigen Schritte der FMEA: die Schwachstellenanalyse, die Risikobewertung und die Verbesserung der Produktkonzeption (vgl. Abschnitt 3.2.2.5). Der Ansatz wurde im Rahmen eines Transferprojekts des SFB 614 an der Antriebselektronik einer Vakuumpumpe angewandt und validiert. Dabei stellte sich heraus, dass die disziplinübergreifende Spezifikation das gemeinsame Verständnis des Gesamtsystems fördert und die Erstellung einer FMEA wesentlich unterstützt [GKP09, S. 1016].

Frühzeitige FTA nach DEYTER ET AL.: Im BMBF-Verbundprojekt InZuMech (Instrumentarium für die frühzeitige Zuverlässigkeitsanalyse mechatronischer Systeme) wurde ein Ansatz zur frühzeitigen FTA auf Basis der Wirkstruktur entwickelt [Gau10], [DGK+09]. Die Systemelemente werden jeweils separat und ausschließlich an ihren Schnittstellen betrachtet. Für jedes Systemelement werden seine lokalen Ausfälle und deren Auswirkung auf die Ausgänge spezifiziert. Ferner wird für jeden Ausgang modelliert, wie und von welchen Eingängen es direkt oder indirekt abhängt. Die Beziehungen zwischen den lokalen Ausfällen und den Ein- und Ausgängen werden über logische Gatter beschrieben. Alle Ein- und Ausgänge können die Zustände „ok“ und „not(ok)“ besitzen; der Zustand „not(ok)“ bildet das Fehlverhalten ab. Zur Beschreibung der Ausfallfortpflanzung wird die „canImply“-Beziehung verwendet. Diese beschreibt welche Implikationen ein Ausfall auf den Ausgang haben kann. Bild 3-44 zeigt die Anwendung der Methode am Beispiel des Systemelements SE. Der Ausgang A1 weist ein Fehlverhalten dann auf, wenn der interne Ausfall Ausfall1 auftritt oder einer der beiden Eingänge fehlerhaft ist. Auf Basis einer derartigen Beschreibung können Fehlerbäume teilautomatisiert generiert werden (Bild 3-44).

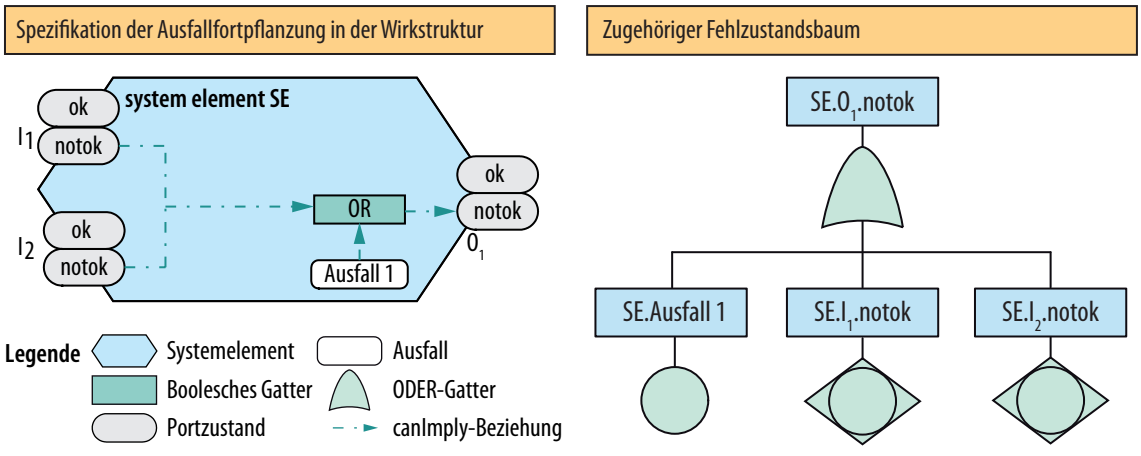


Bild 3-44: Spezifikation der Ausfallfortpflanzung und der zugehörige Fehlzustandsbaum

Bewertung: Der Ansatz nach GAUSEMEIER ET AL. ermöglicht die Durchführung einer FMEA auf Basis einer mit der Spezifikationstechnik CONSENS beschriebenen Produktkonzeption. Mit dem Ansatz nach DEYTER ET AL. ist eine FTA auf Basis der Produktkonzeption möglich. In beiden Fällen wird erkannt, dass viele der für die Durchführung einer FMEA bzw. einer FTA notwendigen Informationen bereits in der Spezifikation der Produktkonzeption abgebildet sind.

3.5.4 FMEA auf Basis eines SysML-Modells nach ALT

ALT erkennt ebenfalls das Potential der Durchführung einer FMEA auf Basis einer mit der SysML oder einer artverwandten Modellierungssprache spezifizierten Produktkonzeption [Alt12, S. 145ff.]. Wird die FMEA basierend auf den in der Produktkonzeption abgebildeten Informationen (Funktionen, Systemstruktur, Verhalten) durchgeführt, so können typische Arbeitsschritte einer FMEA wie Systemdefinition und Schwachstellenanalyse eingespart bzw. effizienter durchgeführt werden [Alt12, S. 146]. Ferner fließen die im Rahmen einer FMEA erarbeiteten Verbesserungsmaßnahmen (z.B. redundante Auslegung von Systemelementen, zusätzliche Überwachungsmechanismen, Degradations- und Warnungskonzept) in die Spezifikation der Produktkonzeption ein [Alt12, S. 147]. Auf der werkzeugtechnischen Seite schlägt ALT die Integration eines SysML-Werkzeugs mit dem FMEA-Werkzeug IQ-RM von APIS über dessen XML-Import-/-Export-Schnittstelle vor [Alt12, S. 147].

Bewertung: Unabhängig von den Arbeiten von POOK schlägt ALT die Durchführung einer FMEA auf Basis eines mit der SysML erstellten Produktmodells vor. ALT kommt zu den gleichen Schlussfolgerungen: der integrierte Einsatz beider Methoden kann zur Einsparung von Prozessschritten und damit einhergehend von Zeit und Geld führen.

3.5.5 MeDISIS (Integration Method of Reliability Analysis in the System Engineering Process)

MeDISIS[43] ist eine Methode zur Absicherung der Zuverlässigkeit eines technischen Systems unter Verwendung von SysML-Modellen und daraus abgeleiteten formalen Teilmodellen [DIK10], [CDI+13]. Ebenso kann die Methode zur Untersuchung der Sicherheit sowie weiterer Verlässlichkeitsaspekte eingesetzt werden [CDI+13]. Die SysML wird zum einen zur Spezifikation des Systemmodells verwendet. Zum anderen werden mit der SysML wiederkehrende Lösungsbausteine beschrieben und in einer Datenbank abgelegt (sogenannte DBD(Dysfunctional Behavior Database)-Datenbank). Diese Lösungsbausteine stellen eine Beschreibung von wiederkehrenden Mustern in Bezug auf Ausfallmöglichkeiten einer Klasse von Systemelementen dar (z.B. von Magnetventilen). Diese Be-

[43] MeDISIS kommt aus dem Französischen und steht für eine Methode zur Integration von Zuverlässigkeitsanalysen in den Systems Engineering Prozess [CDI+13, S. 172].

schreibung umfasst insbesondere die Spezifikation der zugehörigen Ausfallparameter sowie des mit dem Ausfall einhergehenden Fehlerverhaltens. Zum Beispiel können das Fehlverhalten auslösende Ereignis, das Ausfallverhalten im Zeitverlauf mittels einer Wahrscheinlichkeitsverteilung sowie die Auswirkung des Fehlverhaltens auf Systemgrößen beschrieben werden [DIK10, S. 438]. Die Spezifikation der Lösungsbausteine beruht auf einem durch DAVID ET AL. definierten SysML-Profil. Das diesem SysML-Profil zugrunde liegende Metamodell wurde erst mal in [DIK10] vorgestellt und in [CDI+13] erweitert.

Bild 3-45 stellt das der MeDISIS-Methode zugrunde liegende Vorgehen dar [DIK10, S. 436]. Ausgangspunkt ist die Spezifikation des Systemmodells, welche unter Verwendung der SysML geschieht (**Phase 1**). Gegenstand der **Phase 2** ist eine FMEA-basierte Ausfallanalyse. Auf Basis des mit der SysML erstellten Systemmodells erfolgt unter Verwendung der Bausteine aus der DBD-Datenbank eine vollautomatische Erzeugung einer vorläufigen FMEA. Die hierfür zum Einsatz kommenden Algorithmen sind zu finden in [DIK10, S. 439ff.]. Einige Arbeitsschritte der FMEA-Erstellung können dadurch eingespart bzw. effizienter durchgeführt werden [DIK10, S. 442]. Die vorläufige FMEA wird in moderierten FMEA-Workshops mit den Fachexperten durchgesprochen, verfeinert und ggf. angepasst. Das Ergebnis der Phase 2 ist eine verfeinerte vorläufige FMEA auf Systemebene. Danach wird diese FMEA einem Review unterzogen (z.B. wird eine Inspektion der FMEA durchgeführt), woraus sich weitere Anpassungen und Verfeinerungen der FMEA ergeben können (**Phase 3**). Resultat ist eine finale FMEA auf Systemebene. Diese umfasst insbesondere die Festlegung von Gegenmaßnahmen für die gefundenen Schwachstellen. Neue, im Rahmen der Phasen 2 und 3 gewonnene Erkenntnisse in Bezug auf typische Ausfallmöglichkeiten der betrachteten Klassen von Systemelementen werden in die DBD-Datenbank zurückgespiegelt. Die darin abgespeicherten Informationen können in weiteren Projekten wiederverwendet werden, wodurch Kosten und Zeit gespart werden [DIK10, S. 443].

Phase 4 sieht eine weiterführende Analyse unter Heranziehung von formalen Modellen vor (Beispiele für formale Modelle sind Altarica, Figaro, Generalisierte Stochastische Petri Netze (GSPN) und Markoff-Modelle [Rau02], [BB03], [BDR+06], [DIK10, S. 437]). Mit Hilfe dieser formalen Modelle können Teilaspekte des Systems einer detaillierteren Analyse unterzogen werden. Zum Beispiel unterstützen diese Modelle eine Simulation der Ausfallfortpflanzung unter Verwendung von Fehlerinjektionstechniken [DIK10, S. 437]. Basierend auf den Ergebnissen der weiterführenden Analysen können weitere Verbesserungsmaßnahmen abgeleitet werden. Auch hier werden die eventuellen neuen Erkenntnisse in die DBD-Datenbank aufgenommen. In **Phase 5** erfolgt abschließend die Umsetzung der in Phase 3 und Phase 4 ermittelten Verbesserungsmaßnahmen. Das mit der SysML spezifizierte Systemmodell wird entsprechend erweitert und angepasst. Zum Beispiel können zusätzliche Diagnoseeinrichtungen bzw. redundante Systemelemente integriert werden.

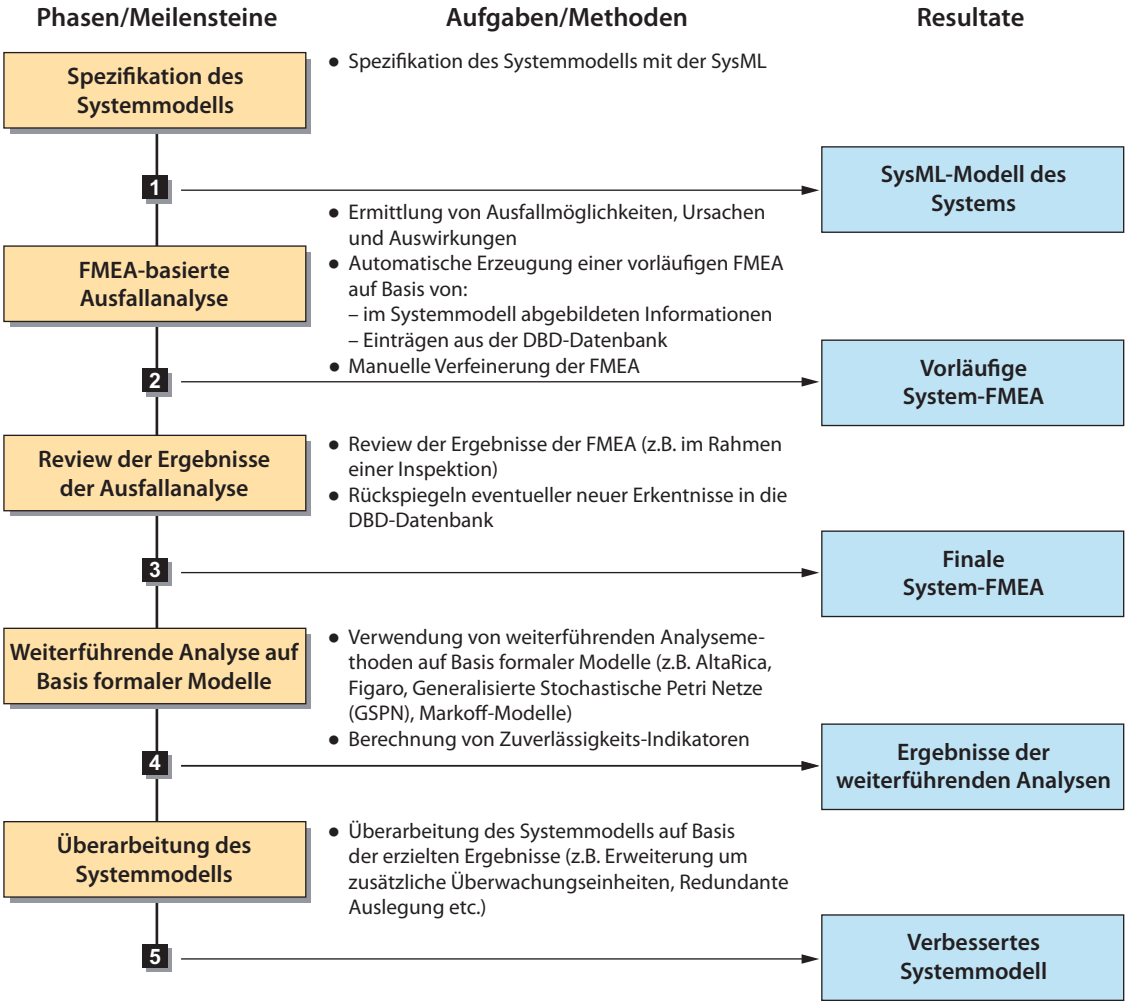


Bild 3-45: Das der MeDISIS-Methode zugrunde liegende Vorgehen

Bewertung: Die MeDISIS-Methode stellt einen datenbankbasierten Ansatz für die Integration von Zuverlässigkeits- und Sicherheitsuntersuchungen in einen Systems Engineering Prozess dar. Zur Abbildung des Produktmodells und der Lösungsbausteine wird die SysML verwendet. Die MeDISIS-Methode sieht zum einen eine FMEA-basierte Analyse vor, wobei die FMEA teilautomatisiert erzeugt wird. Zum anderen werden formale Analysen von Teilmodellaspekten unterstützt. Hilfestellung für Integration weiterer Methoden der Sicherheits- und Zuverlässigkeitstechnik ist nicht gegeben.

3.6 Software-Unterstützung

Zur Absicherung der Zuverlässigkeit und Sicherheit steht eine Menge von etablierten Software-Werkzeugen bzw. Software-Paketen zur Verfügung. Nachfolgend wird ein kurzer Überblick über diese gegeben.

3.6.1 Etablierte Software-Pakete zur Absicherung der Zuverlässigkeit und Sicherheit

In der Industrie werden Software-Werkzeuge bzw. Software-Pakete zur Absicherung der Zuverlässigkeit und Sicherheit zunehmend eingesetzt. Sie unterstützen u.a. die Modellierung von Systemen, die Abbildung von Zuverlässigkeits- bzw. Sicherheitsinformationen (Ausfallraten, Reparaturraten etc.), die etablierten Analysen wie FMEA, FTA und Markoff-Analyse, die zugehörigen mathematischen Berechnungen, die Erstellung der zugehörigen Dokumentation und Berichte sowie die graphische Visualisierung von Resultaten [Wil06]. Auf dem Markt ist eine große Anzahl von Software-Paketen unterschiedlicher Software-Hersteller zu finden. Die bekanntesten sind Reliability Workbench von Isograph, The Synthesis Plattform von ReliaSoft, ITEM ToolKit von ITEM Software und Windchill Quality Solutions von PTC [Iso13-ol], [Rel13a-ol], [Ite13-ol], [Ptc13-ol]. Diese Software-Pakete umfassen jeweils eine Reihe von Software-Modulen, die spezialisierte Funktionen (z.B. FMEA, Weibull-Analyse, FTA, ETA) unterstützen und typischerweise auch als Einzelprodukt erworben werden können. Zum Beispiel genießt das Software-Werkzeug FaultTree+ zur Fehlzustandsbaumanalyse bei den Fahrzeugherstellern eine hohe Verbreitung: dieses kann entweder separat oder als Teil des Software-Pakets Reliability Workbench erworben werden [LPP10, S. 318].

Eine umfassende Übersicht über Software-Werkzeuge zur Absicherung der Zuverlässigkeit und Sicherheit gibt die Studie von WILSON [Wil06]. LÖW ET AL. beschreiben, welche Software-Werkzeuge zur Absicherung der Sicherheit nach IEC61508 bzw. ISO26262 in der Automobilindustrie verwendet werden, wobei nach den einzelnen Phasen des entsprechenden Sicherheitslebenszyklus differenziert wird (vgl. auch Abschnitt 3.1.1 und Abschnitt 3.1.2) [LPP10, S. 318ff.].

Die Software-Module, welche Bestandteile der erwähnten Software-Pakete sind, entstanden historisch gesehen typischerweise als einzelne Software-Werkzeuge. Sie wurden in Isolation voneinander weiterentwickelt. Diese Software-Werkzeuge wurden in der Regel erst nachträglich durch die Software-Hersteller zu einem gemeinsamen Software-Paket zusammengefasst, um der zunehmend stärker werdenden Anforderung der Kunden nach einer ganzheitlichen Lösung mit vereinfachten Lizenzmodellen zu genügen. Hinzu kommt, dass diese zusammengefassten Software-Landschaften sehr oft erst auf Basis von Zukäufen von kleineren Software-Herstellern möglich wurden. Eine zielgerichtete Entwicklung von Software-Paketen, welche verschiedenartige Modellierungs- und Analysemethoden von vornherein zu einem ganzheitlichen Ansatz effizient integriert, fand nicht statt.

Bewertung: Die aufgeführten Software-Pakete sind sehr etabliert und werden in vielen Branchen verwendet. Dennoch fehlt gänzlich ein methodischer Ansatz, welcher eine ganzheitliche Produktmodellierung ermöglicht und dabei einen zusammenhängenden

Einsatz verschiedenartiger Methoden auf Basis eines Produktmodells unterstützt. [44] Eine Erweiterbarkeit der Software-Pakete ist in unzureichendem Maße gegeben. Auch die Unterstützung etablierter Modellierungssprachen zur Beschreibung des Produktmodells wie der SysML ist größtenteils nicht vorhanden. Wenngleich die meisten etablierten Methoden unterstützt werden, ist eine Unterstützung für die Suche und Auswahl der für die Ausgangsfragestellung adäquaten Methoden nicht vorhanden.

3.6.2 medini analyze – ein Software-Werkzeug zur Absicherung der funktionalen Sicherheit

Das Software-Werkzeug medini analyze der ikv++ Technologies unterstützt die Absicherung der funktionalen Sicherheit nach IEC61508 bzw. nach ISO26262 [ikv13-ol]. Es findet zunehmend in der Automobilindustrie Anwendung [SRM13-ol], [SS11a]. Dieses auf der Eclipse-Technologie beruhende Software-Werkzeug ist modular aufgebaut. Bild 3-46 stellt die wichtigsten Funktionsmodule dar. Demnach unterstützt medini analyze die Absicherung der Sicherheit von vornherein: von der Gefahrenanalyse und Risikoeinschätzung über die Spezifikation von Sicherheitszielen und deren Verfeinerung in Sicherheitsanforderungen, die auf der SysML beruhende Spezifikation des Systemmodells, Sicherheitsanalysen wie die FTA und die FMEA und die Spezifikation des Sicherheitskonzepts bis hin zur Spezifikation der HW- und SW-Sicherheitsanforderungen. Ebenso unterstützt wird die auf Basis der HW-Architektur stattfindende Berechnung von Hardware-Metriken mit einer FMEDA unter Verwendung von etablierten Ausfallratenkatalogen. Ferner bietet medini analyze unterstützende Funktionen zur Modellierung und Rückverfolgbarkeit von Querbeziehungen zwischen Modellelementen sowie Erzeugung von Dokumentation und Berichten. Außerdem stellt medini analyze Schnittstellen zu etablierten Software-Werkzeugen bereit, wodurch eine nahtlose Integration in bestehende Unternehmens-IT-Landschaften angestrebt wird. Angeboten werden Schnittstellen zum Anforderungsmanagement-Werkzeug IBM Rational DOORS, zu den SysML-Werkzeugen IBM Rational Rhapsody und Enterprise Architect sowie zum Matlab/Simulink.

---

[44] Stattdessen werden meist Umweglösungen umgesetzt, was folgendes Beispiel zeigt [Rel13b-ol]: Im FMEA-Tool Xfmea (Teil der Synthesis Plattform) wird ein Produktmodell und eine zugehörige FMEA abgebildet. Mit dem FTA-Tool BlockSim (ebenfalls Teil der Synthesis Plattform) wird ein Fehlzustandsbaum auf Basis der in Xfmea abgebildeten Informationen erzeugt, der weiter analysiert und verfeinert wird. Jedoch erfolgt keine Synchronisation zwischen den Tools, da ein zugrunde liegender methodischer Ansatz und eine gemeinsame Datenbasis fehlen. Zum Beispiel wenn das Ausfallverhalten im generierten Fehlzustandsbaum geändert wird, bedeutet es nicht, dass die zugehörigen Daten im FMEA-Tool synchron dazu aktualisiert werden. Auch eine Aktualisierung im FMEA-Tool wird nicht automatisch in den generierten Fehlzustandsbaum übertragen. Der Fehlzustandsbaum müsste in diesem Fall bei jeder Änderung der FMEA erneut generiert werden. Die in der Zwischenzeit vorgenommenen Erweiterungen des Fehlzustandsbaums würden dabei verloren gehen.

8 Matlab/Simulink-Int.	1 Basismodul	2 HARA-Modul
■ Import von Matlab/Simulink-Modellen ■ Rückverfolgung auf Ebene von System-elementen ■ Aktualisierungsfunktion für iteratives Arbeiten mit Matlab/Simulink	■ Management von Sicherheitszielen und Sicherheitsanforderungen ■ Systemmodellierung mit der SysML ■ Unterstützung der Rückverfolgbarkeit ■ Erzeugung von Dokumentation	■ Gefahrenanalyse und Risikoeinschätzung nach ISO26262 ■ Fahrsituationskataloge
7 SysML-Integration	medini analyze safety and reliability engineering	**3 FME(D)A-Modul**
■ Schnittstellen zu den etablierten SysML-Werkzeugen IBM Rational Rhapsody und Enterprise Architect		■ Tabellarische Editoren für die FMEA und die FMEDA ■ Berechnung von Hardware-Metriken nach IEC61508 und ISO26262 ■ Integration mit dem Systemmodell
6 DOORS-Integration	**5 Ausfallratenkataloge**	**4 FTA-Modul**
■ Schnittstelle zum Anforderungs-managementtool IBM Rational DOORS über das Austauschformat ReqIF (Requirements Interchange Format)	■ Bestimmung von Ausfallraten auf Basis von bewährten Ausfallratenkatalogen (z.B. mit der Siemens Norm SN 29500)	■ Graphische Editoren für die FTA ■ Mathematische Berechnungen für die quantitative FTA (z.B. Ausfallwahr-scheinlichkeiten) ■ Integration mit dem Systemmodell

Bild 3-46: Modularisierte Architektur des Software-Werkzeugs medini analyze (in Anlehnung an [ikv13-ol]; Vereinfachte Darstellung)

Bewertung: medini analyze unterstützt viele der mit der Absicherung der funktionalen Sicherheit nach IEC 61508 und ISO 26262 verbundenen Aktivitäten. Es stellt Schnittstellen zu etablierten Software-Werkzeugen wie DOORS und Rhapsody bereit und unterstützt eine SysML-basierte Produktmodellierung sowie Sicherheitsanalysen wie die FTA, die FMEA und die HAZOP. Aus heutiger Sicht sind jedoch die Schnittstellen zu anderen Tools teilweise wenig stabil. Ferner ist kein methodischer Ansatz für die integrative Produktmodellierung und -analyse erkennbar: In der werkzeugtechnischen Umsetzung lassen sich an vielen Stellen Unklarheiten in Bezug auf die Frage feststellen, welche Informationen im Produktmodell wie abgebildet werden müssen, damit die jeweilige Methode effizient eingesetzt werden kann. Ferner wird die Auswahl von Methoden durch das Software-Werkzeug nicht unterstützt. Da es sich um ein kommerzielles und kein Open-Source-Werkzeug handelt, ist die Erweiterbarkeit eingeschränkt.

3.6.3 Mechatronic Modeller

Der Mechatronic Modeller ist die werkzeugtechnische Umsetzung der in Abschnitt 3.4.3 beschriebenen Spezifikationstechnik CONSENS. Er entstand im Rahmen des Forschungsprojekts VireS „Virtuelle Synchronisation von Produktentwicklung und Produktionssystementwicklung“. Der Mechatronic Modeller wird im Rahmen von weiteren Projekten weiterentwickelt und liegt mittlerweile in der Version 2.0 vor [GDK10], [GLL12, S. 107ff.]. Dieses auf der Eclipse-Technologie beruhendes Software-Werkzeug ist modular aufgebaut (der Editor für die Wirkstruktur stellt z.B. ein Modul dar) und stellt Schnittstellen zu anderen Werkzeugen wie IBM Rational DOORS, MS Word und MS Excel

bereit. Bild 3-47 gibt einen kurzen Überblick über die Funktionalität des Mechatronic Modellers.

Funktionsumfang

- Editoren zur Spezifikation der Produktkonzeption
- Integration des Anforderungsaustauschformats ReqIF
- Schnittstelle zum IBM Rational DOORS
- Export/Import von Anforderungen aus MS Excel
- Automatisierte Generierung der technischen Dokumentation (z.B. Erzeugung einer Anforderungsliste für MS Word)
- Reduktion der Komplexität durch Sichtenbildung und Filtern (z.B. Filtern nach Systemelementen, die durch die Softwaretechnik ausgearbeitet werden)
- Plausibilitätsprüfungen im Hinblick auf Korrektheit und Vollständigkeit der Produktkonzeption
- Visualisierung der disziplinübergreifenden Zusammenhänge und Verantwortlichkeiten

Bild 3-47: Funktionsumfang des Mechatronic Modellers in der Version 2.0

Bewertung: Der Mechatronic Modeller stellt eine dedizierte werkzeugtechnische Umsetzung der Spezifikationstechnik CONSENS dar, welche auf die Spezifikationstechnik und die zugehörige Entwicklungsmethodik stark ausgerichtet ist. Es handelt sich hierbei um ein in einem Forschungsprojekt entwickeltes Software-Werkzeug, das als ein Forschungsträger verwendet werden kann. Wenngleich der Mechatronic Modeller derzeit keine Funktionalität für die Analyse der Zuverlässigkeit und Sicherheit bereitstellt, ist eine derartige Funktionserweiterung unter Verwendung des Eclipse-Plugin-Erweiterungsmechanismus realisierbar.

3.7 Bewertung des Stands der Technik und Handlungsbedarf

Im Folgenden wird die Bewertung der in diesem Kapitel vorgestellten Ansätze hinsichtlich der in Abschnitt 2.5 aufgestellten Anforderungen zusammengefasst und der jeweils verbleibende Handlungsbedarf erläutert (Bild 3-48 und Bild 3-49).

A1) Interdisziplinarität: Die ISO 26262 sieht eine disziplinübergreifende Systembetrachtung vor. Auch die Methodik der DFG-Forschergruppe 460 und der Referenzprozess des SFB 614 sind durch eine interdisziplinäre Sichtweise geprägt. Die meisten der Analysemethoden lassen sich zwar für die Arbeitsergebnisse der einzelnen Fachdisziplinen anwenden. Die Betrachtung der fachdisziplinübergreifenden Zusammenhänge bleibt jedoch aus. Dass eine derartige Betrachtung auf Basis der Spezifikation einer Produktkonzeption prinzipiell möglich und sinnvoll ist, zeigen die zahlreichen Methoden aus dem Bereich Absicherung auf Basis des Produktmodells.

A2) Fokus auf die Konzipierung: Alle der vorgestellten Vorgehensmodelle zur Entwicklung zuverlässiger und sicherer mechatronischer Systeme genügen dieser Anforderung. Von den Modellierungssprachen erfüllen die SQMA und CONSENS diese Anforderung.

Bewertung der untersuchten Ansätze hinsichtlich der gestellten Anforderungen.
(Teil 1 von 2)

Bewertungsskala:

○ = nicht erfüllt
◐ = teilweise erfüllt
● = voll erfüllt

		Anforderungen								
		Interdisziplinarität	Fokus auf die Konzipierung	Zukunftsrobustheit und Erweiterbarkeit	Suche, Auswahl und Kombination von Methoden	Ganzheitliche Spezifikation	Produktmodellzentrierte Analyse und Verbesserung	Problemunabhängigkeit	Anwenderakzeptanz	Rechnerunterstützung
		A1	A2	A3	A4	A5	A6	A7	A8	A9
Vorgehensmodelle	IEC 61508 (Sicherheitslebenszyklus)	◐	●	○	◐	◐	◐	◐	◐	○
	ISO 26262 (Sicherheitslebenszyklus)	●	●	○	◐	◐	◐	○	◐	○
	Methodik der DFG-Forschergruppe 460	●	●	◐	○	◐	◐	●	◐	○
	Referenzprozess des SFB614	●	●	◐	○	●	◐	●	◐	○
Methoden der Zuverlässigkeits- und Sicherheitsanalyse	Gefahrenanalysen nach MIL-STD-882 (PHL, PHA, SSHA, SHA, O&SHA)	●	●	○	○	○	◐	○	●	○
	Gefahrenanalyse und Risikoeinschätzung nach ISO 26262	●	●	○	○	○	◐	○	●	○
	HAZOP (Hazard and Operability Study)	●	●	●	○	○	◐	○	●	○
	FTA (Fehlzustandsbaumanalyse) und DFT (Dynamische Fehlzustandsbäume)	◐	◐	◐	○	○	◐	○	●	○
	FMEA (Fehlzustandsart- und -auswirkungsanalyse)	◐	◐	◐	○	○	◐	○	●	○
	Markoff-Analyse	◐	◐	◐	○	○	◐	○	◐	○
	statische und dynamische Bayessche Netze (BN / DBN)	◐	◐	◐	○	○	◐	○	◐	○
Auswahl von Methoden	DIN EN 60300-3-1	◐	●	○	◐	○	○	●	●	○
	IEC 31010	◐	●	○	◐	○	○	◐	●	○
	IEC 61508 und ISO 26262 (Auswahl von Methoden)	●	◐	○	◐	○	○	○	●	○
	Methodik des SFB 614	●	○	●	●	○	○	●	●	◐

Bild 3-48: Bewertung des Stands der Technik hins. der Anforderungen (Teil 1 von 2)

A3) Zukunftsrobustheit und Erweiterbarkeit: Das Referenzmodell des SFB 614 weist eine hohe Erweiterbarkeit auf. Dies gilt ebenso für die Methodik zur Auswahl von Methoden des SFB 614. Diese ermöglicht grundsätzlich die Aufnahme von neuen Methoden, die dann hinsichtlich der vorgegebenen Klassifizierungsmerkmale jeweils charakterisiert werden müssen. Die SysML lässt sich unter Verwendung des Profilmechanismus erweitern, ebenso ist die Spezifikationstechnik CONSENS erweiterbar. Von den Software-Werkzeugen ist der Mechatronic Modeller dieser Anforderung gerecht.

Bewertung der untersuchten Ansätze hinsichtlich der gestellten Anforderungen. *(Teil 2 von 2)*

Bewertungsskala:
○ = nicht erfüllt
◐ = teilweise erfüllt
● = voll erfüllt

		Anforderungen								
		Interdisziplinarität	Fokus auf die Konzipierung	Zukunftsrobustheit und Erweiterbarkeit	Suche, Auswahl und Kombination von Methoden	Ganzheitliche Spezifikation	Produktmodellzentrierte Analyse und Verbesserung	Problemunabhängigkeit	Anwenderakzeptanz	Rechnerunterstützung
		A1	A2	A3	A4	A5	A6	A7	A8	A9
Modellierungs-sprachen	SQMA (Situationsbasierte Qualitative Modellbildung und Analyse)	●	◐	◐	○	◐	●	○	◐	◐
	SysML (Systems Modeling Language)	◐	◐	●	○	●	◐	○	◐	●
	Spezifikationstechnik CONSENS	●	●	●	○	●	◐	○	●	●
Absicherung auf Basis des Produktmodells	FFIP (Functional Failure Identification and Propagation)	●	●	◐	○	◐	●	○	◐	○
	CONSENS-basierte Ansätze (FTA, FMEA)	●	●	○	○	●	●	○	◐	○
	UML-Profil nach Douglass	●	◐	◐	○	●	●	○	◐	○
	FMEA auf Basis des SysML-Modells	◐	◐	◐	○	●	●	○	◐	○
	MeDISIS	◐	◐	◐	○	●	●	○	◐	○
SW-Unterstützung	Software-Pakete (Reliability Workbench, the Synthesis Plattform, ITEM ToolKit, Windchill Quality Solutions)	●	○	○	◐	◐	○	●	◐	◐
	medini analyze	●	◐	○	◐	●	◐	○	◐	◐
	Mechatronic Modeller	●	●	●	○	●	○	●	◐	●

Bild 3-49: Bewertung des Stands der Technik hins. der Anforderungen (Teil 2 von 2)

A4) Suche, Auswahl und Kombination von Methoden: Nur die Methodik zur Auswahl von Methoden des SFB 614 erfüllt diese Anforderung in vollem Umfang. Die Normen DIN EN 60300-3-1, IEC 31010, IEC 61508 und ISO 26262 sind für die Festlegung von Methodenmerkmalen und damit einhergehend für die Unterstützung der Suche und Auswahl von Methoden sehr nützlich.

A5) Ganzheitliche Spezifikation: Der Referenzprozess des SFB 614 stellt die ganzheitliche Beschreibung der Produktkonzeption in den Vordergrund. Von den Modellierungssprachen ermöglichen die SysML sowie CONSENS eine ganzheitliche Beschreibung der Produktkonzeption. Alle vorgestellten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit auf Basis eines Produktmodells bestätigen das hohe Potential für die integrierte Durchführung der Modellierung und Analyse. Sie fokussieren dabei jedoch typischerweise eine bestimmte Methode wie die FTA oder die FMEA. Die Software-Werkzeuge medini analyze und Mechatronic Modeller erfüllen die Anforderung bezogen auf die Konzipierungsphase in vollem Umfang, wobei medini analyze hierbei noch methodische Defizite aufweist.

A6) Produktmodellzentrierte Analyse und Verbesserung: Der Dreh- und Angelpunkt des Referenzprozesses des SFB 614 ist die Spezifikation der Produktkonzeption, wodurch dieser die Anforderung zum großen Teil erfüllt. Lediglich im Hinblick auf das explizite Berücksichtigen von Analyse und Verbesserung besteht noch Optimierungsbedarf. Alle vorgestellten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit können prinzipiell in der Konzipierung auf Basis der Spezifikation der Produktkonzeption durchgeführt werden, wobei eine Anpassung dieser Methoden meist erforderlich ist. Von den Modellierungssprachen erfüllt die SQMA die Anforderungen vollumfänglich. Eine produktmodellzentrierte Analyse und Verbesserung steht bei der SysML und CONSENS zwar nicht im direkten Fokus. Die mit diesen Modellierungssprachen erstellten Produktmodelle stellen jedoch viele der für die Durchführung der Analysen erforderlichen Informationen bereit bzw. können um diese erweitert werden, was die vorgestellten Methoden aus dem Bereich Absicherung der Zuverlässigkeit und Sicherheit auf Basis eines Produktmodells zeigen.

A7) Problemunabhängigkeit: Die Methodik der Forschergruppe 460 und der Referenzprozess des SFB 614 sind branchen- und problemklassenunabhängig. Etablierte Normen wie die ISO 26262 und die IEC 61508 lassen sich in beide Ansätze integrieren. Wenn es um Auswahl von Methoden geht, weisen die DIN EN 60300-3-1 und die Methodik des SFB 614 bzgl. der vorgeschlagenen Auswahl- und Beurteilungskriterien eine hohe Problemunabhängigkeit auf.

A8) Anwenderakzeptanz: Der Großteil der vorgestellten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit findet in der industriellen Praxis eine hohe Verbreitung und genießt eine hohe Akzeptanz. Ebenso erfüllen die Ansätze zur Auswahl von Methoden diese Anforderung. Bei den Modellierungssprachen weist CONSENS die größte Anwenderakzeptanz auf.

A9) Rechnerunterstützung: Für die rechnerunterstützte Spezifikation der Produktkonzeption eignet sich der Mechatronic Modeller am besten. Auch der Einsatz von SysML-Werkzeugen wäre in diesem Zusammenhang denkbar, obwohl hierbei die Erweiterbarkeit gering ist. Für die Auswahl von Methoden stellt lediglich die Methodik des SFB 614 eine Werkzeugunterstützung bereit. Auf dieser könnte in der vorliegenden Arbeit aufgebaut werden.

Keiner der untersuchten Ansätze, auch keine triviale Kombination dieser, erfüllt die gestellten Anforderungen vollumfänglich. Aus der Analyse des Stands der Technik wurde deutlich, dass die meisten Ansätze nur Teilaspekte des Gesamtproblems adressieren. Insbesondere fehlt eine methodische Grundlage für eine integrierte Modellierung, Analyse und Verbesserung der Zuverlässigkeit und Sicherheit eines Produkts auf Basis eines Produktmodells in der Konzipierung. Folglich besteht ein erheblicher Handlungsbedarf für eine *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme*.

4 Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit

In diesem Kapitel wird der Kern der vorliegenden Arbeit vorgestellt – die *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme*. Mit dieser soll es möglich sein, dem aus der Problemanalyse und der Analyse des Stands der Technik abgeleiteten Handlungsbedarf gerecht zu werden.

Dieses Kapitel ist wie folgt aufgebaut: Abschnitt 4.1 gibt einen Überblick über den grundsätzlichen Aufbau der Systematik. In Abschnitt 4.2 wird das Vorgehensmodell der Systematik und seine Einbettung in den Referenzprozess für die Konzipierung erklärt. Abschnitt 4.3 befasst sich mit der rechnerunterstützten Suche, Auswahl und Planung von Methoden ausgehend von der Charakterisierung der Entwicklungsaufgabe. Abschnitt 4.4 befasst sich mit der Modellierung des Produkts unter Berücksichtigung von zuverlässigkeits- und sicherheitsrelevanten Informationen. In Abschnitt 4.5 werden Methoden zur Analyse und Verbesserung vorgestellt, welche für eine frühzeitige Anwendung auf Basis der Spezifikation der Produktkonzeption anepasst wurden. Die prototypische Werkzeugunterstützung für die Modellierung und Analyse der Zuverlässigkeit und Sicherheit wird abschließend in Abschnitt 4.6 erläutert.

Die Vorstellung der Systematik erfolgt im vorliegenden Kapitel auf konzeptioneller Ebene. Zur Veranschaulichung einiger Ansätze werden dabei Demonstratoren des SFB 614 verwendet. Die Validierung der Systematik anhand eines durchgängigen Anwendungsbeispiels erfolgt anschließend in Kapitel 5.

4.1 Die Systematik im Überblick

Die *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* umfasst die folgenden Bestandteile (Bild 4-1):

- ein **Vorgehensmodell** zur Anwendung der Systematik, welches die zu durchlaufenden Phasen, deren Reihenfolge, die zugehörigen Aufgaben und Methoden sowie die wesentlichen Meilensteine und Resultate beschreibt,
- eine **Methodik zur Auswahl und Planung von Methoden** zur Absicherung der Zuverlässigkeit und Sicherheit in der Konzipierung,
- eine **Spezifikationssprache** zur Spezifikation der Produktkonzeption unter besonderer Berücksichtigung von Zuverlässigkeits- und Sicherheitsinformationen,
- **Methoden zur Analyse und Verbesserung** der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit, die auf bewährten Methoden und Verfahren zur Absicherung der Zuverlässigkeit und Sicherheit aufbauen,

- ein Konzept einer **Werkzeugunterstützung** für die Systematik, welches prototypisch realisiert ist.

Bild 4-1: Bestandteile der Systematik

Grundlegende Aspekte der Systematik sind die Definition von Klassifikationsmerkmalen zur Charakterisierung der Entwicklungsaufgabe, die Frage nach geeigneten Mitteln zur Suche, Auswahl und Planung des Einsatzes von Methoden und – nicht zuletzt – nach einer Spezifikationssprache, welche die Modellierung, Analyse und Verbesserung von Zuverlässigkeit und Sicherheit effizient unterstützt. Dabei wird möglichst auf etablierten Methoden und Vorgehensmodellen aufgebaut. In der vorliegenden Arbeit werden vordergründig die Begriffsdefinitionen aus Abschnitt 2.1 verwendet, wobei das von AVIZIENIS ET AL. vorgeschlagene Vokabular den Kern dieser Begriffsdefinitionen bildet [ALR+04, S. 11]. Vor dem Hintergrund der Ergebnisse der Analyse des Stands der Technik, der Bedeutung der Fokussierung auf die Konzipierungsphase und der Zukunftsrobustheit der Systematik wird als Beschreibungssprache die Spezifikationstechnik CONSENS eingesetzt (vgl. Abschnitt 3.4.3). Aus den gleichen Gründen wird ferner zur Strukturierung des Entwicklungsprozesses der Referenzprozess für die Konzipierung selbstoptimierender mechatronischer Systeme herangezogen (vgl. Abschnitt 3.1.4).

Wenngleich für die Zwecke dieser Arbeit gewisse Festlegungen bzgl. der einzusetzenden etablierten Hilfsmitteln (Methoden, Beschreibungssprachen, Klassifizierungsschemen, Vorgehensmodelle etc.) getroffen worden sind, ist die Systematik so ausgelegt, dass es

grundsätzlich möglich ist, auch andere Hilfsmittel zu integrieren. Zum Beispiel könnte als Spezifikationssprache auch die SysML[45] zum Einsatz kommen (vgl. Abschnitt 3.4.2).

4.2 Vorgehensmodell

Im Folgenden wird das Vorgehensmodell für die *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* vorgestellt. Das Vorgehensmodell bildet die methodische Grundlage der Systematik. Es strukturiert den Ablauf der durchzuführenden Aufgaben und begleitet den Anwender bei der Absicherung der Zuverlässigkeit und Sicherheit des Produkts in der Konzipierung.

Die einzelnen Phasen des Vorgehensmodells werden in Abschnitt 4.2.1 erklärt. Danach erfolgt in Abschnitt 4.2.2 die Einordnung des Vorgehensmodells – und damit einhergehend der Systematik selbst – in den Referenzprozess zur Konzipierung selbstoptimierender mechatronischer Systeme des SFB 614.

4.2.1 Aufbau des Vorgehensmodells

Gemäß des Referenzprozesses für die Entwicklung selbstoptimierender mechatronischer Systeme findet die Systematik ihre Anwendung in der Konzipierungsphase (vgl. Abschnitt 3.1.4). Im Folgenden werden die einzelnen Phasen des Vorgehensmodells zur Anwendung der Systematik, die zugehörigen Aufgaben und Methoden sowie die wesentlichen Meilensteine und Resultate vorgestellt. Die Vorstellung erfolgt zunächst losgelöst von den übrigen Tätigkeiten der Konzipierung. Im Abschnitt 4.2.2 wird erklärt, wie die Systematik grundsätzlich anzuwenden ist und wie sich das Vorgehensmodell der Systematik in den Referenzprozess für die Konzipierung einbettet.

Bild 4-2 stellt den Aufbau des Vorgehensmodells zur Anwendung der Systematik in Form eines Phasen-Meilenstein-Diagramms dar. Gezeigt wird die idealtypische Reihenfolge, in der die einzelnen Phasen durchlaufen werden; Iterationen und Rücksprünge werden nicht explizit dargestellt, wenngleich diese in allen Phasen zulässig sind.

Angewendet wird die Systematik i.d.R. durch den Sicherheits- und Zuverlässigkeitsverantwortlichen in Zusammenarbeit mit dem Systemingenieur. Ausgangspunkt ist typischerweise die Beschreibung der Entwicklungsaufgabe. In **Phase 1** erfolgt die Analyse der Entwicklungsaufgabe hinsichtlich der Fragestellungen der Absicherung der Zuverlässigkeit und Sicherheit. Das Ergebnis ist eine charakterisierte Entwicklungsaufgabe. Ausgehend von dieser Charakterisierung findet in **Phase 2** die Suche und Auswahl der ein-

[45] Die in der vorliegenden Arbeit unter Verwendung der Spezifikationstechnik CONSENS erarbeiteten Ergebnisse sind grundsätzlich aufwandsarm auf die SysML übertragbar. Hierzu könnte z.B. das am Heinz Nixdorf Institut in Zusammenarbeit mit der itemis AG entwickelte SysML-Profil für CONSENS zum Einsatz kommen [IKD+13].

zusetzenden Methoden zur Absicherung der Zuverlässigkeit und Sicherheit statt. Außerdem erfolgt hier die Planung des Einsatzes der ausgewählten Methoden. Diese legt fest, wie und in welcher Reihenfolge die ausgewählten Methoden in den Entwicklungsprozess zu integrieren sind. In **Phase 3** wird die Spezifikationstechnik CONSENS derart angepasst, dass die mit ihr erstellte Beschreibung der Produktkonzeption als Basis für die Durchführung der ausgewählten Analysemethoden verwendet werden kann. Abschließend erfolgt in **Phase 4** die eigentliche Absicherung der Zuverlässigkeit bzw. Sicherheit des Produkts statt. Gemeint ist 1) die Spezifikation der Produktkonzeption unter besonderer Berücksichtigung von Zuverlässigkeits- und Sicherheitsinformationen mit Hilfe der erweiterten Spezifikationstechnik, 2) die Durchführung der Analysemethoden auf Basis der Spezifikation der Produktkonzeption sowie 3) die Festlegung und Integration von Verbesserungsmaßnahmen in die Spezifikation der Produktkonzeption. Eine hinsichtlich Zuverlässigkeit bzw. Sicherheit verbesserte Spezifikation der Produktkonzeption ist das Ergebnis dieser finalen Phase.

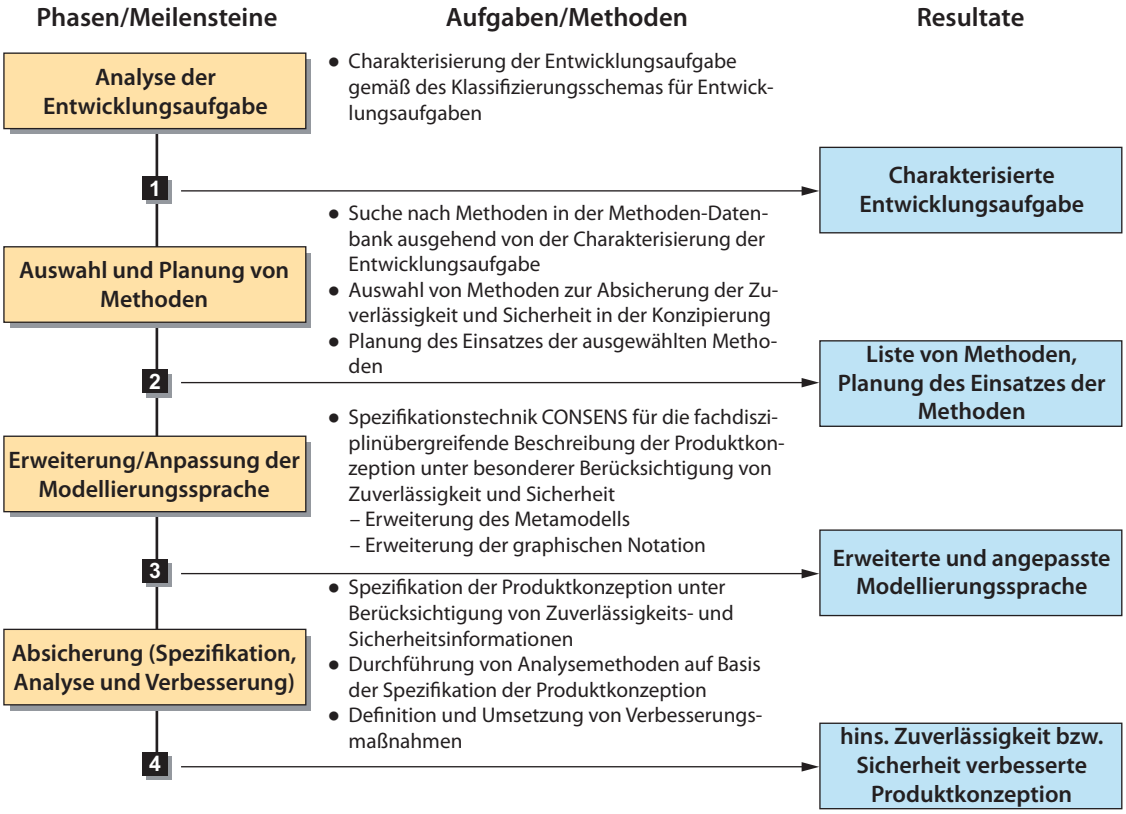


Bild 4-2: Vorgehensmodell zur Anwendung der Systematik

Die Durchführung der einzelnen Phasen wird durch Hilfsmittel unterstützt. Verwendet werden sowohl bestehende Hilfsmittel als auch neue, die im Rahmen dieser Arbeit neu entwickelt wurden. Bild 4-3 fasst die neu entwickelten Hilfsmittel zusammen.

In den nachfolgenden Abschnitten erfolgt eine detailliertere Darstellung der einzelnen Phasen des Vorgehensmodells. Beschrieben werden die durchzuführenden Tätigkeiten, die zugehörigen Hilfsmittel sowie die zu erarbeitenden Resultate.

4.2.1.1 Phase 1 – Analyse der Entwicklungsaufgabe

Die in dieser Arbeit adressierten technischen Systeme unterliegen besonderen Anforderungen und Randbedingungen in Bezug auf die Absicherung ihrer Zuverlässigkeit und Sicherheit. Ziel der ersten Phase der Entwicklungssystematik ist die Charakterisierung der Entwicklungsaufgabe hinsichtlich dieser Fragestellungen der Zuverlässigkeit und Sicherheit. Als Input dient dabei die Beschreibung der Entwicklungsaufgabe.

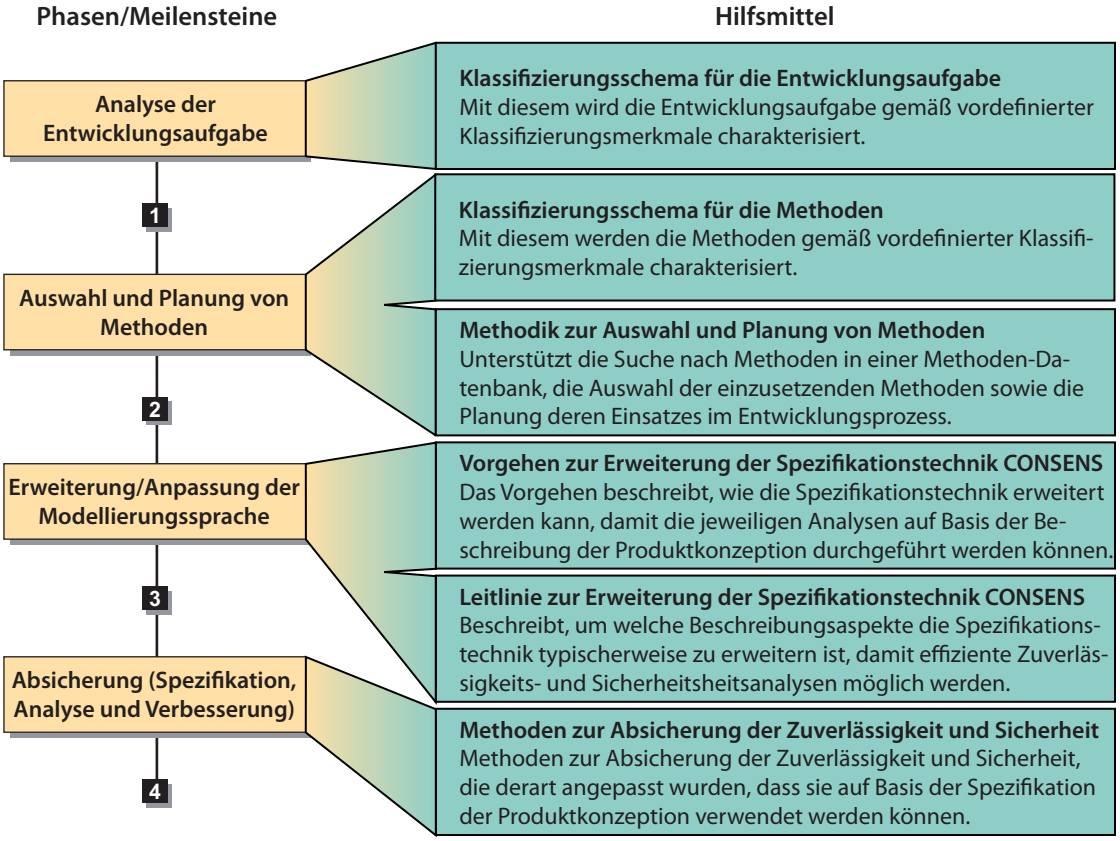


Bild 4-3: Einordnung der neu entwickelten Hilfsmittel in das Vorgehensmodell

Zur Charakterisierung der Entwicklungsaufgabe wird ein in dieser Arbeit entwickeltes *Klassifizierungsschema für die Entwicklungsaufgabe* verwendet. Dieses definiert Klassifizierungsmerkmale und deren mögliche Ausprägungen, die sich aus typischen Fragestellungen der Zuverlässigkeits- und Sicherheitstechnik ergeben. Aufgebaut wird dabei auf etablierten Normen, allem voran auf der DIN EN 60300-3-1 (vgl. Abschnitt 3.3.1). Zum Beispiel wird festgelegt, 1) für welche Branchen das Produkt entwickelt wird (z.B. Automobiltechnik, Bahntechnik etc.), 2) was der zu untersuchende Verlässlichkeitsaspekt ist (Zuverlässigkeit oder Sicherheit), 3) ob es sich um ein komplexes oder ein einfaches System handelt, 4) ob ein neuartiges Systementwurf vorliegt, 5) ob die Analyse von abhängigen Ereignissen von Relevanz ist etc.

Zusammenfassend wird in dieser Phase das folgende **Hilfsmittel** verwendet:

- Klassifizierungsschema für die Entwicklungsaufgabe (vgl. Abschnitt 4.3.1)

Das **Resultat** der ersten Phase ist die entlang des Klassifizierungsschemas *charakterisierte Entwicklungsaufgabe*. Diese Charakterisierung wird als Ausgangspunkt für die weiteren Phasen der Entwicklung im Hinblick auf die Fragestellungen der Zuverlässigkeit und Sicherheit verwendet. Sie dient insbesondere als Basis für die Suche nach geeigneten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit in Phase 2.

4.2.1.2 Phase 2 – Auswahl und Planung von Methoden

Hier erfolgt die Suche, Auswahl und Planung von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit ausgehend von der Charakterisierung der Entwicklungsaufgabe (Resultat der Phase 1). Unterstützt werden diese Tätigkeiten durch die im Rahmen der vorliegenden Arbeit entwickelte *Methodik zur Auswahl und Kombination von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme in der Konzipierung*. Diese Methodik basiert auf der Methodik zur Auswahl von Methoden des SFB 614 nach DOROCIAK ET AL. (vgl. Abschnitt 3.3.5) und erweitert diese; sie ist sehr stark auf die spezifischen Gegebenheiten der Konzipierung ausgerichtet [DGG+13]. Die Methodik umfasst eine Methoden-Datenbank, einen Leitfaden zur Auswahl und Planung von Methoden sowie eine prototypische Werkzeugunterstützung und wird in Abschnitt 4.3 genauer vorgestellt. Jede der in der Methoden-Datenbank abgelegten Methoden wird mit Hilfe des in dieser Arbeit entwickelten *Klassifizierungsschemas für Methoden zur Absicherung der Zuverlässigkeit und Sicherheit* charakterisiert. Zusätzlich werden für jede Methode die zugehörigen Eingangs- und Ausgangsinformationen (*Input-Output-Diagramme*), das zugrunde liegende Vorgehen (*Phasen-Meilenstein-Diagramm*) sowie die Einordnung der Methode in den *Referenzprozess für die Konzipierung* beschrieben. Für jede Methode wird ferner ein *Methoden-Steckbrief* bereitgestellt, welcher diese Informationen in graphischer Form zusammenfasst.

Die Methodik unterstützt den Entwickler darin, die für seine Entwicklungsaufgabe adäquaten Methoden effizient auszuwählen und deren Durchführungsreihenfolge zu planen. Konkret erhält der Entwickler die Informationen, was die wesentlichen Merkmale der jeweiligen Methode sind, wie das zugehörige Vorgehensmodell aussieht, wie die Methoden untereinander zusammenhängen, wie sie prinzipiell miteinander kombiniert werden können und wie eine optimale Durchführungsreihenfolge aussieht.

Zusammenfassend kommen in Phase 2 folgende **Hilfsmittel** zum Einsatz:

- Klassifizierungsschema für Methoden zur Absicherung der Zuverlässigkeit und Sicherheit (vgl. Abschnitt 4.3.2)
- Methodik zur Auswahl und Kombination von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme in der Konzipierung (vgl. Abschnitt 4.3.3)
- Referenzprozess für die Konzipierung selbstoptimierender mechatronischer Systeme des SFB 614 (vgl. Abschnitt 3.1.4)

- Phasen-Meilenstein-Diagramme der Methoden (vgl. Abschnitt 3.2)
- Input-Output-Diagramme der Methoden (vgl. Abschnitt 3.2)
- Methoden-Steckbriefe (vgl. Abschnitt 4.3.2)

Die **Ergebnisse** dieser Phase sind eine *Liste der ausgewählten Methoden* sowie *die Planung des kombinierten Einsatzes dieser Methoden in der Konzipierung*.

4.2.1.3 Phase 3 – Erweiterung/Anpassung der Modellierungssprache

Damit das Produkt hinsichtlich Zuverlässigkeit und Sicherheit in der Konzipierung analysiert und verbessert werden kann, bedarf es einer Beschreibung des grundsätzlichen Aufbaus, der Wirkungsweise und des gewünschten Verhaltens des Systems in einer fachdisziplinübergreifenden Weise. Zu diesem Zweck erfolgt eine fachdisziplinübergreifende Beschreibung der Produktkonzeption unter besonderer Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen und Beziehungen. Hierfür wird *die Spezifikationstechnik CONSENS* (vgl. Abschnitt 3.4.3) erweitert. Konkret erfolgt die Erweiterung des Metamodells und der graphischen Notation der Spezifikationstechnik.

Die Erweiterung der Spezifikationstechnik CONSENS erfolgt ausgehend von der in Phase 2 vorgenommenen Methodenauswahl. Für jede der ausgewählten Methoden wird festgelegt, welche Erweiterungen in Bezug auf das Metamodell und die graphische Notation zu integrieren sind. Verwendet wird hierzu ein im Rahmen der vorliegenden Arbeit entwickeltes *Vorgehensmodell zur Erweiterung der Spezifikationstechnik CONSENS*.

Die im Rahmen dieser Phase eingesetzten **Hilfsmittel** sind:

- die Spezifikationstechnik CONSENS (vgl. Abschnitt 3.4.3)
- das Vorgehensmodell zur Erweiterung der Spezifikationstechnik CONSENS (vgl. Abschnitt 4.4.1)
- die Leitlinie zur Erweiterung der Spezifikationstechnik CONSENS (vgl. Abschnitt 4.4.2)

Das **Resultat** dieser Phase ist die ausgehend von der Methodenauswahl *erweiterte und angepasste Modellierungssprache*. Mit dieser erfolgt in der darauffolgenden Phase 4 die fachdisziplinübergreifende Beschreibung der Produktkonzeption unter besonderer Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen. Die so beschriebene Produktkonzeption dient als Grundlage für die weiteren Analysen und Verbesserungen der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit, welche ebenfalls in Phase 4 stattfinden.

4.2.1.4 Phase 4 – Absicherung (Spezifikation, Analyse, Verbesserung)

Gegenstand der Phase 4 ist die Absicherung der Zuverlässigkeit und Sicherheit des betrachteten Produkts. Zunächst erfolgt hier die Spezifikation der Produktkonzeption unter besonderer Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen. Hierzu wird die *erweiterte Spezifikationstechnik CONSENS* herangezogen (Resultat der Phase 3). Auf Basis der so erstellten Spezifikation der Produktkonzeption findet anschließend die Analyse der Zuverlässigkeit und Sicherheit des zu entwickelnden Produkts statt. Verwendet werden hierzu die in Phase 2 ausgewählten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit. Im Rahmen der Durchführung der Analysemethoden auf Basis der Spezifikation der Produktkonzeption werden zum einen Schwachstellen in der Produktkonzeption im Hinblick auf Zuverlässigkeit bzw. Sicherheit aufgedeckt. Zum anderen erfolgt die Ableitung von Gegenmaßnahmen und deren Integration in die Spezifikation der Produktkonzeption (Verbesserung der Produktkonzeption). Ist eine Umsetzung in der Spezifikation der Produktkonzeption nicht unmittelbar möglich, werden die zu treffenden Maßnahmen für die Umsetzung in der darauffolgenden Entwicklungsphase Entwurf und Ausarbeitung schriftlich festgehalten, die zugehörigen Verantwortlichkeiten festgelegt und die Durchführung der Maßnahmen geplant.

Die Einbettung der Systematik in den Referenzprozess für die Konzipierung wird in Abschnitt 4.2.2 genauer erklärt. An dieser Stelle gilt es jedoch zu betonen, dass es sich bei Phase 4 nicht um eine einmalige Aufgabe handelt, die einem konkreten Schritt des Konzipierungsprozesses zugeordnet werden kann. Vielmehr handelt es sich um eine Abfolge von Aufgaben, welche sich über die gesamte Konzipierung von der Konzipierungsphase „Planen und Klären der Aufgabe“ bis zu der Konzipierungsphase „Konzeptintegration“ erstrecken. Dies liegt in der Natur der Spezifikation der Produktkonzeption, die mit der fortschreitenden Konzipierung zunehmend verfeinert wird.

Zusammenfassend kommen in Phase 4 folgende **Hilfsmittel** zum Einsatz:

- die in Phase 3 erweiterte Spezifikationstechnik CONSENS zur fachdisziplinübergreifenden Beschreibung der Produktkonzeption eines fortschrittlichen mechatronischen Systems (vgl. Abschnitt 3.4.3)
- angepasste Methoden zur Absicherung der Zuverlässigkeit und Sicherheit (vgl. Abschnitt 4.5 für Beispiele)

Das **Resultat** dieser Phase ist *eine hinsichtlich Zuverlässigkeit bzw. Sicherheit verbesserte Produktkonzeption*.

4.2.2 Einbettung in den Referenzprozess für die Konzipierung

Die *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* lässt sich nicht in Isolation vom übrigen Entwicklungsgeschehen anwenden. Vielmehr bettet sich diese in den in Abschnitt 3.1.4 vorgestellten Referenzprozess für die Konzipierung selbstoptimierender Systeme ein.

Bild 4-4 stellt den Konzipierungsprozess für fortschrittliche mechatronische Systeme und die Einbettung des Vorgehensmodells der Systematik in diesen dar. Die Phasen 1, 2 und 3 der Systematik werden im Rahmen der Konzipierungsphase „Planen und Klären der Aufgabe“ durch den Sicherheits- und Zuverlässigkeitsverantwortlichen in Zusammenarbeit mit dem Systemingenieur durchgeführt. [46] Hier erfolgen die Analyse der Entwicklungsaufgabe (Phase 1 der Systematik), die Auswahl und Planung von Methoden (Phase 2) sowie die Erweiterung der Spezifikationstechnik (Phase 3). Diese drei Phasen dienen als Vorbereitung für die Phase 4 der Absicherung, welche den gesamten Konzipierungsprozess begleitet. Abhängig von den Ergebnissen der Auswahl und Planung von Methoden ergeben sich verschiedene Varianten in Bezug auf die Einbettung der zu Phase 4 gehörenden Tätigkeiten in den Entwicklungsprozess (im Bild schematisch dargestellt als Varianten 1 und 2).

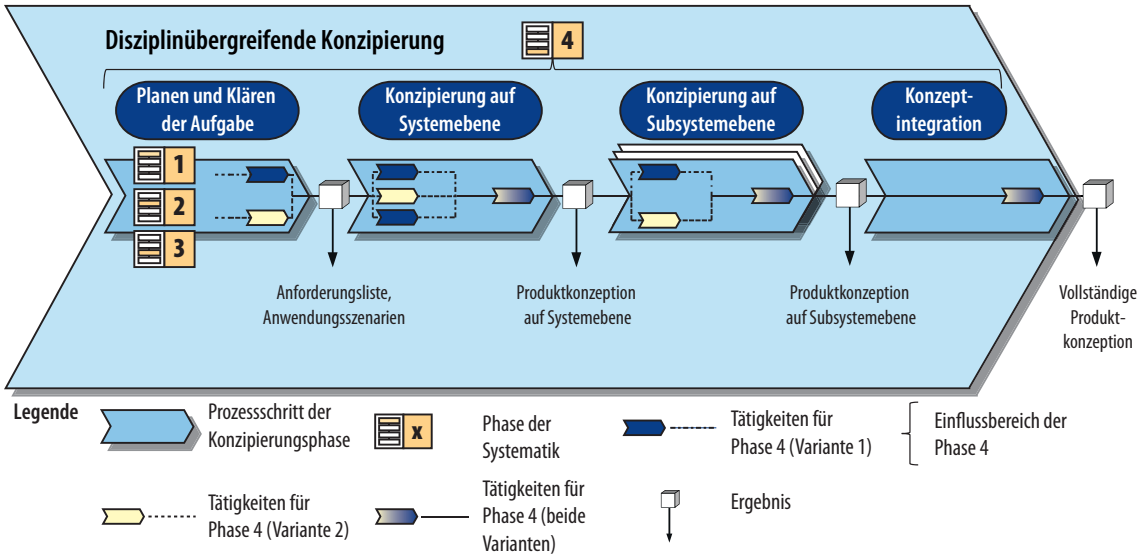


Bild 4-4: Einbettung der Systematik in die Entwicklungsphase Konzipierung

Das Ergebnis ist eine hinsichtlich Zuverlässigkeit bzw. Sicherheit verbesserte Spezifikation der Produktkonzeption. Diese dient als Ausgangspunkt für den weiteren disziplinspezifischen Entwurf und Ausarbeitung und Integration aller Entwicklungsergebnisse.

---

[46] Idealtypisch werden die Phasen 1, 2 und 3 der Systematik im Anschluss an den Prozessschritt „Aufgabenanalyse“ der Konzipierungsphase „Planen und Klären der Aufgabe“ durchgeführt (vgl. Abschnitt 3.1.4). Dennoch ist die Systematik derart ausgelegt, dass mit ihrer Anwendung auch zu späteren Zeitpunkten in der Konzipierung angefangen werden kann. Auch kann z.B. die Phase 2 (Methodenauswahl) im Zuge der fortschreitenden Konzipierung bedarfsgerecht mehrmals durchgeführt werden.

Die Ergebnisse der Zuverlässigkeits- bzw. Sicherheitsanalysen können ferner als Eingangsinformationen für die fachdisziplinspezifischen Methoden zur Absicherung der Zuverlässigkeit und Sicherheit in den weiteren Entwicklungsphasen dienen.

4.3 Rechnerunterstützte Auswahl und Planung von Methoden der Zuverlässigkeit und Sicherheit in der Konzipierung

Im Rahmen der vorliegenden Arbeit entstand *eine Methodik zur Auswahl und Planung von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit eines fortschrittlichen mechatronischen Systems in der Konzipierung*. Die wesentlichen Bestandteile der Methodik sind eine Methoden-Datenbank, ein Leitfaden zur Auswahl und Planung von Methoden sowie eine prototypische rechnertechnische Umsetzung.

Die Suche und Auswahl von Methoden erfolgt ausgehend von der Charakterisierung der Entwicklungsaufgabe mit Hilfe eines für diesen Zweck erarbeiteten Klassifizierungsschemas (Abschnitt 4.3.1). Damit die Suche und Auswahl von Methoden effizient erfolgen kann, ist eine eindeutige und vergleichbare Beschreibung der Methoden von zentraler Bedeutung (einige Methoden wurden in den Abschnitten 3.2 und 3.5 des Stands der Technik vorgestellt). Hierzu entstand ein Klassifizierungsschema für Methoden. Die Beschreibung der Methoden erfolgt in Form von Methoden-Steckbriefen. Beide Hilfsmittel werden in Abschnitt 4.3.2 detailliert vorgestellt. Darauf aufbauend erfolgt in Abschnitt 4.3.3 eine detaillierte Vorstellung der Methodik zur Auswahl und Planung von Methoden und deren Bestandteile.

4.3.1 Charakterisierung der Entwicklungsaufgabe

Zur Charakterisierung der Entwicklungsaufgabe hins. der Fragestellungen der Zuverlässigkeit und Sicherheit wurde im Rahmen der vorliegenden Arbeit ein Klassifizierungsschema für Entwicklungsaufgaben entwickelt. Es basiert auf dem Klassifizierungsschema nach DIN EN 60300-3-1 und umfasst folgende Klassifikationsmerkmale (Bild 4-5):

- **Klassifizierungsmerkmale im Hinblick auf allgemeine Eigenschaften der Entwicklungsaufgabe**
  - **Verlässlichkeitsaspekt:** Hier wird festgelegt, welcher Verlässlichkeitsaspekt für die zugrunde liegende Entwicklungsaufgabe im Vordergrund steht – Zuverlässigkeit oder Sicherheit. Hierbei ist auch eine Mehrfachauswahl möglich. Im Falle der Entwicklung eines sicherheitskritischen Systems steht typischerweise der Verlässlichkeitsaspekt Sicherheit im Mittelpunkt.
  - **Branche:** Hier wird festgelegt, welche Branchen für die zu betrachtende Entwicklungsaufgabe im Mittelpunkt stehen. Diese Information kann z.B. für die spätere Suche und Auswahl von Methoden von Relevanz sein. Einige der Metho-

den sind spezifisch für bestimmte Branchen bzw. werden in bestimmten Branchen aus unterschiedlichen Gründen besonders oft verwendet (z.B. aufgrund der geltenden Gesetze, Normen und Standards).

– **Normen, Standards, etc.:** Einige Normen, Gesetze und Standards fordern bzw. empfehlen den Einsatz von bestimmten Methoden, Vorgehensweisen etc. Darauf wurde bereits in Abschnitt 3.3.3 für die IEC 61508 und in Abschnitt 3.3.4 für die ISO 26262 eingegangen. Dieser Zusammenhang kann mit diesem Klassifizierungsmerkmal spezifiziert werden.

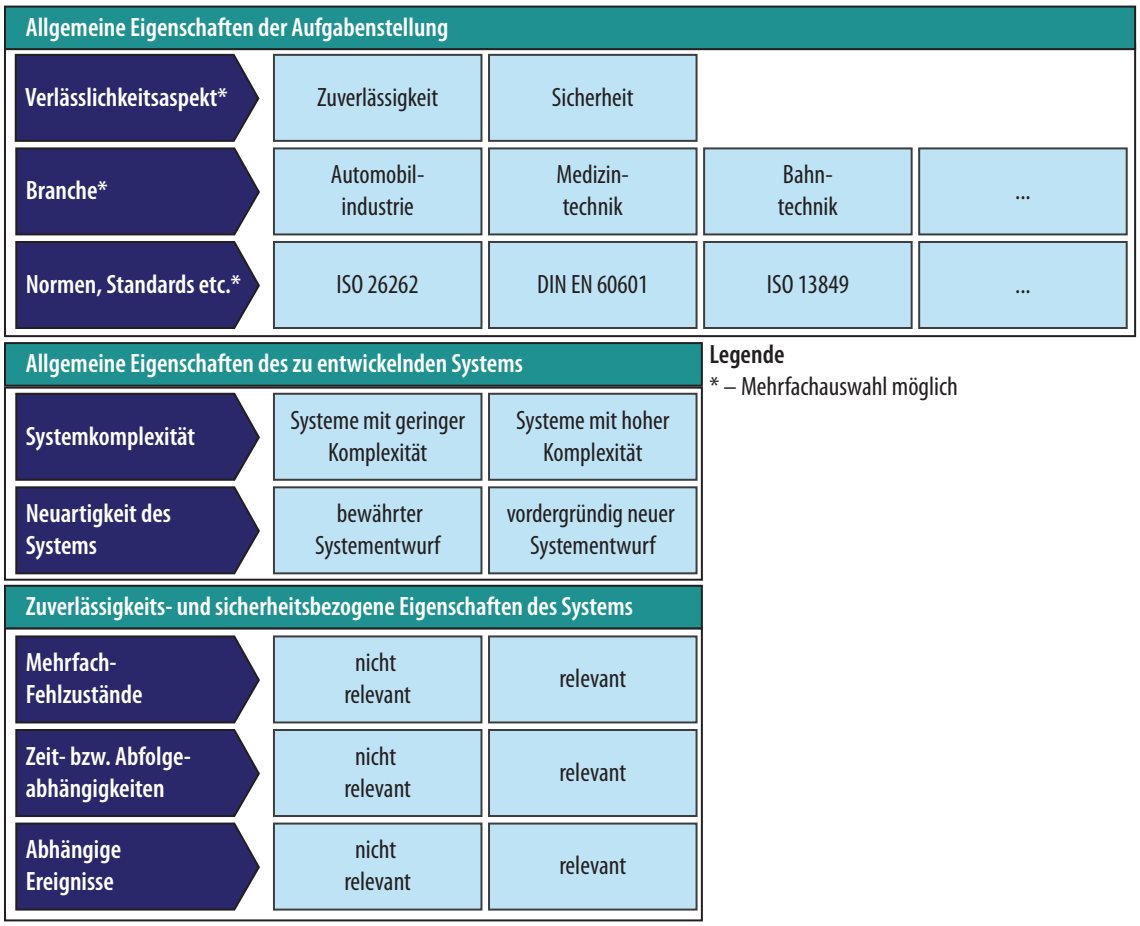


Bild 4-5: Klassifizierungsschema zur Charakterisierung der Entwicklungsaufgabe hinsichtlich der Fragestellungen der Zuverlässigkeit und Sicherheit

- **Klassifizierungsmerkmale im Hinblick auf allgemeine Eigenschaften des zu entwickelnden Systems**

  – **Systemkomplexität:** Hier wird festgelegt, ob es sich um ein komplexes oder ein einfaches System handelt. Komplexe Systeme, die durch Redundanz bzw. diversitäre Merkmale gekennzeichnet sind, erfordern typischerweise tiefergehende Analysen und unter Umständen andere Analysemethoden als einfache Systeme (z.B. ASIC-basierte Winkelsensoren ohne Mikrocontroller) [DIN60300-3-1, S. 12].

- **Neuartigkeit des Systems:** Mit diesem Klassifizierungsmerkmal wird der Grad der Neuartigkeit des Systems spezifiziert. Handelt es sich um einen zum größten Teil neuen Systementwurf, ist im Allgemeinen eine intensivere Analyse erforderlich als es bei bewährten Systementwürfen der Fall ist [DIN60300-3-1, S. 12].

- **Klassifizierungsmerkmale im Hinblick auf zuverlässigkeits- und sicherheitsbezogene Eigenschaften des zu entwickelnden Systems**
  - **Mehrfach-Fehlzustände:** Hier wird festgelegt, ob bezogen auf die zugrunde liegende Entwicklungsaufgabe Kombinationen von Fehlzuständen berücksichtigt werden müssen. Sind derartige Mehrfach-Fehlzustände von Relevanz, so sind spezielle Analysemethoden notwendig, welche diese ins Kalkül ziehen können.
  - **Zeit- bzw. Abfolgeabhängigkeiten:** Es gilt die Frage zu beantworten, ob das Aufeinanderfolgen von Ereignissen in der Absicherung des zu entwickelnden Produkts eine Rolle spielt. Ist dies der Fall, so sind z.B. spezielle Analysemethoden erforderlich, welche diese Zeit- und Abfolgeabhängigkeiten zwischen Ereignissen berücksichtigen können. Beispiele derartiger Methoden sind die dynamischen Fehlzustandsbäume (vgl. Abschnitt 3.2.2.4) und die dynamischen Bayesschen Netze (vgl. Abschnitt 3.2.2.9).
  - **Abhängige Ereignisse**: Hier wird festgelegt, ob der Zusammenhang der Ausfall- bzw. Reparaturmerkmale einer Einheit vom Zustand des Systems abhängt [DIN60300-3-1, S. 12]. Ist dies der Fall, dann müssen spezielle Methoden zum Einsatz kommen wie z.B. die Markoff-Analyse (vgl. Abschnitt 3.2.2.7).

4.3.2 Klassifizierungsschema für Methoden und Methoden-Steckbriefe

Zur eindeutigen und vergleichbaren Beschreibung der Methoden zur Absicherung der Zuverlässigkeit und Sicherheit entstand im Rahmen dieser Arbeit das in Bild 4-6 dargestellte Klassifizierungsschema für Methoden. Im Folgenden wird dieses detailliert erklärt. In diesem Zusammenhang werden Beispiele von Methoden erwähnt, wobei auf die in Abschnitt 3.2 vorgestellten Methoden zurückgegriffen wird.

Das Klassifizierungsschema umfasst vier Merkmalsgruppen, die nachfolgend vorgestellt werden. Die ersten drei dieser Merkmalsgruppen bauen im Wesentlichen auf den Klassifizierungsmerkmalen aus dem Klassifizierungsschema für die Entwicklungsaufgabe auf (vgl. Abschnitt 4.3). Als zusätzliches Klassifizierungsmerkmal kommt in der ersten Merkmalsgruppe die Konzipierungsphase hinzu. Die vierte Merkmalgruppe fokussiert die Eigenschaften der Methoden zur Absicherung der Zuverlässigkeit und Sicherheit:

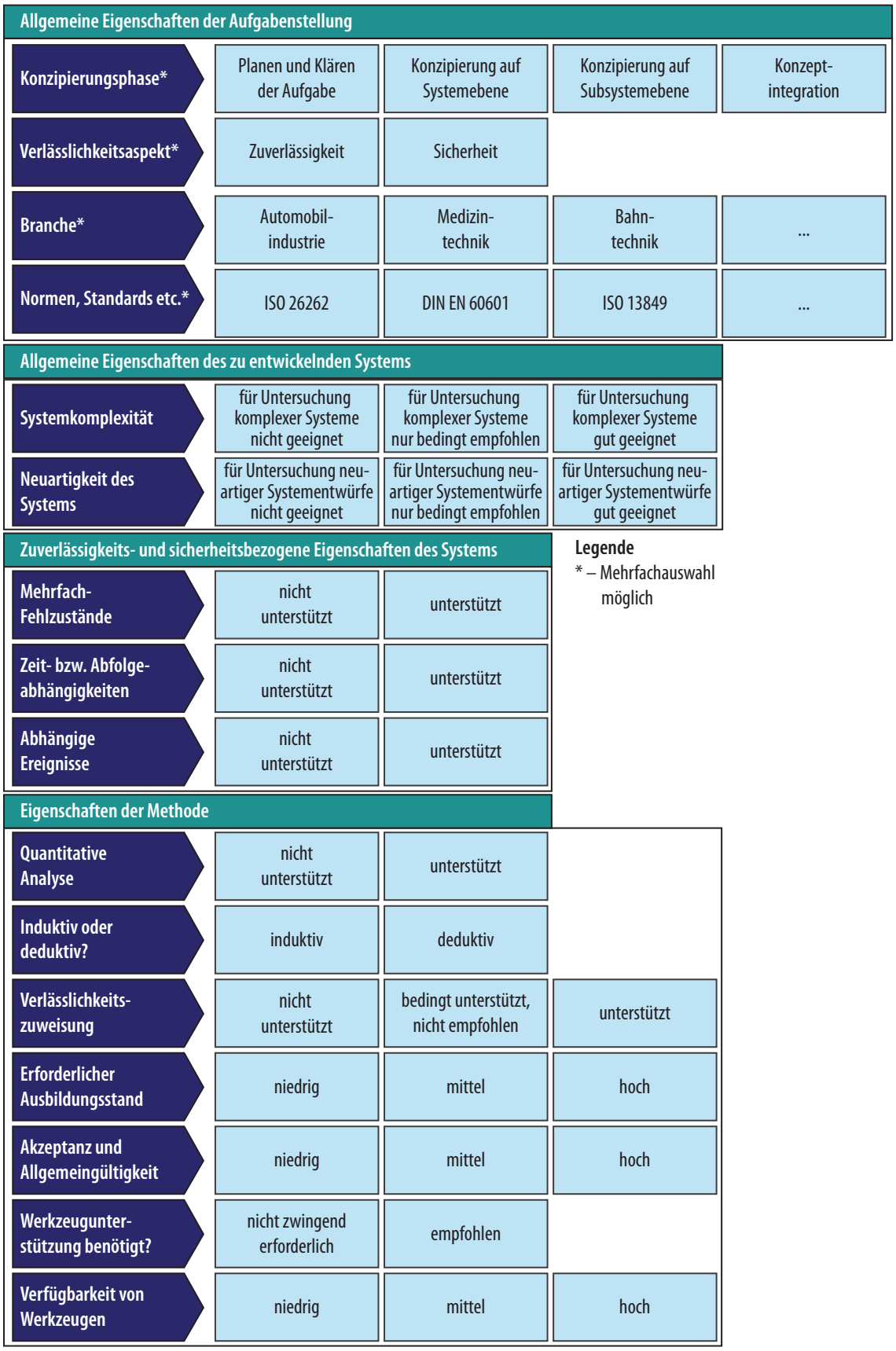


Bild 4-6: Klassifizierungsschema für Charakterisierung der Methoden zur Absicherung der Zuverlässigkeit und Sicherheit

- **Klassifizierungsmerkmale im Hinblick auf allgemeine Eigenschaften der Entwicklungsaufgabe**
  - **Konzipierungsphase:** Es gilt für jede Methode festzulegen, welche der vier Konzipierungsphasen durch diese Methode unterstützt werden. Zum Beispiel eignet sich die Methode SHA besonders für einen Einsatz in der Konzipierungsphase „Konzeptintegration“ (vgl. Abschnitt 3.2.1.4). Bei diesem Klassifizierungsmerkmal ist eine Mehrfachauswahl möglich.
  - **Verlässlichkeitsaspekt:** Hier wird festgelegt, welcher Verlässlichkeitsaspekt von der jeweiligen Methode unterstützt wird – Zuverlässigkeit oder Sicherheit. Wenn die jeweilige Methode für die Untersuchung beider Aspekte sehr gut geeignet ist, ist auch eine Mehrfachauswahl ist möglich.
  - **Branche:** Einige der Methoden sind spezifisch für bestimmte Branchen bzw. werden in bestimmten Branchen aus unterschiedlichen Gründen besonders oft verwendet (z.B. aufgrund der geltenden Gesetze, Normen und Standards). Dieser Zusammenhang kann mit diesem Klassifizierungsmerkmal spezifiziert werden.
  - **Normen, Standards, etc.:** Einige Normen, Gesetze und Standards fordern bzw. empfehlen den Einsatz von bestimmten Methoden, was bereits in Abschnitt 3.3.3 für die IEC 61508 und in Abschnitt 3.3.4 für die ISO 26262 erläutert wurde. Abgebildet wird ein solcher Zusammenhang mit diesem Klassifizierungsmerkmal.
- **Klassifizierungsmerkmale im Hinblick auf allgemeine Eigenschaften des zu entwickelnden Systems**
  - **Systemkomplexität:** Hier wird die Frage adressiert, ob die jeweilige Methode für Untersuchung komplexer Systeme (mit Redundanz etc.) geeignet ist. Eine FMEA (vgl. Abschnitt 3.2.2.5) wird zum Beispiel als eine alleinige Methode für Analyse komplexer Systeme nicht empfohlen [DIN60300-1, S. 13]. Der mit der Durchführung einer FMEA eines komplexen Produkts verbundene Aufwand kann beträchtlich sein [DIN60812, S. 8]. Die Methode kann insbesondere dann schwer beherrschbar werden, wenn die Beziehungen zwischen Ursache und Wirkung einer ungeradlinigen Natur sind [DIN60300-3-1, S. 30]. Ferner können mit einer FMEA komplexe zeitliche Abfolgen, Umgebungsbedingungen etc. nicht ohne Weiteres behandelt werden [DIN60300-3-1, S. 30].
  - **Neuartigkeit des Systems:** Festgelegt wird, ob die jeweilige Methode für die Untersuchung von Systementwürfen geeignet ist, die zum größten Teil neuartig sind. Eine induktive Analyse wie die FMEA bzw. die ETA (vgl. Abschnitt 3.2.2.6) ist für die Untersuchung neuartiger Systeme nicht zu empfehlen [DIN60300-3-1, S. 13]. Eine der wesentlichen Gründe: im Falle neuartiger Systementwürfe sind die Ausfallmöglichkeiten von vielen Systemelementen i.d.R. nicht sehr gut bekannt, da keine bzw. kaum Informationen aus vorherigen Pro-

jekten und Erfahrungen vorliegen. Für die Untersuchung eines neuartigen Systems eignen sich vielmehr deduktive Methoden wie die FTA (vgl. Abschnitt 3.2.2.3). Auch eine HAZOP-Analyse eignet sich hierfür aufgrund ihrer leitwortorientierten systematischen Vorgehensweise sehr gut (vgl. Abschnitt 3.2.2.2).

- **Klassifizierungsmerkmale im Hinblick auf zuverlässigkeits- und sicherheitsbezogene Eigenschaften des zu entwickelnden Systems**
  - **Mehrfach-Fehlzustände:** Beispiele von Analysen, die Mehrfach-Fehlzustände berücksichtigen, sind die FTA und die Markoff-Analyse (vgl. Abschnitt 3.2.2.7) [DIN60300-3-1, S. 13].
  - **Zeit- bzw. Abfolgeabhängigkeiten:** Gemeint sind Analysemethoden, welche die Zeit- und Abfolgeabhängigkeiten zwischen Ereignissen berücksichtigen [DIN60300-3-1, S. 13]. Beispiele sind die dynamischen Fehlzustandsbäume und die dynamischen Bayesschen Netze (vgl. Abschnitt 3.2.2.4 und 3.2.2.9).
  - **Abhängige Ereignisse**: Eine Analysemethode, mit welcher der Zusammenhang der Ausfall- bzw. Reparaturmerkmale einer Einheit vom Zustand des Systems abgebildet werden kann, ist z.B. die Markoff-Analyse [DIN60300-3-1, S. 13].
- **Klassifizierungsmerkmale im Hinblick auf die Eigenschaften der Methode**
  - **Quantitative Analyse:** Hier wird die Frage beantwortet, ob die jeweilige Methode eine quantitative Analyse unterstützt (vgl. Abschnitt 2.1.3 für die zugehörige Definition). FTA und ETA können für quantitative Untersuchungen eingesetzt werden, die Methode HAZOP ist rein qualitativ [DIN60300-3-1, S. 13].
  - **Induktiv oder deduktiv?:** Ist die jeweilige Methode induktiv oder deduktiv (vgl. Abschnitt 2.1.3 für die zugehörigen Definitionen)? Beispiele induktiver Methoden sind die ETA und die FMEA. Deduktiv ist z.B. die FTA.
  - **Verlässlichkeitszuweisung:** Hier wird festgelegt, ob die jeweilige Methode eine quantitative Aufteilung der Anforderungen an die Zuverlässigkeit bzw. Sicherheit unterstützt [DIN60300-3-1, S. 12]. Die Markoff-Analyse und die FTA eignen sich hierfür sehr gut. Die FMEA ist hierfür nicht zu empfehlen und die HAZOP bietet hierfür keine Unterstützung [DIN60300-3-1, S. 13].
  - **Erforderlicher Ausbildungsstand:** Welcher Ausbildungsstand ist für eine effiziente Anwendung der jeweiligen Methode erforderlich (niedrig, mittel oder hoch)? Die Markoff-Analyse erfordert z.B. einen hohen Ausbildungsstand des Anwenders und gilt als komplex und mathematisch aufwändig [VDI4003, S. 46].
  - **Akzeptanz und Allgemeingültigkeit:** Dieses Klassifizierungsmerkmal beschreibt, wie hoch die allgemeine Akzeptanz und Anerkennung durch die Behörden, Kunden etc. ist [DIN60300-3-1, S. 16]. Analysemethoden wie die FTA, die

FMEA und die ETA weisen eine hohe Akzeptanz auf, die Markoff-Analyse eine mittlere [DIN60300-3-1, S. 13].

- **Werkzeugunterstützung benötigt?:** Wird für die Anwendung der Methode eine Werkzeugunterstützung zwingend benötigt oder lassen sich die Ergebnisse auch ohne Weiteres von Hand nachprüfen [DIN60300-3-1, S. 12]? Für komplexere Analysen wie z.B. die Markoff-Analyse ist eine Rechnerunterstützung unabdingbar. Analysen wie HAZOP und FMEA können ohne dedizierte Werkzeugunterstützung, auch papierbasiert, durchgeführt werden.
- **Verfügbarkeit von Werkzeugen:** Hier wird beschrieben, inwiefern für die jeweilige Analysemethode eine Rechnerunterstützung zur Verfügung steht. Die meisten der etablierten Software-Werkzeuge unterstützen etablierte Analysen wie die FTA, die FMEA und die ETA (vgl. auch Abschnitt 3.6.1). Analysen wie die dynamischen Fehlzustandsbäume und Bayessche Netze werden aus derzeitiger Sicht nur von sehr wenigen Werkzeugen unterstützt.

Ferner werden für jede Methode deren **Eingangs- und Ausgangsinformationen** sowie **das zugehörige Vorgehen** beschrieben. Zur Beschreibung der Eingangs- und Ausgangsinformationen kommen die in Abschnitt 3.2 bereits verwendeten Input-Output-Diagramme zum Einsatz. Die zugehörigen Vorgehensmodelle werden in Form von Phasen-Meilenstein-Diagrammen abgebildet (vgl. auch Abschnitt 3.2). Außerdem können der Beschreibung der jeweiligen Methode **weiterführende Dokumente** hinterlegt werden – z.B. Leitfäden zur Verwendung der Methode, Vorlagen, Best Practices etc.

Darüber hinaus werden **Abhängigkeiten zwischen den Methoden** in der Methoden-Datenbank spezifiziert. In Anlehnung an DOROCIAK ET AL. können folgende methodenübergreifende Abhängigkeiten spezifiziert werden: “ist eine Voraussetzung für”, “ist erforderlich für”, “ist eine Weiterentwicklung von”, “wurde weiterentwickelt zu” sowie “lässt sich kombinieren mit” [DGG+13, S. 58]. Zum Beispiel ist die Frühzeitige FMEA nach GAUSEMEIER ET AL. eine Weiterentwicklung der FMEA; die Voraussetzung für die Anwendung der Frühzeitigen FMEA ist eine Beschreibung der Produktkonzeption mit der Spezifikationstechnik CONSENS (vgl. Abschnitt 3.5.3) [GKP09]. Ein weiteres Beispiel: die FMEA kann eine FTA unterstützen und umgekehrt [DIN60812, S. 31], [DG12].

Für jede der in der Methoden-Datenbank abgebildeten Methoden lässt sich ein Steckbrief generieren, welcher eine Beschreibung der jeweiligen Methode, ihrer Inputs und Outputs, der Ausprägungen der Klassifizierungsmerkmale etc. graphisch zusammenfasst. Ein Beispiel eines Methoden-Steckbriefs ist für die Methode FMEA in Bild 4-7 zu sehen.

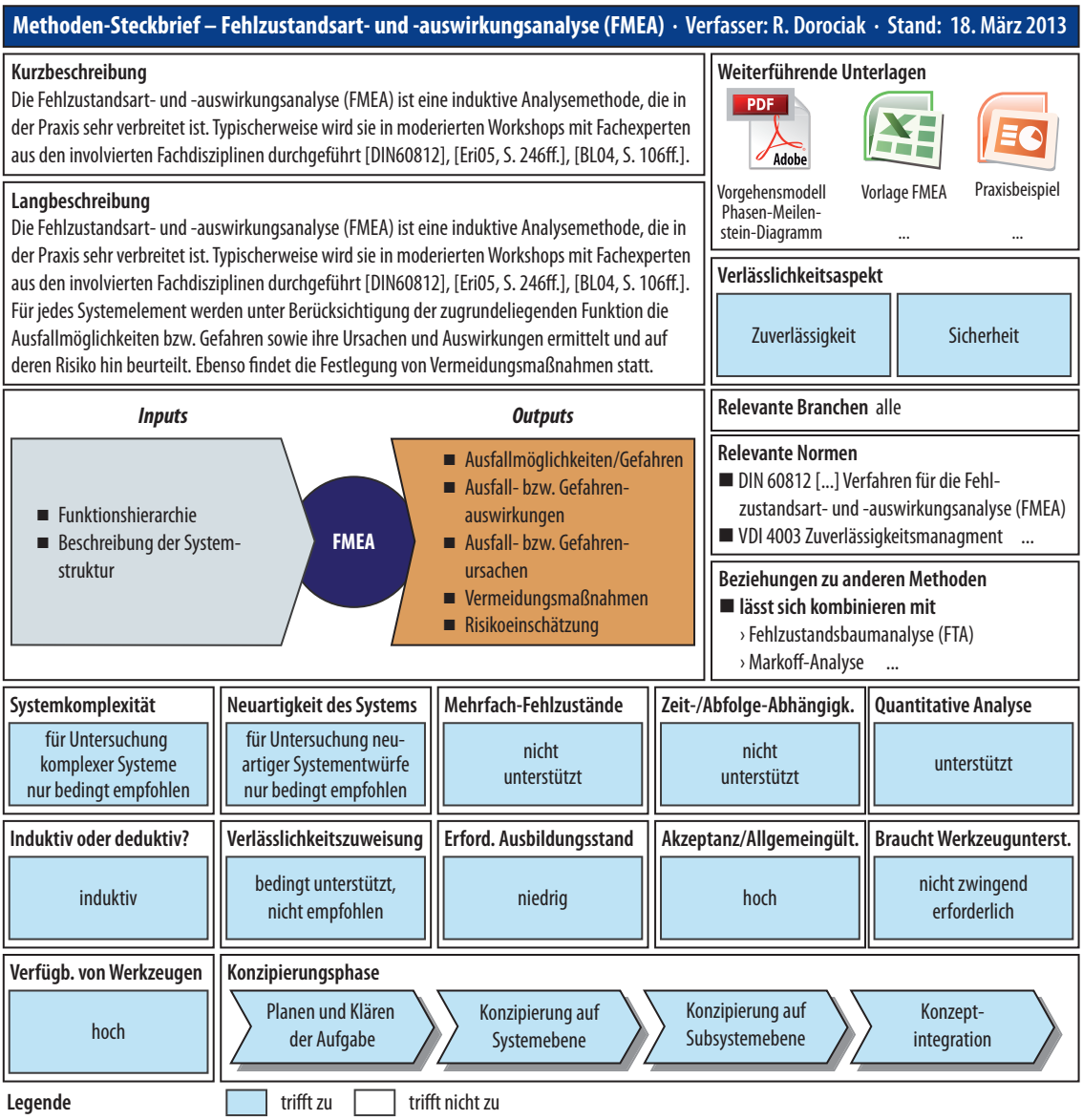


Bild 4-7: Methoden-Steckbrief für die FMEA

4.3.3 Methodik zur Auswahl und Planung von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit in der Konzipierung

Im Folgenden werden zunächst die Bestandteile *der Methodik zur Auswahl und Planung von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit eines fortschrittlichen mechatronischen Systems in der Konzipierung* vorgestellt. Anschließend wird das Arbeiten mit der Methodik erklärt. Die wesentlichen Bestandteile der Methodik sind:

- **eine Methoden-Datenbank:** Sie bildet eine Sammlung von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit und deren Beziehungen zueinander ab. Alle in den Abschnitten 3.2 und 3.5 vorgestellten Methoden sind darin auf die in Abschnitt 4.3.2 beschriebene Art abgebildet [GRS+14]. Die Eingabe der Methoden erfolgt manuell über eine werkzeugtechnisch umgesetzte Eingabemaske (Bild 4-8).

- **ein Leitfaden zur Auswahl und Planung von Methoden:** Dieser unterstützt zum einen die Suche und Auswahl von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit ausgehend von der zugrunde liegenden Entwicklungsaufgabe. Hierzu steht eine rechnertechnisch umgesetzte Suchmaske zur Verfügung; die Suchkriterien entsprechen den Klassifizierungsmerkmalen aus dem Klassifikationsschema für Methoden, das in Abschnitt 4.3.2 vorgestellt wurde. Zum anderen unterstützt der Leitfaden die Planung des (kombinierten) Einsatzes der Methoden.
- **eine prototypische Software-Unterstützung:** Bereitgestellt werden Benutzungsschnittstellen zur Eingabe und Verwaltung von Methoden, zur Suche nach adäquaten Methoden, zur Planung des Einsatzes der Methoden in der Konzipierung etc.

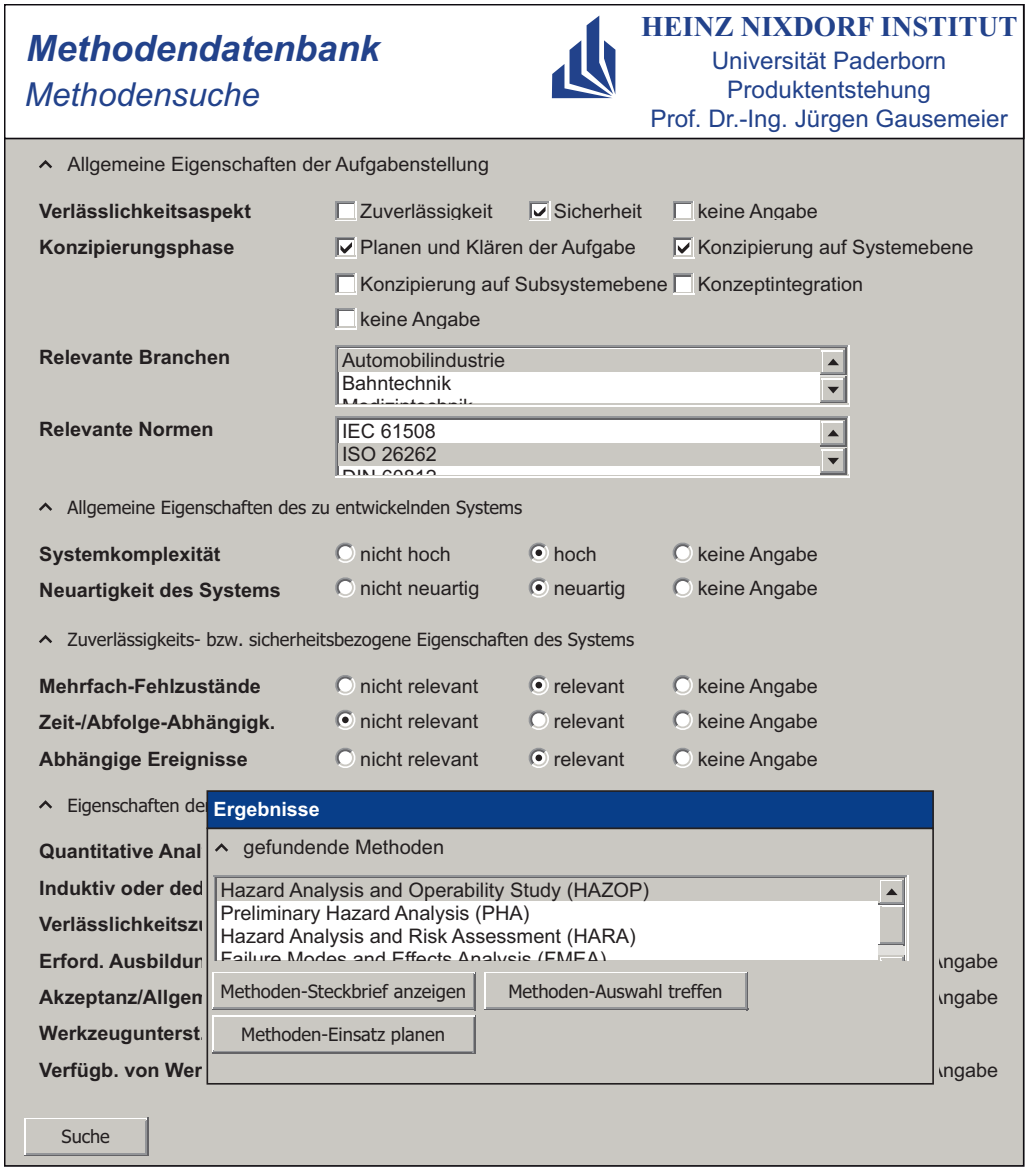


Bild 4-8: Graphische Benutzungsoberfläche der werkzeugtechnischen Umsetzung der Methodik; dargestellt ist die Suchmaske zur Suche nach Methoden

Bild 4-9 visualisiert die Verwendung der Methodik:

- **Schritt (1):** Mit Hilfe der Methodendatenbank wird nach adäquaten Methoden gesucht. Die zur Verfügung stehenden Suchkriterien beruhen auf dem Klassifizierungsschema für Methoden. Als Ergebnis erhält der Entwickler eine Liste von Methoden, die ihn im Rahmen seiner Entwicklungstätigkeit unterstützen können.
- **Schritt (2):** Für jede der gefundenen Methoden kann der Entwickler den zugehörigen Methoden-Steckbrief abrufen. Auf diese Weise erhält er zusätzliche Informationen über die Methode und ihren Einsatz, die ihn bei der endgültigen Auswahl der einzusetzenden Methoden unterstützen (z.B. notwendige Eingangsinformationen, Zusammenhang zu anderen Methoden, Vorgehensmodell, Vorlagen, Beispiele für den erfolgreichen Einsatz etc.). Der Entwickler kann außerdem zu dem Prozessschritt navigieren, in dem die Methode eingesetzt wird. Ebenfalls können Methodenbeschreibungen aus dem Prozess heraus aufgerufen werden [GGD11].
- **Schritt (3):** Der Entwickler legt fest, welche der vorgeschlagenen Methoden verwendet werden sollen. Für die ausgewählten Methoden werden eine Durchführungsreihenfolge sowie die zugehörige Einbettung in den Referenzprozess für die Konzipierung vorgeschlagen. Diese Planung beruht auf den in der Methoden-Datenbank abgebildeten Informationen bzgl. der Input-Output-Zusammenhänge der Methoden und der Zuordnung von Methoden zu den Phasen des Konzipierungsprozesses.

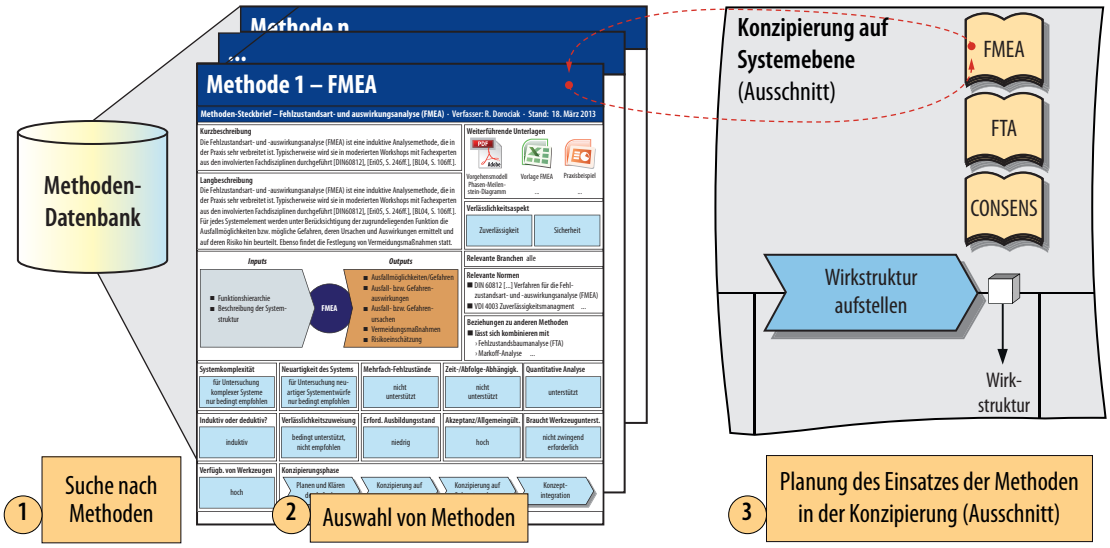


Bild 4-9: Suche und Auswahl von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit in der Konzipierung – Anwendung der Methodik

4.4 Spezifikation des Produkts unter Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen

Damit das Produkt hinsichtlich Zuverlässigkeit und Sicherheit in der Konzipierung analysiert und verbessert werden kann, bedarf es einer Beschreibung des grundsätzlichen

Aufbaus, der Wirkungsweise und des gewünschten Verhaltens des Systems in einer fachdisziplinübergreifenden Weise. Zu diesem Zweck erfolgt eine fachdisziplinübergreifende Beschreibung der Produktkonzeption unter besonderer Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen. Hierzu wird die in Abschnitt 3.4.3 vorgestellte Spezifikationstechnik CONSENS erweitert. Konkret erfolgt die Erweiterung des Metamodells der Spezifikationstechnik und damit einhergehend der zugehörigen graphischen Notation (vgl. Abschnitt 2.1.4).

Diese Erweiterung kann grundsätzlich bei jeder Anwendung der Systematik erfolgen. Es ist aber auch möglich, die Erweiterung unter Verwendung der Systematik einmal für eine Klasse von Produkten zu definieren, wenn die Produkte dieser Klasse hinsichtlich ihrer Eigenschaften eine hohe Ähnlichkeit aufweisen und für sie dieselbe Methodenauswahl verwendet werden kann.

4.4.1 Vorgehen zur Erweiterung der Spezifikationstechnik CONSENS ausgehend von den ausgewählten Methoden

Im Rahmen dieser Arbeit wurde ein *Vorgehen zur Erweiterung der Spezifikationstechnik CONSENS ausgehend von den ausgewählten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit* erarbeitet. Ausgangspunkt bilden die in Phase 2 der Systematik festgelegten, einzusetzenden Methoden zur Absicherung der Zuverlässigkeit und Sicherheit. Ziel ist eine erweiterte Spezifikationstechnik CONSENS, welche eine Beschreibung der Produktkonzeption ermöglicht, die alle für die Durchführung der ausgewählten Methoden relevanten Informationen beinhaltet. Bild 4-10 stellt das Vorgehen graphisch dar:

Phase 1 – Analyse der Methode: Ziel ist die Festlegung der für die Verwendung der jeweiligen Methode notwendigen Erweiterungen des Metamodells der Spezifikationstechnik CONSENS. Hierfür gilt es folgende Punkte zu definieren:

- welche **Modellelemente** für die Modellierung und Analyse der Zuverlässigkeit und Sicherheit mit der jeweiligen Methode zur Verfügung stehen müssen (z.B. müssen für die Durchführung einer FTA auf Basis der Spezifikation der Produktkonzeption die Modellelemente Ausfall, Ausfallauswirkung, Ausfallursache sowie Boolesche Gatter etc. abgebildet werden können),
- welche **Attribute** die Modellelemente haben können (z.B. Schwere einer Ausfallauswirkung, Entdeckungswahrscheinlichkeit einer Ausfallursache),
- wie die Modellelemente prinzipiell untereinander verknüpft werden können (**abstrakte Syntax**) und
- wie gestaltet sich die richtige Verwendung von syntaktisch korrekten Modellen (**Statische Semantik**; sie wird i.d.R. durch Einschränkungen (Constraints) definiert).

In Phase 1 wird ferner untersucht, welche Modellelemente und Beziehungen in welchen der Beschreibungsaspekte der mit CONSENS modellierten Produktkonzeption wie abgebildet werden können. Ist eine derartige Zuordnung nicht möglich, so wird untersucht, welche weiteren Aspekte die disziplinübergreifende Beschreibung des Produkts beinhalten muss, damit sich die jeweilige Methode auf Basis der Beschreibung der Produktkonzeption durchführen lässt. Das Ergebnis ist die Definition der notwendigen Erweiterungen des Metamodells. Diese umfasst die Zuordnung der zu integrierenden Metamodellelementen (Modellelemente und Beziehungen) zu den Beschreibungsaspekten der Spezifikationstechnik CONSENS.

Phase 2 – Definition der graphischen Darstellung: Im Wechselspiel mit der Definition der Erweiterungen des Metamodells (Phase 1) werden hier die notwendigen Erweiterungen der graphischen Notation der Spezifikationstechnik festgelegt. Für die neu hinzunehmenden Modellelemente und Beziehungen des CONSENS-Metamodells wird festgelegt, in welcher Form diese graphisch darzustellen sind (konkrete Syntax). Insbesondere erfolgt eine Auswahl von graphischen Symbolen, die für die Erstellung der Diagramme verwendet werden, sowie die Festlegung von deren Form und Farbe. Zum Beispiel werden unterschiedliche Arten von Ausfällen (interner Ausfall eines Systemelements, fortgepflanzter Ausfall) graphisch unterschiedlich dargestellt.

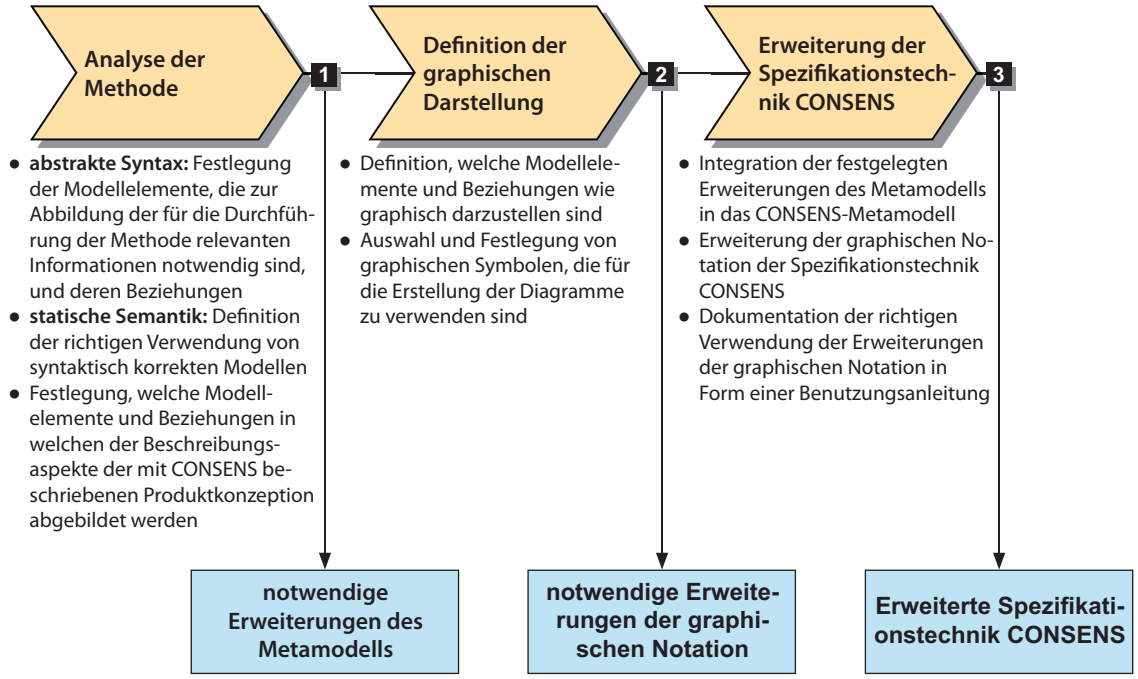


Bild 4-10: Vorgehen zur Erweiterung der Spezifikationstechnik CONSENS ausgehend von der Methodenauswahl (Iterationen nicht dargestellt)

Phase 3 – Erweiterung der Spezifikationstechnik: Aufbauend auf den Ergebnissen der Phasen 1 und 2 werden das Metamodell und die graphische Notation der Spezifikationstechnik erweitert. Ferner wird die Benutzungsdokumentation der Spezifikationstechnik

CONSENS angepasst. Dies betrifft insbesondere die Beschreibung der Bedeutung und der korrekten Verwendung der neu hinzugekommenen graphischen Elemente.

Mit der erweiterten Spezifikationstechnik CONSENS erfolgt die fachdisziplinübergreifende Beschreibung der Produktkonzeption unter besonderer Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen und Beziehungen. Diese Beschreibung dient als Grundlage für die weiteren Analysen und Verbesserungen der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit.

Die Anwendung des Vorgehens zur Erweiterung der Spezifikationstechnik CONSENS wird in Abschnitt 4.4.3 am Beispiel der Integration der Methoden FMEA und FTA detaillierter erklärt.

4.4.2 Leitlinie zur Erweiterung der Spezifikationstechnik CONSENS

Im Rahmen der vorliegenden Arbeit wurde eine Leitlinie zur Erweiterung der Spezifikationstechnik CONSENS erarbeitet. Diese beschreibt, um welche Beschreibungsaspekte die Spezifikationstechnik typischerweise zu erweitern ist, damit Zuverlässigkeits- und Sicherheitsheitsanalysen auf Basis der Spezifikation der Produktkonzeption effizient unterstützt werden. Die Leitlinie ist als eine Orientierungshilfe (Best Practice) zu verstehen. Sie wurde auf Basis der im Rahmen der Problemanalyse und der Analyse des Stands der Technik gewonnenen Erkenntnisse erarbeitet. Die Kernelemente der Leitlinie sind (Bild 4-11):

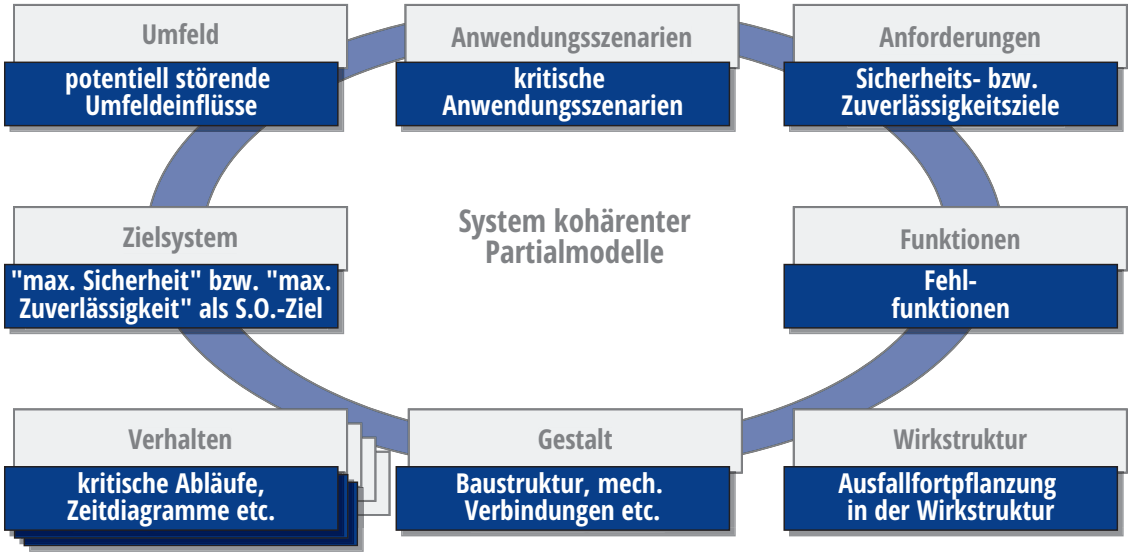


Bild 4-11: Zusätzliche Beschreibungsaspekte zur Unterstützung von Zuverlässigkeits- und Sicherheitsanalysen auf Basis der Spezifikation der Produktkonzeption (idealtypische Darstellung)

- **Potentiell störende Umfeldeinflüsse:** Innerhalb der Beschreibung des Aspekts Umfeld können potentiell störende Umfeldeinflüsse als solche gekennzeichnet werden.

Beispiele sind Temperatur, Feuchtigkeit, Umgebungsreflexionen. Diese potentiell störenden Umfeldeinflüsse können zu Ausfällen bzw. Störungen innerhalb des Systems führen und werden i.d.R. im Rahmen der Spezifikation der Ausfallfortfplanzung in der Wirkstruktur (siehe unten) weiter spezifiziert. Z.B. können Reflexionen von Umfeldobjekten bei radarbasierten Fahrerassistenzsystemen zu sogenannten Geisterobjekten führen. In diesem Fall werden Fahrzeugobjekte durch die Informationsverarbeitung ins Kalkül gezogen, die in der reellen Welt gar nicht existieren; ungewollte Brems- bzw. Lenkeingriffe können die Folge sein und zu einem Unfall führen.

- **Kritische Anwendungsszenarien:** Anwendungsszenarien, die hinsichtlich Sicherheit bzw. Zuverlässigkeit kritisch sein können, werden hervorgehoben und mit zusätzlichen Informationen versehen. Zum Beispiel ist bezogen auf die Lenkfunktion eines Kraftfahrzeugs das Anwendungsszenario „schnelle Fahrt auf der Autobahn“ in Kombination mit einer möglichen Fehlfunktion „Unmotivierte Lenkbewegung ohne Fahrerwunsch“ als sehr kritisch anzusehen und in einer Gefahrenanalyse weiter zu betrachten (vgl. Abschnitt 3.2.2.1).

- **Sicherheits- bzw. Zuverlässigkeitsziele:** Sicherheits- bzw. Zuverlässigkeitsziele sind Sicherheits- bzw. Zuverlässigkeitsanforderungen der obersten Gliederungsebene. Sicherheitsziele werden z.B. mit einer Gefahrenanalyse ermittelt (Beispiel: Verhinderung der Lenkradverriegelung während der Fahrt, vgl. Abschnitt 3.2.2.1). Sie werden dann durch Sicherheitsanforderungen verfeinert und dienen, wie in Abschnitt 2.1.5.3 beschrieben, als Basis für das Aufstellen eines Sicherheitskonzepts.

- **Fehlfunktionen:** Auf Basis der Funktionshierarchie können Fehlfunktionen ermittelt werden. Dies erfolgt im einfachsten Fall durch die Negation der Funktion. Weitere Fehlfunktionen können z.B. unter Verwendung von Methoden wie die HAZOP identifiziert werden (vgl. Abschnitt 3.2.2.2).

- **Ausfallfortpflanzung in der Wirkstruktur:** Gemeint ist die Beschreibung der möglichen internen Fehler der Systemelemente sowie der systemelementübergreifenden Ausfallfortpflanzung innerhalb der Wirkstruktur. Das Thema wird in Abschnitt 4.4.3 genauer vorgestellt.

- **Baustruktur, mechanische Verbindungen etc.:** Hier werden die physischen Bestandteile des Produkts (Bauteile), deren Aggregation (Baugruppen) sowie die mechanischen Verbindungen zwischen diesen beschrieben. Bauteile wie ein Zahnrad können aufgrund mehrerer Ursachen ausfallen (z.B. Zahnbruch, Grübchen etc.) [BL04, S. 96]. Diese Informationen können zur Berechnung des Ausfallverhaltens und Definition von Gegenmaßnahmen für die Mechanik verwendet werden. Dieser Punkt wird in der vorliegenden Arbeit nicht weiter behandelt. Für weiterführende Informationen hierzu sei auf [BL04, S. 92ff.] verwiesen.

- **Kritische Abläufe, Zeitdiagramme etc.:** Gemeint ist die Beschreibung von kritischen Abläufen, Zuständen und Sequenzen. Daher handelt es sich hier um eine

Gruppe von Aspekten. In diesem Zusammenhang ist insbesondere die Darstellung von kritischen zeitlichen Abläufen von Relevanz. Derartige Betrachtungen unterstützen das Sicherstellen der Einhaltung von Fehlertoleranzzeiten, Notbetriebszeiten, die Bestimmung von notwendigen Fehlerreaktionszeiten etc. [ISO26262]. Dieses Thema wird in dieser Arbeit nicht weiter betrachtet.

- **„max. Sicherheit“ bzw. „max. Zuverlässigkeit“ als S.O.-Ziel:** Dieser Punkt ist für s.o. Systeme von Relevanz. Um Zuverlässigkeit und Sicherheit bei der Entwicklung s.o. Systeme von vornherein zu berücksichtigen, empfiehlt es sich, die Punkte „max. Sicherheit“ bzw. „max. Zuverlässigkeit“ als Selbstoptimierungs-Ziele im Zielsystem aufzufassen. Dies ermöglicht die Untersuchung des Zusammenhangs der beiden Ziele zu den übrigen Selbstoptimierungs-Zielen und insbesondere die Berücksichtigung von potentiellen Zielkonflikten. Dieses Thema wird in dieser Arbeit nicht weiter behandelt. Für weitere Informationen zum Thema sei auf [PGD12] verwiesen.

Die Leitlinie wurde bei der Validierung der Systematik am Anwendungsbeispiel Chamäleon angewendet. Diese Validierung wird detailliert in Kapitel 5 vorgestellt.

4.4.3 Erweiterung der Spezifikationstechnik CONSENS am Beispiel der Integration der Methoden FTA und FMEA

Im Folgenden wird das in Abschnitt 4.4.1 vorgestellte Vorgehen zur Erweiterung der Spezifikationstechnik CONSENS am Beispiel der Integration der Fehlzustandsbaumanalyse FTA erklärt:

Phase 1 – Analyse der Methode: Im Zuge der Festlegung der notwendigen Erweiterungen für das Metamodell der Spezifikationstechnik CONSENS erfolgt die Definition der abstrakten Syntax und der statischen Semantik eines Fehlzustandsbaums.

Abstrakte Syntax: Bild 4-12 zeigt die Definition der abstrakten Syntax der Beschreibung eines Fehlzustandsbaums. Sie beschreibt, aus welchen Modellelementen und Beziehungen die Beschreibung eines Fehlzustandsbaums besteht. Das Modellelement „FTA-Modell“ repräsentiert das Gesamtmodell des Fehlzustandsbaums. Die wesentlichen Modellelemente sind hier die Gatter sowie die Ereignisse. Dabei wird zwischen einfachen und zusammengesetzten Ereignissen unterschieden. Einfache Ereignisse werden im Fehlzustandsbaum nicht weiter verfeinert. Zusammengesetzte Ereignisse lassen sich auf weitere Ereignisse zurückführen (vgl. auch Abschnitt 3.2.2.3). Sowohl einfache als auch zusammengesetzte Ereignisse stellen eine Spezialisierung des Modellelements „Ausfall“ dar; sie können mit einer Auftretenswahrscheinlichkeit (quantitativ) versehen werden.

In einer klassischen graphischen Darstellung eines Fehlzustandsbaums werden die Ursache-Wirkungs-Ketten durch Kanten und Gatter zwischen Ereignissen repräsentiert. Gemäß der Definition der abstrakten Syntax dürfen Gatter jeweils zwei Eingänge und einen Ausgang besitzen.

Statische Semantik: Die statische Semantik der Beschreibung eines Fehlzustandsbaums wird in Form von Einschränkungen definiert. Im Falle des Fehlzustandsbaums besteht eine wesentliche Einschränkung darin, dass Zyklen nicht erlaubt sind. Insbesondere darf ein Ereignis in einem Fehlzustandsbaum nicht unmittelbar mit einem anderen Ereignis verbunden werden; als Verbindungsglied muss stets ein Gatter verwendet werden. Eine weitere Einschränkung besteht darin, dass die beiden Eingänge eines Gatters nicht durch ein und das gleiche Ereignis belegt werden dürfen.

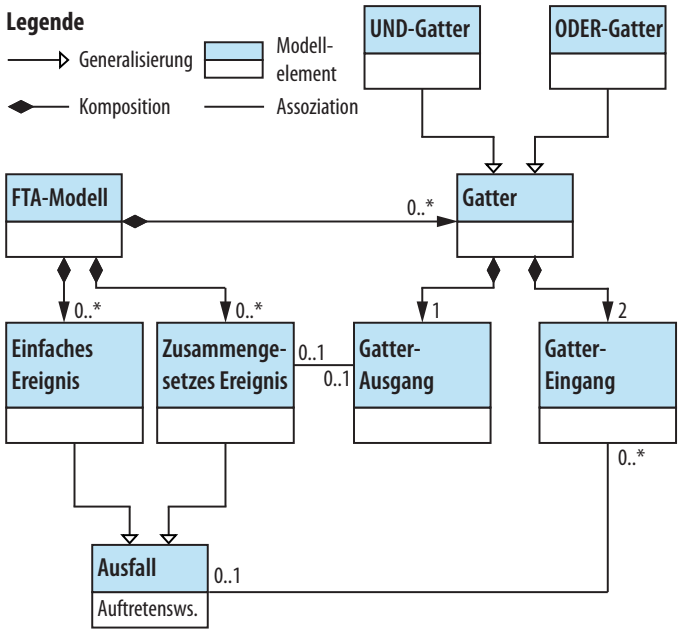


Bild 4-12: Metamodell der Beschreibung eines Fehlzustandsbaums (Ausschnitt; Fokus: abstrakte Syntax); vereinfachte Darstellung: insbesondere sind die Attribute der Modellelemente nicht dargestellt

Festlegung der zu erweiternden Beschreibungsaspekte: Anschließend wird festgelegt, in welchen Beschreibungsaspekten einer mit CONSENS modellierten Produktkonzeption die für die Durchführung einer FTA notwendigen Informationen und Beziehungen abzubilden sind. Da sich die Ausfälle auf Systemelemente beziehen, ist in diesem Fall der Beschreibungsaspekt Wirkstruktur von zentraler Bedeutung. Die Spezifikationstechnik CONSENS ist derart zu erweitern, dass in der Wirkstruktur die potentiellen Ausfälle (z.B. Verschleiß, Kurzschluss, Überspannung) der Systemelemente sowie deren Fortpflanzung und die damit einhergehende Auswirkung auf weitere Systemelemente modellierbar sind. Insbesondere soll es möglich sein, auf Basis der Beschreibung der Ausfallfortpflanzung in der Wirkstruktur Fehlzustandsbäume automatisch zu generieren.

Phase 2 – Definition der graphischen Darstellung: Basierend auf den in Phase 1 erarbeiteten Festlegungen bzgl. der Abbildung von internen Ausfällen und Ausfallfortpflanzung wird in Phase 2 des Vorgehens die graphische Notation der angestrebten Erweiterung definiert. Bild 4-13 stellt eine skizzenhafte Darstellung der erarbeiteten Ideen dar. Dargestellt wird die angestrebte Erweiterung der Wirkstruktur um zusätzliche Informationen (links) sowie der äquivalente Fehlzustandsbaum (rechts). Tabelle 4-1 fasst die festgelegten Symbole der graphischen Notation für die wesentlichen Elemente der abstrakten Syntax (Gatter, interner Ausfall, Ursache-Wirkungs-Beziehung) zusammen.

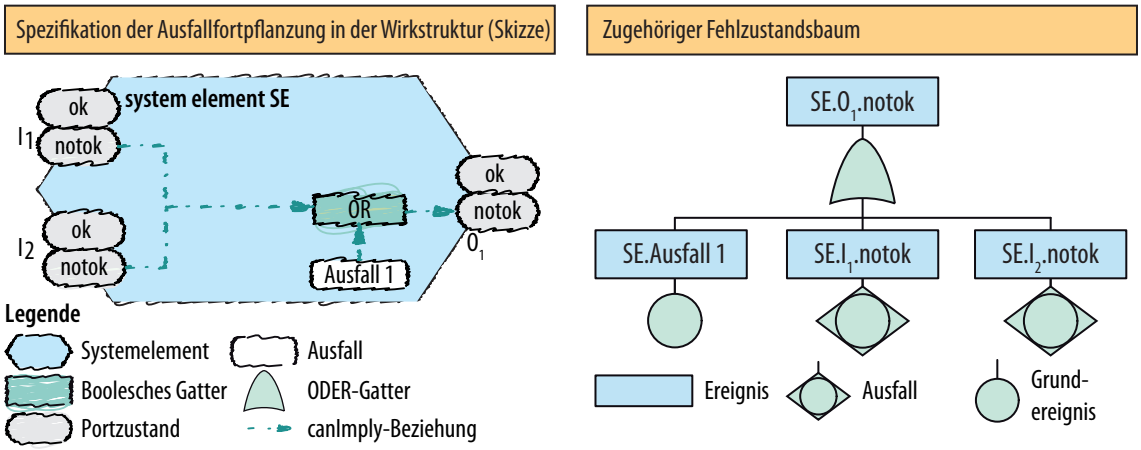


Bild 4-13: Skizzenhafte Darstellung der Überlegungen bzgl. der Erweiterungen der graphischen Notation (in Anlehnung an [DGK+09])

Phase 3 – Erweiterung der Spezifikationstechnik: Nach der Festlegung der für die Integration der FTA notwendigen Erweiterungen des Metamodells und der graphischen Notation erfolgt in Phase 3 die Erweiterung der Spezifikationstechnik CONSENS. Bild 4-14 zeigt einen Ausschnitt des Metamodells der Spezifikationstechnik CONSENS (vgl. Abschnitt 3.4.3), welches es zu erweitern gilt. Dargestellt werden die relevanten Modellelemente und Beziehungen des Aspekts Wirkstruktur, da dieser für die Integration der Methode FTA von Relevanz ist.

Tabelle 4-1: Elemente der graphischen Notation für die Spezifikation der Ausfallfortpflanzung in der Wirkstruktur

Modellelement	Graphische Notation	Beschreibung
Boolesches Gatter		Stellt einen Booleschen Operator dar (z.B. UND, ODER).
Interner Ausfall		Stellt einen potentiellen Ausfall eines Systemelements dar mit seinem Ursprung in diesem Systemelement.
Eingehender bzw. ausgehender Ausfall		Stellt Ausfälle dar, die nach außen propagiert werden bzw. diejenigen, die ihren Ursprung außerhalb des Systemelements haben, dieses jedoch beeinflussen.
Ursache-Wirkungs-Beziehung		Stellt die Ursache-Wirkungs-Beziehung zwischen Ausfällen (internen sowie eingehenden und ausgehenden) dar.

Das zentrale Modellelement „Wirkstruktur-Modell“ repräsentiert das Partialmodell Wirkstruktur. Es kann mehrere Systemelemente enthalten, die wiederum weitere untergeordnete Systemelemente besitzen können. Jedes Systemelement kann Flüsse und Ports besitzen. Ein jeder Fluss wird durch eine Menge von übertragenen Elementen charakterisiert. Es wird zwischen Informations-, Material- und Energieflusselementen unterschieden (in Bild nicht dargestellt). Ein Fluss darf ausschließlich gleichartige Flusselemente übertragen. Dadurch wird auch die Art des Flusses determiniert (werden z.B. Energieflusselemente übertragen, so ist der zugehörige Fluss ein Energiefluss). Quelle und Ziel

eines zwischen zwei Systemelementen verlaufenden Flusses sind die Ports der Systemelemente. Die Abschnitte eines Flusses zwischen Quell- und Ziel-Port werden rechnerintern durch das Element Flussabschnitt abgebildet.

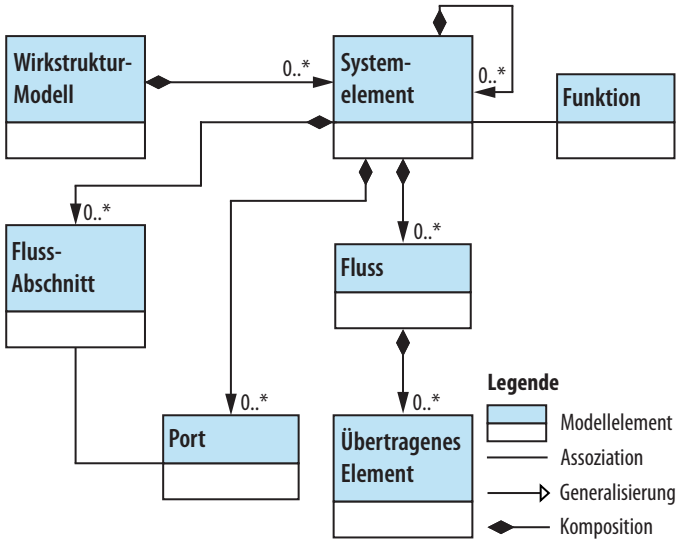


Bild 4-14: Das Metamodell des Partialmodells Wirkstruktur der Spezifikationstechnik CONSENS (Ausschnitt; Vereinfachte Darstellung) [HNI12]

Erweiterung des Metamodells: Bild 4-15 zeigt das auf Basis der Ergebnisse der Phase 1 erweiterte Metamodell der Spezifikationstechnik CONSENS. Ebenfalls ist der Zusammenhang zu den in Phase 2 erarbeiteten Erweiterungen der graphischen Notation dargestellt. Innerhalb eines Systemelements können Ausfälle sowie Gatter modelliert werden. Diese können untereinander über gerichtete Ursache-Wirkungs-Beziehungen verbunden werden.

Der Port eines Systemelements kann mehrere Portzustände besitzen, welche zur Abbildung ein- und ausgehender Ausfälle genutzt werden. Die Portzustände bilden den Normalzustand (ok) sowie potentielle Fehlzustände ab (z.B. Emergency, Fail-Safe, Fail-Danger). Die zu den Fehlzuständen korrespondierenden Portzustände können ebenfalls Ziel bzw. Quelle einer Ursache-Wirkungs-Beziehung sein. Bild 4-15 stellt darüber hinaus den Zusammenhang zu den Erweiterungen der graphischen Notation dar (rote Pfeile).

Sollen auch weitere Methoden auf Basis der Produktkonzeption durchgeführt werden, so gilt es, die Spezifikationstechnik in analoger Weise anzupassen. Um z.B. eine FMEA durchführen zu können, reicht es aus, das Metamodell zu erweitern. Ausfallmöglichkeiten, Ausfallursachen und Ausfallauswirkungen können unter Verwendung der bestehenden Modelelemente „interner Ausfall“, „Portzustand“ (beide Spezialisierungen des Modellelements „Ausfall“) sowie „Ursache-Wirkungs-Beziehung“ abgebildet werden. Somit besteht die notwendige Erweiterung des Metamodells insbesondere darin, dass für das Modellelement „Ausfall“ folgende zusätzliche Attribute definiert werden: „Schwere_qualitativ“, „Auftretenswahrscheinlichkeit_qualitativ“, „Entdeckungswahrscheinlichkeit_qualitativ“ (vgl. auch Abschnitt 3.2.2.5).

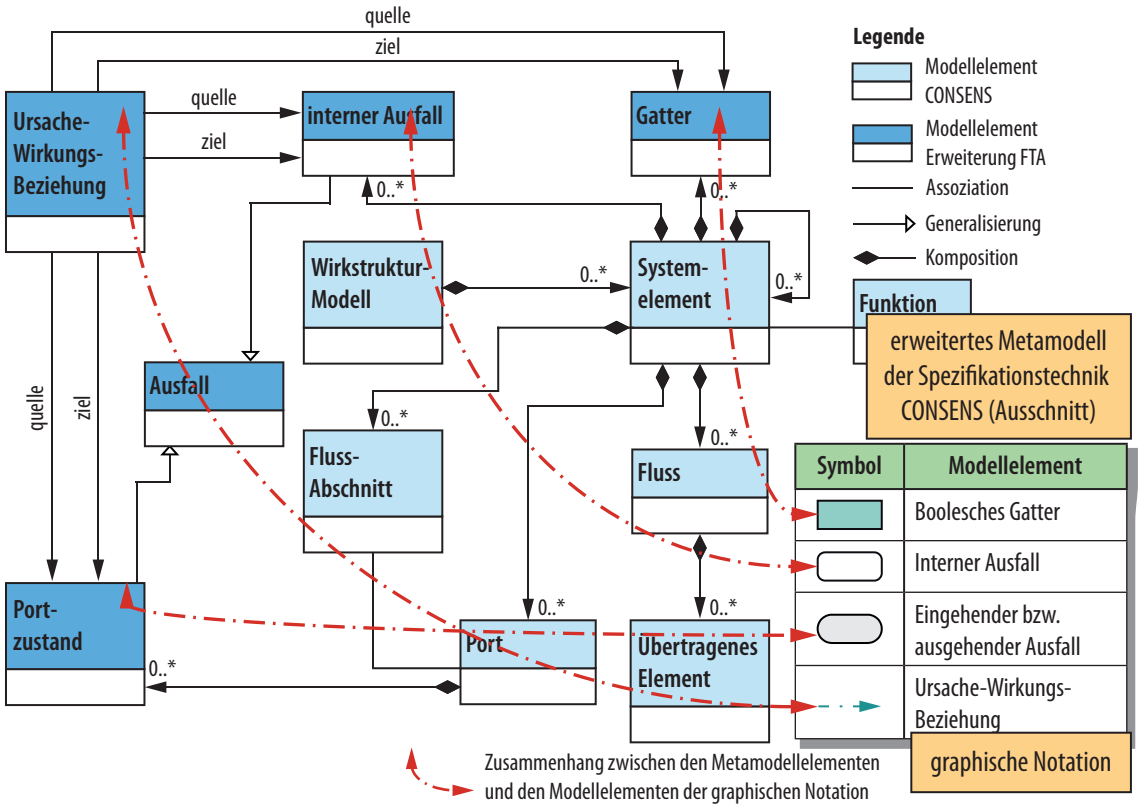


Bild 4-15: Erweitertes Metamodell von CONSENS und der Zusammenhang zur graphischen Notation (Vereinfachte Darstellung)

4.5 Angepasste Methoden zur Analyse und Verbesserung

Im Folgenden werden ausgewählte Beispiele von Methoden vorgestellt, die derart angepasst wurden, dass sie auf Basis der Spezifikation der Produktkonzeption durchgeführt werden können. Die Vorstellung erfolgt am Beispiel des Feder-Neige-Moduls des RailCabs (vgl. auch Abschnitt 2.2.3) [ADG+09, S. 64ff.]. Das Feder-Neige-Modul dient zur Erhöhung des Fahrkomforts: die von den Unebenheiten in der Schiene eingeleiteten Störungen werden so gut wie nicht mehr auf den Wagenkasten übertragen [NBP14-ol]. Jedes Feder-Neige-Modul verfügt über drei Servozylinder zur Dämpfung von Schwingungen und zum Neigen des Fahrzeugaufbaus. Die Servozylinder bestehen aus je einem Hydraulikzylinder, einem 4/4-Wege-Ventil, einer Regelung des Servozylinders und einer Regelung des Hydraulikventils [ADG+09]. Bild 4-16 zeigt einen Ausschnitt der Spezifikation der Produktkonzeption des Servozylinders des Feder-Neige-Moduls.

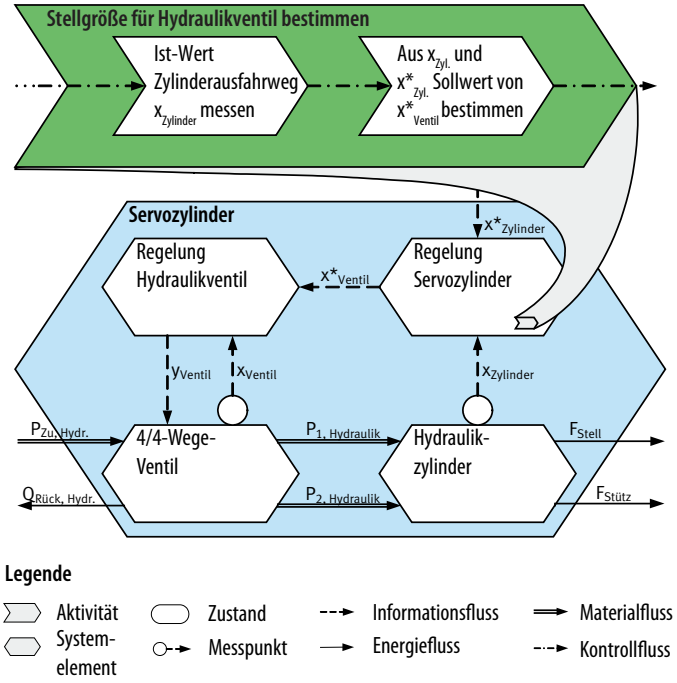


Bild 4-16: Wirkstruktur des Servozylinders des Feder-Neige-Moduls (Ausschnitt; in Anlehnung an [GKP09])

4.5.1 Spezifikation der Ausfallfortpflanzung innerhalb der Produktkonzeption

Mit der in Abschnitt 4.4.3 vorgestellten, erweiterten Spezifikationstechnik CONSENS ist es möglich, die Ausfallfortpflanzung innerhalb der Produktkonzeption zu spezifizieren. Bild 4-17 zeigt die um die Beschreibung der Ausfallfortpflanzung erweiterte Spezifikation der Wirkstruktur. Das Systemelement „Regelung Hydraulikventil“ besitzt drei durch Ports abgebildete Schnittstellen zu anderen Systemelementen „HV_1“, „HV_2“ (beide eingehend) und „HV_3“ (ausgehend). Der Port „HV_3“ bildet die Schnittstelle zwischen der „Regelung Hydraulikventil“ und dem „4/4-Wege-Ventil“. Ein möglicher Fehler am Port „HV_3“ besteht darin, dass die Regelung Hydraulikventil keine Schaltstellung Y_{Ventil} mehr an das 4/4-Wege-Ventil ausgibt. Im Rahmen der Analyse der Zuverlässigkeit werden drei potentielle Ursachen hierfür identifiziert. Zu dem skizzierten Fehler kommt es, wenn die Regelung Hydraulikventil defekt ist („F1“), wenn die Energieversorgung der Regelung Hydraulikventil ausgefallen ist („HV_2.notok“) oder wenn die Regelung Servozylinder keine Sollschieberlage X^*_{Ventil} liefert („HV_1.notok“).

4.5.2 Automatisierte Erzeugung eines Fehlzustandsbaums

Auf Basis einer derartigen Beschreibung ist es möglich, einen Fehlzustandsbaum automatisch zu erzeugen. Bild 4-18 zeigt einen derartigen, aus der Spezifikation der Ausfallfortpflanzung des Servozylinders ausgeleiteten Fehlzustandsbaum. Als Hauptereignis wurde hierbei der Ausfall „Regelung Hydraulikventil gibt keine Schaltstellung Y_{Ventil} mehr an 4/4-Wege-Ventil aus“ gewählt.

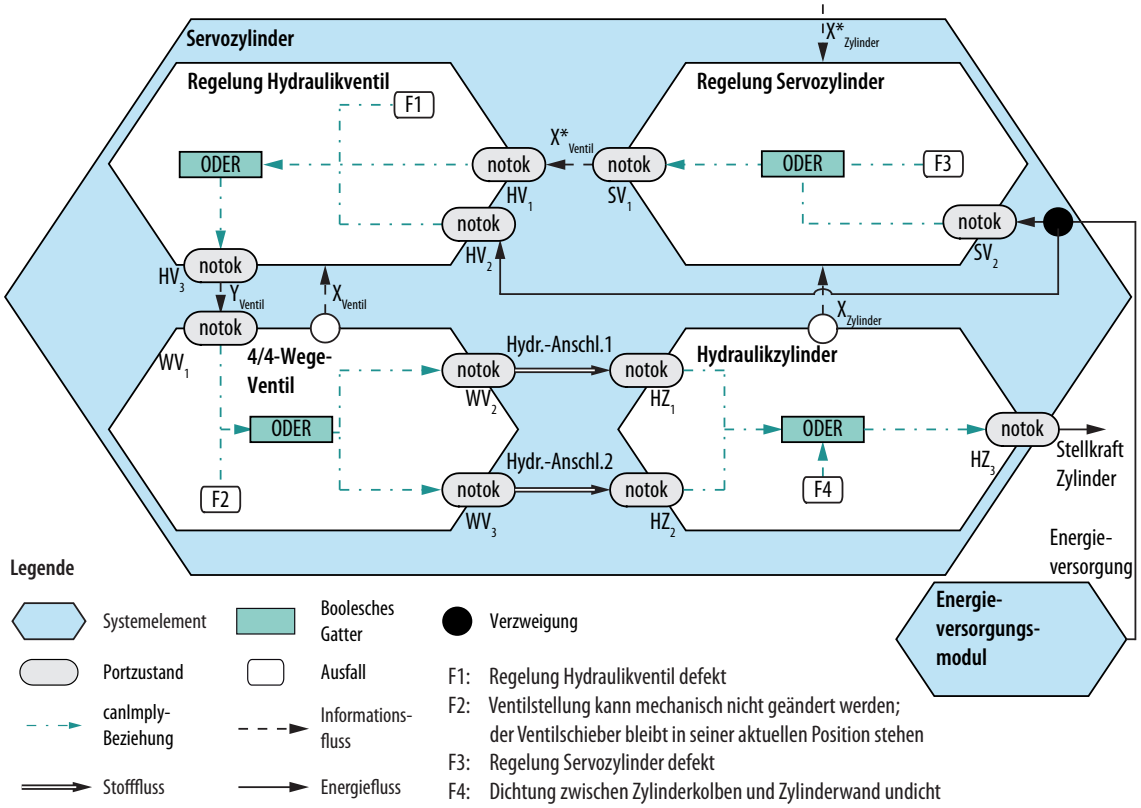


Bild 4-17: Spezifikation der Ausfallfortpflanzung in der Wirkstruktur des Servozylinders des Feder-Neige-Moduls (Ausschnitt)

4.5.3 Automatisierte Erzeugung einer FMEA-Tabelle

Analog lässt sich aus der Spezifikation der Ausfallfortpflanzung eine initial befüllte FMEA-Tabelle automatisch erzeugen. Tabelle 4-2 zeigt eine derartige FMEA-Tabelle.

4.5.4 Durchführung BN-orientierter Analysen

Die in Abschnitt 3.2.2.8 vorgestellten, auf Bayesschen Netzen (BN) beruhenden Analysen stellen ein weiteres Beispiel von Analysemethoden dar, die auf Basis der Spezifikation der Produktkonzeption durchgeführt werden können. Voraussetzung hierfür ist die Abbildung der Spezifikation der Ausfallfortpflanzung auf ein BN. Im Rahmen der vorliegenden Arbeit entstand ein Algorithmus, welcher diese Abbildung unterstützt [Dor12]. Die internen Fehler sowie die ein- und ausgehenden Portfehlzustände werden jeweils als Knoten des BN abgebildet, die Beziehungen zwischen den internen Fehlern und den Portfehlzuständen jeweils als Kanten. Danach erfolgt das Befüllen der Tabellen der bedingten Wahrscheinlichkeiten der Knoten. Für jeden Knoten werden die bedingten Wahrscheinlichkeiten in Bezug auf die möglichen Werte der Variablen spezifiziert, die mit seinen Elternknoten assoziiert sind. Elternlose Knoten des BN werden direkt mit Auftretenswahrscheinlichkeiten versehen. Siehe Abschnitt 3.2.2.8 für mehr Informationen hierzu.

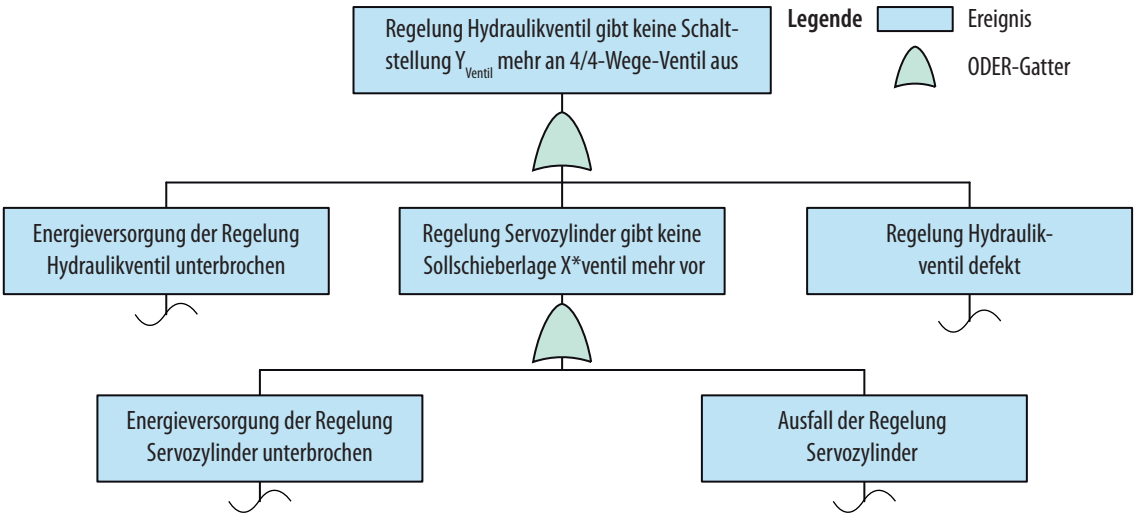


Bild 4-18: Ein aus der Spezifikation der Ausfallfortpflanzung automatisch generierter Fehlzustandsbaum (Ausschnitt)

Zur Unterstützung des Abbildungsalgorithmus wurde ein Katalog von Abbildungsvorschriften erarbeitet. Bild 4-19 stellt eine Abbildungsvorschrift zur Abbildung einer UND-Fortpflanzungsbeziehung auf ein BN dar. Für detailliertere Informationen zu dem Abbildungsalgorithmus und den Abbildungsvorschriften siehe [Dor12].

Fehlzustandsart- und -auswirkungsanalyse (FMEA) › Modul: Servozylinder				
System-element	**Ausfall-möglichkeit**	**Ausfall-auswirkung**	**Ausfall-ursache**	**...**
Regelung Hydrau-likventil	Regelung Hydraulikven-til gibt keine Schaltstellung Y_{Ventil} mehr an 4/4-Wege-Ventil aus	Ventil ändert den Druck an den Ausgängen nicht	Regelung Servozylinder gibt keine Sollschieberlage X^*_{Ventil} mehr vor	...
			Regelung Hydraulikventil defekt	
			Energieversorgung der Regelung Hydraulikventil unterbrochen	
4/4-Wege-Ventil	Ventil sperrt ungewollt	Hydraulikzylin-der bleibt an der aktuellen Position stehen	Elektrische Versorgung unter-brochen	
			Magnetspule beschädigt	
...	...	...	...	...

Tabelle 4-2: Eine aus der Spezifikation der Ausfallfort-pflanzung automatisch erzeugte FMEA-Tabelle (Ausschnitt) [DG10]

Ein derart erzeugtes BN ermöglicht, wie in Abschnitt 3.2.2.8 beschrieben, probabilistische Analysen. Dies wird am Beispiel des Hauptereignisses „Das 4/4-Wege-Ventil ändert den Druck an den Ausgängen nicht“ („WV_2.notok“) kurz erklärt. Gemäß der Spezifikation der Ausfallfortpflanzung tragen die Fehlerursachen „F1“, „HV_3.notok“, „F3“, „SV_2.notok“ und „F2“ zum betrachteten Ausfall „WV_2.notok“ potentiell bei.

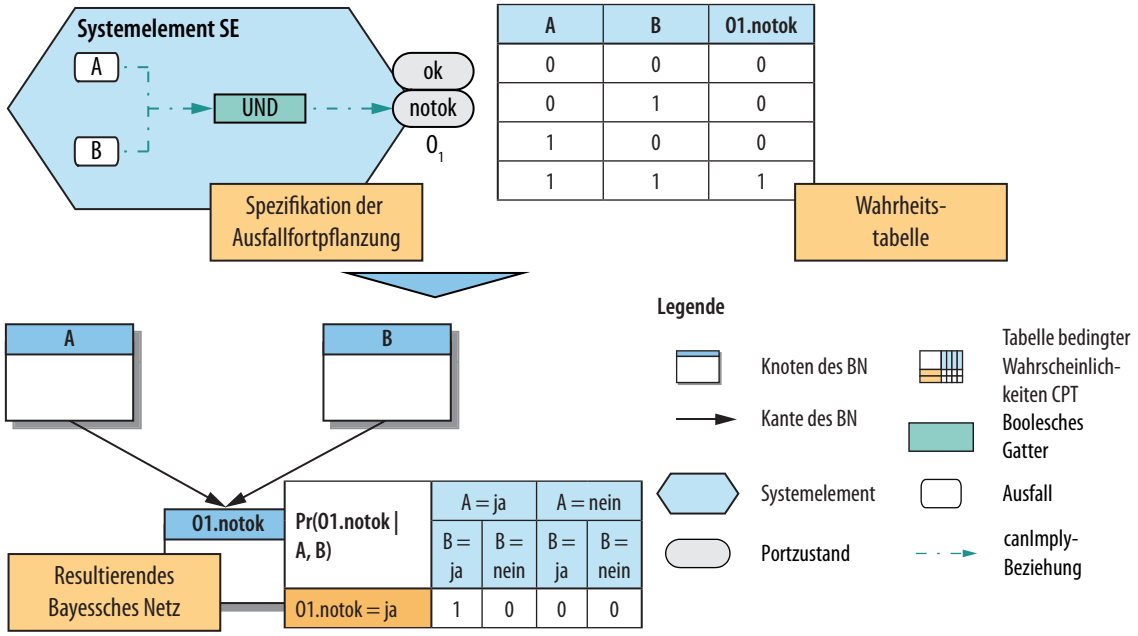


Bild 4-19: Auszug aus dem Katalog von Abbildungsvorschriften; dargestellt ist die Abbildungsvorschrift für das UND-Gatter (Ausschnitt) [Dor12]

Mittels der in Abschnitt 3.2.2.8 vorgestellten rückwärtsgerichteten Analyse kann auf Basis des BN berechnet werden, mit welcher Wahrscheinlichkeit die jeweilige Fehlerursache zum betrachteten Ausfall führt (die sogenannte „Fussel/Vesely-Importanz“). Als Basis für diese Analyse wurden die in Tabelle 4-3 abgebildeten Ausfallraten der Fehlerursachen verwendet. Die Ergebnisse sind ebenfalls in Tabelle 4-3 abgebildet. Demnach sind die Ausfälle „F1“ und „F3“ die wahrscheinlichsten Ursachen des Ausfalls „WV2.notok“ mit Wahrscheinlichkeit von jeweils ca. 25 %. Für weiterführende Informationen und Ergebnisse hierzu siehe [Dor12], [DG10].

Ausfall	Ausfallrate (pro Stunde)	Fussel/Vesely-Importanz
F1	$5{,}11 \times 10^{-7}$	0,2416
HV_3.notok	$4{,}02 \times 10^{-7}$	0,1901
SV_2.notok	$3{,}28 \times 10^{-7}$	0,1551
F3	$5{,}23 \times 10^{-7}$	0,2473
F2	$3{,}51 \times 10^{-7}$	0,1660

Tabelle 4-3: Die Ausfallraten und die zugehörigen Fussel/Vesely-Importanzen für die ausgewählten Ausfälle [Dor12]

Ebenso kann die Spezifikationstechnik CONSENS derart erweitert werden, dass die auf dynamischen Bayesschen Netzen beruhenden Analysen integriert werden können; Bild 4-20 stellt dies für das Priority-AND-Gatter dar (vgl. Abschnitt 3.2.2.9). Für detailliertere Informationen hierzu sei auf [DG12] verwiesen.

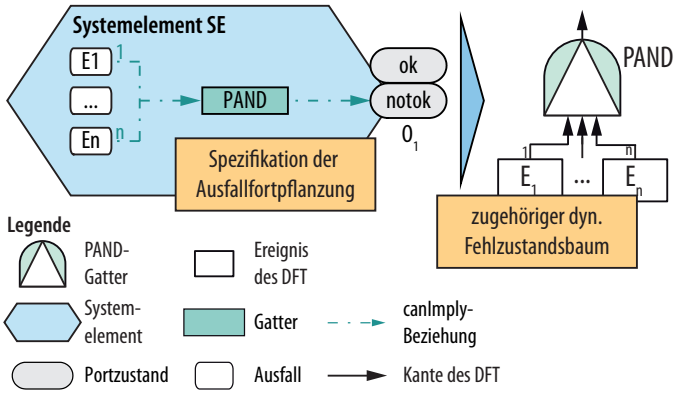


Bild 4-20: Spezifikation der Ausfallfortpflanzung mit dem Priority-AND-Gatter und der zugehörige dynamische Fehlzustandsbaum [DG12]

4.6 Werkzeugunterstützung für Modellierung und Analyse

Damit das Anwenden der Systematik durch die Entwickler effizient erfolgen kann, ist eine Softwareunterstützung von zentraler Bedeutung. Die Softwareunterstützung muss dabei die Durchführung aller Phasen der Systematik unterstützen. Sie muss daher drei wesentliche Funktionen zur Verfügung stellen: 1) eine Suchfunktion für die Suche, Auswahl und Planung des Einsatzes von Methoden, 2) eine Editierfunktion für die Modellierung der Produktkonzeption unter besonderer Berücksichtigung von zuverlässigkeits- und sicherheitsbezogenen Informationen sowie 3) eine Analysefunktion, welche eine Analyse der Produktkonzeption hinsichtlich Zuverlässigkeit und Sicherheit ermöglicht. Die Umsetzung der Verbesserungen (Gegenmaßnahmen) in der Spezifikation der Produktkonzeption erfolgt ebenfalls unter Verwendung der Editierfunktion. Die prototypische Rechnerunterstützung für die Suche, Auswahl und Planung von Methoden wurde bereits in Abschnitt 4.3 vorgestellt. Im Folgenden erfolgt eine Vorstellung der prototypischen Rechnerunterstützung für die übrigen zwei Punkte (Modellierung und Analyse).

Die Werkzeugunterstützung wurde als eine Erweiterung für das in Abschnitt 3.6.3 vorgestellte Software-Werkzeug Mechatronic Modeller realisiert. Dieses Werkzeug stellt eine werkzeugtechnische Umsetzung der Spezifikationstechnik CONSENS dar [GDP+10]. Es basiert auf der Eclipse GMF Technologie (Graphical Modeling Framework) und weist eine modulare Architektur auf. Die Werkzeugunterstützung für Modellierung und Analyse wurde in Form von zusätzlichen Software-Modulen umgesetzt, welche in die modulare Architektur des Modellers integriert wurden. Die Umsetzung erfolgte für die in Abschnitt 4.5 beschriebene Methodenauswahl. Unterstützt werden sowohl die klassischen als auch die dynamischen Bayesschen Netze.

- **Editor zur Spezifikation der Ausfallfortpflanzung:** Realisiert wurde eine Erweiterung des standardmäßig vorhandenen Editors für die Wirkstruktur. Sie ermöglicht die Spezifikation der Ausfallfortpflanzung mit der in Abschnitt 4.5.1 vorgestellten Notation (Bild 4-21 (1)). Eine Voraussetzung hierfür stellte die Erweiterung des Metamo-

dells der Spezifikationstechnik CONSENS dar, auf dem die werkzeugtechnische Realisierung des Mechatronic Modellers beruht. Diese wurde entsprechend der in Abschnitt 4.4 vorgestellten Vorgehensweise vorgenommen.

- **Editor für die FMEA:** Ein tabellarischer Editor wurde umgesetzt, welcher das Arbeiten mit einem FMEA-Formblatt ermöglicht. Die Inhalte des FMEA-Formblatts werden zum großen Teil aus dem der Spezifikation der Ausfallfortpflanzung zugrunde liegenden Datenmodell bezogen (2).
- **Modul für BN-orientierte probabilistische Analysen:** Dieses Modul unterstützt die in Abschnitt 3.2.2.8 vorgestellten, auf BN beruhenden probabilistischen Analysen. Es stellt insbesondere Dialoge zur Darstellung der Analyseergebnisse bereit (3).
- **Modul zur Abbildung der Spezifikation auf ein Bayessches Netz:** Es handelt sich um ein internes Modul, welches die Abbildung der Spezifikation der Ausfallfortpflanzung auf ein BN implementiert. Es wird stets intern durch das Modul zu BN-orientierten probabilistischen Analysen aufgerufen.

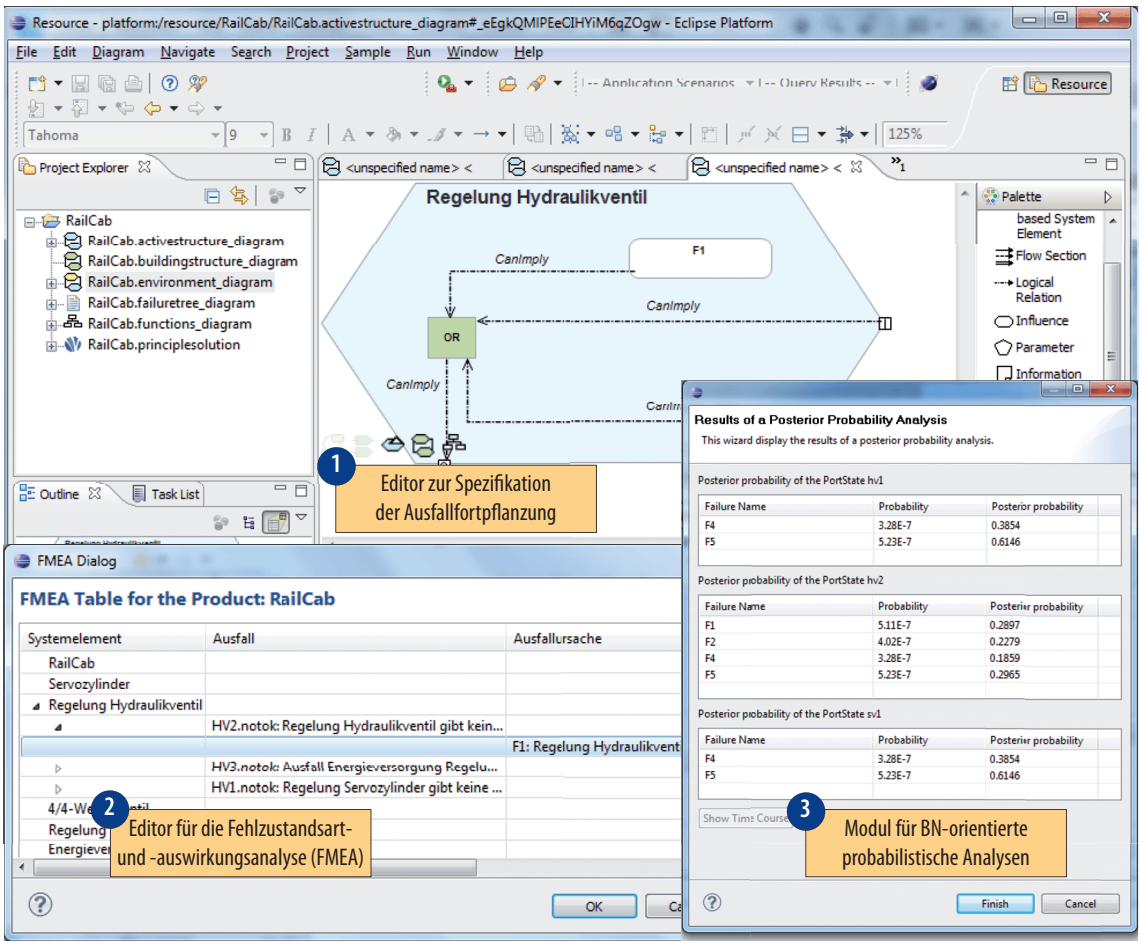


Bild 4-21: Graphische Benutzungsoberfläche des Mechatronic Modellers mit den Zusatzfunktionen zur Modellierung und Analyse

5 Validierung der Systematik

In diesem Kapitel erfolgt die Validierung der im vorhergehenden Kapitel vorgestellten *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme.* Diese erfolgt anhand des X-by-Wire[47]-Versuchsfahrzeugs Chamäleon [NJT08], [GRS14]. Insbesondere wird gezeigt, wie die Systematik anzuwenden ist und was die dabei zu erarbeitenden wesentlichen Ergebnisse sind.

Zunächst wird in Abschnitt 5.1 ein kurzer Überblick über die X-by-Wire-Technologie gegeben. In diesem Zusammenhang werden insbesondere der derzeitige Stand der Umsetzung der X-by-Wire-Technologie und die damit verbundenen Herausforderungen erklärt. Anschließend wird in Abschnitt 5.2 das X-by-Wire-Versuchsfahrzeug Chamäleon vorgestellt. Gegenstand der Abschnitte 5.3 bis 5.6 ist die Anwendung der einzelnen Phasen der Systematik am Beispiel des Chamäleons. Abschließend erfolgt in Abschnitt 5.7 die Bewertung der Systematik hinsichtlich der im Rahmen der Problemanalyse aufgestellten Anforderungen.

5.1 Überblick über die X-by-Wire-Technologie

Als X-by-Wire wird ein System bezeichnet, welches folgende zwei energetisch entkoppelte Regelkreise aufweist [WIH+04, S. 2]:

- einen Regelkreis zur Erzeugung der fahrdynamischen Wirkung (z.B. Radverstellung für die Lenkfunktion, Erzeugung der Bremsmomente für die Bremsfunktion) und
- einen Regelkreis zur Erzeugung einer Rückmeldung für den Fahrer, die ihm eine gefühlvolle Betätigung der jeweiligen Funktion (z.B. der Lenkfunktion) ermöglicht.

Beide Regelkreise umfassen ein Grundsystem, eine Sensorik, eine Aktorik sowie eine Informationsverarbeitung (vgl. Abschnitt 2.2.1.2). Die Sensorik und Aktorik sind an das Fahrzeug bzw. den Fahrer über mechanische Schnittstellen angebunden [WIH+04, S. 2f.]. Die Kopplung zwischen den beiden Regelkreisen erfolgt über Informationsaustausch [WIH+04, S. 3]. Charakteristisch für X-by-Wire-Systeme ist, dass einige mechanische Verbindungen und Elemente überflüssig werden (z.B. die in den klassischen Lenkungen zur Übertragung der Lenkbefehle vom Lenkrad an das Lenkgetriebe dienende Lenksäule). Ihre Funktionen werden durch Sensorik, Aktorik und Informationsverarbeitung übernommen.

Demnach ist ein Steer-by-Wire-System durch zwei wesentliche Merkmale charakterisiert (Bild 5-1): Zum einen wird der Lenkbefehl von einem Bedienelement (z.B. Lenkrad, Joystick) über ein Steuergerät elektrisch zu einem Aktor weitergeleitet, der den Lenkbefehl

[47] Die Bezeichnung X-by-Wire beschreibt eine Klasse von Systemen wie Brake-by-Wire-, Drive-by-Wire-, Fly-by-Wire-, Steer-by-Wire-Systeme etc.

an den gelenkten Rädern über die Lenkachse ausführt [PH13, S. 447]. Zum anderen wird der Fahrzustand haptisch über das Bedienelement an den Fahrer zurückgemeldet [PH13, S. 447].

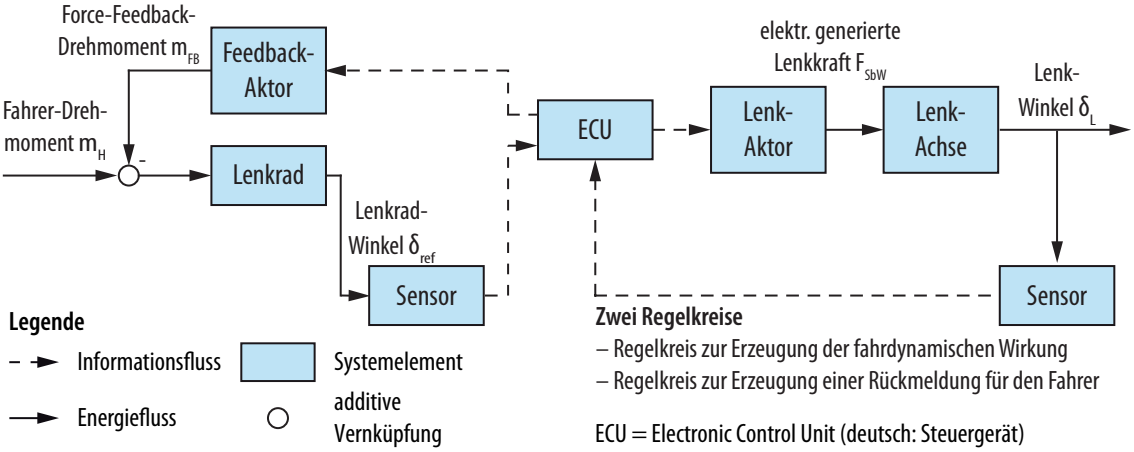


Bild 5-1: Grundsätzlicher Aufbau eines Steer-by-Wire-Systems ohne mechanische Rückfallebene (in Anlehnung an [Wro10, S. 16])

Die X-by-Wire-Technologie ist heute in verschiedenen technischen Bereichen anzutreffen. In der Concorde wurde in den 1970er Jahren das erste analoge Fly-by-Wire-System im zivilen Flugzeugbau umgesetzt [PH13, S. 447]. Die Firma Airbus führte im Jahre 1987 mit dem A320 ein Verkehrsflugzeug mit Fly-by-Wire-Technologie ohne mechanische Rückfallebene ein [PH13, S. 447]. Throttle-by-Wire (elektronisches Gaspedal, E-Gas) war das erste by-wire-System im Automobilbau. Es wurde bei Verbrennungsmotoren Anfang der 1980er Jahre eingeführt und wird bis heute in Großserie gefertigt [BB12, S. 666], [PH13, S. 447], [WIH+04, S. 2]. Auch Shift-by-Wire hatte bisher in das Kraftfahrzeug Einzug gehalten (Beispiele: automatisierte Schaltgetriebe (ASG) und Doppelkupplungsgetriebe) [BB12, S. 666f.], [WIH+04, S. 2]. Reine Brake-by-Wire- und Steer-by-Wire-Funktionen wurden bislang nur in Spezial- und Prototypenfahrzeugen realisiert [PH13, S. 447], [Con14-ol]. Serientauglich sind derzeit nur Zwischenlösungen mit einer mechanischen Rückfallebene wie die Überlagerungslenkung vorhanden [PH13, S. 409ff.].

5.1.1 Herausforderung: Verzicht auf die mechanische Rückfallebene

Wesentliche Voraussetzung für den Markterfolg der X-by-Wire-Fahrzeuge besteht in einer geeigneten Verbindung einer umfassenden Funktionalität mit einer sehr hohen Verfügbarkeit und Sicherheit [WIH+04, S. 7]. Der für reine X-by-Wire-Systeme charakteristische Verzicht auf die mechanische Rückfallebene bedeutet zusätzliche Anforderungen hinsichtlich Sicherheit, Zuverlässigkeit und Verfügbarkeit. Dies stellt aus heutiger Sicht eine der wesentlichen Hürden für die serientaugliche Einführung von Steer-by-Wire-Systemen dar [PH13, S. 458], [WIH+04, S. 2]. Der Grund: Im Gegensatz zu elektronischen Systemelementen kann ein mechanisches System basierend auf Fachkenntnissen und Erfahrungswerten im Allgemeinen derart ausgelegt und dimensioniert werden, dass „es bei

Einhaltung der spezifizierten Beanspruchungsgrenzen innerhalb der vorgesehenen Nutzungsdauer nach menschlichem Ermessen nicht ausfallen wird“ [PH13, S. 449]. Aus diesem Grund wurden auf dem Weg zu reinen X-by-Wire-Systemen bislang nur Zwischenstufen serienreif umgesetzt – X-by-Wire-Systeme mit mechanischer Rückfallebene. Beispiel – Überlagerungslenkung: hier wird der Lenkwunsch des Fahrers durch eine gezielte Lenkwinkelüberlagerung um einen additiv aufgebrachten Überlagerungswinkel ergänzt [PH13, S. 409]. Funktional können zwar derartige Systeme die Eigenschaften eines reinen Steer-by-Wire-Systems darstellen. Aufgrund des Beibehaltens der mechanischen Rückfallebene sind Bauraumvorteile jedoch nicht gegeben [PH13, S. 449]. Hinsichtlich der Absicherung der Sicherheit reicht es aus – da eine mechanische Rückfallebene vorhanden ist – die elektronischen Systemelemente nach dem Fail-Silent-Prinzip umzusetzen: beim Erkennen eines Ausfalls werden die elektronischen Systemelemente abgeschaltet und beeinflussen die Lenkfunktion folglich nicht mehr (vgl. Abschnitt 2.1.5.3) [PH13, S. 449]. Eine eingeschränkte Lenkfunktion wird im Falle eines Ausfalls über die mechanische Rückfallebene sichergestellt [PH13, S. 449].

5.1.2 Absicherung der Sicherheit von X-by-Wire-Systemen

Als wesentliches Mittel zu Erreichung einer hohen Ausfallsicherheit bei X-by-Wire-Systemen nennen WINNER ET AL. die Fehlertoleranz [WIH+04, S. 4f.]. Konkret werden statische Redundanz für mechanische und elektrische Systemelemente und dynamische Redundanz für elektromechanische und mechatronische Systemelemente vorgeschlagen, die bereits in Anhang A1.1 ausführlich erläutert wurden [WIH+04, S. 5]. Ebenso kann analytische Redundanz verwendet werden (vgl. Anhang A1.1). Außerdem ist auch die Umsetzung eines Degradationskonzepts zu empfehlen [WIH+04, S. 5f.]. Gemeint ist die Reduzierung des Funktionsumfangs im Falle eines Fehlers. Die grundsätzlichen Degradationsstufen Fail-Operational, Fail-Safe, Fail-Reduced, Fail-Silent wurden bereits in Abschnitt 2.1.5.3 detailliert erklärt. Ein beispielhaftes Degradationskonzept wird für das Anwendungsbeispiel Chamäleon in Abschnitt 5.6.1 eingeführt.

Aufgrund der Faktoren Kosten, Raumbedarf und Gewicht gilt es für X-by-Wire-Fahrzeuge, einen geeigneten Kompromiss zwischen dem Grad der Fehlertoleranz und der Zahl der Redundanzen zu finden [WIH+04, S. 5]. Ein in der Automobilindustrie häufig anzutreffender Ansatz zur Realisierung von kostengünstigen eigensicheren Systemelementen besteht darin, nur die ausfallkritischen Strukturen redundant auszuführen [WIH+04, S. 6]. Beispiele: Sensoren für das Fahrpedal, die Drosselklappe und das Lenkradmoment einer elektromechanischen Servolenkung [WIH+04, S. 6], [Rei11, S. 15; S. 243; S. 261]. Darüber hinaus kommen oft Ausführungen zum Einsatz, die über eine Eigendiagnoselogik ein Teil der Ausfälle erkennen können (z.B. durch gegenläufige Signale, Signal-Range-Checks etc.) [WIH+04, S. 6]. Ebenso muss die Stromversorgung unter allen Betriebsbedingungen ausfallsicher sein [HES11, S. 242f.]. Das traditionelle 12/14-Volt-Netz reicht hierfür nicht aus [HES11, S. 243].

5.2 Anwendungsbeispiel: X-by-Wire-Versuchsfahrzeug Chamäleon

Das elektrische Versuchsfahrzeug Chamäleon ist ein Demonstrator des SFB 614 (Bild 5-2). Es handelt sich um ein fortschrittliches mechatronisches X-by-Wire-System; sein intelligentes Verhalten beruht auf dem in Abschnitt 2.2.3 vorgestellten Wirkparadigma der Selbstoptimierung. Das Chamäleon verfügt über eine hohe Anzahl an Freiheitsgraden und ermöglicht das Einbeziehen von Unsicherheiten, die aus schwer vorhersehbaren Fahrt- und Streckenverläufen resultieren [BHS+13].

X-by-Wire-Versuchsfahrzeug Chamäleon

Radmodul mit drei Elektromotoren

Joystick als Bedienelement

Bild 5-2: Das X-by-Wire-Versuchsfahrzeug Chamäleon; es besitzt vier identische Radmodule, als Bedienelement wird ein Joystick verwendet [GRS+14]

Das Chamäleon stellt ein reines X-by-Wire-Fahrzeug dar: es wird ausschließlich elektrisch aktuiert; eine mechanische Kopplung zwischen Bedienelement und Aktorik ist nicht vorhanden[48]. Als Bedienelement kommt ein Joystick zum Einsatz (Bild 5-2). Mit dem Fahrzeug kann eine Person befördert werden, wobei eine Maximalgeschwindigkeit von etwa 50 km/h erreicht werden kann. Aufgrund der verwendeten Leichtbaumethoden beträgt das Leergewicht des Fahrzeugs lediglich ca. 280 kg [BHS+13], [GRS14].

Das Chamäleon besitzt vier baugleiche Radmodule, welche die Fahrwerkfunktionen Lenken, Antreiben, Bremsen, Federn und Dämpfen an den einzelnen Rädern erbringen (Bild 5-2). Die Ausführung dieser Funktionen erfolgt in jedem der Radmodule jeweils über drei Elektromotoren (je ein Motor für die Lenkfunktion, die Antriebsfunktion und die aktive Federung) [GRS14]. Dadurch werden Einzelrad-Allradantrieb, Einzelrad-Allradlenkung und aktive Federung ermöglicht. Aufgrund einer derartigen Realisierung kann, abgesehen vom Sturz, in alle relevanten Freiheitsgrade der Radbewegung gezielt eingegriffen werden [BHS+13]. Das System ist dadurch insbesondere in der Lage, selbst bei holprigen Fahrstrecken Unebenheiten optimal auszugleichen und dabei eine hohe Traktion der Fahrantriebe zu gewährleisten [LW10, S. 41]. Die Bremsfunktion kann zum einen durch

---

[48] Eine Ausnahme bildet eine mechanische Nothandbremse [GRS14].

den Antriebsmotor erreicht werden. Zum anderen kann eine Bremsung mittels Einzelradlenkung durch Lenkung der Räder nach innen erreicht werden [GRS+14]. Die Hauptvorteile einer derartigen Umsetzung bestehen in einer höheren Funktionalität, einer systemimmanenten Redundanz und einem Bauraumgewinn [PH13, S. 450].

Die Energieversorgung des Chamäleons erfolgt über einen in die Bodengruppe des Fahrzeugs integrierten Lithium-Ionen-Akku [LW10, S. 41]. Der Energiespeicher stellt für die Elektromotoren genügend Leistung zur Verfügung, um das Fahrzeug für ca. eine Stunde in Bewegung zu setzen [LW10, S. 41]. Kern der technischen Implementierung der Informationsverarbeitung des Chamäleons stellt die MicroAutoBox der Firma dSPACE dar.

Im SFB 614 wurden anhand des Chamäleons die Vorteile des Einsatzes von Methoden der Selbstoptimierung für ein vernetztes Fahrzeugregelsystem untersucht und validiert. Konkret ging es um eine s.o. Fahrzeugregelung im Hinblick auf die Vertikal- und Längsdynamik, das Energiemanagement sowie die Rekonfiguration der Fahrwerksaktorik [SFB11]. Die Probefahrten u.a. auf einem ADAC-Testgelände, bei Messen sowie bei Vorstellungen der Universität Paderborn bestätigen das hohe Potential der fortschrittlichen Technik und das hohe Öffentlichkeitsinteresse [LW10, S. 41]. Das Chamäleon eignet sich zudem als eine Simulationsplattform z.B. zur Erprobung neuer Lenkstrategien [KGB+10]. Für den öffentlichen Straßenverkehr ist Chamäleon nicht zugelassen [LW10, S. 41].

Nachfolgend werden die Phasen der im Rahmen der vorliegenden Arbeit entwickelten *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* anhand der Konzipierung des Chamäleons erklärt. Ein besonderes Augenmerk wird hierbei auf die Lenkfunktion des Chamäleons gelegt.

5.3 Phase 1 – Analyse der Entwicklungsaufgabe

Im Rahmen dieser Phase wird zur Charakterisierung der Entwicklungsaufgabe das in Abschnitt 4.3 vorgestellte Klassifizierungsschema verwendet. Das Chamäleon ist ein sicherheitsrelevantes Automobilsystem. Dies betrifft insbesondere die Lenkfunktion: Ein plötzlicher Ausfall der Lenkfunktion kann gefahrbringende Konsequenzen mit sich ziehen. Daher steht die Absicherung der Sicherheit im Vordergrund.

Für Systeme mit hohen Anteilen an elektrischen/elektronischen Systemelementen wie das Chamäleon ist die Norm IEC 61508 heranzuziehen. Für Teilaspekte der Absicherung kann ferner die ISO 26262 zum Einsatz kommen, da sie als eine automobiltechnikspezifische Ableitung der IEC 61508 auf die Gegebenheiten der Kraftfahrzeuge besser zugeschnitten ist (vgl. Abschnitte 3.1.1 und 3.1.2).

Das Chamäleon ist ein komplexes System. Kennzeichnend für seine Komplexität ist allem voran der Einsatz der Selbstoptimierung im Sinne eines vernetzten Fahrzeugregelsystems. Bezogen auf die Neuartigkeit des Systems handelt es sich um ein herausforderndes Forschungsvorhaben.

Im Zusammenhang mit der Absicherung der Sicherheit ist eine Untersuchung von sowohl Einzel- als auch von Mehrfachfehlzuständen von Bedeutung. Zeit- bzw. Abfolgeabhängigkeiten sollen bei der Absicherung nicht im Fokus stehen. Abhängige Ereignisse sind hingegen von hoher Bedeutung.

5.4 Phase 2 – Auswahl und Planung von Methoden

In dieser Phase findet die Auswahl und Planung von Methoden zur Absicherung der Sicherheit des Chamäleons statt. Bild 5-3 stellt das zugehörige Vorgehen dar. Basis hierfür bildet das Klassifizierungsschema für Methoden (vgl. Abschnitt 4.3.2).

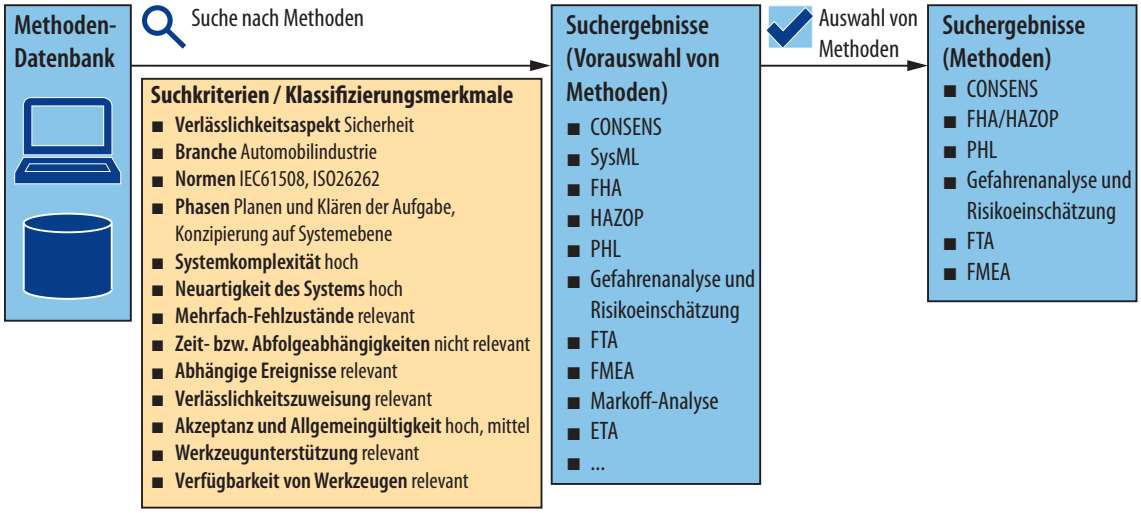


Bild 5-3: Suche und Auswahl von Methoden zur Absicherung der Sicherheit des Chamäleons in den frühen Phasen der Konzipierung

Die Ausprägungen der meisten Klassifizierungsmerkmale ergeben sich aus der Charakterisierung der Entwicklungsaufgabe in Phase 1. Für das Validierungsbeispiel stehen im Kontext des vorliegenden Kapitels die Konzipierungsphasen „Planen und Klären der Aufgabe“ und „Konzipierung auf Systemebene“ im Mittelpunkt. Darüber hinaus werden folgende Merkmale im Hinblick auf die zuverlässigkeits- bzw. sicherheitsbezogenen Eigenschaften des Systems als Basis für die Methodensuche ins Kalkül gezogen: Die zu verwendenden Analysemethoden sollten eine quantitative Aufteilung von Sicherheitsanforderungen unterstützen. Der erforderliche Ausbildungsstand spielt bei der Auswahl der zu verwendenden Analysemethoden eine geringe Rolle. Die Akzeptanz der Methode ist insbesondere im Hinblick auf den Nachweis der Sicherheit für Kunden und Behörden ein wichtiges Auswahlkriterium. Eine Werkzeugunterstützung ist wünschenswert, wobei die Verfügbarkeit von Werkzeugen eine wichtige Rolle spielt.

Resultat ist eine Vorauswahl von Methoden aus der Methoden-Datenbank. Darauf basierend findet eine Auswahl von Methoden statt. Das skizzierte Vorgehen wird von der in Abschnitt 4.3 vorgestellten werkzeugtechnischen Umsetzung der Methodik zur Auswahl und Planung der Methoden unterstützt. Für die Absicherung der Sicherheit des Chamäleons wurden im Rahmen der vorliegenden Arbeit die Spezifikationstechnik CONSENS,

Funktionale Gefahrenanalyse FHA, Vorläufige Gefahrenliste PHL, Gefahrenanalyse und Risikoeinschätzung nach ISO 26262, Fehlzustandsbaumanalyse FTA und Fehlzustandsart- und -auswirkungsanalyse FMEA ausgewählt.

Als Alternativen für die einzusetzende Modellierungssprache standen CONSENS und die SysML zur Verfügung. Die Wahl fiel auf CONSENS aufgrund der starken Ausrichtung dieser Spezifikationstechnik auf fortschrittliche mechatronische Systeme und auf die Konzipierung. Wenngleich das Chamäleon als Nicht-Serienfahrzeug nach Maßgabe der IEC Norm 61508 entwickelt wird, wird die Gefahrenanalyse und Risikoeinschätzung nach ISO 26262 aufgrund ihrer starken Ausrichtung auf die automobiltechnischen Systeme für Teilaspekte der Absicherung herangezogen. Ferner wurde festgelegt, dass die funktionale Gefahrenanalyse FHA zusammen mit einer Hazard and Operability Study HAZOP zum Einsatz kommen wird, und zwar auf Basis einer ersten vorläufigen Beschreibung der Funktionalität des Chamäleons. Mit der kombinierten FHA und HAZOP können Gefahren auf Gesamtsystemebene leitwortorientiert ermittelt werden.

Nachdem die Auswahl der zu verwendenden Methoden getroffen wurde, findet die Planung des Einsatzes der Methoden statt. Diese wird ebenfalls von der werkzeugtechnischen Umsetzung der Methodik zur Auswahl und Planung von Methoden unterstützt. Basis für die Planung stellen die Input-Output-Diagramme der Methoden dar (vgl. hierzu auch Abschnitt 3.2). Berücksichtigt wird ferner der in der Methoden-Datenbank abgebildete Zusammenhang zwischen der jeweiligen Methode und der zugehörigen Phase des Referenzprozesses.

Tabelle 5-1 fasst die mit Hilfe der Methoden-Datenbank ausgewählten Methoden zusammen und stellt deren Inputs und Outputs dar (vgl. hierzu auch die Input-Output-Diagramme der Methoden in Abschnitt 3.2). Ebenso abgebildet wird die zugehörige Phase des Referenzprozesses für die Konzipierung (vgl. Abschnitt 3.1.4). Selbstredend können auf eine analoge Weise auch andere (z.B. unternehmensspezifische) Produktentwicklungsprozessmodelle als Basis verwendet werden. Im Rahmen der Auswahl der Methoden findet auch eine weitere Anpassung an die zugrunde liegende Entwicklungsaufgabe und den Entwicklungsprozess statt. Zum Beispiel wird festgelegt, dass die in der Konzipierung auf Systemebene durchzuführenden FMEA und FTA auf Basis der vorläufigen Architekturannahmen stattfinden und zur Erstellung eines funktionalen Sicherheitskonzepts eingesetzt werden.

Auf dieser Basis erfolgt die Planung des Einsatzes der Methoden. Insbesondere werden die Reihenfolge des Einsatzes der Methoden sowie der Zeitpunkt bezogen auf den Produktentwicklungsprozess festgelegt. Einige der Methoden aus Tabelle 5-1 werden in der Konzipierungsphase „Planen und Klären der Aufgabe“ auf Basis der Spezifikation der Produktkonzeption in dem bis dahin vorliegenden Stand durchgeführt; Bild 5-4 stellt das Ergebnis der Planung des Methodeneinsatzes für diese Phase graphisch dar. Andere Methoden kommen in der Konzipierungsphase „Konzipierung auf Systemebene“ zum Einsatz, wobei auch ein Einsatz im Rahmen der „Konzipierung auf Subsystemebene“ für die Untersuchung der Subsysteme möglich ist (Bild 5-5).

Die Auswahl und Planung des Einsatzes der Methoden wird im Sicherheitsplan dokumentiert, welcher ein Hilfsmittel zur Planung, Management und Durchführung von sicherheitsbezogenen Aktivitäten in der Produktentwicklung darstellt (Arbeitspakete, Zieltermine, Meilensteine, Arbeitsprodukte, Verantwortlichkeiten, Ressourcen etc.) und typischerweise ein Teil des Projektplans ist [ISO26262-1, S. 15].

Tabelle 5-1: Mit Hilfe der Methoden-Datenbank ausgewählte Methoden, ihre Inputs, Outputs und die zugehörige Phase im Produktentwicklungsprozess

Nr.	Inputs	Analysemethode	Outputs	Phase
1	● vorläufige Funktionsbeschreibung	**Funktionale Gefahrenanalyse FHA**	● Gefahren auf Gesamtsystemebene	Planen und Klären der Aufgabe
2	● Umfeldmodell ● Anwendungsszenarien	**Vorläufige Gefahrenliste PHL**	● Gefahren auf Gesamtsystemebene ● Gefahrenauswirkungen auf Gesamtsystemebene	Planen und Klären der Aufgabe
3	● Umfeldmodell ● Anwendungsszenarien ● vorläufige Funktionsbeschreibung	**Gefahrenanalyse und Risikoeinschätzung**	● Gefahren auf Gesamtsystemebene ● Gefahrenbringende Ereignisse auf Gesamtsystemebene ● Risikoeinschätzung ● Sicherheitsziele mit ASIL-Einstufungen	Planen und Klären der Aufgabe
4	● Umfeldmodell ● Anwendungsszenarien ● vorläufige Funktionsbeschreibung ● Sicherheitsziele mit ASIL-Einstufungen ● vorläufige Architekturannahmen	**(Vorläufige) Fehlzustandsart- und -auswirkungsanalyse FMEA hinsichtlich Sicherheit**[1]	● sicherheitsrelevante Ausfallmöglichkeiten/Gefahren ● Gefahrenauswirkungen ● Gefahrenursachen ● Vermeidungsmaßnahmen (funktionale Sicherheitsanforderungen) ● Risikoeinschätzung (Risikoprioritätszahl)	Konzipierung auf Systemebene
5	● Umfeldmodell ● Anwendungsszenarien ● vorläufige Funktionsbeschreibung ● Sicherheitsziele mit ASIL-Einstufungen ● vorläufige Architekturannahmen	**(Vorläufige) Fehlzustandsbaumanalyse FTA hinsichtlich Sicherheit**[1]	● sicherheitsrelevante Ausfallmöglichkeiten/Gefahren ● Gefahrenauswirkungen insb. Ausfallfortpflanzung ● Vermeidungsmaßnahmen (funktionale Sicherheitsanforderungen)	Konzipierung auf Systemebene

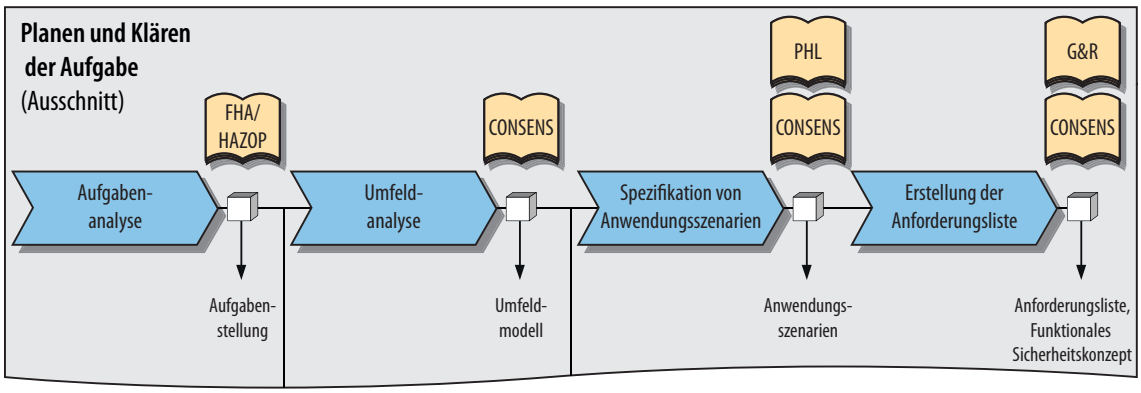
ASIL – Automotive Sicherheits-Integritätslevel

[1] – Auf Basis der Analyseergebnisse entsteht das Funktionale Sicherheitskonzept, welches die ermittelten funktionalen Sicherheitsanforderungen an das zu entwickelnde System beschreibt und diese den vorläufigen Architekturelementen zuordnet. [ISO26262-3, S. 12].

5.5 Phase 3 – Erweiterung/Anpassung der Modellierungssprache

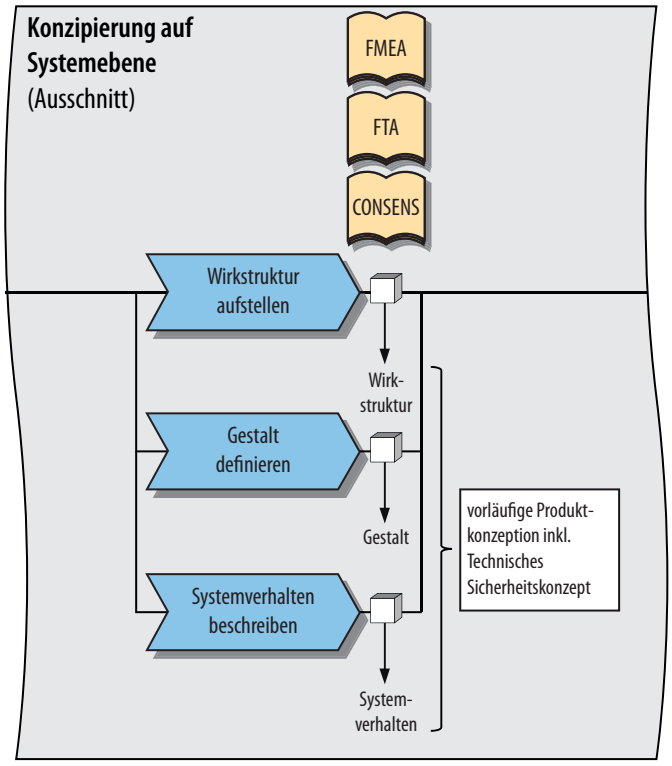
In dieser Phase wird die zu verwendende Modellierungssprache derart erweitert, dass sich die in Phase 2 ausgewählten Methoden auf Basis der Spezifikation der Produktkonzeption

durchführen lassen. Wie in Abschnitt 4.4 erklärt, werden hierzu das Metamodell und die graphische Notation der Spezifikationstechnik CONSENS erweitert. Erweiterungen der Spezifikationstechnik CONSENS, die im Rahmen der Validierung der Systematik am Chamäleon umgesetzt wurden, betreffen schwerpunktmäßig die Partialmodelle Anforderungen, Anwendungsszenarien, Funktionen sowie Umfeld/Wirkstruktur (vgl. die Leitlinie zur Erweiterung der Spezifikationstechnik CONSENS, Abschnitt 4.4.2).



PHL: Vorläufige Gefahrenliste FHA: Funktionale Gefahrenanalyse HAZOP: Hazard and Operability Study G&R: Gefahrenanalyse und Risikoeinschätzung

Bild 5-4: Einbettung der ausgewählten Methoden in die Konzipierungsphase „Planen und Klären der Aufgabe“



FMEA: Fehlzustandsart- und -auswirkungsanalyse FTA: Fehlzustandsbaumanalyse

Bild 5-5: Einbettung der ausgewählten Methoden in die Konzipierungsphase „Konzipierung auf Systemebene“; dargestellt ist eine zeitliche Einordnung hinsichtlich der Inputs und Outputs der jeweiligen Methode

Die Spezifikation der Anwendungsszenarien gilt als einer der wesentlichen Inputs für die Methoden PHL und die Gefahrenanalyse und Risikoabschätzung. Auf Basis der Input-Output-Diagramme der beiden Methoden (vgl. Abschnitt 3.2) lässt sich festhalten, dass

die Beschreibung eines Anwendungsszenarios die Spezifikation der gefahrenbringenden Ereignisse, der potentiellen Gefahren (auf Gesamtsystemebene) und deren Auswirkungen sowie die zugehörige Risikoeinschätzung und Sicherheitsziele umfassen sollte. Bild 5-6 zeigt eine beispielhafte Vorlage für die Beschreibung eines Anwendungsszenarios, welche die Abbildung der sicherheitsrelevanten Informationen berücksichtigt.

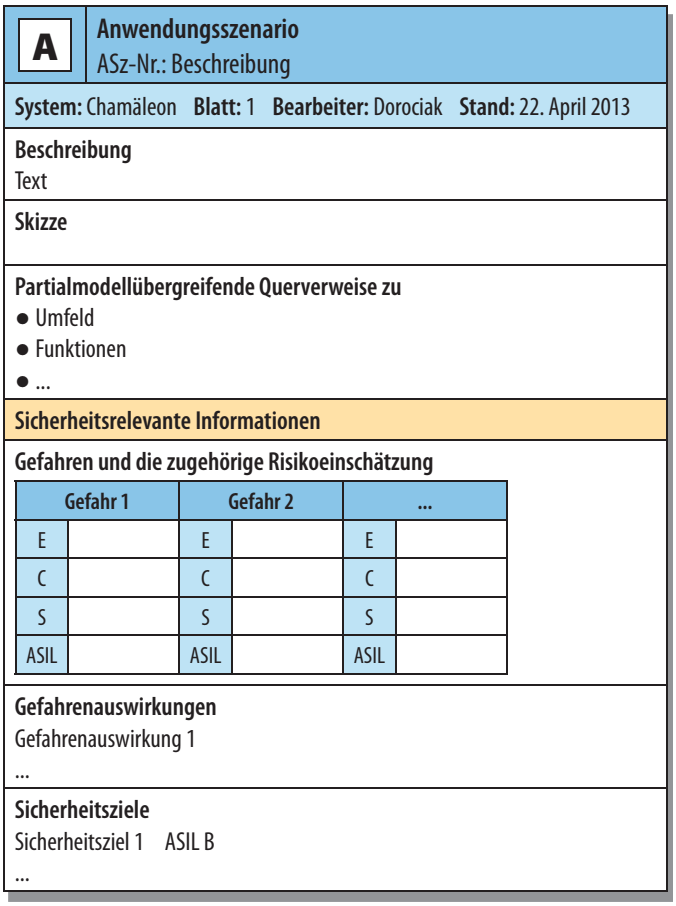


Bild 5-6: Eine erweiterte Vorlage für die Beschreibung eines Anwendungsszenarios, welche die Beschreibung der zugehörigen sicherheitsrelevanten Informationen vorsieht (in Anlehnung an die Vorlage aus [GFD+08, S. 93]; der Bereich „Sicherheitsrelevante Informationen" stellt den Kern der Erweiterung dar)

Ebenso kommt im Rahmen der Validierung die in Abschnitt 4.4.3 beschriebene Erweiterung der Spezifikationstechnik CONSENS zum Einsatz, die eine integrative Durchführung einer FMEA und einer FTA auf Basis der Spezifikation der Produktkonzeption ermöglicht. Bild 5-7 fasst die zugehörigen Erweiterungen der Spezifikationstechnik CONSENS graphisch zusammen.

5.6 Phase 4 – Absicherung (Spezifikation, Analyse, Verbesserung)

Hier erfolgt die Absicherung der Zuverlässigkeit und Sicherheit des betrachteten Systems. Diese findet unter Verwendung der ausgewählten Analysemethoden auf Basis der Spezifikation der Produktkonzeption statt, die mit Hilfe der erweiterten Spezifikationstechnik (Ergebnis der Phase 3) modelliert wurde. Im Folgenden werden die einzelnen Spezifikations- und Analyseschritte für die Lenkfunktion des Chamäleons erklärt. Dies

geschieht entlang der einzelnen Phasen der Konzipierung (siehe Phase 2). In diesem Zusammenhang wird auch die Festlegung von Verbesserungsmaßnahmen erklärt. Das Ergebnis wird eine hinsichtlich Zuverlässigkeit und Sicherheit der Lenkfunktion verbesserte Spezifikation der Produktkonzeption sein.

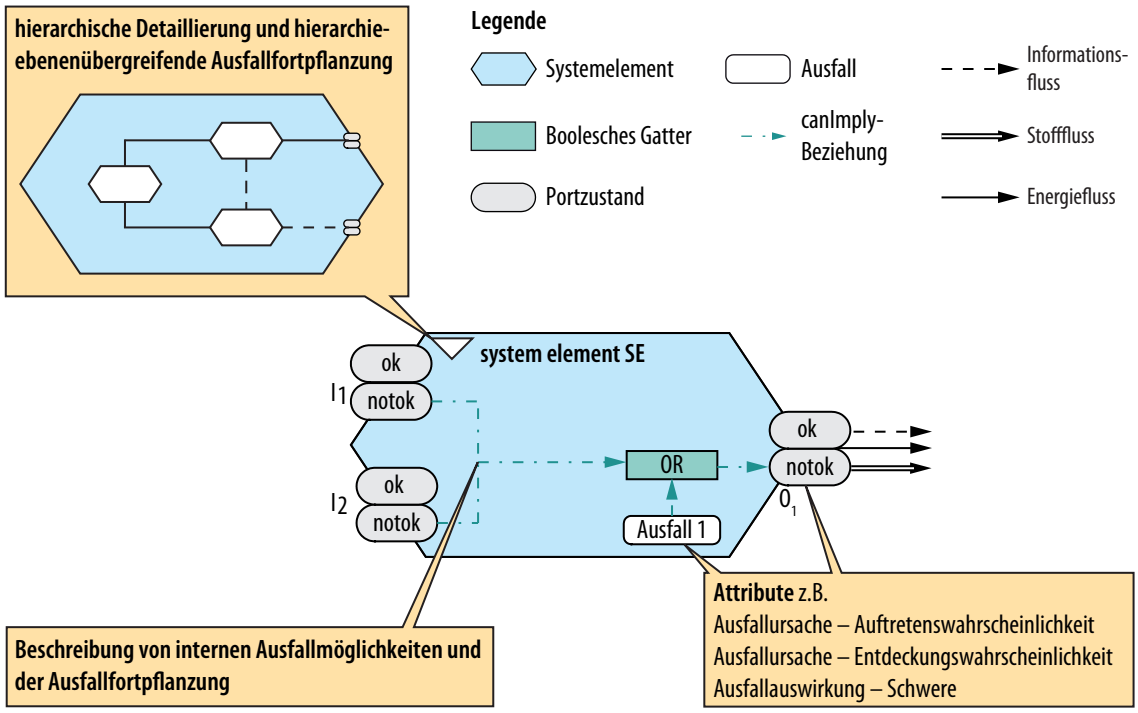


Bild 5-7: Erweiterung des Partialmodells Wirkstruktur um Konstrukte zur Beschreibung der Ausfallmöglichkeiten, Ausfallursachen, Ausfallauswirkungen sowie deren Beziehungen zueinander (Ausfallfortpflanzung)

Im Rahmen der Konzipierungsphase „Planen und Klären der Aufgabe“ findet zuerst eine Analyse der Entwicklungsaufgabe statt (vgl. Abschnitt 3.1.4), die bereits in Abschnitt 5.3 adressiert wurde. Daraus wurden insbesondere die wesentlichen Funktionen des Chamäleons deutlich: „Chamäleon antreiben“, „Chamäleon bremsen“, „Chamäleon lenken“, „Chamäleon federn“, „Chamäleon dämpfen“ und „mit dem Fahrer interagieren“ (Bild 5-8). Diese vorläufige Funktionsbeschreibung wird mit der fortschreitenden Konzipierung weiter verfeinert.

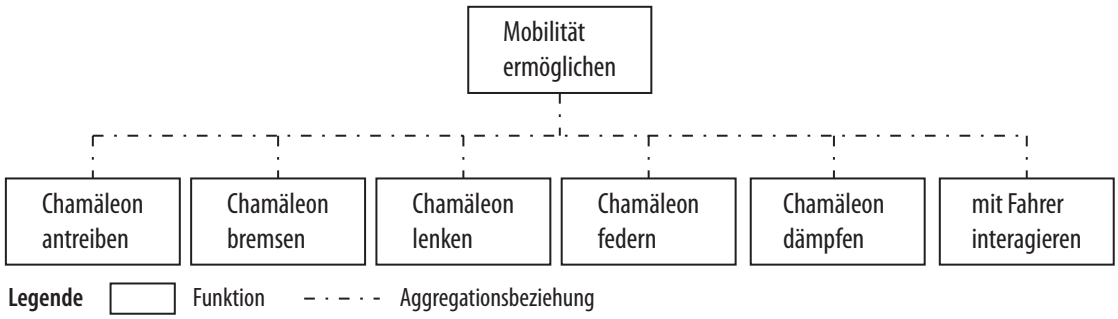


Bild 5-8: Vorläufige Beschreibung der Funktionen des Chamäleons auf Basis der Analyse der Entwicklungsaufgabe

Auf Basis dieser vorläufigen Funktionsbeschreibung kann eine erste funktionale Gefahrenanalyse durchgeführt werden. Die FHA-Analyse erfolgt hierbei in Kombination mit einer HAZOP-Analyse entlang der HAZOP-Leitworte „NO / FAILS“, „LESS / MORE“ und „INADVERTENT“. Tabelle 5-2 zeigt die Ergebnisse einer derartigen Analyse für die Funktion „Chamäleon lenken“. Die wesentlichen Gefahren sind: 1) unmotivierte Lenkbewegung während der Fahrt, 2) keine Lenkreaktion trotz Lenkwunsch und 3) ungewollte Änderung des Lenkwinkels während des Lenkvorgangs.

Tabelle 5-2: Ergebnisse einer funktionalen Gefahrenanalyse FHA unter Heranziehung von HAZOP-Leitworten für die Lenkfunktion des Chamäleons

Funktionale Gefahrenanalyse mit HAZOP-Leitworten			
System: Chamäleon **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 15. Februar 2013			
Nr.	**Funktion**	**Leitwort**	**Gefahr**
FH-1	Chamäleon lenken	INADVERTENT	Unmotivierte Lenkbewegung (ohne Fahrerwunsch) während der Fahrt
FH-2		NO / FAILS	keine Lenkreaktion trotz Lenkwunsch / Ausfall Lenkfunktion
FH-3		LESS / MORE	Änderung des Lenkwinkels (Vergrößerung bzw. Verkleinerung) während des Lenkvorgangs

Auf Basis der Analyseergebnisse kann eine Beschreibung der Fehlfunktionen des Systems erstellt bzw. um die ermittelten Gefahren erweitert werden (vgl. Abschnitt 4.4.2). Bild 5-9 stellt eine derartige vorläufige Beschreibung der Fehlfunktionen dar.

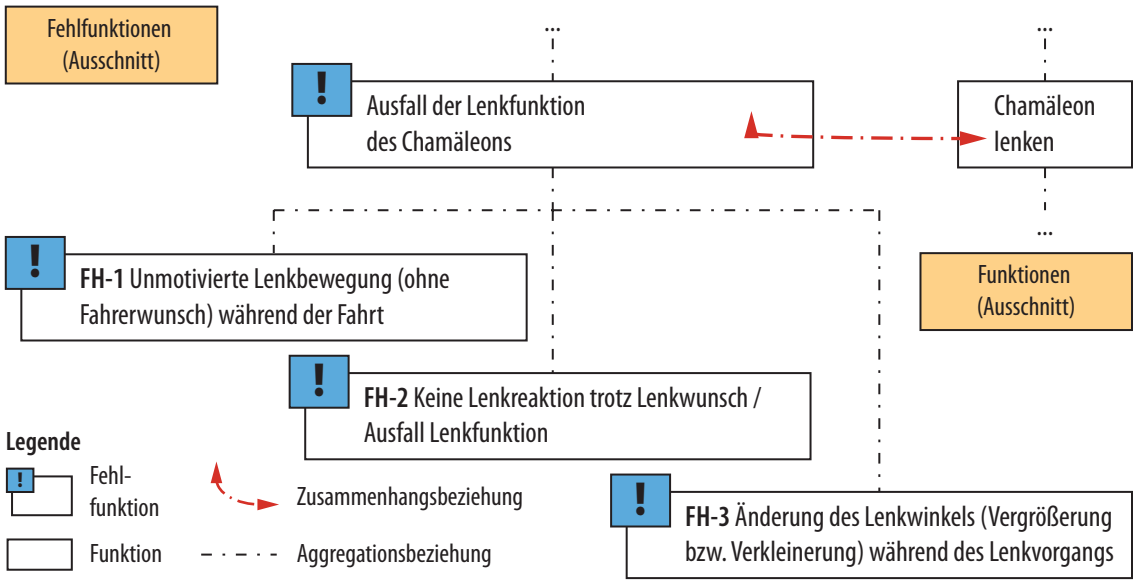


Bild 5-9: Vorläufige Beschreibung der Fehlfunktionen

Nach der Analyse der Aufgabenstellung findet gemäß des Referenzprozesses für die Konzipierung eine Umfeldanalyse statt (vgl. Abschnitt 3.1.4). Das Resultat ist ein Umfeldmodell (Bild 5-10). Aus der Darstellung im Umfeldmodell wird dabei insbesondere das folgende Merkmal der heutigen Straßenverkehrsinfrastruktur deutlich [Wro10, S. 25]: die

Personen- und Güterströme finden auf mehrspurigen Verkehrswegen statt. Diese Verkehrswege weisen zum Teil parallele Fahrbahnen für gleichgerichteten und entgegen gerichteten Verkehr auf. Immanent sind für die Straßenverkehrsinfrastruktur außerdem feststehende Einrichtungen wie Leitplanken, Verkehrsschilder etc.

Für die im Rahmen der FHA ermittelten Gefahren wird auf Basis des Umfeldmodells eine vorläufige Gefahrenliste erstellt (vgl. Abschnitt 3.2.1.1). Die Ergebnisse der FHA zeigen, dass ein erhebliches Gefahrenpotential darin besteht, dass ein Fahrzeugführer die Kontrolle über sein Fahrzeug verliert. Es ergeben sich folgende in der vorläufigen Gefahrenliste dokumentierte Gefahrenauswirkungen (Tabelle 5-3): 1) das Fahren in den Gegenverkehr, 2) Kollision mit anderen Verkehrsteilnehmern (z.B. mit anderen Fahrzeugen, mit Radfahrern, mit Fußgängern etc.), 3) Kollision mit fest stehenden Einrichtungen (z.B. Leitplanke, Verkehrsschild etc.) und 4) ein Auffahrunfall.

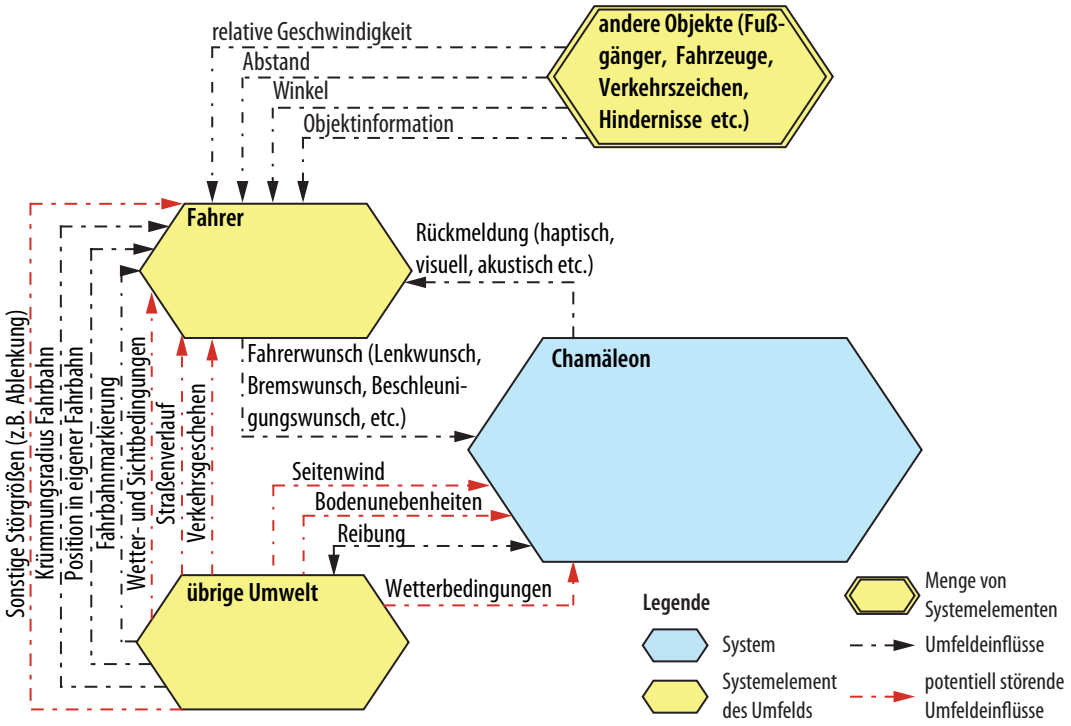


Bild 5-10: Umfeldmodell des Chamäleons (Ausschnitt); potentiell störende Einflüsse sind als solche gekennzeichnet

Für das Chamäleon lassen sich u.a. folgende Anwendungsszenarien (ASz) identifizieren:

- **ASz-1:** „Fahren mit niedriger Geschwindigkeit (bis 20 km/h)“,
- **ASz-2:** „Fahren mit mittlerer Geschwindigkeit (zwischen 21 km/h und 50 km/h)“,
- **ASz-3:** „Parkieren“,
- **ASz-4:** „Wenden bei langsamer Fahrt mit kleinstmöglichem Wendekreis“,
- **ASz-5:** „Testfahrten auf Testgelände“,

- **ASz-6:** „Aufladen des Akkumulators an einer Ladestation“,
- **ASz-7:** „Ausstellung auf einer Messe“,
- **ASz-8:** „Reparatur des Fahrzeugs“ und
- **ASz-9:** „Verwendung als Simulationsplattform“.

Tabelle 5-3: Vorläufige PHL für die Lenkfunktion des Chamäleons (Ausschnitt)

Preliminary Hazard List (PHL)		
System: Chamäleon **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 22. April 2013		
Einheit	**Gefahr**	**Gefahrenauswirkung**
Lenkfunktion des Chamäleons	**FH-1** Unmotivierte Lenkbewegung (ohne Fahrerwunsch) während der Fahrt	**HC-1** Kollision mit dem Gegenverkehr
		HC-2 Kollision mit anderen Verkehrsteilnehmern (z.B. andere Fahrzeuge, mit Radfahrern, mit Fußgängern etc.)
		HC-3 Kollision mit fest stehenden Einrichtungen (z.B. Leitplanke, Verkehrsschild etc.)
		HC-4 Auffahrunfall
	FH-2 keine Lenkreaktion trotz Lenkwunsch / Ausfall Lenkfunktion	**HC-1** Kollision mit dem Gegenverkehr
		HC-2 Kollision mit anderen Verkehrsteilnehmern
		HC-3 Kollision mit fest stehenden Einrichtungen
		HC-4 Auffahrunfall
	FH-3 Änderung des Lenkwinkels (Vergrößerung bzw. Verkleinerung) während des Lenkvorgangs	**HC-1** Kollision mit dem Gegenverkehr
		...

Das Anwendungsszenario „ASz-1: Fahren mit niedriger Geschwindigkeit (bis 20 km/h)“ ist in Bild 5-11 als ein Steckbrief dargestellt. Dieser umfasst neben allgemeinen Angaben wie Name des Anwendungsszenarios, Stand und Bearbeiter auch eine textuelle Beschreibung des Anwendungsszenarios sowie eine Skizze zur graphischen Veranschaulichung des Anwendungsszenarios. Sicherheitsrelevante Informationen liegen in einer ersten Konkretisierung der Beschreibung noch nicht vor und werden mit dem zunehmenden Fortschreiten der Konzipierung als Resultat von Sicherheitsanalysen ergänzt.

Anschließend wird die Gefahrenanalyse und Risikoeinschätzung nach ISO 26262 für die Lenkfunktion des Chamäleons durchgeführt. Hierzu werden Kombinationen von Anwendungsszenarien und der mit der FHA ermittelten Gefahren beurteilt (vgl. auch Abschnitt 3.2.2.1). Tabelle 5-4 fasst ausgewählte Ergebnisse der Analyse zusammen. Demnach ist das gefahrenbringende Ereignis einer unmotivierten Lenkbewegung bei einer Fahrt bei mittlerer Geschwindigkeit als am sicherheitskritischsten einzustufen. Es wird folglich mit einem ASIL-Level C versehen. Bezogen auf eine Fahrt bei einer niedrigen Geschwindigkeit ist das Auftreten einer unmotivierten Lenkbewegung weniger sicherheitskritisch. Die Gründe: die Schwere eines möglichen Schadens ist niedriger und die Beherrschbarkeit der Fahrsituation durch den Fahrer ist höher. Ein derartiges gefahrenbringendes Ereignis ist daher mit einem kleineren ASIL A einzustufen.

A **Anwendungsszenario**
ASz-1: Fahren mit niedriger Geschwindigkeit (bis 20 km/h)

System: Chamäleon **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 22. April 2013

Beschreibung
Gemeint ist das Fahren mit niedriger Geschwindigkeit. Niedrig bedeutet in diesem Zusammenhang kleiner 20 km/h. Als Bedienelement dient ein Joystick, mit dem die Längs- und Querbewegung des Fahrzeugs angesteuert werden kann. Konkret erfolgt über den Joystick die Fahrtrichtungsvorgabe bzw. der Lenkwunsch sowie die Antriebsvorgabe (Beschleunigen bzw. Abbremsen).

Skizze

Partialmodellübergreifende Querverweise zu
- Umfeld

Bild 5-11: Anwendungsszenario „ASz-1: Fahren mit niedriger Geschwindigkeit (bis 20 km/h)“

Tabelle 5-4: Gefahrenanalyse und Risikoeinschätzung für die Lenkfunktion des Chamäleons (in Anlehnung an [Wro10, S. 137f.], [LPP10, S. 215ff.])

Gefahren- und Risikoanalyse für die Lenkfunktion des Chamäleons

System: Chamäleon **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 15. Februar 2013

Nr.	Anwendungsszenarien / Gefahren	**ASz1** Fahren bei niedriger Geschwindigkeit		**ASz2** Fahren bei mittlerer Geschwindigkeit		**ASz3** Parkieren		...	ASIL-Level
1	**FH-1** Unmotivierte Lenkbewegung (ohne Fahrerwunsch) während der Fahrt	E	E4	E	E4	E	E4		ASIL C
		C	C2	C	C3	C	C1		
		S	S1	S	S2	S	S1		
		ASIL	ASIL A	ASIL	ASIL C	ASIL	QM		
2	**FH-2** keine Lenkreaktion trotz Lenkwunsch / Ausfall Lenkfunktion	E	E4	E	E4	E	E4		ASIL C
		C	C2	C	C3	C	C1		
		S	S1	S	S2	S	S1		
		ASIL	ASIL A	ASIL	ASIL B	ASIL	QM		
3	**FH-3** Änderung des Lenkwinkels (Vergrößerung bzw. Verkleinerung) während des Lenkvorgangs	E	E4	E	E4	E	E4		ASIL A
		C	C1	C	C1	C	C1		
		S	S1	S	S2	S	S1		
		ASIL	QM	ASIL	ASIL A	ASIL	QM		

Da es sich aber beim Chamäleon nicht um ein Serienfahrzeug handelt, ist die IEC 61508 und nicht die ISO 26262 maßgebend. Dennoch wurde zur Bestimmung der notwendigen

Risikominderung die Gefahrenanalyse und Risikoeinschätzung nach ISO 26262 herangezogen und die Automotive-Sicherheits-Integritätslevel verwendet. Eine derartige Abweichung ist möglich, soweit eine gute Begründung vorliegt. In diesem konkreten Fall ist die Abweichung darin begründet, dass die ISO 26262 auf die spezifischen Gegebenheiten der Kraftfahrzeuge wesentlich besser zugeschnitten ist als die Grundnorm IEC 61508. Da jedoch die meisten der weiteren Aktivitäten des Sicherheitslebenszyklus nach Maßgabe der IEC 61508 durchgeführt werden, ist eine Festlegung des Sicherheits-Integritätslevels SIL notwendig. Hierzu wird die in Tabelle 5-5 dargestellte Äquivalenz-Matrix verwendet. Die gefahrenbringenden Ergebnisse aus Tabelle 5-4 erhalten demnach die folgenden SIL-Einstufungen: FH-1 und FH-2 werden mit SIL 2 und FH-3 mit SIL 1 versehen.

ISO 26262	IEC 61508	Anmerkungen
ASIL	SIL	
	SIL 4	Im Automotive-Bereich keine elektronischen Systeme mit SIL-4-Anforderungen
ASIL D	SIL 3	Ein ASIL-D-System ist ein SIL-3-System, jedoch nicht umgekehrt
ASIL C	s. Anmerkungen	Entwurfsanforderungen in etwa SIL 2 Verifikationsanforderungen in etwa SIL 3
ASIL B	SIL 2	
ASIL A	SIL 1	
QM		

Dies ist nur eine Leitlinie. Dennoch müssen die ASIL-x-Anforderungen erfüllt sein, wenn ein als SIL y entwickeltes System in einer ASIL-x-Anwendung eingesetzt werden soll und umgekehrt.

Tabelle 5-5: Gegenüberstellung von SIL (IEC 61508) und ASIL (ISO 26262) [LPP10, S. 15]

5.6.1 Sicherheitsziele und sicherer Zustand

Auf Basis der Ergebnisse der Gefahrenanalyse und Risikoeinschätzung erfolgt, wie in Abschnitt 3.2.2.1 beschrieben, die Festlegung der Sicherheitsziele [ISO26262-3, S. 11]. Tabelle 5-6 fasst die Sicherheitsziele für die Lenkfunktion des Chamäleons, die zugehörigen Gefahren aus der Gefahrenanalyse und Risikoeinschätzung und die SIL-Einstufung zusammen. Für jedes der festgelegten Sicherheitsziele wird, sofern möglich, ein sicherer Zustand definiert [ISO26262-3, S. 11]. Kommt es zu einem Fehler mit Sicherheitszielverletzungspotential, so muss in den sicheren Zustand übergangen werden (vgl. auch Abschnitt 2.1.5.3).

Bei einem reinen Steer-by-Wire-System ohne mechanische Rückfallebene wie dem Chamäleon kommt es darauf an, dass auch im Fehlerfall die komplette bzw. eingeschränkte Lenkfunktion verfügbar bleibt. Die Verfügbarkeit des Fahrzeug trotz eines aufgetretenen Fehlers muss erhalten bleiben, da im Gegensatz zu Systemen mit mechanischer Rückfallebene kein sicherer Zustand nach dem Ausfall einer Komponente existiert [PH13, S. 457],

[WIH+04, S. 6]. Es handelt sich also um ein Fail-Operational-System gemäß der Definition aus Abschnitt 2.1.5.3. Bild 5-12 zeigt eine Gegenüberstellung der Strategien zum Umgang mit Ausfällen in einem Fail-Safe- und in einem Fail-Operational-System.

Tabelle 5-6: Liste von Sicherheitszielen für die Lenkfunktion des Chamäleons

Liste von Sicherheitszielen für die Lenkfunktion des Chamäleons			
System: Chamäleon **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 15. Februar 2013			
Nr.	**Sicherheitsziel**	**zugehörige Gefahr**	**SIL**
SZ1	Unmotivierte Lenkbewegung (ohne Fahrerwunsch) während der Fahrt vermeiden	**FH-1** Unmotivierte Lenkbewegung (ohne Fahrerwunsch) während der Fahrt	SIL 2*
SZ2	Ausfall Lenkfunktion (keine Lenkreaktion trotz Lenkwunsch) vermeiden	**FH-2** keine Lenkreaktion trotz Lenkwunsch / Ausfall Lenkfunktion	SIL 2*
SZ3	Änderung des Lenkwinkels (Vergrößerung bzw. Verkleinerung) während des Lenkvorgangs vermeiden	**FH-3** Änderung des Lenkwinkels (Vergrößerung bzw. Verkleinerung) während des Lenkvorgangs	SIL 1

* – SIL 2 für Entwurfsanforderungen, SIL 3 für Verifikationsanforderungen

Dieser schrittweise Übergang von einem fehlerfreien Zustand über Warnzustände bzw. Betriebszustände mit eingeschränkter Funktionsfähigkeit bis hin zu einem sicheren Zustand wird als Warn- und Degradationskonzept bezeichnet [ISO26262-1, S. 18]. Bild 5-13 zeigt ein beispielhaftes Warn- und Degradationskonzept für das Chamäleon, welches in Anlehnung an die Publikationen von PFEFFER/HARRER und WINNER ET AL. definiert wurde [PH13, S. 457], [WIH+04, S. 7f.]:

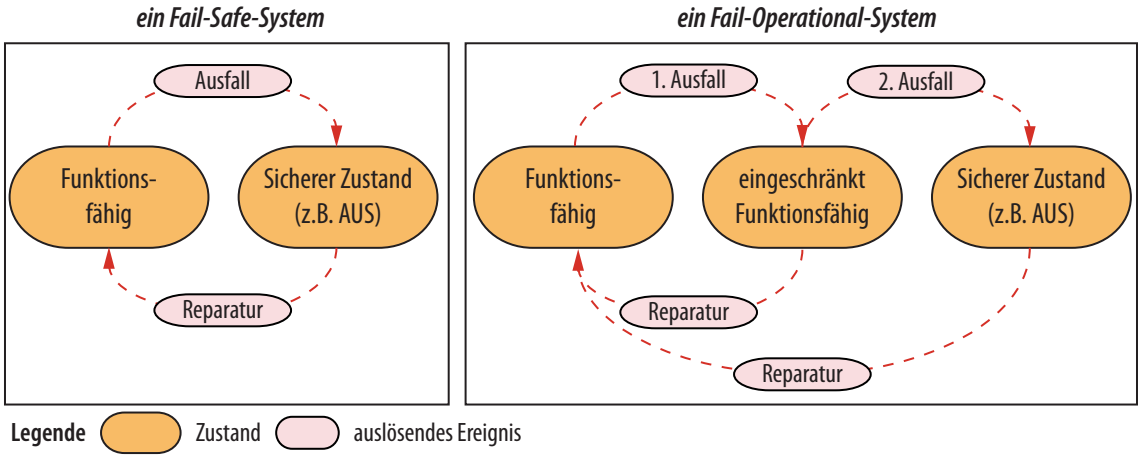


Bild 5-12: Strategien zum Umgang mit Ausfällen in einem Fail-Safe- und einem Fail-Operational-System (vereinfachte Darstellung; in Anlehnung an [Wro10, S. 26])

Im Falle des Ausfalls des Force-Feedback-Aktors (E1) kann das Fahrzeug nach wie vor betrieben werden. Der Fahrer wird über eine Warnlampe und eine Fehleranzeige (z.B. „Ausfall Force-Feedback“) informiert. Das Fahrzeug bleibt für den Fahrer beherrschbar. Fällt ein Lenkwinkelsensor eines Radmoduls aus, kann die Lenkfunktion nur einge-

schränkt dargestellt werden. Als Fehlerreaktion eignen sich eine Begrenzung der Maximalgeschwindigkeit und eine Fahrerwarnung; ein sicherer degradierter Betriebszustand kann so erreicht werden. Bei Ausfall des Lenkmotors wird die Lenkfunktion unter Umständen stark beeinträchtigt. In diesem Fall wird in einen Notlauf-Betrieb gewechselt, der durch eine weitere Reduzierung der Maximalgeschwindigkeit (z.B. auf max. 8 km/h) charakterisiert ist. Die Restfunktionalität ist dabei für eine gegebene Restfahrstrecke bzw. Restbetriebsdauer mit einer ausreichend niedrigen Ausfallwahrscheinlichkeit zu gewährleisten, so dass das Fahrzeug durch den Fahrer in den Stillstand gebracht werden kann („Limp Home“) [WIH+04]. Zusätzlich kann die Regelungsstrategie auf Lenkung mit dem Antriebsmotor des betroffenen Radmoduls umgeschaltet werden [Lur14]: Hier kann das Rad je nach Situation einzeln abgebremst oder beschleunigt werden[49]. Bei Ausfall eines weiteren Aktors (z.B. des Antriebsmotors) muss ein Übergang in den endgültigen sicheren Zustand eingeleitet werden – hierzu wird eine Restfunktion für eine kurze Zeit bereitgestellt und das Fahrzeug ggf. auch mit einer aktiv eingeleiteten Abbremsung zum Stillstand gebracht [PH13, S. 457], [WIH+04].

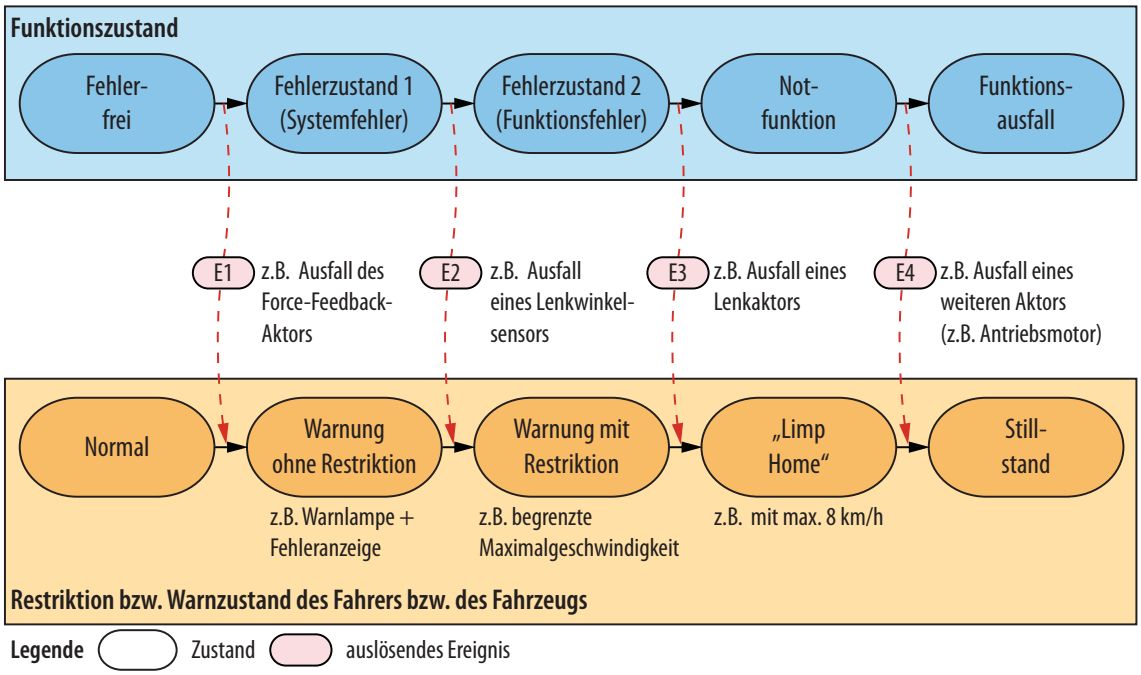


Bild 5-13: Beispielhaftes Warn- und Degradationskonzept für das Chamäleon (in Anlehnung an [PH13, S. 457], [WIH+04, S. 7f.])

5.6.2 Funktionales Sicherheitskonzept

Basierend auf dem in Bild 5-1 dargestellten grundsätzlichen Aufbau eines Steer-by-Wire-Systems ohne mechanische Rückfallebene sowie den Ergebnissen aus der Konzipierungsphase „Planen und Klären der Aufgabe“ werden in der „Konzipierung auf Systemebene“

[49] Das Funktionsprinzip ähnelt dem eines Elektronischen Stabilitätsprogramms (ESP), wo eine gezielte Abbremsung der ausgewählten Räder möglich ist.

erste Annahmen bzgl. der Systemstruktur getroffen. Diese vorläufige Systemstruktur umfasst die Systemelemente Joystick, Energieversorgung, Informationsverarbeitung und für jedes Radmodul jeweils die Systemelemente Lenkwinkelsensor, Lenkmotor, Mechanik (Bild 5-14). Die Mechanik stellt die Verbindung zwischen Lenkmotor und Rad dar und umfasst den Lenkhebel, die Lenkstange und den Radträger. Auf dieser Basis erfolgt die Spezifikation der Ausfallfortpflanzung gemäß der in Abschnitt 4.4.3 vorgestellten Methode. Für jedes Systemelement werden seine internen Ausfallmöglichkeiten spezifiziert und mit Hilfe von Booleschen Gattern zueinander in Bezug gesetzt. Ebenso werden für die Flüsse die Ausfallmöglichkeiten untersucht und abgebildet. Gemeint sind hierbei insbesondere Übertragungsfehler etc. Die so erstellte Spezifikation der Ausfallfortpflanzung ist in Bild 5-14 zu sehen.

Tabelle 5-7 beinhaltet die Beschreibung der in Bild 5-14 beschriebenen Ausfälle. Die Verletzung des Sicherheitsziels SZ1 „Unmotivierte Lenkbewegung (ohne Fahrerwunsch) während der Fahrt vermeiden“ wird durch den Portzustand „nok“ des Ports „O1“ des Systemelements „Mechanik“ dargestellt. Durch eine rückwärtsgerichtete Verfolgung der Ausfallfortpflanzungspfade können in der Spezifikation der Ausfallfortpflanzung die möglichen Ursachen für die Sicherheitszielverletzung gefunden werden.

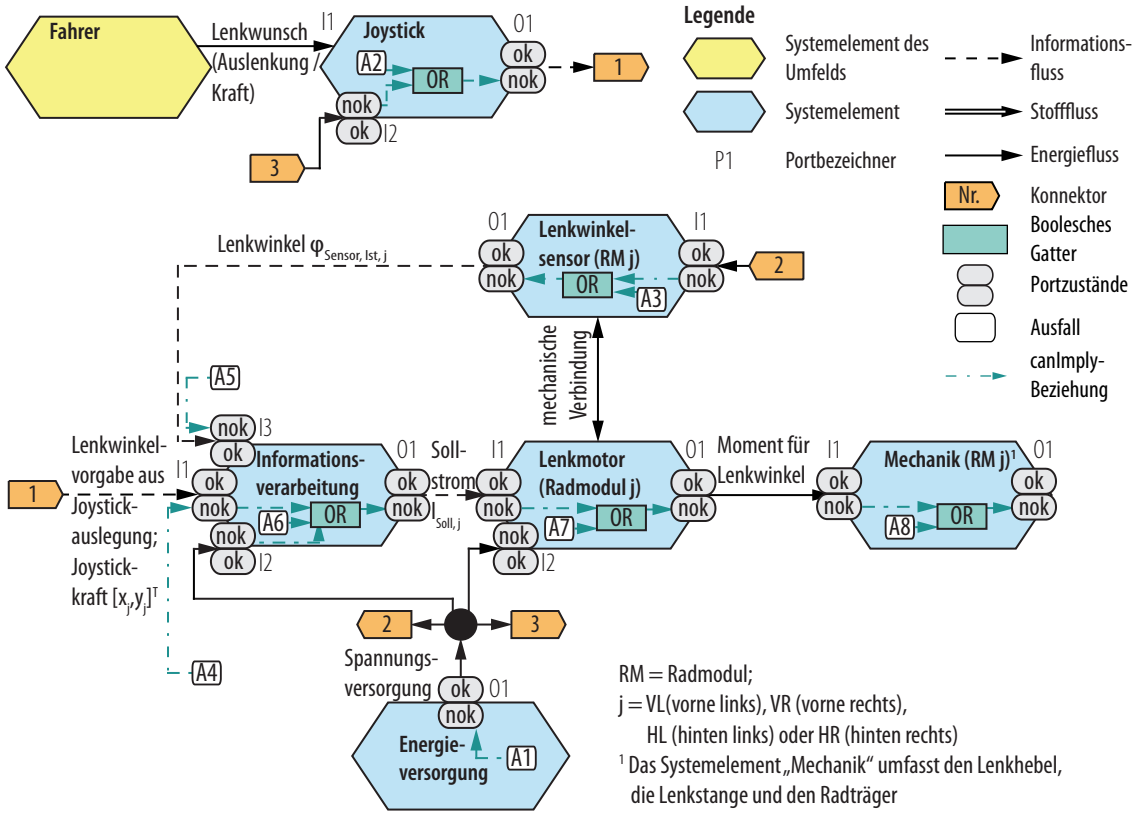


Bild 5-14: Spezifikation der Ausfallfortpflanzung in der vorläufigen Systemstruktur für das Sicherheitsziel SZ1 (Ausschnitt; für die Beschreibung der einzelnen Ausfälle siehe Tabelle 5-7); der Force-Feedback-Regelkreis ist nicht dargestellt

Aus dem in der Spezifikation der Produktkonzeption abgebildeten Informationen und deren Zusammenhänge lässt sich eine FMEA-Tabelle automatisiert erzeugen. Tabelle 5-8 zeigt eine derartige FMEA-Tabelle für das Validierungsbeispiel. Die Vollständigkeit der so erzeugten FMEA-Tabelle hängt in hohem Maße von der Vollständigkeit der Ausfallspezifikation innerhalb der Produktkonzeption statt. Im Zuge der fortschreitenden Konzipierung findet die Verfeinerung der Spezifikation der Produktkonzeption und der Spezifikation der Ausfallfortpflanzung statt. Die anfangs nur rudimentär beschriebenen Ausfallmöglichkeiten wie „Ausfall Lenkwinkelsensor“ werden genauer spezifiziert. Dies gilt auch für die Ausfallursachen und Auswirkungen. Zum Beispiel kann der vorerst allgemein beschriebene Ausfall „Keine Spannungsversorgung bzw. Spannungsversorgung störend beeinflusst (z.B. Über-, Unterspannung)“ in folgende Ausfallmöglichkeiten verfeinert werden: „Drift“, „Oszillation“, „Unterspannung“, „Überspannung“, „Spannungsspitzen“, wobei Checklisten wie die aus der ISO26262 herangezogen werden können [ISO26262-5, S. 41].

Tabelle 5-7: Beschreibung der in Bild 5-14 spezifizierten Ausfälle

Ausfallbezeichnung	Beschreibung
Energieversorgung.A1	Ausfall Energieversorgung
Energieversorgung.O1.nok	Keine Spannungsversorgung bzw. Spannungsversorgung störend beeinflusst (z.B. Über-, Unterspannung)
Joystick.A2	Ausfall Joystick
Joystick.O1.nok	Joystick stellt keine bzw. falsche Lenkwinkelvorgabe bereit
Lenkwinkelsensor.A3	Ausfall Lenkwinkelsensor
Lenkwinkelsensor.O1.nok	Lenkwinkelsensor stellt aufgrund eines Ausfalls keine bzw. falsche Lenkwinkelinformation bereit
A4	Übertragungsfehler Lenkwinkelvorgabe
A5	Übertragungsfehler Lenkwinkelinformation
Informationsverarbeitung.A6	Fehler in der Informationsverarbeitung
Informationsverarbeitung.O1.nok	Aufgrund eines Fehlers stellt die Informationsverarbeitung einen falschen bzw. keinen Sollstrom bereit
Lenkmotor.A7	Ausfall Lenkmotor
Lenkmotor.O1	Der Lenkmotor stellt aufgrund eines Fehlers keines bzw. falsches Moment für Lenkwinkel bereit
Mechanik.A8	Ausfall in der Mechanik
Mechanik.O1.nok	Es werden keine bzw. falsche Radeinschlagswinkel eingestellt, die von der gewünschten bzw. erwarteten abweicht

Ferner lässt sich aus der Spezifikation der Produktkonzeption ein Fehlzustandsbaum automatisiert generieren. Ein für die Untersuchung des Sicherheitsziels SZ1 „Unmotivierte Lenkbewegung (ohne Fahrerwunsch) während der Fahrt vermeiden“ auf Basis der Spezifikation der Produktkonzeption erzeugter Fehlzustandsbaum ist in Bild 5-15 zu sehen. Aus dieser Darstellung lassen sich insbesondere die kritischen Pfade erkennen, die potentiell zu einer Verletzung des Sicherheitsziels SZ1 führen können. Diese gilt es vor dem Hintergrund der Absicherung der funktionalen Sicherheit zu untersuchen. Ferner ist aus dem Fehlzustandsbaum deutlich, dass der Ausfall der Energieversorgung ein Common

Cause Failure ist (Ausfall infolge gemeinsamer Ursache; vgl. Abschnitt 2.1.2). Es ist von zentraler Bedeutung derartige sicherheitskritische abhängige Ausfälle auszuschließen.

Tabelle 5-8: Eine auf Basis der Spezifikation der Produktkonzeption automatisiert erzeugte FMEA-Tabelle für die Lenkfunktion des Chamäleons

Fehlzustandsart- und -auswirkungsanalyse (FMEA)					
System: Chamäleon **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 18. Februar 2013					
Nr.	**Systemelement**	**Ausfallmöglichkeit**	**Ausfallauswirkung(en)**	**Ausfallursache(n)**	**...**
1	Energieversorgung	Ausfall Energieversorgung	Keine Spannungsversorgung bzw. Spannungsversorgung störend beeinflusst (z.B. Über-, Unterspannung)		...
2	Joystick	Ausfall Joystick	Joystick stellt keine bzw. falsche Lenkwinkelvorgabe bereit	Keine Spannungsversorgung bzw. Spannungsversorgung störend beeinflusst (z.B. Über-, Unterspannung)	...
3	Lenkwinkelsensor	Ausfall Lenkwinkelsensor	Lenkwinkelsensor stellt aufgrund eines Ausfalls keine bzw. falsche Lenkwinkelinformation bereit	Keine Spannungsversorgung bzw. Spannungsversorgung störend beeinflusst (z.B. Über-, Unterspannung)	...
4	Informationsverarbeitung	Fehler in der Informationsverarbeitung	Aufgrund eines Fehlers stellt die Informationsverarbeitung einen falschen bzw. keinen Sollstrom bereit	Keine Spannungsversorgung bzw. Spannungsversorgung störend beeinflusst (z.B. Über-, Unterspannung)	...
5	Lenkmotor	Ausfall Lenkmotor	Der Lenkmotor stellt aufgrund eines Fehlers keines bzw. falsches Moment für Lenkwinkel bereit	Keine Spannungsversorgung bzw. Spannungsversorgung störend beeinflusst (z.B. Über-, Unterspannung)	...
6	Mechanik	Ausfall in der Mechanik	Es werden keine bzw. falsche Radeinschlagswinkel eingestellt, die von der gewünschten bzw. erwarteten abweicht	S: Schwere der Ausfallauswirkung	...

Für die gefundenen Ausfallursachen werden Gegenmaßnahmen in Form von funktionalen Sicherheitsanforderungen definiert und in dem Fehlzustandsbaum abgebildet. Aus einer derartigen Analyse ergibt sich das funktionale Sicherheitskonzept für die Lenkfunktion des Chamäleons, welches die festgelegten funktionalen Sicherheitsanforderungen und deren Zuordnung zu den Systemelementen beschreibt (Tabelle 5-9).

Das Systemelement „Mechanik“ umfasst den Lenkhebel, die Lenkstange und den Radträger. Es repräsentiert die Verbindung zwischen dem Lenkmotor und dem Rad. Der Lenkmotor überträgt die rotatorische Bewegung des Motors mit Hilfe des Lenkhebels in eine translatorische Bewegung der Lenkstange. Die Bewegung der Lenkstange bewirkt über einen Hebel am Radträger eine Verdrehung des Radträgers und damit einhergehend des Rades um die Lenkachse [Lor08, S. 20]. Bild 5-16 stellt diesen Zusammenhang graphisch dar.

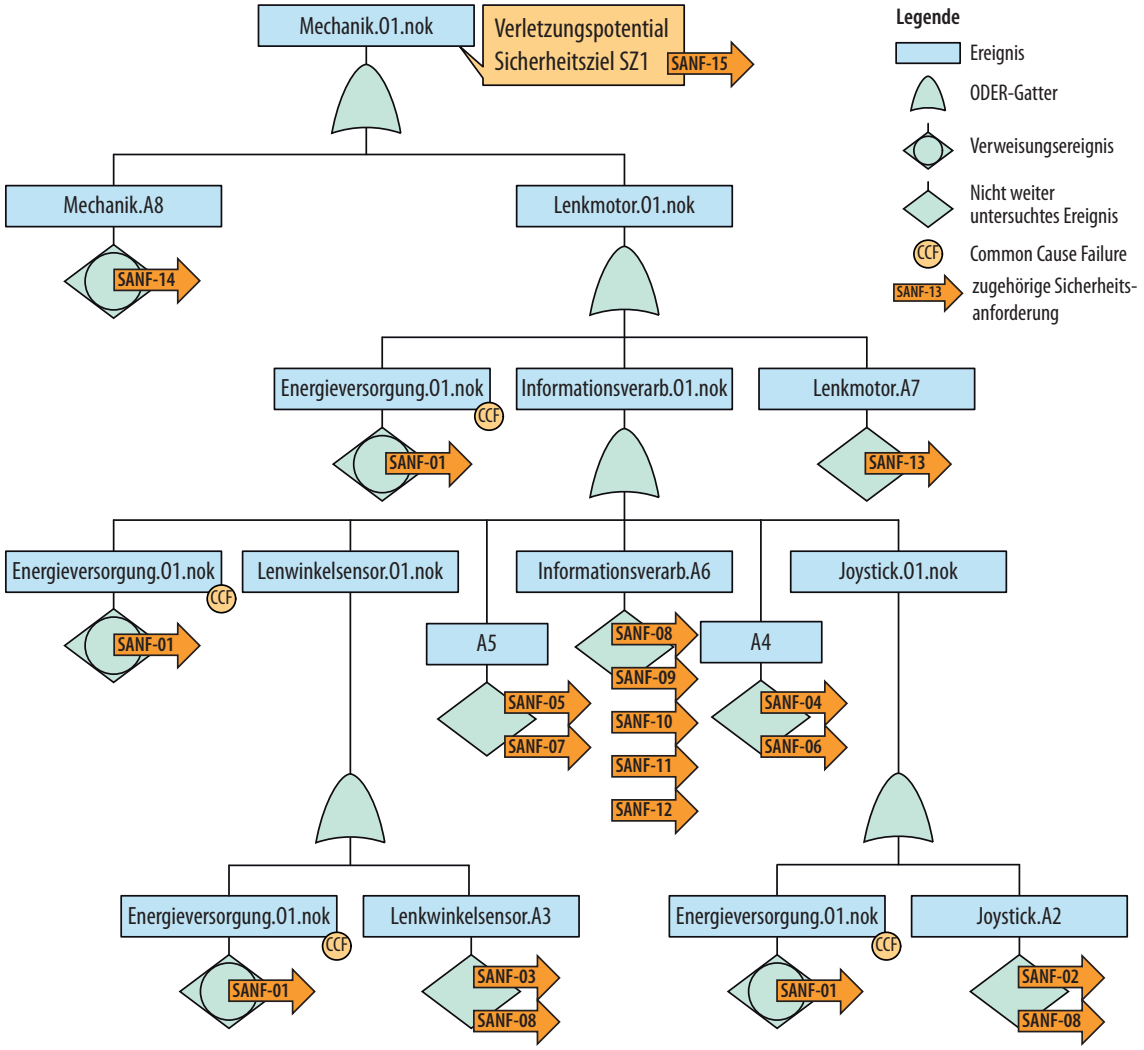


Bild 5-15: Ein aus der Spezifikation der Produktkonzeption automatisiert generierter Fehlzustandsbaum für die Untersuchung des Sicherheitsziels SZ1

5.6.3 Informationsverarbeitung des Chamäleons

Im Zuge der fortschreitenden Konzipierung wurde die Spezifikation der Produktkonzeption des Chamäleons weiter konkretisiert. Dies betrifft insbesondere die Beschreibung der Informationsverarbeitung des Chamäleons, welche die Selbstoptimierung realisiert. Hierfür wurde die Entwicklungssystematik zur Integration kognitiver Funktionen in selbstoptimierende Systeme verwendet [Dum11]. Zur Strukturierung der Informationsverarbeitung wurde dabei die OCM-Architektur verwendet (vgl. Abschnitt 2.2.3).

Tabelle 5-9: Aus der Analyse der Ausfallfortpflanzung resultierende funktionale Sicherheitsanforderungen für das Sicherheitsziel SZ1

Funktionales Sicherheitskonzept › Funktionale Sicherheitsanforderungen für das Sicherheitsziel SZ1		
System: Chamäleon **Sicherheitsziel:** SZ1 **SIL-Level:** SIL2 **Norm:** IEC61508 **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 14. Februar 2013		
Nr.	**Sicherheitsanforderung**	**Systemelement**
SANF-01	Eine ausfallfreie Spannungsversorgung muss sichergestellt werden.	Batterie-Management-System
SANF-02	Das Bedienelement ist plausibilisierbar auszuführen.	Joystick
SANF-03	Der Lenkwinkelsensor ist plausibilisierbar auszuführen.	Lenkwinkelsensor
SANF-04	Die Bedienelementinformationen müssen vom Joystick gegen Übertragungsfehler abgesichert werden (z.B. durch Übertragung von zusätzlichen Informationen wie Checksumme und Botschäftszähler).	Joystick
SANF-05	Die Lenkwinkelinformationen müssen vom Lenkwinkelsensor gegen Übertragungsfehler abgesichert werden (z.B. durch Übertragung von zusätzlichen Informationen wie Checksumme und Botschäftszähler).	Lenkwinkelsensor
SANF-06	Die vom Joystick übertragene Informationen sind vor ihrer Verarbeitung auf Übertragungsfehler zu überprüfen (z.B. durch Auswertung von zusätzlich zu den Nutzdaten übertragenen Informationen wie Checksumme und Botschaftszähler).	Informationsverarbeitung
SANF-07	Die von den Lenkwinkelsensoren übertragene Lenkwinkelinformationen sind vor ihrer Verarbeitung auf Übertragungsfehler zu überprüfen (z.B. durch Auswertung von zusätzlich zu den Nutzdaten übertragenen Informationen wie Checksumme und Botschaftszähler).	Informationsverarbeitung
SANF-08	Die Informationsverarbeitung muss in der Lage sein, Fehler in der Sensorik durch entsprechende Plausibilisierung zu erkennen (z.B. Lenkwinkelsensor, Bedienelement).	Informationsverarbeitung
SANF-09	Die Informationsverarbeitung muss die Erzeugung von falschen Eingangssignalen für den Lenkmotor verhindern. Dies betrifft sowohl die Software als auch die zugrundeliegende Hardware (z.B. Mikroprozessor, RAM, ROM, ADC etc.).	Informationsverarbeitung
SANF-10	Fehler im Aktorverhalten (Lenkmotor, Mechanik) müssen durch die Informationsverarbeitung detektiert werden (z.B. durch Rücklesung, Plausibilisierung etc.).	Informationsverarbeitung
SANF-11	Die Informationsverarbeitung setzt ein Sicherheitskonzept um, welches das Potential für eine Sicherheitszielverletzung erkennt und als Fehlerreaktion einen Übergang in den sicheren Zustand entlang des Degradationskonzepts durchführt.	Informationsverarbeitung
SANF-12	Die Informationsverarbeitung ist zu überwachen.	Informationsverarbeitung
SANF-13	Die Aktorik ist plausibilisierbar auszulegen.	Lenkmotor
SANF-14	Die Mechanik ist so auszulegen bzw. mit Sicherungsmaßnahmen abzusichern, die nach dem neuesten Stand der Wissenschaft und Technik konstruktiv möglich sind.	Mechanik

Bild 5-17 stellt die Informationsverarbeitung des Chamäleons und ihren Zusammenhang zum Grundsystem dar. Der Fokus liegt hierbei auf den wesentlichen Schnittstellen [GDD+10]:

- **Kognitiver Operator:** Hier wird die Selbstoptimierung in ihrem Kern umgesetzt. Zur Verwendung kommt hierbei im Falle des Chamäleons vordergründig die Mehrzieloptimierung[50].

[50] Die Mehrzieloptimierung „ermöglicht eine gleichzeitige Optimierung mehrerer Zielfunktionen, die einander gegenläufig sind. Zudem können diese Ziele unterschiedlich ausgeprägt sein. Die Lösung dieses Optimierungsproblems ist eine Menge optimaler Kompromisse, eine sog. Pareto-Menge. Diese wird in

- **Reflektorischer Operator:** Hier werden vordergründig die globale Lenkstrategie sowie die globale Antriebsstrategie und die globale Regelstrategie für die aktive Federung abgebildet. Kern stellt der globale Regler dar, welcher die lokalen Regler der einzelnen Radmodule (Bestandteil der untergeordneten Controller-Ebene) koordiniert.
- **Controller:** Für jedes Radmodul werden hier die lokalen Regler für die Lenkfunktion, Antriebsfunktion und die aktive Federung realisiert.
- **Grundsystem inkl. Sensorik und Aktorik:** Die Ebene umfasst im Wesentlichen die Sensorik, die Aktorik, das mechanische Grundsystem sowie die Energieversorgung.

Die Informationsverarbeitung stellt ein zentrales Element der Architektur des Chamäleons dar. Sie ermittelt alle relevanten Einwirkungen und Zustandsgrößen und bestimmt die Stellgrößen für die Aktorik. In der Informationsverarbeitung erfolgt die Umsetzung der Selbstoptimierung sowie der fahrdynamischen Grundfunktionen Antreiben, Bremsen, Lenken, Dämpfen und Federn.

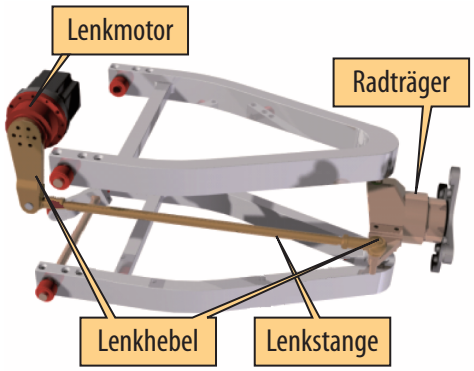


Bild 5-16: Darstellung der mechanischen Elemente, welche den Lenkmotor mit dem Radträger verbinden (in Anlehnung an [Lor08, S. 21]

In diesem Zusammenhang bestehen viele Schnittstellen zwischen der Informationsverarbeitung und den Radmodulen, welche einen wesentlichen Teil des Grundsystems darstellen. Bild 5-18 zeigt die Wirkstruktur des Radmoduls. Im Mittelpunkt stehen die Systemelemente Rad, die drei Motoren (Antriebsmotor, Lenkmotor und Motor für aktive Federung) sowie die zugehörige Sensorik und Mechanik. Für Details zur Umsetzung der Selbstoptimierung im Chamäleon siehe [GDD+10].

---

einer Datenbank hinterlegt. Einordnen lässt sich dieses Verfahren in die zweite Phase des Selbstoptimierungsprozesses, der Zielbestimmung. Die Mehrzieloptimierung liefert eine allgemeine Optimierungsmethode, welche in vielen Optimierungsproblemen zur Lösungsfindung hinzugezogen wird. Die Lösung von Mehrzieloptimierungsproblemen umfasst viele verschiedene Ansätze. Diese belaufen sich auf die Berechnung eines einzelnen paretooptimalen Punktes bis hin zu Verfahren der Approximation der gesamten (globalen) Paretomenge“ [Dum11, S. 176].

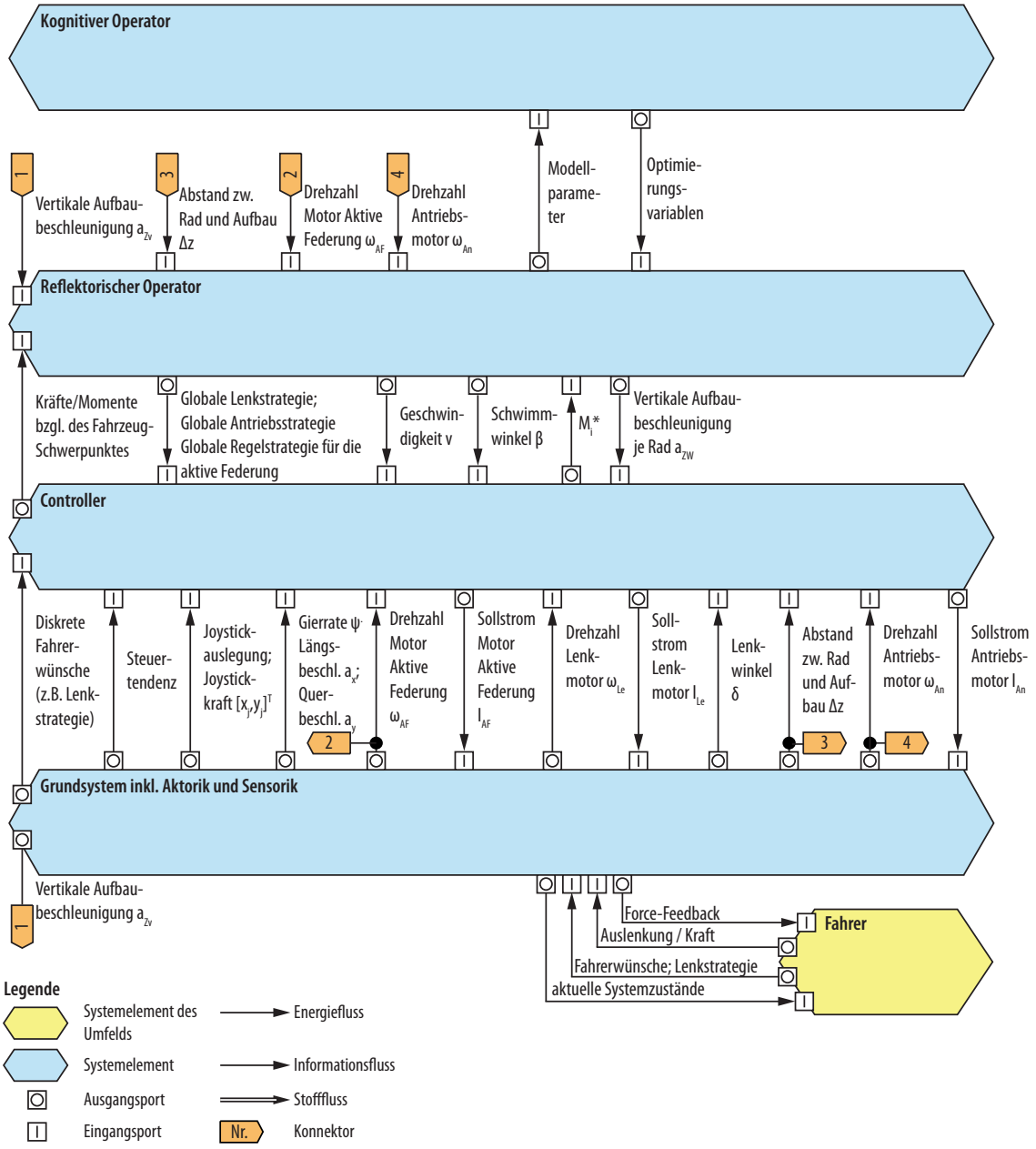


Bild 5-17: Struktur der Informationsverarbeitung des Chamäleons und der Zusammenhang mit dem Grundsystem entlang der OCM-Architektur (innere Struktur nicht dargestellt; Interkation mit Umfeld nur ausschnittsweise gezeigt)

Die Spezifikation der Wirkstruktur des Radmoduls beschreibt seine wesentlichen Systemelemente und ihre Beziehungen zueinander. Der Antriebsmotor zum Beispiel ist mit dem oberen sowie dem unteren Querlenker jeweils über Elastomere verbunden. Die beiden Querlenker dienen zur Befestigung des Radträgers sowie der Federung des Fahrzeugs. Die Federung wird durch die am unteren Querlenker angebrachte Torsionsstabfeder unterstützt. Durch den Einsatz der Elastomere werden die Bewegungen des Antriebsmotors gedämpft. Der Lenkmotor ist am Längsträger des Fahrzeugaufbaus befestigt (in Bild 5-18 nicht dargestellt). Der Motor für aktive Federung ist mechanisch mit dem

oberen Querlenker verbunden. Ferner besitzt jedes Radmodul jeweils einen Lenkwinkelsensor, einen vertikalen Beschleunigungssensor sowie einen Niveausensor. Der Lenkwinkelsensor misst den durch den Lenkmotor eingestellten Lenkwinkel und reicht den so ermittelten Messwert an die Informationsverarbeitung zwecks Regelung weiter. Mit dem vertikalen Beschleunigungssensor wird die vertikale Aufbaubeschleunigung pro Rad gemessen. Der Niveausensor dient zur Messung des Abstands zwischen Fahrzeugaufbau und Rad.

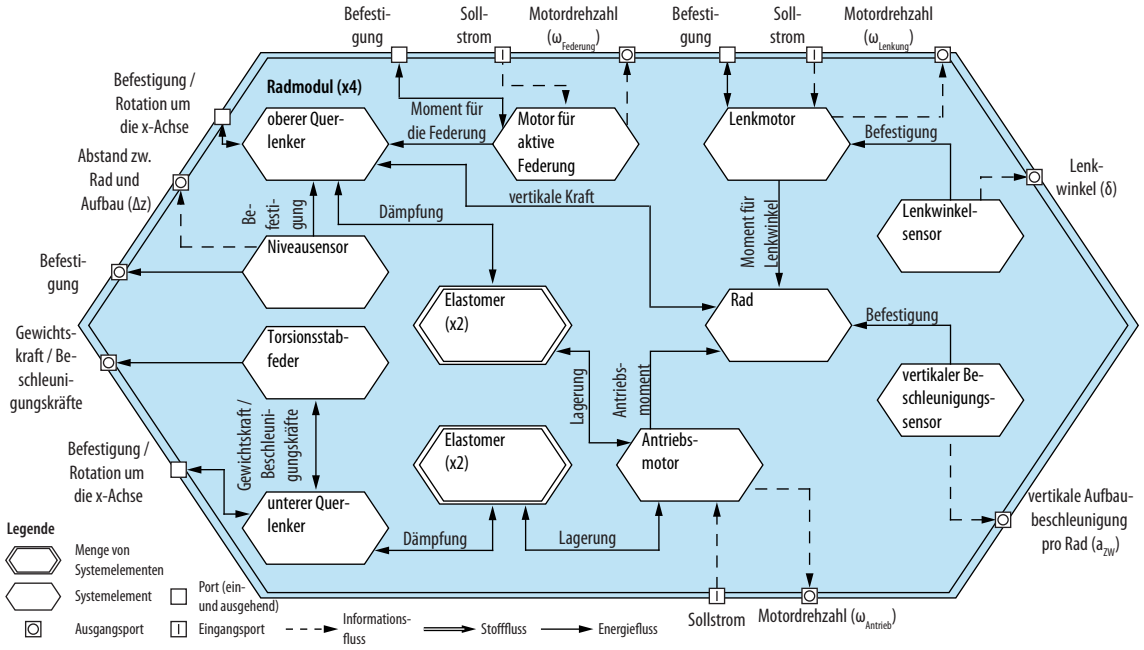


Bild 5-18: Wirkstruktur des Radmoduls des Chamäleons

5.6.4 Auf dem Weg zum technischen Sicherheitskonzept

Im Zuge der Analysen zur Erarbeitung des funktionalen Sicherheitskonzepts wurde deutlich, dass die Absicherung der funktionalen Sicherheit den gesamten mechatronischen Regelkreis betrifft. Zusammenfassend können Fehler in folgenden Subsystemen zu einer Verletzung des Sicherheitsziels SZ1 führen [PH13, S. 394]:

- Fehler in der Energieversorgung
- Fehler in den externen Signalen und in der Sensorik (inkl. Übertragungsfehler)
- Fehler in der Informationsverarbeitung (inkl. Fehler in der Motoransteuerung)
- Fehler in der Aktorik
- Fehler im Grundsystem

Auf Basis des funktionalen Sicherheitskonzepts erfolgt die Erarbeitung eines technischen Sicherheitskonzepts [ISO26262-4, S. 11]. Dieses umfasst die Spezifikation der technischen Sicherheitsanforderungen und deren Zuordnung zu den Systemelementen

[ISO26262-1, S. 17]. Technische Sicherheitsanforderungen sind eine Konkretisierung der funktionalen Sicherheitsanforderungen aus dem funktionalen Sicherheitskonzept und stellen die angestrebte technische Lösung dar [ISO26262-1, S. 17]. Im Folgenden werden Überlegungen bzgl. eines möglichen technischen Sicherheitskonzepts vorgestellt.

5.6.4.1 Absicherung der Energieversorgung

Eine ausfallsichere Spannungsversorgung ist für ein Steer-by-Wire-System essentiell [PH13, S. 457]. Eine Möglichkeit stellt die Einrichtung einer zweiten redundanten Spannungsversorgung. Dies ist jedoch mit erheblichen Zusatzaufwand und Kosten verbunden (vordergründig zusätzliche Batterie) [WIH+04]. Auf jeden Fall müssen an die Energieversorgung hohe Anforderungen hinsichtlich Ausfallsicherheit gestellt werden. Beispiele für mögliche Sicherheitsmaßnahmen sind Batterieüberwachung, unabhängige Überwachung von den Batteriezellen, Einsatz von sicheren Batteriezellen (Vermeidung eines Einflusses auf andere Batteriezellen beim Ausfall, Vermeidung eines unkontrollierten Öffnens der Batteriezelle etc.) [SRM13-ol].

5.6.4.2 Überwachung externer Signale und der Sensorik

Für das korrekte Erbringen der Lenkfunktion sind externe Signale und Sensoren erforderlich (z.B. ist der gemessene Radeinschlagswinkel für die Lenkfunktion von hoher Bedeutung). Fehler in den empfangenen Signalen bzw. Fehlfunktionen der Sensoren können die Lenkfunktion störend beeinflussen. Eine Verletzung der Sicherheitsziele ist ohne zusätzliche Sicherheitsmechanismen nicht auszuschließen [PH13, S. 394]. Aus diesem Grund gilt es die Sicherheitsrelevanz der Eingangssignale zu bewerten und entsprechende Sicherheitsmechanismen vorzusehen. Typische Maßnahmen sind Einsatz von plausibilisierbar ausgeführten Sensoren, Überwachung und Plausibilitätsprüfung der Eingangswerte sowie Absicherung der Datenkommunikation gegen Übertragungsfehler. Zum Beispiel wird im Chamäleon der Lenkwinkelsensor LWS3 verwendet, der aufgrund seiner Architektur und interner Sicherheitsmechanismen einen sehr plausiblen Messwert an das Steuergerät übergibt [Rei10, S. 95].

Ebenso gilt es die Sensoren und die Verbindungsleitungen zum Steuergerät im Zuge der Auswertung der Eingangssignale zu überwachen [SZ13, S. 108]. Hierzu können folgende Verfahren verwendet werden, mit denen Sensorfehler, Kurzschlüsse zur Batteriespannung und Masse, Leitungsunterbrechungen etc. erkannt werden können [SZ13, S. 108]:

- Überwachung der Versorgungsspannung des Sensors,
- Überprüfung des erfassten Werts auf den zulässigen Wertebereich,
- Plausibilitätsprüfung bei Vorliegen von Zusatzinformationen.

Beispiel – Messung der Radeinschlagwinkel der Räder. Die Radeinschlagwinkel der Räder werden im Chamäleon zum einen mit Hilfe der Lagesensorik der Lenkmotoren

(Encoder) ermittelt [Lor08, S. 54]. Hierbei werden vordefinierte Kennfelder[51] verwendet [Lor08, S. 19f.]. Zum anderen können die Radeinschlagswinkel aus den Messgrößen der Lenkwinkelsensoren ermittelt werden [Lor08, S. 54]. Die aus diesen zwei Quellen stammenden Messwerte können gegenseitig verglichen und plausibilisiert werden.

Ferner ist die Datenkommunikation gegen Übertragungsfehler abzusichern. Erforderlich sind Maßnahmen gegen Verfälschung der Nachricht, Auslassen von Nachrichten etc. Tabelle 5-10 fasst typische Fehlerarten in Bezug auf die Datenkommunikation und in Bezug auf analoge bzw. digitale Input-/Output-Schnittstellen. Ebenso stellt sie einige der typischen Maßnahmen zur Absicherung der externen Signale und deren Übertragung dar [LPP10, S. 258], [ISO26262-5, S. 42f.], [PH13, S. 394]. Zur Erhöhung der für die X-by-Wire-Systeme essentiellen Verfügbarkeit wird im Fehlerfall sehr oft auf einen Signalersatzwert überblendet [PH13, S. 394].

Tabelle 5-10: Typische Fehlerarten für Datenkommunikation sowie analoge und digitale Input-Output-Schnittstellen sowie beispielhafte Absicherungsmaßnahmen

Typische Fehlerarten		Maßnahmen zur Absicherung der exterenen Signale und deren Übertragung
Datenkommunikation	**analoge bzw. digitale Input-/Output-Schnittstellen**	
● Verfälschung der Nachricht ● Verzögerung der Nachricht ● Auslassen von beabsichtigten Nachrichten ● Ungewollte Wiederholung derselben Nachricht ● Vertauschung der Reihenfolge ● Einfügen von unbeabsichtigten Nachrichten ● Manipulation/Maskerade (die Nachricht wird derart verändert, dass der Empfänger sie dem falschen Sender zuordnet)	● Gleichstrom-Fehlermodell: - „Stuck-at"-Fehler (es wird stets ein permanenter Wert ausgegeben z.B. LOW-Signalpegel) - „Stuck-open"-Fehler - Open - Hochimpedanz-Ausgang - Nebenschlüsse ● Drift ● Oszillation	● Überwachung Timeout ● Überwachung Botschaftszähler ● Überwachung Checksumme ● Überwachung Wertebereich ● Sprungüberwachung etc.
[LPP10, S. 258]; [ISO26262-5, S. 43]	[ISO26262-5, S. 42]	[PH13, S. 394]

Analytische Sensor-Fehlerredundanz für die Querdynamik des Chamäleons

Die Funktionen der Querdynamik beruhen im Wesentlichen auf dem Lenkradwinkel δ, der Gierrate $\dot{\psi}$ und der Querbeschleunigung $\ddot{y}$. Wie bereits dargestellt, werden größere Fehler der zugehörigen Sensoren durch Plausibilitätsprüfungen etc. erkannt und führen zu einer entsprechenden Fehlerreaktion [Ise07b, S. 224]. Aufgrund der Tatsache, dass diese Signale über das fahrdynamische Verhalten gekoppelt sind, können diese zum Aufbau eines analytisch redundanten Sensorsystems verwendet werden [Ise07b, S. 224] (vgl. Anhang A1.1 für eine Definition der analytischen Redundanz). In seiner Doktorarbeit

[51] Es handelt sich hierbei um 2D-Kennfelder. Grundlage ist die Abhängigkeit der Radeinschlagwinkel der vier Räder von der Lenkwinkelvorgabe und der Lage des Momentanpols [Lor08, S. 19].

schlägt LURYE ein Konzept für die Realisierung der analytischen Sensor-Fehlerredundanz für das Chamäleon vor [Lur14]. Dieses adressiert insbesondere die Querdynamik des Chamäleons und dabei die Lenkfunktion. Basis stellt hierbei das Einspurmodell, welches um die Betrachtung der Hinterrad-Funktionen (insbesondere der Lenkung der Hinterräder) erweitert wurde [Ise06, S. 47f.], [MW04, S. 547ff.].

Die Strategien zur Ermittlung der Querdynamikgrößen des Chamäleons mittels analytischer Redundanz nach LURYE sind in Bild 5-19 dargestellt. Im Falle eines Sensorausfalls kann auf einen Messwert zurückgegriffen werden, der aus den Messwerten der anderen Sensoren berechnet wurde. Beispiel – Gierrate: Im Normalfall wird die Gierrate $\dot{\psi}$ vom Gierratensensor des Chamäleons gemessen. Fällt der Gierratensensor aus, so kann ein Ersatzwert für die Gierrate dennoch aus den Lenkwinkelinformationen und der Querbeschleunigung berechnet werden. Ein weiteres Beispiel stellt die Berechnung einer Ersatzgröße für den Messwert Lenkwinkel Vorderrad bzw. Hinterrad (δ_V bzw. δ_H) im Falle eines Ausfalls des zugehörigen Sensors dar. Für diesen Zweck werden die Messwerte des Lenkwinkels Hinterrad bzw. Vorderrad (δ_H bzw. δ_V), der Querbeschleunigung $\ddot{y}$ und der Gierrate $\dot{\psi}$ verwendet.

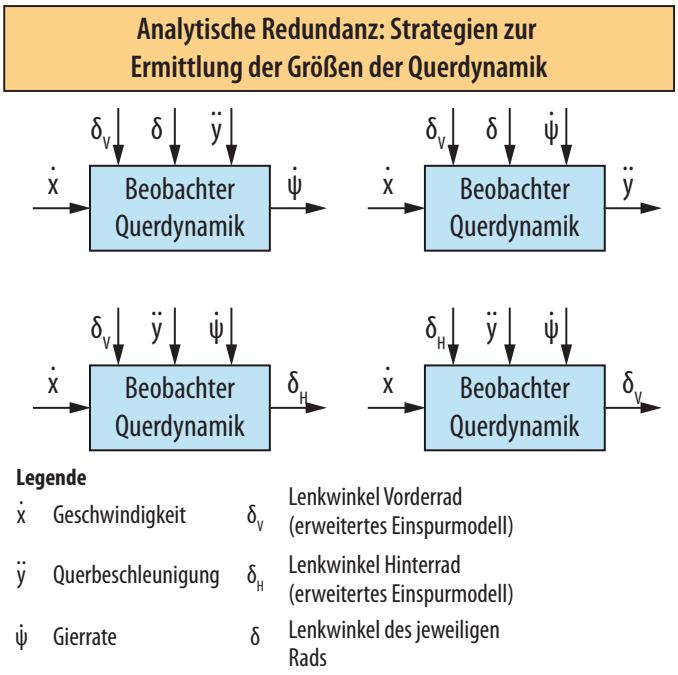


Bild 5-19: Strategien zur Ermittlung der Querdynamikgrößen des Chamäleons mittels analytischer Redundanz nach LURYE [Lur14]

5.6.4.3 Überwachungskonzept für die Informationsverarbeitung

Die Informationsverarbeitung nimmt beim Chamäleon eine zentrale Stellung ein (vgl. auch Abschnitt 5.6.3). Hier werden die wesentlichen Anteile der Funktionen und die Selbstoptimierung realisiert. Kern der technischen Implementierung der Informationsverarbeitung des Chamäleons stellt die MicroAutoBox der Firma dSPACE dar.

Aufgrund der für ein Steer-by-Wire-System charakteristischen Entkopplung des Bedienelements von der Lenkaktorik ist eine permanente Überwachung der lenkfunktionrelevanten Subsysteme zwingend erforderlich. Dadurch soll u.a. verhindert werden, dass aufgrund eines Fehlers ein unmotivierter Aktoreneingriff und damit einhergehend ein ungewollter Lenkvorgang erfolgt. Um den mit der SIL-Einstufung verbundenen Diagnosedeckungsgrad zu erreichen, ist eine Überwachung der MicroAutoBox notwendig. Hierzu kann z.B. das aus den E-Gas-Anwendungen bekannte 3-Ebenen-Überwachungskonzept[52] zum Einsatz kommen [PH13, S. 395f.]. Die Software-Funktionen werden dabei in folgende drei Ebenen aufgeteilt (Bild 5-20).

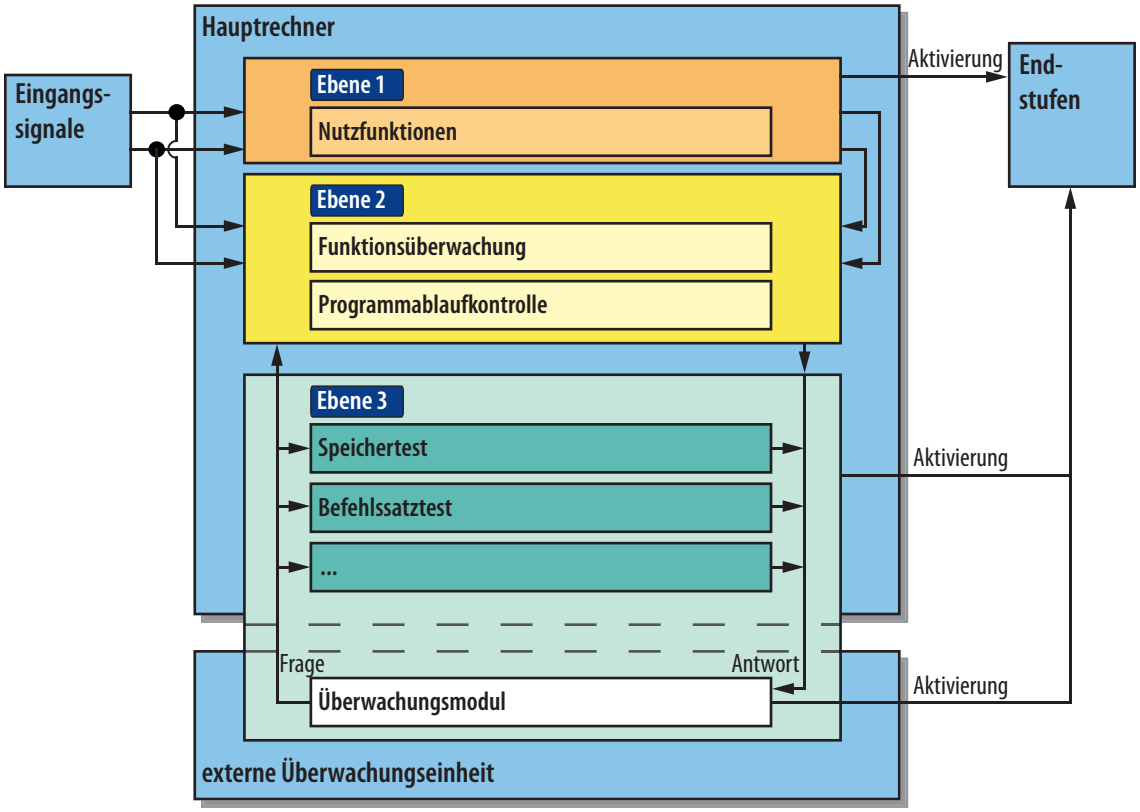


Bild 5-20: Grundsätzlicher Aufbau des 3-Ebenen-Überwachungskonzepts (in Anlehnung an [Arb13, S. 14], [PH13, S. 427])

Die **Ebene 1** umfasst folgende Aufgaben und Funktionen [PH13, S. 395f.], [LPP10, S. 249ff.]:

- **Nutzfunktionen**: Gemeint ist die Bereitstellung der eigentlichen Lenkfunktionalität. Dies umfasst insbesondere das Einlesen des vom Bedienelement bereitgestellten

[52] Es handelt sich um das so genannte 3-Ebenen-Konzept bzw. E-Gas-Konzept, welches für die Steuerung von Otto- und Dieselmotoren eingeführt und im Rahmen des Arbeitskreises EGAS durch die Automobilhersteller in Zusammenarbeit mit den Steuergeräteherstellern abgestimmt und standardisiert wurde [Arb13], [Rei12, S. 182], [PH13, S. 395f. und S. 427ff.], [LPP10, S. 249ff.], [SZ13, S. 103ff.].

Lenkwunsches, die Berechnung der Soll-Radeinschlagswinkel und die Ansteuerung der Lenkmotoren.

- **Anwendungsspezifische Diagnosefunktionen:** Diese dienen zur Absicherung der Lenkfunktionalität während des Betriebs und sind somit sehr anwendungsspezifisch [LPP10, S. 250]. Gemeint sind Diagnosefunktionen wie Überwachung und Plausibilisierung von Systemeingängen und -ausgängen sowie Sensoren und Aktoren für die spezifische Lenkfunktionalität [PH13, S. 395]. Zum Beispiel kann für den Zweck der Plausibilisierung ein Vergleich zwischen dem erwarteten und dem gemessenen Radeinschlagswinkel erfolgen [LPP10, S. 250].
- **Fehlerreaktion:** Gemeint sind Funktionen zur Steuerung der Systemreaktionen im Falle eines Ausfalls [Arb13, S. 14].

Die Zielsetzung der **Ebene 2** besteht darin, „die Restfehler in der Software [zu] erkennen und [zu] beherrschen“ [LPP10, S. 250]. Hierdurch soll sichergestellt werden, dass systematische Fehlerursachen wie z.B. Programmierfehler bzw. sporadische RAM-Fehler erkannt werden und nicht zu einer Fehlfunktion führen können [PH13, S. 428]. Die Ebene 2 umfasst folgende Aufgaben und Funktionen:

- **Überwachung der Funktionen der Ebene 1**: Hierzu werden die sicherheitsrelevanten Lenkfunktionen der Ebene 1 mit diversitären Algorithmen[53] nachgebildet.
- **Vergleich zwischen den Ergebnissen der Ebenen 1 und 2:** Die Ergebnisse der beiden Umsetzungen der jeweiligen sicherheitsrelevanten Funktionen werden miteinander verglichen. Die Ausgabewerte müssen dabei innerhalb einer erlaubten Toleranzgrenze liegen [PH13, S. 395]. Andernfalls werden entsprechende Fehlerreaktionen eingeleitet.
- **Programmablaufkontrolle:** Hier erfolgt die Überwachung des Programmablaufs. Insbesondere wird überwacht, ob eine Task spezifikationsgemäß regelmäßig aktiviert und korrekt ausgeführt wird und ob bestimmte Nachrichten in den erwarteten zeitlichen Abständen regelmäßig eintreffen [SZ13, S. 104].
- **Fehlerreaktion:** Gemeint sind Funktionen zur Steuerung der Systemreaktion im Falle eines Ausfalls [Arb13, S. 14].

In **Ebene 3** werden Systemdiagnosefunktionen ausgeführt [PH13, S. 396]. Ziel ist die Erkennung von Fehlern und eine entsprechende Fehlerreaktion [LPP10, S. 250]. Insbesondere sollen fehlerhafte Operationen des Funktionsrechners (Rechenkern, betroffene Bereiche im RAM/ROM etc.) erkannt und eine entsprechende Reaktion eingeleitet werden. Die Funktionen der Ebene 3 sind physikalisch auf zwei Hardware-Einheiten aufge-

[53] Gemeint sind „erheblich unterschiedliche Algorithmen zur Berechnung der Ausgabewerte“ [PH13, S. 395].

teilt. Neben dem Funktionsrechner kommt ein externer Überwachungsrechner zum Einsatz, der unabhängig von dem Funktionsrechner agiert [Rei12, S. 182]. Die Ergebnisse der beiden Rechner werden über eine Schnittstelle ausgetauscht [PH13, S. 396]. Die Sicherheitsmaßnahmen der Ebene 3 sind anwendungsunabhängig [PH13, S. 396]. Sie umfassen insbesondere [PH13, S. 396], [Rei12, S. 380]:

- Überwachung der korrekten Umwandlung der analogen Signale
- Überwachung der Speicherbereiche
- Überwachung der korrekten Durchführung der Befehle und Speicherzugriffe
- Überwachung der Abschaltpfade zu den sicherheitsrelevanten Endstufen (damit im Fehlerfall ein sicheres Abschalten gewährleistet ist)
- Logische und zeitliche Programmablaufkontrolle
- Überwachung des Betriebssystems
- Überwachung des in der Software umgesetzten Vergleichsalgorithmus (Vergleich der Ergebnisse der Ebenen 1 und 2)
- Prüfung Mikroprozessorkern des Funktionsrechners
- Überwachung des Funktionsrechners und der externen Überwachungseinheit mittels Frage-Antwort-Spiel (für eine detaillierte Beschreibung siehe [Arb13, S. 30])

Im Fehlerfall werden die Systemreaktionen unabhängig vom Funktionsrechner ausgeführt [Arb13, S. 14]. Wird in einer der drei Ebenen ein sicherheitsrelevanter Fehler erkannt, so findet die Überführung des Systems in den sicheren Zustand entlang der Degradationsstrategie statt (vgl. Abschnitt 5.6.1). Eine Möglichkeit für eine Fehlerreaktion besteht z.B. in der Begrenzung des Lenkwinkels auf einen Notlaufwert. Ein weiteres Beispiel einer möglichen Fehlerreaktion ist das Abschalten der Endstufe [Arb13, S. 33]. Beide der skizzierten Fehlerreaktionen können mit den in Bild 5-20 dargestellten Aktivierungssignalen umgesetzt werden, die sowohl vom Funktionsrechner als auch vom Überwachungsrechner bedient werden können. Kommt analytische Redundanz zur Verwendung, so kann im Falle des Ausfalls eines Lenkmotors die degradierte Lenkfunktion mittels des Antriebsmotors dargestellt werden (z.B. durch Abbremsen des betroffenen Rads, ähnlich wie es mit einem ESP-System geschieht).

Im Zusammenhang mit der Software ist die Sicherherstellung der **Rückwirkungsfreiheit** (engl. freedom from interference) von zentraler Bedeutung [KB13-ol]. Gemeint ist das Nichtvorhandensein von kaskadierenden Fehlern zwischen zwei oder mehreren Elementen, die zu einer Verletzung von Sicherheitsanforderungen führen könnten [ISO26262-1, S. 8]. Im Zuge der Festlegung der SIL für die Software-Elemente ergeben sich i.d.R. funktionale Gruppen mit unterschiedlichen SIL-Einstufungen [KB13-ol, S. 58]. Diese Gruppen gilt es durch geeignete Maßnahmen so voneinander zu trennen, dass sich diese

nicht gegenseitig störend beeinflussen [KB13-ol, S. 58]. Dadurch werden die Entwicklungsaufwände deutlich reduziert, da ansonsten die gesamte Software nach dem höchsten SIL-Level entwickelt werden müsste [KB13-ol, S. 58]. Im Allgemeinen ist die Rückwirkungsfreiheit für Software durch drei Eigenschaften definiert: 1) sichere Speicherzugriffe (z.B. durch Einsatz von MPU (Memory Protection Unit) zum Schutz von Speicherpartitionen vor unberechtigten Zugriffen), 2) korrekte zeitliche Ausführung (z.B. durch Programmablaufkontrolle) und 3) sicherer Datenaustausch (Absicherung der Datenkommunikation mittels CRC-Checksumme und Botschaftszähler) [KB13-ol, S. 58].

5.6.4.4 Überwachung Aktorik

Der Lenkmotor wird zur Umsetzung des gewünschten Radeinschlagswinkels verwendet. Eine Fehlfunktion im Lenkmotor kann zur Verletzung des Sicherheitszieles führen[54] (vgl. hierzu auch die Design-FMEA im Anhang A2). Daher gilt es Sicherheitsmaßnahmen mit einem entsprechend hohen Diagnosedeckungsgrad vorzusehen. Damit im Fehlerfall der Übergang in den sicheren Zustand entlang des Degradationskonzepts erfolgen kann, muss das System in der Lage sein, die Aktorik ausreichend schnell zu deaktivieren bzw. deren Funktion ausreichend schnell einzuschränken. Hierzu wird, wie bereits beschrieben, ein Abschaltpfad für die Lenkaktorik vorgesehen. Die Deaktivierung bzw. Begrenzung reichen alleine nicht aus [PH13, S. 396]. Aufgrund von Kurzschlüssen im Elektromotor können z.B. ungewollte, dem Lenkwunsch des Fahrers entgegengerichtete Motordrehmomente erzeugt werden [PH13, S. 396]. Der ungewollte Stromfluss sollte unterbunden werden. Hierzu gilt es Sicherheitsmaßnahmen im und außerhalb des Elektromotors vorzusehen [PH13, S. 396]. Derartige Sicherheitsmaßnahmen können z.B. einen konstruktiven Ausschluss von Motor- bzw. Zuleitungskurzschlüssen, Vermeidung des Stromflusses im Fehlerfall durch Einsatz von zusätzlichen Einrichtungen sowie Überwachung der Aktorik umfassen [PH13, S. 396].

5.6.4.5 Absicherung Grundsystem

Das Grundsystem ist bei der Absicherung der funktionalen Sicherheit ebenfalls ins Kalkül zu ziehen. Für die hier im Fokus stehende Lenkfunktion ist vor allem die Mechanik gemeint. Bricht zum Beispiel der Lenkhebel, so wird kein Drehmoment des Lenkmotors auf das Rad mehr übertragen. Als Konsequenz ist die Lenkung des Rads nicht mehr möglich (siehe auch die Design-FMEA für das Chamäleon im Anhang A2). Daher gilt es die Mechanik, insbesondere den Hebelarm, konstruktiv abzusichern. Hierbei sind methodisches Konstruieren, die Wahl von geeigneten Werkstoffen, eine adäquate Fertigung, eine entsprechende Dimensionierung etc. von zentraler Bedeutung [ISO13489-2, S. 12ff.].

---

[54] Die meisten Fehlfunktionen entstehen durch Überlast, Isolationsfehler, die zu Kurzschlüssen führen, sowie aufgrund von mechanischen Ursachen [Roc98, S. 1-1].

5.7 Bewertung der Systematik hinsichtlich der Erfüllung der Anforderungen

Abschließend wird die im Rahmen der vorliegenden Arbeit entwickelte *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* anhand der Anforderungen aus Abschnitt 2.5 bewertet. Hierfür wird für jede Anforderung erläutert, inwiefern sie durch die Systematik erfüllt wird (Bild 5-21):

A1) Interdisziplinarität: Die Nutzung eines zentralen disziplinübergreifenden Modells der Produktkonzeption über alle Phasen des Produktentwicklungsprozesses hinweg ermöglicht die Abbildung der Anteile der einzelnen Fachdisziplinen und deren Zusammenhänge. Dadurch, dass dieses zentrale Produktmodell als Basis für Analysen der Zuverlässigkeit bzw. Sicherheit verwendet wird, können die disziplinübergreifenden Zusammenhänge (insbesondere disziplinübergreifende Ausfallfortfplanzungspfade) zielgerichtet untersucht und entsprechende Verbesserungsmaßnahmen umgesetzt werden.

A2) Fokus auf die Konzipierung: Der im Rahmen dieser Arbeit als Grundlage verwendete Referenzprozess für die Entwicklung selbstoptimierender mechatronischer Systeme (Abschnitt 3.1.4) gliedert sich in die fachdisziplinübergreifende Konzipierung und die darauf folgende Phase Entwurf und Ausarbeitung. Die entwickelte Systematik fokussiert eindeutig die fachdisziplinübergreifende Konzipierung. Die Phasen des Vorgehensmodells der Systematik ordnen sich in den Konzipierungsprozess ein und begleiten diesen von vornherein, von der Phase „Planen und Klären der Aufgabe“ bis zu der Phase „Konzeptintegration“. Ebenso ist das Klassifizierungsschema für die Entwicklungsaufgabe stark auf die Konzipierungsphase ausgerichtet (vgl. Abschnitt 4.3).

A3) Zukunftsrobustheit und Erweiterbarkeit: Kern der Systematik bildet eine Methoden-Datenbank, die bedarfsgerecht um weitere Methoden erweitert werden kann. Gemeint sind hierbei insbesondere auch Analysemethoden, die im Rahmen der fortschreitenden Entwicklung des Stands der Technik und Forschung im Zusammenhang mit Zukunftsthemen wie Cyber-Physical-Systems etc. noch entwickelt werden. Ferner baut die Systematik auf der Spezifikationstechnik CONSENS auf, die ebenfalls eine hohe Erweiterbarkeit und Zukunftsrobustheit aufweist. Die Systematik stellt außerdem entsprechende Erweiterungspunkte bereit wie das Vorgehen zur Erweiterung der Spezifikationstechnik CONSENS (vgl. Abschnitt 4.4.1). Sie ist ferner so aufgebaut, dass sie grundsätzlich für eine Verwendung mit anderen Spezifikationssprachen wie der SysML, mit anderen Vorgehensmodellen etc. aufwandsarm angepasst werden kann.

A4) Suche, Auswahl und Kombination von Methoden: Der Methodik zur Auswahl von Methoden – ein wesentlicher Bestandteil der Systematik – unterstützt die zielgerichtete und systematische Suche, Auswahl und Kombination von Methoden. In der Methoden-Datenbank sind Methoden zur Absicherung der Zuverlässigkeit und Sicherheit abgelegt. Jede Methode ist entlang eines standardisierten Klassifizierungsschemas einheitlich charakterisiert und mit einem Steckbrief prägnant beschrieben, was die Suche und Auswahl von Methoden in besonderem Maße unterstützt. Außerdem bildet die Methoden-

Charakterisierung die Input-Output-Zusammenhänge der Methoden sowie deren Zuordnung zu den Phasen des Referenzprozesses für die Konzipierung selbstoptimierender mechatronischer Systeme ab, wodurch die Planung des Einsatzes der Methoden unterstützt wird (vgl. Abschnitt 4.3).

A5) Ganzheitliche Spezifikation: Die Systematik baut auf der Spezifikationstechnik CONSENS auf, die eine ganzheitliche Beschreibung der Produktkonzeption ermöglicht. Gemeint ist hierbei die Abbildung aller relevanten Beschreibungsaspekte und deren Zusammenhänge. Die Systematik stellt Hilfsmittel zur Erweiterung der Spezifikationstechnik für die Zwecke der Modellierung und Analyse der Sicherheit und Zuverlässigkeit bereit (siehe auch Abschnitt 4.4). Hierbei werden insbesondere Anpassungen der Spezifikationstechnik unterstützt, die für den Einsatz etablierter Methoden zur Absicherung der Sicherheit und Zuverlässigkeit auf Basis der Spezifikation der Produktkonzeption notwendig sind.

A6) Produktmodellzentrierte Analyse und Verbesserung: Im Mittelpunkt der Systematik steht die Modellierung der Produktkonzeption. Die Spezifikation der Produktkonzeption enthält Informationen, die als Inputs für Analysemethoden zur Absicherung der Zuverlässigkeit und Sicherheit des Produkts dienen. Mit Hilfe dieser Analysen können Schwachstellen in der Produktkonzeption gefunden werden. Die meisten der Methoden unterstützten die Ermittlung von Gegenmaßnahmen für die identifizierten Schwachstellen (z.B. redundante Auslegung, Rückfallmechanismen etc.), die in die Spezifikation der Produktkonzeption integriert werden. Zusammenfassend unterstützt die Systematik eine produktmodellzentrierte Analyse und Verbesserung der Sicherheit und Zuverlässigkeit des Produkts.

A7) Problemunabhängigkeit: Die Systematik kann zur Absicherung der Zuverlässigkeit und Sicherheit technischer Produkte jeder Art verwendet werden. Sie ist weder auf die Art des zu entwickelnden Produkts noch auf eine oder mehrere Normen der Zuverlässigkeits- und Sicherheitstechnik ausgerichtet. Vielmehr können Produkte unterschiedlicher Branchen, diverse Produktarten, Normen etc. durch sie abgedeckt werden. Denn die Systematik ermöglicht eine uneingeschränkte Erweiterung der zugrunde liegenden Methoden-Datenbank um neue Methoden. Das Vorgehensmodell sieht als Phase 1 die Analyse der Entwicklungsaufgabe vor, um eine auf sie abgestimmte Auswahl und Planung von zu verwendenden Methoden zu unterstützten.

A8) Anwenderakzeptanz: Um eine hohe Akzeptanz der Systematik zu gewährleisten, wird auf etablierten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit aufgebaut (vgl. Abschnitt 3.2). Zur Beschreibung der Produktkonzeption wird die Spezifikationstechnik CONSENS verwendet, die eine hohe Gebrauchstauglichkeit und Aufgabenangemessenheit aufweist (vgl. Abschnitt 3.4.3). Ebenso ist eine prototypische Rechnerunterstützung für die Systematik vorhanden (vgl. Abschnitte 4.3 und 4.6).

A9) Rechnerunterstützung: Im Rahmen der vorliegenden Arbeit erfolgte die Umsetzung einer prototypischen Werkzeugunterstützung. Zum einen wurde ein Software-Prototyp zur werkzeugtechnischen Umsetzung der Methodik zur Auswahl von Methoden entwickelt (vgl. Abschnitt 4.3). Zum anderen erfolgte die Umsetzung von Zusatzmodulen für das Modellierungswerkzeug Mechatronic Modeller, welche die Verwendung von Analysemethoden zur Absicherung der Zuverlässigkeit und Sicherheit auf Basis der Spezifikation der Produktkonzeption werkzeugtechnisch unterstützen (vgl. Abschnitt 4.6).

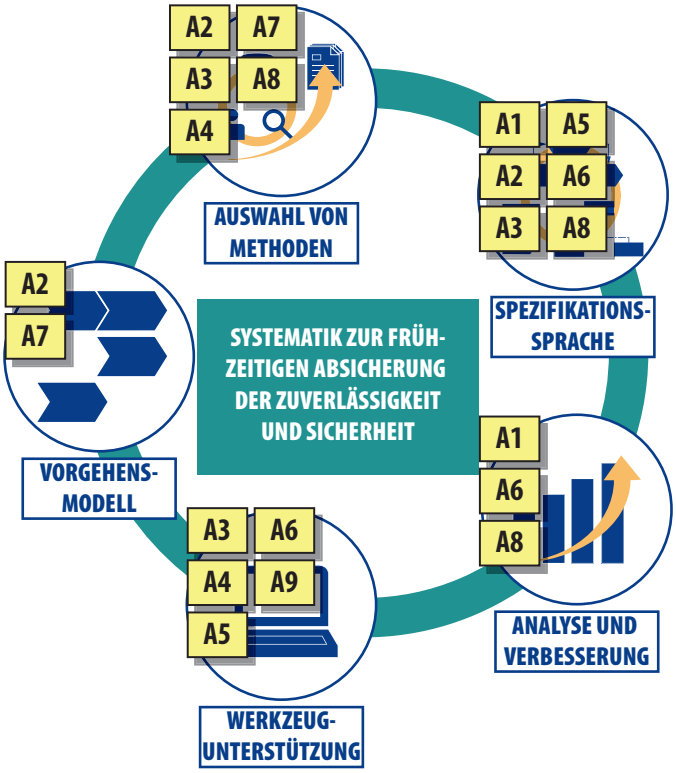


Bild 5-21: Erfüllung der gestellten Anforderungen durch die erarbeitete Systematik

Zusammenfassend lässt sich festhalten, dass die vorgestellte *Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme* alle Anforderungen vollumfänglich erfüllt. Sie eignet sich dafür, die Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme effizient zu unterstützen, was am Anwendungsbeispiel des X-by-Wire-Versuchsfahrzeugs Chamäleon validiert wurde.

6 Zusammenfassung und Ausblick

Moderne technische Erzeugnisse des Maschinenbaus und verwandter Branchen wie der Automobilindustrie, Bahntechnik und Medizintechnik realisieren ihre vielfältige Funktionalität durch das synergetische Zusammenwirken der Fachdisziplinen Maschinenbau, Elektrik/Elektronik, Regelungstechnik und Softwaretechnik. Die rasant fortschreitende Entwicklung der Informations- und Kommunikationstechnik ermöglicht eine deutliche Erweiterung der Funktionalität derartiger Systeme. Die informationstechnische Vernetzung solcher Systeme schreitet ebenfalls schnell voran. Insgesamt eröffnen sich faszinierende Perspektiven, die über die klassische Mechatronik weit hinausgehen: mechatronische Systeme mit inhärenter Teilintelligenz, die untereinander stark vernetzt sind. Diese Perspektive wird durch Begriffe wie Selbstoptimierung, Cyber-Physical-Systems, Intelligente Technische Systeme etc. charakterisiert. Die Entwicklung derartiger fortschrittlicher mechatronischer Systeme ist herausfordernd. Dies gilt in besonderem Maße für die Absicherung der Zuverlässigkeit und Sicherheit solcher Systeme.

Ein Lösungsansatz ist die **frühzeitige Absicherung der Zuverlässigkeit und Sicherheit auf Basis der Spezifikation der Produktkonzeption**. Diese erfolgt bereits in der Konzipierung und zwar auf Basis einer ganzheitlichen, fachdisziplinübergreifenden Spezifikation der Produktkonzeption des fortschrittlichen mechatronischen Systems unter Verwendung etablierter Absicherungsmethoden. Folgende **Nutzenpotentiale** gehen damit einher:

- **Frühzeitige Fehlervermeidung:** Schwachstellen werden bereits sehr früh im Produktentwicklungsprozess, und zwar in der Konzipierung aufgedeckt. Für diese werden Abstellmaßnahmen frühzeitig festgelegt und umgesetzt.
- **Berücksichtigung disziplinübergreifender Zusammenhänge:** Die Absicherung der Zuverlässigkeit und Sicherheit auf Basis einer ganzheitlichen, fachdisziplinübergreifenden Spezifikation der Produktkonzeption ermöglicht das Berücksichtigen von disziplinübergreifenden Zusammenhängen. Insbesondere können disziplinübergreifende Ausfallfortpflanzungspfade ins Kalkül gezogen werden.
- **Reduzierung von Iterationsschleifen:** Die frühzeitige Absicherung reduziert die Anzahl von nachträglichen, zeitraubenden und kostenintensiven Iterationsschleifen und Produktänderungen. Dadurch können Zeit und Geld gespart werden.

Im Zusammenhang mit der Entwicklung zuverlässiger und sicherer Systeme bestehen die wesentlichen **Herausforderungen** in der zunehmenden Systemkomplexität und der verstärkten Interdisziplinarität fortschrittlicher mechatronischer Systeme. Hinzu kommt, dass die etablierten Entwicklungsmethodiken von heute eine frühzeitige Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme noch unzureichend unterstützen. Insbesondere wird die effiziente Auswahl und Planung der für die jeweilige Aufgabenstellung adäquaten Methoden nicht hinreichend unterstützt. Ferner

kommen die etablierten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit aus derzeitiger Sicht i.d.R. erst vergleichsweise spät im Produktentwicklungsprozess zum Einsatz.

Um diesen Herausforderungen zu begegnen, muss die Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme von vornherein methodisch unterstützt werden. Notwendig sind in diesem Kontext ein systematisches Vorgehensmodell sowie dedizierte Hilfsmittel zur Spezifikation der Produktkonzeption unter Berücksichtigung von Sicherheit und Zuverlässigkeit sowie zur Auswahl und Planung von Methoden. Vor diesem Hintergrund sind ferner Methoden zur Absicherung der Zuverlässigkeit und Sicherheit notwendig, die bereits in der Konzipierung auf Basis der Spezifikation der Produktkonzeption einsetzbar sind. Wesentlich ist, dass diese Methoden auf etablierten Methoden der Zuverlässigkeits- und Sicherheitstechnik aufbauen.

Im Rahmen der vorliegenden Arbeit wurden verwandte Ansätze des **Stands der Technik** untersucht. Konkret erfolgte eine Untersuchung von 1) Vorgehensmodellen zur Entwicklung zuverlässiger und sicherer mechatronischer Systeme, 2) etablierten Methoden zur Zuverlässigkeits- und Sicherheitsanalyse, 3) Hilfsmittel zur Auswahl von Methoden, 4) Modellierungssprachen zur Beschreibung des Produktmodells, 5) Methoden zur Absicherung der Zuverlässigkeit und Sicherheit auf Basis der Spezifikation des Produktmodells sowie 6) verwandten Software-Werkzeugen. Die betrachteten Ansätze stellen – wenn überhaupt – nur Teillösungen dar. Eine ganzheitliche Systematik zur frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit existiert nicht. Aus den genannten Gründen besteht ein hoher **Handlungsbedarf** für die angestrebte Systematik.

Die erarbeitete Systematik baut auf einigen der verwandten Ansätze auf. Sie erweitert diese und ergänzt sie um neu entwickelte Hilfsmittel. Die wesentlichen Bestandteile der Systematik sind dabei:

- ein **Vorgehensmodell**, welches die Anwendung der Systematik systematisiert und die zu durchlaufenden Phasen, deren Reihenfolge, die zugehörigen Aufgaben und Methoden sowie die dabei zu erarbeitenden Ergebnisse beschreibt,
- eine **Methodik zur Auswahl und Planung** von Methoden, welche die Suche, Auswahl und Kombination von Methoden zur Absicherung der Zuverlässigkeit und Sicherheit ausgehend von der zugrunde liegenden Aufgabenstellung in der Konzipierung unterstützt,
- eine **Spezifikationssprache**, die eine ganzheitliche, fachdisziplinübergreifende Spezifikation der Produktkonzeption unter Berücksichtigung von zuverlässigkeits- und sicherheitsrelevanten Informationen ermöglicht,
- **Methoden zur Analyse und Verbesserung**, welche auf etablierten Methoden zur Absicherung der Zuverlässigkeit und Sicherheit beruhen und die Analyse und Verbesserung des Produkts hinsichtlich Zuverlässigkeit und Sicherheit unterstützen,

- ein Konzept für eine **Werkzeugunterstützung**, welche die Auswahl und Planung von Methoden, sowie die Spezifikation, Analyse und Verbesserung der Produktkonzeption in Form eines Software-Prototyps werkzeugtechnisch umsetzt.

Die **Validierung** der Systematik erfolgte anhand der Konzipierung des X-by-Wire-Versuchsfahrzeugs Chamäleon. Das Vorgehensmodell der Systematik wurde hierfür vollständig durchlaufen, die vorgesehenen Hilfsmittel eingesetzt und die zugehörigen Resultate erarbeitet. Insgesamt erfüllt die Systematik die an sie gestellten Anforderungen in vollem Umfang.

Auf dem in dieser Arbeit adressierten Gebiet der frühzeitigen Absicherung der Zuverlässigkeit und Sicherheit fortschrittlicher mechatronischer Systeme besteht noch **weiterer Forschungsbedarf**. Die Systematik kann um weitere Verlässlichkeitsaspekte wie Verfügbarkeit, Instandhaltbarkeit und Zugriffssicherheit (Security) erweitert werden. Gerade für die technischen Systeme von morgen, die zunehmend intelligent und vernetzt sein werden (Cyber-Physical-Systems, Internet der Dinge, Car-2-X-Communication, In-Vehicle-Services) wird der Verlässlichkeitsaspekt Security eine immer größere Rolle spielen. In diesem Zusammenhang ist insbesondere die integrative Absicherung der funktionalen Sicherheit und der Zugriffssicherheit ein bisher unzureichend gelöstes Problem [Bur13]. Ein weiteres Thema für weiterführende Arbeiten stellt die SysML-orientierte Umsetzung und Evaluierung der Systematik dar. Zwar stehen im Mittelpunkt der entwickelten Systematik die Spezifikationstechnik CONSENS und ihre werkzeugtechnische Umsetzung (der Mechatronic Modeller). Grundsätzlich ist die Systematik jedoch so ausgelegt, dass sie aufwandsarm auf die SysML übertragen werden kann. Weiterführende Arbeiten könnten diesen Punkt fokussieren.

Das übergeordnete Ziel des Sonderforschungsbereichs 614 „Selbstoptimierende Systeme des Maschinenbaus“, in dessen Rahmen die vorliegende Arbeit entstand, ist eine neue Schule des Entwurfs intelligenter technischer Systeme. Bei dem Entwurf derartiger fortschrittlicher Systeme ist die Absicherung der Zuverlässigkeit und Sicherheit von herausragender Bedeutung. Die angestrebte neue Schule muss diesem Umstand angemessen Rechnung tragen. Auf dem Weg zu diesem Ziel stellt die im Rahmen dieser Arbeit entwickelte Systematik einen wichtigen Baustein dar.

Abkürzungs- und Formelverzeichnis

Abkürzungen

ABS	Antiblockier-System
ACC	Adaptive Cruise Control
ASIC	Application Specific Integrated Circuit
ASIL	Automotive Sicherheitsintegritäts-Level
ASz	Anwendungsszenario
AVT	Aufbau- und Verbindungstechnik
BCM	Body Controller Module
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMS	Batterie-Management-System
BN	Bayessches Netz
bspw.	beispielsweise
bzw.	beziehungsweise
CAD	Computer Aided Design
CAN	Controller Area Network
CONSENS	CONceptual design Specification technique for the ENgineering of complex Systems
CPS	Cyber-Physical-Systems
CRC	Cyclic Redundancy Check
DBD	Dysfunctional Behavior Database
DBN	Dynamisches Bayessches Netz
DFT	Dynamischer Fehlzustandsbaum
DoD	Department of Defence
E/E/PE	elektrische, elektronische und programmierbare Systeme
ECC	Error Correction Code

ECU	Electronic Control Unit
EMV	Elektromagnetische Verträglichkeit
engl.	englisch
EPS	Electric Power Steering
ESP	Elektronisches Stabilitäts-Programm
ETA	Ereignisbaumanalyse (Event Tree Analysis)
etc.	et cetera
FDEP	Functional Dependency
FFIP	Functional Failure Identification and Propagation
FFL	Functional-Failure Logic
FH	Functional Hazard
FHA	Funktionale Gefahrenanalyse (Functional Hazard Analysis)
FMEA	Fehlzustandsart- und -auswirkungsanalyse (Failure Mode and Effect Analysis)
FMEDA	Failure Modes, Effects and Diagnostics Analysis
FSC	Funktionale Sicherheitskonzept
FT	Fehlzustandsbaum (Fault Tree)
FTA	Fehlzustandsbaumanalyse (Fault Tree Analysis)
ggf.	gegebenenfalls
GM	General Motors
GMF	Graphical Modeling Framework
GSPN	Generalisierte Stochastische Petri Netze
HALT	Highly Accelerated Life Test
HAZOP	Hazard and Operability Study
hins.	hinsichtlich
HW	Hardware
IC	Integrated Circuit
INCOSE	International Council on Systems Engineering
inkl.	inklusive

insb.	insbesondere
IV	Informationsverarbeitung
LIN	Local Interconnect Network
LM	Lösungsmuster
MBSE	Modellbasiertes Systems Engineering
MeDISIS	Integration Method of Reliability Analysis in the System Engineering Process
MID	spritzgegossene Schaltungsträger (Molded Interconnect Devices)
mind.	mindestens
MISRA	Motor Industry Software Reliability Association
MOST	Media Oriented Systems Transport
MPU	Memory Protection Unit
MTTF	mittlere Lebensdauer bis zum Ausfall (Mean Time To Failure)
O&SHA	Operating and Support Hazard Analysis
OCM	Operator-Controller-Modul
OMG	Object Management Group
OOPN	Objektorientierte Probabilistische Netze (Object-Oriented Probabilistic Networks)
OOSEM	Object Oriented Systems Engineering Method
PAND	Priority-AND
PHA	Vorläufige Gefahrenanalyse (Preliminary Hazard Analysis)
PHL	Vorläufige Gefahrenliste (Preliminary Hazard List)
QM	Qualitätsmanagement
RAM	Random Access Memory
RIR	Reduction in Risk
ROM	Read Only Memory
RPZ	Risikoprioritätszahl
RUP	Rational Unified Process
s.o.	selbstopimierend

S.O.	Selbstopimierung
SADT	System Analysis and Design Techniques
SE	Systems Engineering
SFB	Sonderforschungsbereich
SHA	System-Gefahrenanalyse (System Hazard Analysis)
SIL	Sicherheitsintegritäts-Level
sog.	sogenannte
SQMA	Situationsbasierte Qualitative Modellbildung und Analyse
SSHA	Subsystem-Gefahrenanalyse (Subsystem Hazard Analysis)
SW	Software
SysML	Systems Modeling Language
SYSMOD	Systems Modeling Process
SZ	Sicherheitsziel
TSC	Technisches Sicherheitskonzept
u.a.	unter anderem
u.U.	unter Umständen
UML	Unified Modeling Language
usw.	und so weiter
vgl.	vergleiche
XML	Extensible Markup Language
z.B.	zum Beispiel

Wesentliche Formeln

$P(\cdot)$	Wahrscheinlichkeit
$F(t)$	Ausfallwahrscheinlichkeit
τ	Lebensdauer einer Einheit
$R(t)$	Überlebenswahrscheinlichkeit
$f(t)$	Ausfalldichte
$\lambda(t)$	Ausfallrate

Literaturverzeichnis

Publikationen

[aca09] ACATECH – DEUTSCHE AKADEMIE FÜR TECHNIKWISSENSCHAFTEN (Hrsg.): Intelligente Objekte – klein, vernetzt, sensitiv – Eine neue Technologie verändert die Gesellschaft und fordert zur Gestaltung heraus (acatech BEZIEHT POSITION – Nr. 5). Springer-Verlag, Berlin, 2009

[aca11] ACATECH – DEUTSCHE AKADEMIE FÜR TECHNIKWISSENSCHAFTEN (Hrsg.): Cyber-Physical Systems – Innovationsmotor für Mobilität, Gesundheit, Energie und Produktion (acatech POSITION). Springer-Verlag, Berlin, 2011

[aca12] ACATECH – DEUTSCHE AKADEMIE FÜR TECHNIKWISSENSCHAFTEN (Hrsg.): agendaCPS – Integrierte Forschungsagenda Cyber-Physical-Systems (acatech STUDIE) Springer-Verlag, Berlin, 2012

[ADG+09] ADELT, P.; DONOTH, J.; GAUSEMEIER, J.; GEISLER, J.; HENKLER, S.; KAHL, S.; KLÖPPER, B.; KRUPP, A.; MÜNCH, E.; OBERTHÜR, S.; PAIZ, C.; PORRMANN, M.; RADKOWSKI, R.; ROMAUS, C.; SCHMIDT, A.; SCHULZ, B.; VÖCKING, H.; WITKOWSKI, U.; WITTING, K.; ZNAMENSHCHYKOV, O.: Selbstoptimierende Systeme des Maschinenbaus – Definition, Anwendungen, Konzepte. HNI-Verlagsschriftenreihe, Band 234, 2009

[Age13-ol] AGENA: AgenaRisk – product website. Unter: http://www.agenarisk.com/, 29. Dezember 2013

[AHJ+10] ANDERSSON, H.; HERZOG, E.; JOHANSSON, G.; JOHANSSON, O.: Experience from Introducing Unified Modeling Language/Systems Modeling Language at Saab Aerosystems. In: Systems Engineering, Vol. 13, No.4, 2010

[ALR+04] AVIZIENIS, A.; LAPRIE, J.-C.; RANDELL, B.; LANDWEHR, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, Jan-Mar 2004

[Alt12] ALT, O.: Modellbasierte Systementwicklung mit SysML. Carl Hanser Verlag, München, 2012

[Arb13] ARBEITSKREIS EGAS: Standardisiertes E-Gas Überwachungskonzept für Benzin und Diesel Motorsteuerungen. Arbeitskreis EGAS, Version 5.5, Stand: 5. Juli 2013

[Aut13a-ol] AUTO, MOTOR UND SPORT ONLINE: Rückruf für Toyota Prius: Materialermüdung an den Bremsen (5. Juni 2013). Unter: http://www.auto-motor-und-sport.de/news/rueckruf-fuer-toyota-prius-materialermuedung-an-den-bremsen-7211203.html, 10. September 2013

[Aut13b-ol] AUTO BILD.DE: Toyota Massenrückruf – Airbag löst falsch aus (18. Oktober 2013). Unter: http://www.autobild.de/artikel/toyota-massenrueckruf-4416998.html, 18. Oktober 2013

[AW95] ÅSTRÖM, K. J.; WITTENMARK, B.: Adaptive Control. 2nd Edition, Addison-Wesley Publishing Company, 1995

[BAG+11] BAUER, F.; ANACKER, H.; GAUKSTERN, T.; GAUSEMEIER, J.; JUST, V.: Analyzing the Dynamic Behavior of Mechatronic Systems within the Conceptual Design. In: Proceedings of the International Conference on Engineering Design (ICED), Copenhagen, 2011

[BB03] BOUISSOU, M.; BON, J.-L.: A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. In: Reliability Engineering and System Safety, Volume 82, Issue 2, Elsevier Science Ltd., Oxford, 2003, S. 149-163

[BB12] BREUER, B.; BILL, K.H. (Hrsg.): Bremsenhandbuch – Grundlagen, Komponenten, Systeme, Fahrdynamik. 4. Auflage, ATZ/MTZ-Fachbuch, Springer Fachmedien Wiesbaden, 2012

[BC10] BONE, M.; CLOUTIER, R.: The Current State of Model Based Systems Engineering: Results from the OMG™ SysML Request for Information 2009. In: Proceedings of the 8th Annual Conference on Systems Engineering Research (CSER), 2010

[BCS10] BOUDALI, H.; CROUZEN, P.; STOELINGA, M.: A Rigorous, Compositional, and Extensible Framework for Dynamic Fault Tree Analysis. In: IEEE Transaction on Dependable and Secure Computing, Vol. 7, No. 2, April-June, 2010, S. 128-143

[BD05] BOUDALI, H.; DUGAN, J.B.: A discrete-time Bayesian network reliability modeling and analysis framework. In: Reliability Engineering and System Safety, Vol. 87, Elsevier Science Ltd., Oxford, 2005, S. 337-349

[BDR+06] BOITEAU, M.; DUTUIT, Y.; RAUZY, A.; SIGNORET, J.-P.: The AltaRica data-flow language in use: modeling of production availability of a multi-state system. . In: Reliability Engineering and System Safety, Volume 91, Issue 7, Elsevier Science Ltd., Oxford, 2006, S. 747-755

[Ben05] BENDER, K. (Hrsg): Embedded Systems – qualitätsorientierte Entwicklung. Springer-Verlag, Berlin Heidelberg, 2005

[BGJ+09] BERTSCHE, B.; GÖHNER, P.; JENSEN, U.; SCHINKÖTHE, W.; WUNDERLICH, H.-J.: Zuverlässigkeit mechatronischer Systeme – Grundlagen und Bewertung in frühen Entwicklungsphasen. Springer-Verlag, Berlin, 2009

[BHS+13] BÖCKER, J.; HEMSEL, T.; SEXTRO, W.; TRÄCHTLER, A.: Teilprojekt D2 – Vernetzte selbstoptimierende Module und Systeme – Entwicklung und Implementierung von Verfahren zur Selbstoptimierung auf Gesamtsystemebene in den Bereichen Energiemanagement, Fahrdynamikregelung und Verlässlichkeit. In: Abschlussbericht des Sonderforschungsbereichs (SFB) 614 „Selbstoptimierende Systeme des Maschinenbaus“, 2013

[Bie03] BIEGERT, U.: Ganzheitliche modellbasierte Sicherheitsanalyse von Prozessautomatisierungssystemen. Dissertation, Institut für Automatisierungs- und Softwaretechnik (IAS), Universität Stuttgart. IAS-Forschungsbericht, Band 2/2003, Shaker Verlag,, Aachen, 2003

[Bir07] BIROLINI, A.: Reliability Engineering. Theory and Practice. 5. Auflage, Springer-Verlag Berlin Heidelberg, 2007

[BKL+06] BLANKE, M.; KINNAERT, M.; LUNZE, J.; STAROSWIECKI, M.: Diagnosis and Fault-Tolerant Control. 2nd Edition, Springer-Verlag, Berlin Heidelberg, 2006

[BL04] BERTSCHE, B.; LECHNER, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau: Ermittlung von Bauteil- und System-Zuverlässigkeiten. 3. Auflage, Springer-Verlag, Berlin, 2004

[Bor10] BORGEEST, K.: Elektronik in der Fahrzeugtechnik – Hardware, Software, Systeme und Projektmanagement. 2. Auflage, ATZ/MTZ-Fachbuch, Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden, 2010

[BPM+01] BOBBIO, A.; PORTINALE, L.; MINICHINO, M.; CIANCAMERLA, E.: Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. In: Reliability Engineering and System Safety, Vol. 71, Elsevier Science Ltd., Oxford, 2001, p. 249 – 260

[Bra07] BRABAND, J: Funktionale Sicherheit. In: FENDRICH, L. (Hrsg.): Handbuch Eisenbahninfrastruktur. Springer-Verlag, Berlin, 2007, S. 649-699

[Bra11] BRAND, E.: Die Richtlinie 4007: Zuverlässigkeitsziele, Ermittlung, Überprüfung, Festlegung, Nachweis – Überblick über die Arbeit des Fachausschusses Zuverlässigkeitsmanagement. In: 25. Fachtagung Technische Zuverlässigkeit (TTZ 2011), Leonberg bei Stuttgart. VDI-Berichte 2146, VDI-Verlag, Düsseldorf, 2011

[BSK+06] BÖCKER. J.; SCHULZ, B.; KNOKE, T.; FRÖHLEKE, N.: Self-Optimization as a Framework for Advanced Control Systems. In: 32nd Annual Conference of the IEEE Industrial Electronics Society (IECON), November, 7-10, Paris, France, 2006

[Bur13] BURTON, S.: Safety and Security – A Proposal for a combined approach. In: 5. EU-ROFORUM-Jahrestagung “ISO 26262”, 17.-19. September 2013

[Cas12] CASSADY, C. R.: An Introduction to Probability Models in Reliability and Maintainability. Tutorial Notes. In: The Annual Reliability and Maintainability Symposium – RAMS, Jan. 23-26, Reno, Nevada, USA, 2012

[CBM+12a] CODETTA-RAITERI, D., BOBBIO, A., MONTANI, S., PORTINALE, L.: A dynamic Bayesian network based framework to evaluate cascading effects in a power grid. In: Engineering Applications of Artificial Intelligence, Vol. 25, Elsevier Science Ltd., Oxford, 2012, S. 683-697

[CBM+12b] CODETTA-RAITERI, D.; BOBBIO, A.; MONTANI, S.; PORTINALE, L.: A dynamic Bayesian network based framework to evaluate cascading effects in a power grid. Engineering Applications of Artificial Intelligence 25(4), 2012

[CD05] CRANE, M.L.; DINGEL, J.: UML vs. Classical vs. Rhapsody Statecharts: Not All Models are Created Equal. In: Proceeding of the 8th International Conference on Model Driven Engineering Languages and Systems, 2005

[CDI+13] CRESSENT, R.; DAVID, P.; IDASIAK, V.; KRATZ, F.: Designing the database for a reliability aware Model-Based System Engineering process. In: Reliability Engineering and System Safety, Volume 111, Elsevier Science Ltd., Oxford, 2013, S. 171-182

[Cod05] CODETTA-RAITERI, D.: The Conversion of Dynamic Fault Trees to Stochastic Petri Nets, as a case of Graph Transformation- In: Electronic Notes in Theoretical Computer Science, Vol. 127, Elsevier Science Ltd., Oxford, 2005, S. 45–60

[Cod11] CODETTA-RAITERI, D.: Integrating several formalisms in order to increase Fault Trees' modeling power. In: Reliability Engineering and System Safety, Volume 96, Elsevier Science Ltd., Oxford, 2011, S. 534-544

[Con14-ol] CONTINENTAL AG: Die Zukunft heißt 'Brake by Wire'. Unter: http://www.continental-corporation.com/www/portal_com_de/allgemein/hidden/innovation/inno_bbwire_de.html, 15. Januar 2014

[CSD00] COPPIT, D.; SULLIVAN, K.J.; DUGAN, J.B.: Formal Semantics of Models for Computational Engineering: A Case Study on Dynamic Fault Trees. In: Proceedings of the 11th International Symposium on Software Reliability Engineering (ISSRE), 2000, S. 270-282.

[Czi08] CZICHOS, H.: Mechatronik – Grundlagen und Anwendungen technischer Systeme. 2 Auflage, Vieweg+Teubner Verlag |GWV Fachverlage GmbH, Wiesbaden, 2008

[DAG+13] DUMITRESCU, R; ANACKER, H.; GAUSEMEIER, J.: Design Framework for the Integration of Cognitive Functions into Intelligent Technical Systems In: Journal of Production Engineering – Research and Development, Volume 7, Issue 1, Springer-Verlag Berlin Heidelberg, 2013

[DBA+07] DONAT, R. BOUILLAUT, L.; AKNIN, P.; LERAY, P.; LEVY, D.: A Generic Approach to Model Complex System Reliability using Graphical Duration Models. In: Mathematical Methods in Reliability: Methodology and Practice (MMR 2007), July 1-4, Glasgow, United Kingdom, 2007

[DBB92] DUGAN, J.B.; BAVUSO, S.J.; BOYD, M.A.: Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems. In: IEEE Transactions on Reliability, Vol. 41, No.3, September, 1992, S. 363-377

[DG10] DOROCIAK, R.; GAUSEMEIER, J.: Absicherung der Zuverlässigkeit komplexer mechatronischer Systeme auf Basis der domänenübergreifenden Prin-ziplösung. In: 25. Fachtagung Technische Zuverlässigkeit (TTZ 2011), Leonberg bei Stuttgart. VDI-Berichte 2146, VDI-Verlag, Düsseldorf, 2011

[DG12] DOROCIAK, R.; GAUSEMEIER, J.: Modeling of the Failure Propagation of an Advanced Mechatronic System within the Specification of its Principle Solution. In: Proceedings of the International Design Conference – DESIGN, May 21-24, Dubrovnik, Croatia, 2012

[DGG+13] DOROCIAK, R.; GAUKSTERN, T.; GAUSEMEIER, J.; IWANEK, P., VAßHOLZ, M.: A methodology for the Improvement of Dependability of Self-Optimizing Systems. In: Journal of Production

Engineering – Research and Development, Volume 7, Issue 1, Springer-Verlag Berlin Heidelberg, 2013

[DGK+09] DEYTER, S.; GAUSEMEIER, J.; KAISER, L.; POESCHL, M.: Modeling and Analyzing Fault-Tolerant Mechatronic Systems. In: Proceedings of the 17th International Conference on Engineering Design (ICED), Stanford, USA, 2009

[DIK10] DAVID, P.; IDASIAK, V.; KRATZ, F.: Reliability study of complex physical systems using SysML. In: Reliability Engineering and System Safety, Volume 95, Issue 4, Elsevier Science Ltd., Oxford, 2010, S. 431-450

[Dor12] DOROCIAK, R.: Early Probabilistic Reliability Analysis of Mechatronic Systems. In: The Annual Reliability and Maintainability Symposium – RAMS, Jan. 23-26, Reno, Nevada, USA, 2012

[Dou09] DOUGLASS, B.P.: Analyze system safety using UML within the IBM Rational Rhapsody environment. White Paper, IBM Corporation, Somers, NY, USA, 2009

[Dou13-ol] DOUGLASS, B.P.: Top 10 modeling hints for system engineers: #5 Only 4 (+1) diagrams are required (19. November 2013). Unter: http://www.ibm.com/developerworks/rational/library/top-10-modeling-hints-system-engineers-06/, 29. November 2013

[Dum11] DUMITRESCU, R.: Entwicklungssystematik zur Integration kognitiver Funktionen in fortgeschrittene mechatronische Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 286, Paderborn, 2011

[Ech90] ECHTLE, K.: Fehlertoleranzverfahren. Springer-Verlag, Berlin, 1990

[Eck08] ECKERT, C.: IT-Sicherheit: Konzepte – Verfahren – Protokolle. 5. Auflage, Oldenbourg Wissenschaftsverlag GmbH, München, 2008

[Ehr03] EHRLENSPIEL, K.: Integrierte Produktentwicklung. Carl Hanser Verlag, München, 2003

[EKL07] EHRLENSPIEL, K.; KIEWERT, A.; LINDEMANN, U.: Cost-Efficient Design. Springer-Verlag, Berlin Heidelberg, 2007

[Eri05] ERICSON, C. A.: Hazard Analysis Techniques for System Safety. John Wiley & Sons, Inc., Hoboken, New Jersey, 2005

[Eri11] ERICSON, C. A.: Reliability versus System Safety. In: Journal of System Safety, Vol. 46, No. 4, July-August, 2011, S. 18–19

[Est08] ESTEFAN, J.: Survey of Model-Based Systems Engineering (MBSE) Methodologies (RevB). In: INCOSE MBSE Initiative, INCOSE MBSE Focus Group, California, 2008

[Fa13] FORSCHUNGSUNION WIRTSCHAFT – WISSENSCHAFT; ACATECH – DEUTSCHE AKADEMIE FÜR TECHNIKWISSENSCHAFTEN: Deutschlands Zukunft als Produktionsstandort sichern – Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0, April 2013

[FG13] FELDHUSEN, J.; GROTE, K.-H. (Hrsg.): Pahl/Beitz Konstruktionslehre – Methoden und Anwendungen erfolgreicher Produktentwicklung. 8. Auflage, Springer-Verlag Berlin Heidelberg 2013

[FKP+07] FAHRMEIR, L.; KÜNSTLER, R.; PIGEOT, I.; TUTZ, G.: Statistik – Der Weg zur Datenanalyse. 6. Auflage, Springer-Lehrbuch, Springer-Verlag, Berlin Heidelberg, 2007

[FMN+94] FENELON, P.; MCDERMID, J. A.; NICOLSON, M.; PUMFREY, D. J.: Towards integrated safety analysis and design. In: SIGAPP Appl. Comput. Rev. Vol. 2, No. 1, ACM, New York, USA, 1994

[FMS12] FRIEDENTHAL, S.; MOORE, A.; STEINER, R.: A Practical Guide to SysML – The Systems Modeling Language. 2nd Edition, Morgan Kaufmann OMG Press, Elsevier Inc., Waltham, MA, USA, 2012

[Foc13-ol] FOCUS MONEY ONLINE: Toyota ruft Minivans in Nordamerika zurück: Können wegrollen (27. September 2013). Unter: http://www.focus.de/finanzen/news/auto-toyota-ruft-minivans-in-nordamerika-zurueck-koennen-wegrollen_aid_1114142.html, 18. Oktober 2013

[Föl90] FÖLLINGER, O.: Regelungstechnik. 6. Auflage, Hüthig Buch Verlag, 1990

[Fri00] FRIIS-HANSEN, A.: Bayesian Networks as a Decision Support Tool in Marine Applications. PhD Thesis, Department of Naval Architecture and Offshore Engineering, Technical University of Denmark, Kgs. Lyngby, Dezember, 2000

[Gau10] GAUSEMEIER, J. (Hrsg): Frühzeitige Zuverlässigkeitsanalyse mechatronischer Systeme. Carl Hanser Verlag, München, 2010

[GB12] GOBLE, W. M.; BUKOWSKI, J. V.: Applying Reliability Engineering Techniques & Best Practices to Achieve Functional Safety. Tutorial Notes. In: The Annual Reliability and Maintainability Symposium – RAMS, Jan. 23-26, Reno, Nevada, USA, 2012

[GDD+10] GAUSEMEIER, J.; DONOTH, J.; DUMITRESCU, R.; TRÄCHTLER, A.; REINOLD, P.: Self-Optimization – an approach for intelligent mechatronics exemplified by an X-by-wire vehicle. In: the 8th IEEE International Conference on Industrial Informatics (INDIN), July 13-16, 2010, Osaka, Japan, 2010, pp. 757−762

[GDK10] GAUSEMEIER, J.; DOROCIAK, R.; KAISER, L.: Computer-Aided Modeling of the Principle Solution of Mechatronic Systems – A Domain-Spanning Methodology for the Conceptual Design of Mechatronic Systems. In: Proceedings of the ASME 2010 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference (IDETC/CIE2010), August 15-18, Montreal, Canada, 2010

[GDP+10] GAUSEMEIER, J.; DOROCIAK, R.; POOK, S.; NYßEN, A.; TERFLOTH, A.: Computer-Aided Cross-Domain Modeling of Mechatronic Systems. In: Proceedings of the International Design Conference, May 17th-20th 2010, Dubrovnik, 2010

[GEK01] GAUSEMEIER, J.; EBBESMEYER, P.; KALLMEYER, F.: Produktinnovation – Strategische Planung und Entwicklung der Produkte von morgen. Carl Hanser Verlag, München, 2001

[GF06] GAUSEMEIER, J.; FELDMANN, K.: Integrative Entwicklung räumlicher elektronischer Baugruppen. Carl Hanser Verlag, München, 2006

[GFD+08] GAUSEMEIER, J.; FRANK, U.; DONOTH, J.; KAHL, S.: Spezifikationstechnik zur Beschreibung der Prinziplösung selbstoptimierender Systeme des Maschinenbaus. Konstruktion Teil 1 7/8-2008, Teil 2 9/2008

[GGD11] GAUSEMEIER, J.; GAUKSTERN, T.; DOROCIAK, R.: Integrierte Entwicklungsumgebung für die Konzipierung mechatronischer Systeme. In: Mechatronik 2011, Dresden, 31. März und 1. April, 2011

[GID+13] GAUSEMEIER, J.; IWANEK, P.; DOROCIAK, R.; STILLE, K.S.; BÖCKER, J.: Konzipierung eines selbstoptimierenden hybriden Energiespeichersystems unter besonderer Berücksichtigung der Verlässlichkeit. In: 9. Paderborner Workshop Entwurf mechatronischer Systeme, 18. - 19. April 2013, Paderborn, 2013

[GKP09] GAUSEMEIER, J.; KAISER, L.; POOK, S.: FMEA von komplexen mechatronischen Systemen auf Basis der Spezifikation der Prinziplösung. In: ZWF – Zeitschrift für wirtschaftlichen Fabrikbetrieb, 104(2009), 2009, S. 1011-1017

[GLL12] GAUSEMEIER, J.; LANZA, G.; LINDEMANN, U. (Hrsg.): Produkte und Produktionssysteme integrativ konzipieren – Modellbildung und Analyse in der frühen Phase der Produktentstehung. Carl Hanser Verlag, München, 2012

[GP14] GAUSEMEIER, J.; PLASS, C.: Zukunftsorientierte Unternehmensgestaltung – Strategien, Geschäftsprozesse und IT-Systeme für die Produktion von morgen. Carl Hanser Verlag, München, 2014

[GRS+14] GAUSEMEIER, J.; RAMMIG, F.J.; SCHÄFER, W.; SEXTRO, W. (Hrsg.): Dependability of Self-Optimizing Mechatronic Systems. Lecture Notes in Mechanical Engineering, Springer-Verlag, Berlin, 2014 (to be published)

[GRS14] GAUSEMEIER, J.; RAMMIG, F.J.; SCHÄFER, W. (Hrsg.): Design Methodology for Intelligent Technical Systems – Develop Intelligent Technical Systems of the future. Lecture Notes in Mechanical Engineering, Springer-Verlag, Berlin, 2014 (to be published)

[Han13-ol] HANDELSBLATT ONLINE: China lässt gegenüber VW die Muskeln spielen (20. März 2013). Unter: http://www.handelsblatt.com/unternehmen/industrie/rueckrufaktion-china-laesst-gegenueber-vw-die-muskeln-spielen/7956068.html, 25. März 2013

[Har87] HAREL, D.: Statecharts: A visual formalism for complex systems. In: Science of Computer Pro-gramming, Vol. 8 Iss. 3, 1987, pp. 231-274

[Hel09a] HELMIG, E.: Die Airbag-Entscheidung im Kontext zum Gemeinschaftsrecht - Vertragsrelevanz für die Automobilindustrie. PHI Haftpflicht international - Recht & Versicherung, Heft 05/2009, S. 190 – 191

[Hel09b] HELMIG, E.: Zur Haftung eines Fahrzeugherstellers für die Fehlauslösung von Airbags. Urteilsanmerkung zu BGH, Urteil v. 16.06.2009 (Az.: VI ZR 107/08) in Deutsches Autorecht (DAR), 12/2009, S .691 – 692

[HES11] HEIßING, B.; ERSOY, M.; GIES, S. (Hrsg.): Fahrwerkhandbuch – Grundlagen, Fahrdynamik, Komponenten, Systeme, Mechatronik, Perspektiven. 3. Auflage, ATZ/MTZ-Fachbuch, Vieweg+Teubner Verlag |Springer Fachmedien Wiesbaden GmbH, 2011

[Hil12] HILLENBRAND, M.: Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik / Elektronik Architekturen von Fahrzeugen. Dissertation, Institut für Technik und Informationsverarbeitung, Karlsruher Institut für Technologie. Steibuch Series on Advances in Information Technology, Band 4, KIT Scientific Publishing, Karlsruhe, 2012

[HK13] HALANG, W. A.; KONAKOVSKY, R. M.: Sicherheitsgerichtete Echtzeitsysteme. 2. Auflage, Springer-Verlag Berlin Heidelberg, 2013

[HNB+02] HABERFELLNER, R.; NAGEL, P.; BECKER, M.; BÜCHEL, A.; VON MASSOW, H.: Systems Engineering – Methodik und Praxis. 11. Auflage, Orell Füssli Verlag für Verlag Industrielle Organisation, Zürich, 2002

[HNI11] HEINZ NIXDORF INSTITUT: Entwicklungsdokumentation Mechatronic Modeller Release 1.0. Heinz Nixdorf Institut der Universität Paderborn, Stand: 4. Oktober 2011

[HNI12] HEINZ NIXDORF INSTITUT: Entwicklungsdokumentation Mechatronic Modeller Release 1.0. Technische Dokumentation. Heinz Nixdorf Institut, Universität Paderborn, Stand: 22. März 2012

[HSM+02] HIRTZ, J.; STONE, R. B.; MCADAMS, D. A.; SZYKMAN, S.; WOOD, K. L.: A functional basis for engineering design: Reconciling and evolving previous efforts. Research in Engineering Design 13(2002), Springer-Verlag New York, 2002, p. 65 – 82

[HTF96] HARASHIMA, F.; TOMIZUKA, M.; FUKUDA, T.: Mechatronics – „What Is It, Why and How?“ An Editorial. In: IEEE/ASME Transactions on Mechatronics, Volume 1, Nr. 1, 1996

[IKD+13] IWANEK, P.; KAISER, L.; DUMITRESCU, R.; NYßEN, A.: Fachdisziplinübergreifende Systemmodellierung mechatronischer Systeme mit SysML und CONSENS. In: Tag des Systems Engineering 2013, 6.-8. Nov. 2013, Stuttgart, Carl Hanser Verlag, München, 2013

[ikv13-ol] IKV++ TECHNOLOGIES AG: medini analyze – ISO 26262 in einem integrierten Werkzeug. Webseite des Produkts. Unter: http://www.ikv.de/index.php/de/products/functional-safety, 18. Dezember 2013

[Ise06] ISERMANN, R.: Fahrdynamik-Regelung – Modellbildung, Fahrerassistenzsysteme, Mechatronik. ATZ/MTZ-Fachbuch, Friedr. Vieweg & Sohn Verlag | GWV Fachverlage GmbH, Wiesbaden, 2006

[Ise07a] ISERMANN, R.: Fehlertolerante mechatronische Systeme, Teil 1. In: at – Automatisierungstechnik 55 (2007), Oldenbourg Verlag, München, 2007

[Ise07b] ISERMANN, R.: Fehlertolerante mechatronische Systeme, Teil 2. In: at – Automatisierungstechnik 55 (2007), Oldenbourg Verlag, München, 2007

[Ise08] ISERMANN, R.: Mechatronische Systeme – Grundlagen. 2. Auflage, Springer-Verlag Berlin Heidelberg, 2008

[Iso13-ol] ISOGRAPH, INC.: Reliability Workbench. Unter: http://www.isograph-software.com/2011/software/reliability-workbench/, 12. Dezember 2013

[Ite13-ol] ITEM SOFTWARE: ITEM Toolkit. Unter: http://www.itemsoft.com/item_toolkit.html, 15. Dezember 2013

[JN07] JENSEN, F.V.; NIELSEN, T.D.: Bayesian Networks and Decision Graphs, 2nd Edition. In: JORDAN, M.; KLEINBERG, J.; SCHÖLKOPF, B. (Eds): Information Science and Statistics, Springer-Verlag New York, 2007

[Kai14] KAISER, L.: Rahmenwerk zur Modellierung einer plausiblen Systemstruktur mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, Band 327, Paderborn, 2013

[KB13-ol] KEUL, S.; BROCK, H.: Mixed-ASIL-Systeme praktisch realisieren. ElektronikAutomotive, Sonderheft Funktionale Sicherheit, WEKA FACHMEDIEN GmbH, Juli, 2013. Online unter: http://vector.com/portal/medien/cmc/press/Vector/Safety_ElektronikAutomotive_201307_PressArticle_DE.pdf, 5. Juli 2013

[KBA13-ol] KRAFTFAHRT-BUNDESAMT: Rückrufe. Unter http://www.kba.de/cln_031/nn_1176910/DE/-Fahrzeugtechnik/Marktueberwachung__Rueckrufe/Rueckrufe/rueckrufe__node.html, 18. September 2013

[KGB+10] KREFT, S.; GAUSEMEIER, J.; BERSSENBRÜGGE, J.; LORENZ, W.; TRÄCHTLER, A.: Integration eines voll-aktiven X-by-wire Versuchsfahrzeugs in eine VR-basierte Simulationsumgebung. In: 9. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung, HNI-Verlagsschriftenreihe, Band 274, Paderborn, 2010

[KGD10] KAHL, S.; GAUSEMEIER, J.; DUMITRESCU, R.: Interactive Visualization of Development Processes in Mechatronic Engineering. In: Proceedings of the 1st International Conference on Modelling and Management of Engineering Processes (MMEP). Cambridge, UK, July 19-20, 2010

[KM13] KJÆRULFF, U.B.; MADSEN, A.L.: Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis. In: JORDAN, M.; KLEINBERG, J.; SCHÖLKOPF, B. (Eds): Information Science and Statistics. 2nd Edition, Springer Science+Business Media, New York, 2013

[KTJ10] KURTOGLU, T.; TUMER, I.Y.; JENSEN, D.C.: A functional failure reasoning methodology for evaluation of conceptual system architectures. Research in Engineering Design 21(2010), Springer-Verlag, New York, 2010, p. 209 – 234

[Lev95] LEVESON, N.G.: Safeware: System Safety and Computers. Addison-Wesley Professional, Boston, MA, USA, 1995

[Lor08] LORENZ, W.: Strukturierung und Implementierung der Gesamtfahrzeugregelung für ein vollaktives X-by-Wire Versuchsfahrzeug unter Echtzeitbedingungen. Diplomarbeit, Fakultät für Maschinenbau, Universität Paderborn, 2008

[LP07] LANGSETH, H.; PORTINALE, L.: Bayesian networks in reliability. In: Reliability Engineering and System Safety, Vol. 92 (2007), Elsevier Science Ltd., Oxford, 2007, p. 92 – 108

[LPP10] LÖW, P.; PABST, R.; PETRY, E.: Funktionale Sicherheit in der Praxis – Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten. dpunkt.verlag GmbH, Heidelberg, 2010

[Lun13a] LUNZE, J.: Regelungstechnik 1 – Systemtheoretische Grundlagen, Analyse und Entwurf einschleifiger Regelungen. 9. Auflage, Springer-Verlag Berlin Heidelberg, 2013

[Lun13b] LUNZE, J.: Regelungstechnik 2 – Mehrgrößensysteme, Digitale Regelung. 7. Auflage, Springer-Verlag Berlin Heidelberg, 2013

[Lur14] LURYE, O.: Reliability and Safety of an X-by-Wire demonstrator vehicle. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, zu erscheinen in der HNI-Verlagsschriftenreihe, Paderborn, 2014 (geplant)

[LW10] LEPPIN, E.; WITTMANN, B.: Chamäleon auf Rädern – Hochintegrierte, kompakte Getriebe im Antrieb eines flexiblen Versuchsfahrzeugs. In: Der Konstrukteur ASB, 2010

[Man99] MANZ, S.: Prozessüberwachung unter Verwendung des qualitativen Modellierungsverfahren SQMA. Jahrestagung Deutsche Forschungsvereinigung für Mess-, Steuer- und Regelungstechnik, Forschungsbericht Nr. 99-1, 1999

[Mey11] MEYER, O.: Ermittlung von Zuverlässigkeitszielen und Produkthaftung. In: 25. Fachtagung Technische Zuverlässigkeit (TTZ 2011), Leonberg bei Stuttgart. VDI-Berichte 2146, VDI-Verlag, Düsseldorf, 2011

[MH06] MILES, R.; HAMILTON, K.: Learning UML 2.0 – A Pragmatic Introduction to UML. O'Reilly Media, Inc., Sebastopol, CA, USA, 2006

[MHD+07] MÜLLER, M.; HÖRMANN, K.; DITTMANN, L.; ZIMMER, J.: Automotive SPICE in der Praxis – Interpretationshilfe für Anwender und Assessoren. dpunkt.Verlag, Heidelberg, 2007

[MNF10] MARQUEZ, N.; NEIL, M.; FENTON, N.: Improved reliability modeling using Bayesian networks and dynamic discretization. In: Reliability Engineering and System Safety, Volume 95, Elsevier Science Ltd., Oxford, 2010, S. 412-425

[Möh04] MÖHRINGER, S.: Entwicklungsmethodik für mechatronische Systeme. Habilitationsschrift, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 156, Paderborn, 2004

[MP10] MEYNA, A.; PAULI, B.: Zuverlässigkeitstechnik, Quantitative Bewertungsverfahren. 2. Auflage, Carl Hanser Verlag, München, 2010

[MRL11] MERLE, G.; ROUSSEL, J.-M.; LESAGE, J.-J.: Dynamic Fault Tree Analysis Based on the Structure Function. In: The Annual Reliability and Maintainability Symposium – RAMS, Jan. 24-27, Lake Buena Vista, FL, USA, 2011, S. 1-6

[Mur02] MURPHY, K.P.: Dynamic Bayesian Networks: Representation, Inference and Learning. PhD Thesis, University of California, Berkeley, 2002

[MW04] MITSCHKE, M.; WALLENTOWITZ, H: Dynamik der Kraftfahrzeuge. 4. Auflage, VDI-Buch, Springer-Verlag, Berlin, 2004

[Nas02] NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA): Fault Tree Handbook with Aerospace Applications. Version 1.1, 2002

[Nau00] NAUMANN, R.: Modellierung und Verarbeitung vernetzter intelligenter mechatronischer Systeme. Fortschrittsbericht VDI Reihe 20, Nr. 318, VDI Verlag, Düsseldorf, 2000

[NBP14-ol] NEUE BAHNTECHNIK PADERBORN: RailCab – Projektwebseite. Unter: http://railcab.de, 20. Juni 2014

[NJT08] NACHTIGAL, V.; JÄKER, K.-P.; TRÄCHTLER, A.: Development and Control of a Quarter-Vehicle Testbed for a Fully Active X-by-Wire Demonstrator. In: 9th International Symposium on Advanced Vehicle Control (AVEC), October 6-9, Kobe, Japan, 2008

[Nor11] NORTH, K.: Wissensorientierte Unternehmensführung – Wertschöpfung durch Wissen. Gabler Verlag | Springer Fachmedien Wiesbaden GmbH, 5. Auflage, 2011

[OK12] O'CONNOR, P.; KLEYNER, A.: Practical Reliability Engineering. 5th edition, John Wiley & Sons, Ltd., Chichester, West Sussex, United Kingdom, 2012

[OMG11] OBJECT MANAGEMENT GROUP (OMG): OMG Unified Modeling Language (OMG UML), Superstructure. Sprachspezifikation der UML Version 2.4, OMG Document Number: ptc/2010-11-14, Januar, 2011

[PBF+07] PAHL, G.; BEITZ, W.; FELDHUSEN, J.; GROTE, K.-H.: Konstruktionslehre – Grundlagen erfolgreicher Produktentwicklung – Methoden und Anwendung. 7. Auflage, Springer Verlag, Berlin, 2007

[PCM10] PORTINALE, L.; CODETTA-RAITERI, D.; MONTANI, S.: Supporting reliability engineers in exploiting the power of Dynamic Bayesian Networks. In: International Journal of Approximate Reasoning, Vol. 51, Elsevier Science Ltd., Oxford, 2010, S. 179-195

[PGD12] POOK, S.; GAUSEMEIER, J.; DOROCIAK, R.: Securing the reliability of tomorrow's systems with Self-Optimization. In: The Annual Reliability and Maintainability Symposium – RAMS, Jan. 23-26, Reno, Nevada, USA, 2012

[PH13] PFEFFER, P.; HARRER, M. (Hrsg.): Lenkungshandbuch. 2. Auflage, ATZ/MTZ-Fachbuch, Springer Fachmedien, Wiesbaden, 2013

[Poo11] POOK, S.: Eine Methode zum Entwurf von Zielsystemen selbstoptimierender mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn. HNI-Verlagsschriftenreihe, Band 296, Paderborn, 2011

[Ptc13-ol] PTC, INC.: Windchill Quality Solutions. Unter: http://www.ptc.com/products/windchill/quality/, 17. Dezember 2013

[Rau02] RAUZY, A.: Mode automata and their compilation into fault trees. In: Reliability Engineering and System Safety, Volume 78, Issue 1, Elsevier Science Ltd., Oxford, 2002, S. 1-12

[Rec09-ol] RECHTSLUPE – NACHRICHTEN AUS RECHT UND STEUERN: Der Airbag im Schlagloch. Unter: http://www.rechtslupe.de/zivilrecht/der-airbag-im-schlagloch-311682, 11. November 2009

[Rei04] REICHEL, R.: Steuersysteme im Flugzeug – Fly-By-Wire. In: at – Automatisierungstechnik 52 (2004), Oldenbourg Verlag, München, 2004

[Rei10] REIF, K. (Hrsg): Fahrstabilisierungssysteme und Fahrerassistenzsysteme. Bosch Fachinformation Automobil, Vieweg+Teubner Verlag |Springer Fachmedien Wiesbaden GmbH, 2010

[Rei11] REIF, K. (Hrsg.): Bosch Autoelektrik und Autoelektronik – Bordnetze, Sensoren und elektronische Systeme. 6. Auflage, Vieweg + Teubner Verlag | Springer Fachmedien Wiesbaden GmbH, 2011

[Rei12] REIF, K. (Hrsg.): Automobilelektronik – eine Einführung für Ingenieure. 4. Auflage, ATZ/MTZ-Fachbuch, Vieweg+Teubner Verlag |Springer Fachmedien Wiesbaden GmbH, 2012

[Rel13a-ol] RELIASOFT CORPORATION: The Synthesis Platform. Unter: http://www.reliasoft.com/synthesis/index.htm, 10. Dezember 2013

[Rel13b-ol] RELIABILITY HOTWIRE – the eMagazine for the Reliability Professional: Reliability Basics – Complex Risk Analysis of System-Level Effects. Unter: http://www.weibull.com/hotwire/issue133/relbasics133.htm, 28. Dezember 2013

[RGD10] RONGXING, D.; GUOCHUN, W.; DECUN, D.: A New Assessment Method for System Reliability Based on Dynamic Fault Tree. In: Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA), May 11-12, Changsha, China, 2010, S. 219-222

[RLH96] Reinhart, G.; Lindemann, U.; Heinzl, J.: Qualitätsmanagement – Ein Kurs für Studium und Praxis. Springer-Verlag, Berlin Heidelberg, 1996

[RNJ+09] REINOLD, P.; NACHTIGAL, V.; JÄKER, K.-P.; TRÄCHTLER, A:. Control Strategy for the Lateral and Longitudinal Dynamics of a Fully Active X-by-wire Test Vehicle. In: Proceedings of the European Control Conference (ECC), August 23-26, Budapest, Hungary, 2009, pp. 4241-4246

[Roc98] ROCKWELL AUTOMATION AG: Grundlagen für die Praxis – Motorschutz – Notwendigkeit des Motorschutz, Schutzbedürfnis des Motors, Schutzmethoden. Fachbuch zum Thema Motormanagement, Publikation WP Protect, Januar 1998

[Rot00] ROTH, K.-H.: Konstruieren mit Konstruktionskatalogen – Band 1: Konstruktionslehre. 3. Auflage, Springer-Verlag, Berlin, 2000

[Sch07] SCHULZ, G.: Regelungstechnik 1 – Lineare und Nichtlineare Regelung, Rechnergestützter Reglerentwurf. 3. Auflage, Oldenbourg Wissenschaftsverlag GmbH, München, 2007

[Sch08] SCHULZ, G.: Regelungstechnik 2 – Mehrgrößenregelung, Digitale Regelungstechnik, Fuzzy-Regelung. 2. Auflage, Oldenbourg Wissenschaftsverlag GmbH, München, 2008

[SFB08] SONDERFORSCHUNGSBEREICH 614: Finanzierungsantrag für den Sonderforschungsbereich 614 „Selbstoptimierende Systeme des Maschinenbaus“ für die 3. und letzte Förderperiode, 2. Halbjahr 2009 bis 1. Halbjahr 2013. Universität Paderborn, 2008

[SFB11] SONDERFORSCHUNGSBEREICH 614: Selbstoptimierende Systeme des Maschinenbaus – Intelligente Maschinen für die Märkte von morgen. Informationsbroschüre, Heinz Nixdorf Institut der Universität Paderborn, 2011

[SMD+12] SONDERMANN-WÖLKE, C.; MEYER, T.; DOROCIAK, R.; GAUSEMEIER, J.; SEXTRO, W.: Early Development of Advanced Condition Monitoring for the Self-Optimizing Guidance Module of a Railway Vehicle based on its Principle Solution. In: 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference – PSAM & ESREL, June 25-29, Helsinki, Finland, 2012

[SO92] SOUZA E SILVA, E. DE; OCHOA, P.M.: State space exploration in Markov models. In: Proceedings of the 1992 ACM SIGMETRICS Joint International Conference on Measurement and Modeling of Computer Systems, Newport, Rhode Islands, USA, S. 152-166

[Spi09-ol] SPIEGEL ONLINE: Blockiertes Gaspedal: Toyota plant Rückruf von 3,8 Millionen Autos (30. September 2009). Unter: http://www.spiegel.de/auto/aktuell/blockiertes-gaspedal-toyota-plant-rueckruf-von-3-8-millionen-autos-a-652205.html, 1. Oktober 2009

[Spi10-ol] SPIEGEL ONLINE: Tödliche Gefahr durch Airbag: Honda ruft 379.000 Autos zurück (10. Februar 2010), Unter: http://www.spiegel.de/auto/aktuell/toedliche-gefahr-durch-airbag-honda-ruft-379-000-autos-zurueck-a-676931.html, 20. Februar 2010

[Spi12a-ol] SPIEGEL ONLINE: Rückrufaktion in Deutschland – Was Toyota-Kunden jetzt wissen müssen (14. November 2012). Unter: http://www.spiegel.de/auto/aktuell/die-wichtigsten-infos-zur-toyota-rueckrufaktion-a-867156.html, 11. Dezember 2012

[Spi12b-ol] SPIEGEL ONLINE: Prius-Rückrufaktion – Toyota muss 1,1 Milliarden Dollar an US-Kunden zahlen (27. Dezember 2012). Unter: http://www.spiegel.de/wirtschaft/unternehmen/toyota-muss-us-kunden-nach-rueckrufaktion-1-1-milliarden-dollar-zahlen-a-874728.html, 29. Dezember 2012

[Spi13a-ol] SPIEGEL ONLINE: Loses Lenkrad: Nissan ruft 841.000 Autos in die Werkstätten (23. Mai 2013). Unter: http://www.spiegel.de/auto/aktuell/rueckruf-nissan-ruft-841-000-autos-in-die-werkstaetten-a-901400.html, 26. September 2013

[Spi13b-ol] SPIEGEL ONLINE: Möglicher Defekt am Gaspedal: Nissan ruft 910.000 Autos in die Werkstätten (26. September 2013). Unter: http://www.spiegel.de/auto/aktuell/nissan-ruft-841-000-autos-in-die-werkstaetten-a-924683.html, 26. September 2013

[Spi13-ol] SPIEGEL ONLINE: Enthüllung über Stuxnet-Virus: Obamas Cyber-Angriff auf Irans Atomanlagen. Unter: http://www.spiegel.de/netzwelt/netzpolitik/usa-und-israel-sollen-stuxnet-virus-gegen-iran-entwickelt-haben-a-836401.html, 24. August 2013

[SRM13-ol] SODEN, M.; REDTENBACHER, A.; MARUHN, M: Modellgetrieben zum technischen Sicherheitskonzept. ElektronikAutomotive, Sonderheft Funktionale Sicherheit, WEKA FACHMEDIEN GmbH, Juli, 2013. Online unter: http://www.elektroniknet.de/automotive/sonstiges/artikel/99098/, 5. Juli 2013

[SS11a] SCHÖLZKE, M.; SODEN, M.: Erprobung einer modellbasierten integrierten Werkzeuglösung für funktionale Sicherheit bei General Motors. In: 11. EUROFORUM Jahrestagung „Software im Automobil“, 6./7. Juli 2011, Stuttgart, 2011

[SS11b] SMITH, D.J.; SIMPSON, K.G.L.: Safety Critical Systems Handbook – A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition) and Related Standards. 3rd Edition, Butterworth-Heinemann, an imprint of Elsevier Ltd., Oxford, UK, 2011

[Sta13-ol] STATISTA GMBH: Anzahl der durch das Kraftfahrt-Bundesamt eingeleiteten Rückrufaktionen. Unter: http://de.statista.com/statistik/daten/studie/6753/umfrage/Rückrufaktionen-durch-das-Kraftfahrt-Bundesamt-seit-1998, 20. Oktober 2013

[Ste07] STEFFEN, D.: Ein Verfahren zur Produktstrukturierung für fortgeschrittene mechatronische Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 207, Paderborn, 2007

[Sto96] STOREY, N.: Safety-Critical Computer Systems. Addison-Wesley, 1996

[STP+12] SIERLA, S.; TUMER, I.; PAPAKONSTANTINOU, N.; KOSKINEN, K.; JENSEN, D.: Early integration of safety to the mechatronic system design process by the functional failure identification and propagation framework. Mechatronics 22(2012), 2012

[Süd13-ol] SÜDDEUTSCHE.DE: Rückrufe wegen DSG -- Doppelkupplungsgetriebe wird für VW zum Dauerproblem (12. Juni 2013). Unter: http://www.sueddeutsche.de/auto/rueckrufe-wegen-dsg-doppelkupplungsgetriebe-wird-fuer-vw-zum-dauerproblem-1.1695010, 3. September 2013

[SVE+07] STAHL, T.; VOLTER, M.; EFFTINGE, S.; HASSE, A.: Modellgetriebene Softwareentwicklung: Techniken, Engineering, Management. 2. Auflage, dpunkt.verlag, Heidelberg, 2007

[SZ13] SCHÄUFFELE, J.; ZURAWKA, T.: Automotive Software Engineering: Grundlagen, Prozesse, Methoden und Werkzeuge effizient einsetzen. 5. Auflage, ATZ/MTZ-Fachbuch, Springer Fachmedien, Wiesbaden, 2013

[Tag14] TAGESSCHAU ONLINE: Erneute Rückrufaktion – GM findet die nächsten Fehler (21. Mai 2014). Unter: http://www.tagesschau.de/wirtschaft/gm-rueckruf108.html, 24. Mai 2014

[Taz11] TAZIR, N.: Viel diskutiert, selten wirklich angewendet – Systems Engineering. In: Produktdatenjournal Nr. 2/2011, ProSTEP iViP e.V., Darmstadt, 2011

[TBG04] TICHY, M.; BECKER, B.; GIESE, H.: Component Templates for Dependable Real-Time Systems. Technical Report tr-ri-04-253. In: Proceedings of the 2nd International Fujaba Days 2004, Darmstadt, 2004

[Toy10-ol] TOYOTA: Fragen und Antworten für Toyota Kunden: Rückrufaktion „Gaspedal“ für Toyota in Europa (Stand: 04.02.10). Unter: http://www.toyota.de/about/news_and_events/recall-statement-faq.tmex, 6. Februar 2010

[Trö05] TRÖSTER, F.: Steuerungs- und Regelungstechnik für Ingenieure. 2. Auflage, Oldenbourg Wissenschaftsverlag GmbH, München, 2005

[Wei07] WEILKIENS, T.: Systems Engineering with SysML/UML – Modeling, Analysis, Design. The MK/OMG Press, Morgan Kaufmann Publishers, an imprint of Elsevier, Inc., Burlington, MA, USA, 2007

[WHW12] WINNER, H.; HAKULI, S.; WOLF, G. (Hrsg.): Handbuch Fahrerassistenzsysteme. 2. Auflage, Vieweg+Teubner Verlag |Springer Fachmedien Wiesbaden GmbH, 2012

[WIH+04] WINNER, H.; ISERMANN, R.; HANSELKA, H.; SCHÜRR, A.: Wann kommt By-Wire auch für Bremse und Lenkung? Steuerung und Regelung von Fahrzeugen und Motoren. In: 2. Fachtagung Steuerung und Regelung von Kraftfahrzeugen und Verbrennungsmotoren – AUTOREG 2004, 2. und 3. März 2004, Wiesloch, 2004

[Wil06] WILLIS, R: Survey of Support Software for Reliability Engineering. Washington Chapter, Society of Reliability Engineers, April, 2006

[WMS+12] WEBER, P.; MEDINA-OLIVA, G.; SIMON, C.; IUNG, B.: Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence, Vol. 25, Iss. 4, 2012, p. 671 – 682

[Wro10] WROBLEWSKI, D.: Konzept einer fehlertoleranten, elektrohydraulischen steer-by-wire Lenkung für langsam fahrende Fahrzeuge. Dissertation, Fakultät für Maschinenbau und Schiffstechnik der Universität Rostock, 2010

Normen und Richtlinien

[CENELEC50126] EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION (CENELEC): CENELEC EN 50126:1999. Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 1999

[DIN19225] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN 19 225: Messen, Steuern, Regeln – Benennung und Einteilung von Reglern. Beuth-Verlag, Berlin, 1981

[DIN19226] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN EN 61025: Fehlzustandsbaumanalyse. Beuth-Verlag, Berlin, 2007

[DIN31000] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN ISO 31000: Risikomanagement – Grundsätze und Leitlinien. Norm-Entwurf, Beuth-Verlag, Berlin, 2011

[DIN40041] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN 40 041: Zuverlässigkeit – Begriffe. Beuth-Verlag, Berlin, 1990

[DIN60300-3-1] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN EN 60300-3-1: Zuverlässigkeitsmanagement – Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik. Beuth-Verlag, Berlin, 2005

[DIN60812] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA). Beuth-Verlag, Berlin, 2006

[DIN61014] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN EN 61014: Programme für das Zuverlässigkeitswachstum. Beuth-Verlag, Berlin, 2004

[DIN61025] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN EN 61025: Fehlzustandsbaumanalyse. Beuth-Verlag, Berlin, 2007

[DIN61165] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN EN 61165: Anwendung des Markoff-Verfahrens. Beuth-Verlag, Berlin, 2007

[DIN61703] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN EN 61703: Mathematische Ausdrücke für Begriffe der Funktionsfähigkeit, Verfügbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft. Beuth-Verlag, Berlin, 2002

[DIN820-120] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN 820-120: Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen. Beuth-Verlag, Berlin, 2012

[DIN820-120] DEUTSCHES INSTITUT FÜR NORMUNG E.V. (DIN): DIN 820-120: Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen. Beuth-Verlag, Berlin, 2012

[ECE-R79] UNITED NATIONS ECONOMIC AND SOCIAL COUNCIL (ECE): Regulation No. 79 (ECE-R79): Uniform provisions concerning the approval of vehicles with regard to steering equipment. United Nations Economic and Social Council (ECE), 2005

[IEC31010] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC/FDIS 31010: Risk management — Risk assessment techniques. Final Draft, IEC, Geneva, Switzerland, 2009

[IEC61508] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, Parts 1-7. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC61508-1] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 1: General Requirements. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC61508-2] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC61508-3] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 3: Software requirements. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC61508-4] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 4: Definitions and abbreviations. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC61508-5] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 5: Examples of methods for the determination of safety integrity levels. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC61508-6] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC61508-7] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems – Part 7: Overview of techniques and measures. Edition 2.0, IEC, Geneva, Switzerland, 2010

[IEC-TR-62380] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC TR 62380: Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs. Technical Report, IEC, Geneva, Switzerland, 2004

[IEEE1413-1] THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE): IEEE Std 1413.1-2002 IEEE Guide for Selecting and Using Reliability Predictions Based on IEEE 1413. The Institute of Electrical and Electronics Engineers, Inc., New York, NY, USA, 2003

[IEV191] INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC): IEC 60050: International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service. IEC, Geneva, Switzerland, 1990

[ISO13489-2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation. Beuth Verlag, Berlin, 2003

[ISO26262] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety, Parts 1-10. Beuth Verlag, Berlin, 2011

[ISO26262-1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 1: Vocabulary. Beuth Verlag, Berlin, 2011

[ISO26262-10] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 10: Guideline on ISO 26262. Beuth Verlag, Berlin, 2011

[ISO26262-2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 2: Management of functional safety. Beuth Verlag, Berlin, 2011

[ISO26262-3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 3: Concept phase. Beuth Verlag, Berlin, 2011

[ISO26262-4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 4: Product development at the system level. Beuth Verlag, Berlin, 2011

[ISO26262-5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 5: Product development at the hardware level. Beuth Verlag, Berlin, 2011

[ISO26262-6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 6: Product development at the software level. Beuth Verlag, Berlin, 2011

[ISO26262-7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 7: Production and operation. Beuth Verlag, Berlin, 2011

[ISO26262-8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 8: Supporting processes. Beuth Verlag, Berlin, 2011

[ISO26262-9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 26262: Road vehicles – Functional safety – Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses. Beuth Verlag, Berlin, 2011

[ISO9000] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): ISO 9000: Quality management systems - Fundamentals and Vocabulary. ISO, Geneva, Switzerland, 2005

[MIL-HDBK-217] UNITED STATES OF AMERICA DEPARTMENT OF DEFENSE: MIL-HDBK-217F: Military Handbook – Reliability Prediction of Electronic Equipment, 1990

[MIL-HDBK-338] UNITED STATES OF AMERICA DEPARTMENT OF DEFENSE: MIL-HDBK-338B: Military Handbook – Electronic Reliability Design Handbook, 1998

[MIL-STD-882] UNITED STATES OF AMERICA DEPARTMENT OF DEFENSE: MIL-STD-882: System Safety Program Requirements / Standard Practice for System Safety. Revision E, 11 May 2012

[SAE ARP926] SOCIETY OF AUTOMOTIVE ENGINEERS (SAE): SAE ARP926: Design analysis procedure for failure modes, effects and criticality analysis (FMECA). Aerospace Recommended Practice, 1967

[SN29500] SIEMENS AG: Siemens Norm SN 29500, Ausfallraten Bauelemente. CT SR Corporate Standardization & Regulation, München and Erlangen, 2004

[VDA3-1] VERBAND DER AUTOMOBILINDUSTRIE (VDA): VDA 3, Teil 1: Qualitätsmanagement in der Automobilindustrie – Zuverlässigkeitssicherung bei Automobilherstellern und Lieferanten – Zuverlässigkeitsmanagement. 3. Auflage, Verband der Automobilindustrie e.V. (VDA), Frankfurt, 2000

[VDI/VDE3542-1] VEREIN DEUTSCHER INGENIEURE (VDI); VERBAND DER ELEKTROTECHNIK, ELEKTRONIK, INFORMATIONSTECHNIK (VDE): VDI/VDE 3542, Blatt 1: Sicherheitstechnische Begriffe für Automatisierungssysteme – Qualitative Begriffe. Beuth-Verlag, Berlin, 2000

[VDI/VDE3542-2] VEREIN DEUTSCHER INGENIEURE (VDI); VERBAND DER ELEKTROTECHNIK, ELEKTRONIK, INFORMATIONSTECHNIK (VDE): VDI/VDE 3542, Blatt 2: Sicherheitstechnische Begriffe für Automatisierungssysteme – Quantitative Begriffe und Definitionen. Beuth-Verlag, Berlin, 2000

[VDI2206] VEREIN DEUTSCHER INGENIEURE (VDI): VDI 2206: Entwicklungsmethodik für mechatronische Systeme. Beuth-Verlag, Berlin, 2004

[VDI2221] VEREIN DEUTSCHER INGENIEURE (VDI): VDI 2221: Methodik zum Entwickeln und Konstruieren technischer Systeme und Produkte. Beuth-Verlag, Berlin, 1993

[VDI4001-2] VEREIN DEUTSCHER INGENIEURE (VDI): VDI 4001, Blatt 2: Terminologie der Zuverlässigkeit. Beuth-Verlag, Berlin, 2006

[VDI4003] VEREIN DEUTSCHER INGENIEURE (VDI): VDI 4003: Zuverlässigkeitsmanagement. Beuth-Verlag, Berlin, 2012

[VDI4007] VEREIN DEUTSCHER INGENIEURE (VDI): VDI 4007: Zuverlässigkeitsziele - Ermittlung, Überprüfung, Festlegung, Nachweis. Beuth-Verlag, Berlin, 2007

Gerichtsurteile

[BGH-2-StR-549/89] BUNDESGERICHTSHOF (BGH): Strafrechtliche Produkthaftung: Lederspray. Urteil vom 6. Juli 1990 (Aktenzeichen 2 StR 549/89), 1990

[BGH-VI-ZR-107/08] BUNDESGERICHTSHOF (BGH): Zur Haftung eines Fahrzeugherstellers für die Fehlauslösung von Airbags. Urteil vom 16. Juni 2009 (Aktenzeichen VI ZR 107/08), 2009

[BGH-VI-ZR-158/94] BUNDESGERICHTSHOF (BGH): Überprüfungs- und Befundsicherungspflicht des Herstellers kohlensäurehaltiger Mineralwässer. Urteil vom 9. Mai 2009 (Aktenzeichen VI ZR 158/94), 1995

Anhang

Inhaltsverzeichnis Seite

A1 Ergänzende Erläuterungen zur Problemanalyse und zum Stand der Technik

A1.1 Exkurs: Fehlertolerante Systemarchitekturen

Redundanz (engl. redundancy) bedeutet das „Vorhandensein von mehr als den erforderlichen Mitteln für die Ausführung einer Funktion“ [LPP10, S. 336]. Alle Formen der Fehlertoleranz beruhen auf Redundanz [Sto96, S. 124]. Bild A-1 zeigt die grundsätzlichen Arten der Redundanz [Sto96, S. 124 ff.], [Hil12, S. 62], [Ech90]:

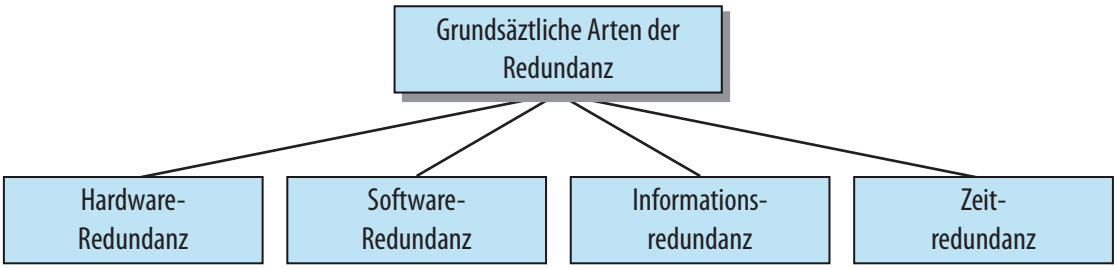


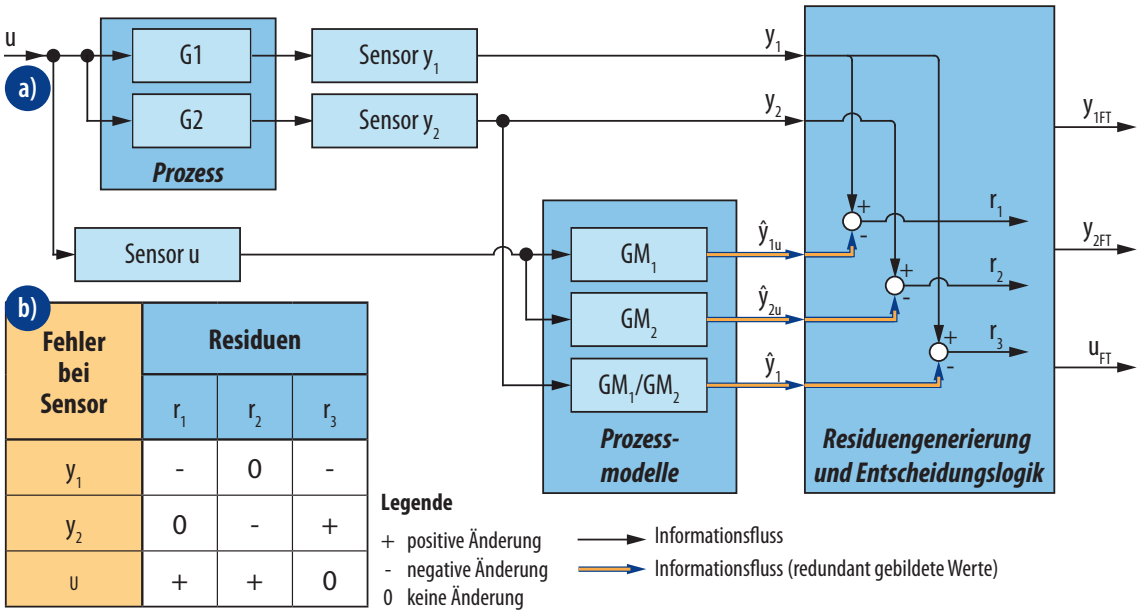
Bild A-1: Arten der Redundanz (in Anlehnung an [Hil12, S. 62] nach [Ech90])

Hardware Redundanz ist die Erweiterung eines Systems um zusätzliche für den Normalbetrieb nicht notwendige Systemelemente auf der Ebene der elektronischen Hardware [Sto96, S. 125]. Beispiel – Triple Modular Redundancy (TMR) [TBG04], [Sto96, S. 124]: Beim Einsatz der TMR wird die zu erbringende Funktion von drei gleichartigen, unabhängigen Systemelementen erbracht. Auf Basis der Outputs dieser Systemelemente trifft ein Voter eine Mehrheitsentscheidung: es wird das Ergebnis weitergereicht, welches von mindestens zwei der redundanten Systemelemente gemeldet wurde.

Software Redundanz ist „die Erweiterung eines Systems um zusätzliche für den Nutzbetrieb entbehrliche Funktionen“, die auf der Software-Ebene erfolgt [Hil12, S. 62], [Ech90]. Dabei werden zwei Arten funktionaler Redundanz unterschieden: Zusatzfunktionen und diversitäre Redundanz. **Zusatzfunktionen** sind Funktionen, „deren Spezifikation sich von den Spezifikationen aller Nutzbetriebs-Funktionen unterscheidet (folglich sind auch die Implementierungen verschieden)“ [Ech90], [Hil12, S. 63]. Ein Beispiel hierfür stellen Überwachungsfunktionen dar, welche im Falle der Überschreitung einer Abweichungsschwelle entsprechende Maßnahmen einleiten [Hil12, S. 63]. **Diversitäre Redundanz** bedeutet „die Erfüllung der Spezifikation einer Nutzbetriebs-Funktion durch mehrere verschiedenartig implementierte [Systemelemente]“ [Ech90]. Ein Beispiel hierfür ist diversitäre Software. Es handelt sich hierbei um mindestens zwei Software-Komponenten, welche dieselbe Funktion erbringen und durch unterschiedliche Programmierteams unter Verwendung unterschiedlicher Programmiersprachen und Compilern entwickelt wurden [Ise07a, S. 174]. Eine Ausprägung hiervon ist die Technik des N-Version Programming [Sto96, S. 145]: Hier werden N verschiedene Implementierungen eines

Programms verwendet, die auf derselben Spezifikation basieren und damit einhergehend das gleiche Ergebnis herbeiführen sollten. Stimmen nicht alle der erhaltenen Ergebnisse miteinander überein, so wird bei N >2 eine Mehrheitsentscheidung getroffen. Bei N=2 kann keine Mehrheitsentscheidung getroffen werden. Abhilfe schafft in solch einem Fall zum Beispiel die Wiederholung der Berechnung und ein erneuter Vergleich.

Die sogenannte **analytische Redundanz** beruht auf der Abbildung von Relationen zwischen unterschiedlichen Signalen in einem mathematischen Modell (Prozessmodell). Bild A-2 a) stellt ein beispielhaftes Umsetzungsschema dar:



b)

Fehler bei Sensor	Residuen		
	r_1	r_2	r_3
y_1	-	0	-
y_2	0	-	+
u	+	+	0

Bild A-2: Analytische Sensor-Redundanz für einen Prozess mit einem gemessenen Eingang u und zwei gemessenen Ausgängen y1 und y2: a) für alle drei Messwerte erfolgt eine Bildung redundanter Werte und Residuen und darauf aufbauend der fehlertoleranten Werte; b) zugehörige Fehler-Symptom-Tabelle

Aus allen drei Messwerten (Eingang u und Ausgänge y_1 und y_2) werden unter Heranziehung der Prozessmodelle GM_1 und GM_2 drei redundante Signale $\hat{y}_1$, $\hat{y}_{1u}$ und $\hat{y}_{2u}$ gebildet. Im Subsystem „Residuengenerierung und Entscheidungslogik“ werden zum einen aus den redundanten Signalen und den ursprünglichen Ausgangsignalen Residuen r_1, r_2 und r_3 bestimmt. Zum anderen erfolgt hier unter Verwendung der Entscheidungslogik die Bildung der fehlertoleranten Ausgangssignale y_{1FT}, y_{2FT} und u_{FT}. Die Entscheidungslogik beruht auf der in Bild A-2 b) dargestellten Fehler-Symptom-Tabelle. Diese beschreibt eindeutige Muster für die Fehler der drei Sensoren [Ise07a, S. 178].

Analytische Redundanz kommt zum Beispiel bei einem Gierraten-Sensor für das ESP System zum Einsatz [Ise07a, S. 178]. Verwendet wird hierbei ein vereinfachtes Modell des Lenkverhaltens. Eingang des Modells ist der Lenkradwinkel, Ausgang die über einen

Gierraten-Sensor ermittelte Gierrate. Kern der analytischen Redundanz bilden Prozessmodelle, welche aus der Querbeschleunigung und der Differenz der Drehzahlsignale einen Wert der Gierrate nachbildet, welcher dann der Entscheidungseinheit zugeführt wird.

Informationsredundanz bezieht sich auf die Nutzung von zusätzlichen Informationen, die über die für das Erbringen der Funktion notwendigen Informationen hinausgehen. Ziel ist es, potentielle Fehler zu detektieren und zu tolerieren. Informationsredundanz kann unter Heranziehung von Software- bzw. Hardware-Techniken umgesetzt werden [Sto96, S. 125]. Ein Beispiel stellt das sogenannte Parity Bit-Verfahren dar, mit dem gewisse Fehler im Speicher entdeckt werden können [IEC61508-7, S. 18]. Die Grundidee besteht darin, durch Hinzufügen eines so genannten Parity Bits, das Gewicht des Speicher-Worts (die Anzahl von logischen Einsen) systematisch auf eine gerade oder ungerade Zahl zu bringen [Rei12, S. 11]. Die Entscheidung ob eine gerade oder ungerade Zahl von Einsen maßgeblich ist, wird in Abhängigkeit von der Ausgangs-Problemstellung getroffen [IEC61508-7, S. 18]. Bei jedem Lesevorgang wird das Gewicht des Worts überprüft. Wird eine falsche Anzahl von logischen Einsen gefunden (z.B. eine ungerade Zahl obwohl eine gerade Zahl erwartet wird), so wird eine Fehlermeldung generiert [IEC61508-7, S. 18]. Ein weiteres Beispiel ist das zyklische Blocksicherungsverfahren (Cyclic Redundancy Check, CRC), welches aufwändigere Berechnung zur Fehlererkennung nutzt. Für mehr Informationen siehe hierzu [Rei12, S. 11], [Bor10, S. 92].

Zeitredundanz bedeutet die Erzeugung „über den Zeitbedarf des Normalbetriebs hinausgehender zusätzlicher Zeit, die einem funktionell redundanten System zur Funktionsausführung zur Verfügung steht“ [Ech90], [Hil12, S. 63]. Diese zusätzliche Zeit wird verwendet, um potentielle Fehler zu erkennen bzw. zu tolerieren, zum Beispiel durch Wiederholung einer Berechnung und Vergleich der berechneten Ergebnisse [Sto96, S. 125]. Damit lassen sich unter anderem transiente Fehler erkennen.

In der praktischen Umsetzung kommen meist Mischformen der oben genannten Redundanzarten vor [Sto96, S. 126].

In der elektronischen Hardware werden für fehlertolerante Systeme grundsätzlich zwei Anordnungen unterschieden: statische und dynamische Redundanz. **Statische Redundanz** ist in Bild A-3 schematisch dargestellt [Ise07a, S. 173ff.]: Zum Einsatz kommen drei oder mehr parallel angeordnete Subsysteme, die alle dasselbe Eingangssignal haben und alle aktiv sind. Die Ausgangssignale der redundanten Subsysteme werden an einen Voter weitergegeben, der diese Signale vergleicht und auf Basis einer Mehrheitsentscheidung entscheidet, welches der Signale korrekt ist. Beispiel – „2 aus 3 Systeme“: hier wird das Signal von zwei übereinstimmenden Kanälen weitergegeben, das abweichende Signal wird als fehlerhaft angenommen und ignoriert bzw. maskiert [Ise07a, S. 174]. In diesem Fall kann ein Ausfall eines einzigen Subsystems toleriert werden. Die Fehlertoleranz kann durch eine redundante Auslegung des Voters noch weiter verbessert werden [Ise07a, S. 174]. Nachteile der statischen Redundanz sind hohe Kosten, höherer Energieverbrauch,

höheres Gewicht etc. [Ise07a, S. 174]. Ferner ist sie im Falle von Ausfällen infolge gemeinsamer Ursache (Common Cause Failures) nicht wirksam [Ise07a, S. 174].

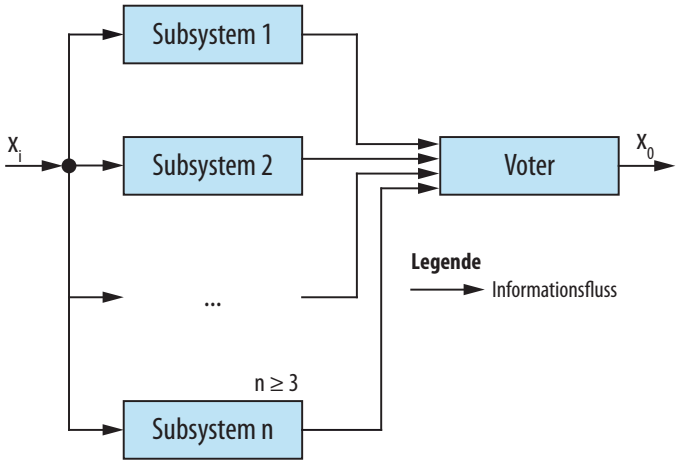


Bild A-3: Statische Redundanz: mehrere redundante Subsysteme mit Mehrheitsentscheidung und Fehlerausblendung („m aus n Systeme“); alle Subsysteme sind aktiv [Ise07a, S. 174]

Die **dynamische Redundanz** kommt mit einer kleineren Zahl von Subsystemen aus, erfordert hierfür aber eine erhöhte Informationsverarbeitung [Ise07a, S. 174]: Bild A-4 zeigt eine Minimalkonfiguration für die dynamische Redundanz. Eins der redundanten Subsysteme (hier Subsystem 1) ist im Normalbetrieb aktiv. Tritt ein Fehler im Betrieb des aktiven Subsystems auf und wird dieser durch die Fehlererkennung erkannt, so erfolgt eine Rekonfiguration. Es wird auf die Reservereinheit umgeschaltet (hier: Subsystem 2); das fehlerhafte Subsystem wird außer Betrieb genommen [Ise07a, S. 174]. In der in Bild A-4 betrachteten Konfiguration ist die Reserveeinheit permanent in Betrieb. Diese als **„hot standby“** bezeichnete Konfiguration hat den Vorteil, dass die Umschaltzeit kurz ist. Nachteilig ist, dass das Reservesystem aufgrund des permanenten Aktivseins altert und verschleißt [Ise07a, S. 174].

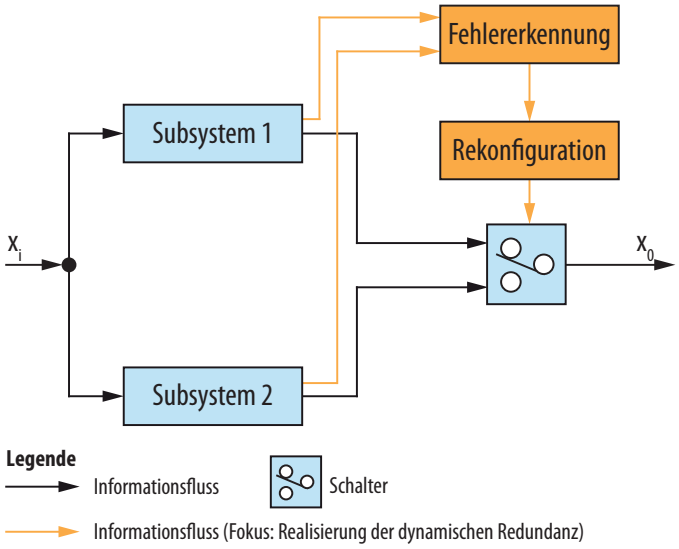


Bild A-4: Dynamische Redundanz – „hot standby“ Konfiguration: die Reserveeinheit ist permanent aktiv [Ise07a, S. 174]

Bild A-5 zeigt eine andere Konfiguration für dynamische Redundanz – die **„cold standby“** Konfiguration. Hier ist die Reserveeinheit standardmäßig nicht in Betrieb. Der

für die „hot standby“ Konfiguration charakteristische Alterung des Reservesystems kommt hier nicht vor. Die „cold standby“ Konfiguration benötigt zwei weitere Schalter an den Eingängen der redundant ausgelegten Subsysteme, die durch die Rekonfigurationseinheit betätigt werden. Ferner benötigt sie typischerweise mehr Zeit für den Umschaltvorgang, da die Startzeit des Reservesystems zusätzlich anfällt [Ise07a, S. 174]. Für beide Konfigurationen ist die Leistung der Fehlererkennung sehr wichtig, da nur im Falle der Fehlererkennung eine Rekonfiguration angestoßen werden kann [Ise07a, S. 174].

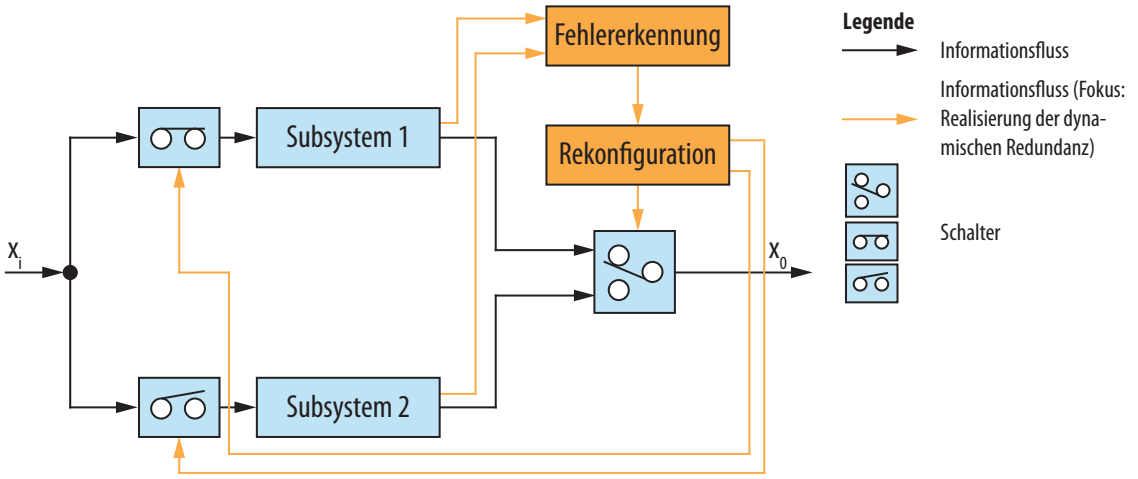


Bild A-5: Dynamische Redundanz – „cold standby“ Konfiguration: die Reserveeinheit ist im Normalbetrieb inaktiv [Ise07a, S. 174]

A1.2 Berechnung der Zuverlässigkeitskenngrößen bei nichtelementaren Systemstrukturen

Methode der minimalen Ausfallschnitte

Gegeben sein ein System, welches aus mehreren Subsystemen besteht. Unter einem Ausfallschnitt ist jede Kombination von Subsystemen zu verstehen, dessen kombiniertes Ausfallen zum Ausfall des Gesamtsystems führt [BL04, S. 175]. Ein Ausfallschnitt heißt minimal, wenn er keine anderen Ausfallschnitte als eine echte Teilmenge enthält [MP10, S. 259]. Für das in Bild 2-10 dargestellte System ergeben sich folgende Minimalschnitte [BL04, S. 175]:

C_1 = {Subsystem 1, Subsystem 2}, C_2 = {Subsystem 3, Subsystem 4},
C_3 = {Subsystem 1, Subsystem 4, Subsystem 5} und
C_4 = {Subsystem 2, Subsystem 3, Subsystem 5},

Bild A-6 stellt die Minimalschnitte graphisch dar. Das Gesamtsystem fällt aus, wenn alle Subsysteme wenigstens eines Minimalschnitts ausgefallen sind. Es ergibt sich die folgende Boolesche Funktion zur Beschreibung des Systemausfalls (die Notation mit Balken oben stellt einen Ausfall dar):

$$\bar{y} = (\overline{Subsystem\ 1} \wedge \overline{Subsystem\ 2}) \vee (\overline{Subsystem\ 3} \wedge \overline{Subsystem\ 4}) \vee (\overline{Subsystem\ 1} \wedge \overline{Subsystem\ 4} \wedge \overline{Subsystem\ 5}) \vee (\overline{Subsystem\ 2} \wedge \overline{Subsystem\ 3} \wedge \overline{Subsystem\ 5})$$

Gleichung A-1: Funktion zur Berechnung des Systemausfalls ausgehend von den Minimalschnitte

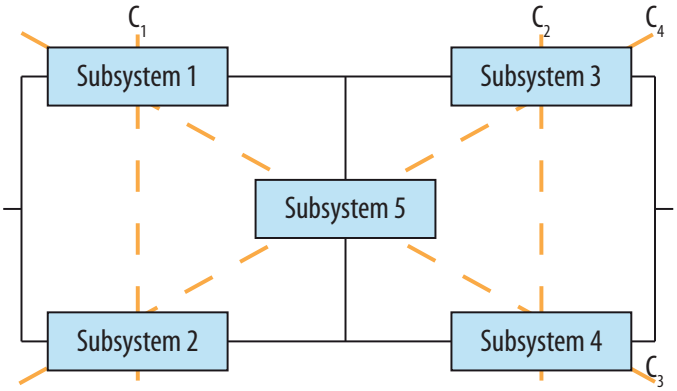


Bild A-6: Minimalschnitte in einer Brückenanordnung [BL04, S. 175]

Methode der minimalen Erfolgspfade

Unter einem Erfolgspfad ist eine Kombination von Subsystemen zu verstehen, aus kombinierten Funktionsfähigkeit dessen die Funktionsfähigkeit des Gesamtsystems resultiert [BL04, S. 176]. Ein Erfolgspfad heißt minimal, wenn er keine anderen Erfolgspfade als eine echte Teilmenge enthält [MP10, S. 257]. Für das in Bild 2-10 dargestellte System ergeben sich folgende minimale Erfolgspfade [BL04, S. 176]:

P_1 = {Subsystem 1, Subsystem 3}, P_2 = {Subsystem 2, Subsystem 4},
P_3 = {Subsystem 1, Subsystem 4, Subsystem 5} und
P_4 = {Subsystem 2, Subsystem 3, Subsystem 5},

Bild A-7 stellt die minimalen Erfolgspfade graphisch dar. Das Gesamtsystem ist funktionsfähig, wenn mindestens einer der minimalen Erfolgspfade funktionsfähig ist. Die Funktionsfähigkeit des Gesamtsystems lässt sich wie folgt darstellen [BL04, S. 176]:

$$y = (Subsystem\ 1 \wedge Subsystem\ 3) \vee (Subsystem\ 2 \wedge Subsystem\ 4) \vee (Subsystem\ 1 \wedge Subsystem\ 4 \wedge Subsystem\ 5) \vee (Subsystem\ 2 \wedge Subsystem\ 3 \wedge Subsystem\ 5)$$

Gleichung A-2: Funktion zur Berechnung der Funktionsfähigkeit für ein System ausgehend von den minimalen Erfolgspfaden

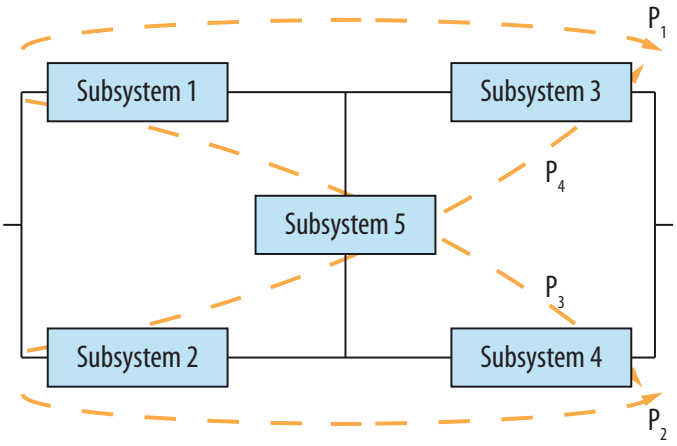


Bild A-7: Minimale Erfolgspfade in einer Brückenanordnung [BL04, S. 176]

Zur Ermittlung von minimalen Ausfallschnitten bzw. minimalen Erfolgspfaden werden Fehlzustandsbäume herangezogen (vgl. Abschnitt 3.2.2.3) [Nas02, S. 157 ff.], [Eri05, 198ff.]. Der Übergang zu Wahrscheinlichkeiten erfolgt bei den beiden Methoden z.B. mit Hilfe des Poincaréschen Algorithmus (Inklusions-Exklusions-Methode) bzw. des Top-Down-Algorithmus [BL04, S. 177]. Für eine Beschreibung dieser sei auf [MP10, S. 263 ff.] und [Eri05, S. 199 ff.] verwiesen.

A1.3 Ausgewählte Wahrscheinlichkeitsverteilungen zur Beschreibung des Ausfallverhaltens technischer Systeme

Exponentialverteilung

Für ein exponential verteiltes Ausfallverhalten lassen sich die Zuverlässigkeitsgrößen wie folgt beschreiben [BL04, S. 41]:

Überlebenswahrscheinlichkeit	$R(t) = e^{-\lambda t}$
Ausfallwahrscheinlichkeit	$F(t) = 1 - e^{-\lambda t}$
Ausfalldichte	$f(t) = \lambda \cdot e^{-\lambda t}$
Ausfallrate	$\lambda(t) = \lambda = konst$
Mittlere Lebensdauer bis zum Ausfall	$MTTF = E(\tau) = \frac{1}{\lambda}$ τ: Lebensdauer der Einheit

Gleichung A-3: Wesentliche Kenngrößen für eine konstante Ausfallrate λ(t) = λ = const (Exponentialverteilung) [BL04, S. 41]

Für konstante Ausfallrate gilt, dass die MTTF die Zeitdauer angibt, bei der die Einheit noch mit 37 % Wahrscheinlichkeit funktionsfähig ist [Ise07a, S. 171]. Diese Feststellung beruht auf folgender mathematischen Berechnung: $R(MTTF) = e^{-\lambda \cdot \frac{1}{\lambda}} = e^{-1} \approx 0{,}368 \approx 37\%$.

Für ein beispielhaftes Gerät mit konstanter Ausfallrate $\lambda = 0{,}0002$ Ausfälle pro Stunde gilt folgendes: die mittlere Lebensdauer bis zum Ausfall beträgt $MTTF = \frac{1}{\lambda} = 5000$ Stunden. Die Überlebenswahrscheinlichkeit des Geräts zum Zeitpunkt 10000 Stunden beträgt $R(10000) = e^{-\lambda \cdot 10000} = e^{-2} \approx 0{,}135$. Angenommen, dass das Gerät 6000 Stunden funktionsfähig war, beträgt der Erwartungswert für die Restlebensdauer MTTF(6000) = MTTF = 5000 Stunden. Die Wahrscheinlichkeit für die Funktionsfähigkeit nach weiteren 10000 Stunden beträgt $R(16000|6000) = R(10000) \approx 0{,}135$.

Aus dem obigen Beispiel wird deutlich, dass sich die Zuverlässigkeitsmodellbildung bei einer konstanten Ausfallrate besonders einfach gestaltet. Dies gilt nicht nur für die oben dargestellten Kenngrößen, sondern auch für Ausfallraten zusammengesetzter Systeme. Zum Beispiel ergibt sich die Gesamtausfallrate eines Seriensystems durch die Summation der Ausfallraten der einzelnen Subsysteme [MP10, S. 117]. Aufgrund dieser einfachen Modellbildung wird in der Praxis inkorrekterweise auch dann mit einer konstanten Ausfallrate gerechnet, wenn diese nicht konstant ist [MP10, S. 117].

Ist die zugrunde liegende Lebensdauerverteilung bekannt, so lässt sich das Ausfallverhalten eines Systems bzw. eines Systemelements grafisch anschaulich darstellen [BL04, S. 36]. Bild A-8 zeigt den Verlauf der Zuverlässigkeitskenngrößen bei konstanter Ausfallrate (Exponentialverteilung) für verschiedene Ausfallraten ($\lambda = 2$, $\lambda = 1$ und $\lambda = 0{,}5$):

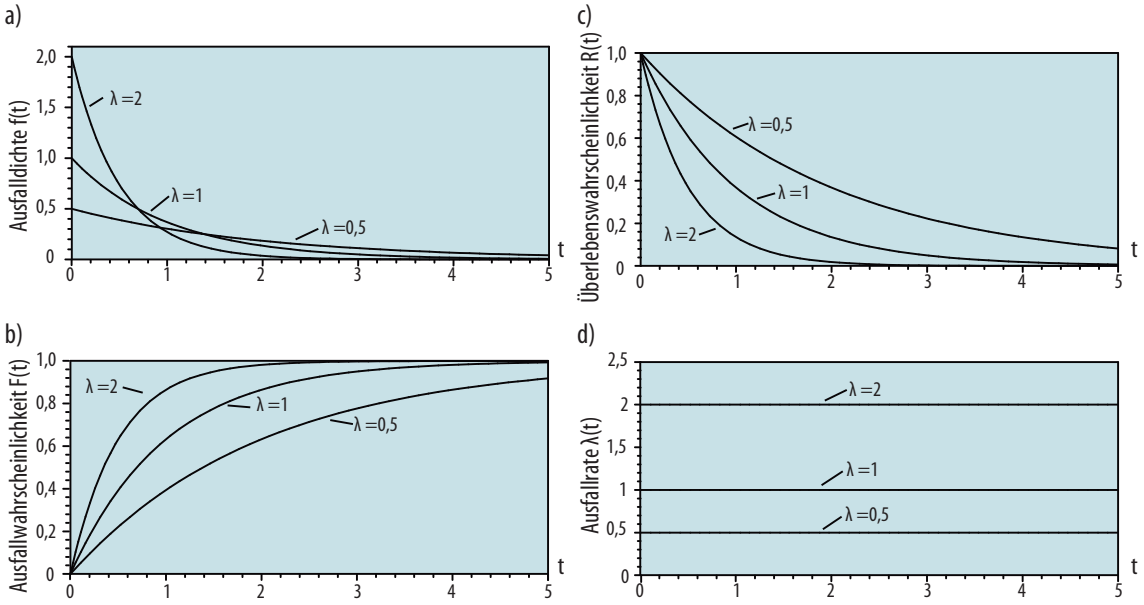


Bild A-8: Verlauf der Zuverlässigkeitskenngrößen bei konstanter Ausfallrate (Exponentialverteilung) [BL04, S. 40]

Aus der graphischen Darstellung wird folgendes ersichtlich [BL04, S. 41]: Die Ausfallrate bleibt unabhängig vom betrachteten Zeitpunkt gleich groß (Bild A-8 d)). Die Ausfalldichte fällt kontinuierlich ab (a), ebenso die Überlebenswahrscheinlichkeit (c). Die Ausfallwahrscheinlichkeit nimmt entsprechend kontinuierlich zu (b). Bezogen auf die noch funktionsfähigen Systemelemente fällt zu einem bestimmten Zeitpunkt immer ein gleich großer Prozentsatz der Systemelemente aus, da die Ausfallrate ja konstant ist. Damit eignet sich die Exponentialverteilung zur Beschreibung von Zufallsausfällen (Bereich 2 der Badewannenkurve) besonders gut.

Weibullverteilung

Das mit der Exponentialverteilung beschriebene Ausfallverhalten kann im Maschinenbau nur sehr selten beobachtet werden [BL04, S. 41]. Zur Beschreibung des Ausfallverhaltens maschinenbaulicher Erzeugnisse wird meist eine andere Lebensdauerverteilung – die Weibullverteilung – herangezogen [BL04, S. 37 und 41ff.].

Die **Weibullverteilung** ermöglicht die Abbildung von unterschiedlichen Arten des Ausfallverhaltens. Sie wird durch zwei bzw. drei Parameter definiert. Die zweiparametrige Weibullverteilung besitzt als Parameter die charakteristische Lebensdauer T und den Formparameter b [BL04, S. 42]. Die charakteristische Lebensdauer T ist „eine Art Mittelwert und gibt damit an, wo ungefähr die Mitte der Verteilung ist“ [BL04, S. 42]. Der Formparameter bildet die Streuung der Ausfallzeiten und die Form der Ausfalldichte ab [BL04, S. 42]. Bei einer zweiparametrigen Weibullverteilung werden die Ausfälle stets ab dem Zeitpunkt t = 0 beschrieben. Um Ausfälle zu beschrieben, die erst ab einem Zeitpunkt t_0 anfangen, wird die dreiparametrige Weibullverteilung herangezogen [BL04, S. 42]. Neben den beiden Parameter T und b besitzt diese zusätzlich einen dritten Parameter, die ausfallfreie Zeit t_0. Bild A-9 zeigt wie sich der Verlauf der Ausfalldichte in Abhängigkeit vom Parameter b verändert [BL04, S. 46]:

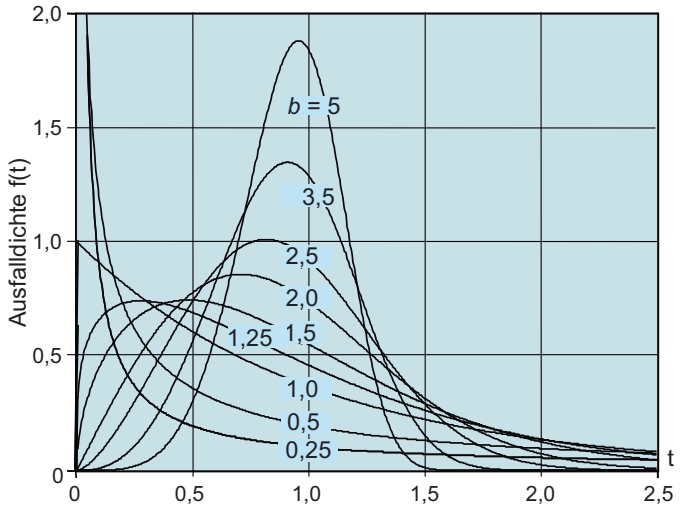


Bild A-9: Verlauf der Ausfalldichte der Weibullverteilung für unterschiedliche Formparameter b (charakteristische Lebensdauer T = 1, ausfallfreie Zeit t_0=0) [BL04, S. 44]

- für b < 1 gilt: hier nehmen die Ausfallraten mit zunehmender Lebensdauer ab.

- für b = 1 gilt: hier ist die Ausfallrate konstant. Es ergibt sich exakt die Exponentialverteilung.
- für b > 1 gilt: mit zunehmender Lebensdauer steigen die Ausfallraten deutlich an.

Es ergeben sich folgende Zuverlässigkeitsgrößen:

Überlebenswahrscheinlichkeit	$R(t) = e^{-\left(\frac{t-t_0}{T-t_0}\right)^b}$
Ausfallwahrscheinlichkeit	$F(t) = 1 - e^{-\left(\frac{t-t_0}{T-t_0}\right)^b}$
Ausfalldichte	$f(t) = \frac{dF(t)}{dt} = \frac{b}{T-t_0} \cdot \left(\frac{t-t_0}{T-t_0}\right)^{b-1} \cdot e^{-\left(\frac{t-t_0}{T-t_0}\right)^b}$
Ausfallrate	$\lambda(t) = \frac{f(t)}{R(t)} = \frac{b}{T-t_0} \cdot \left(\frac{t-t_0}{T-t_0}\right)^{b-1}$
Mittlere Lebensdauer bis zum Ausfall	$MTTF = E(\tau) = t_0 + T \cdot \Gamma\left(1 + \frac{1}{b}\right)$
	Γ: die Gammafunktion mit $\Gamma(n) = \int_0^\infty e^{-x} x^{n-1} dx$
	τ: Lebensdauer der Einheit

Gleichung A-4: Wesentliche Kenngrößen für die dreiparametrige Weibullverteilung (bei $t_0 = 0$ ergeben sich die Kenngrößen für die zweiparametrige Weibullverteilung) [BL04, S. 43], [MP10, S. 65]

Bild A-10 zeigt den Verlauf der Ausfallwahrscheinlichkeit der Weibullverteilung für unterschiedliche Formparameter b, Bild A-11 bildet den Verlauf der Überlebenswahrscheinlichkeit ab.

Die drei beschriebenen Wertebereiche von b lassen sich den Bereichen der Badewannen kurve eindeutig zuordnen (Bild A-12). Die Weibullverteilungen mit b < 1 eignen sich zur Beschreibung der Frühausfälle (abnehmende Ausfallrate). Die Weibullverteilungen mit b = 1 ermöglichen die Abbildung der Zufallsausfälle (konstante Ausfallrate). Schließlich können mit Weibullverteilungen mit b > 1 Verschleiß- und Ermüdungsausfälle beschrieben werden (zunehmende Ausfallrate).

Für eine detaillierte Darstellung der Exponential- und der Weibullverteilung sowie weiterer Lebensdauerverteilungen siehe [BL04, S. 36 ff.], [MP10, 58 ff.], [Bir07, S. 419 ff.].

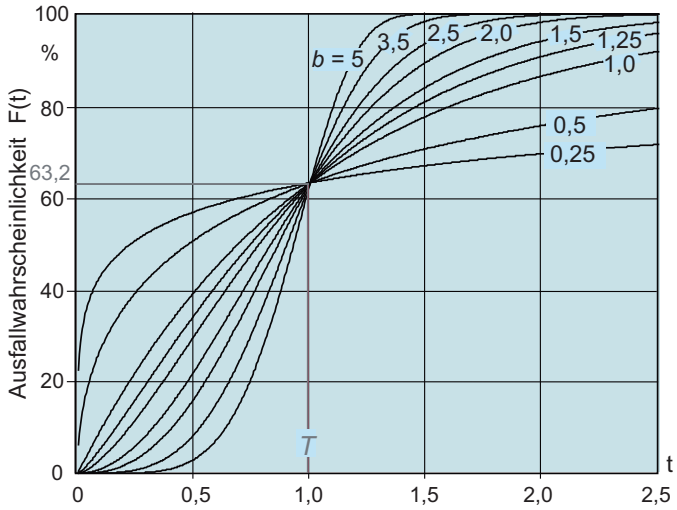


Bild A-10: Verlauf der Ausfallwahrscheinlichkeit der Weibullverteilung für unterschiedliche Formparameter b (charakteristische Lebensdauer T = 1, ausfallfreie Zeit t_0=0) [BL04, S. 44]

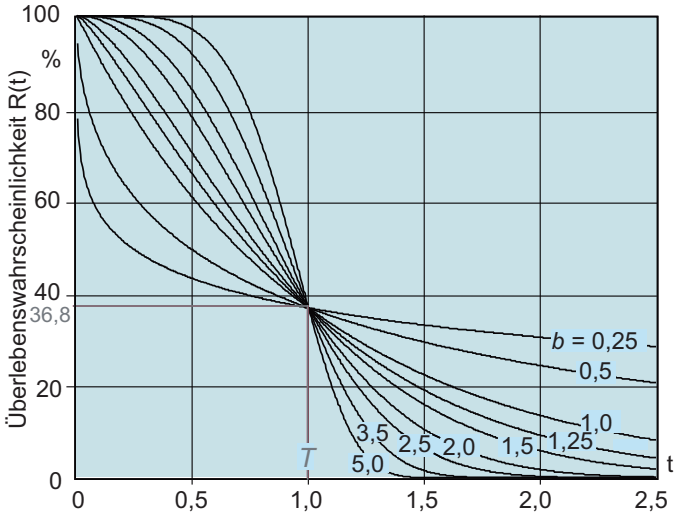


Bild A-11: Verlauf der Überlebenswahrscheinlichkeit der Weibullverteilung für unterschiedliche Formparameter b (charakteristische Lebensdauer T = 1, ausfallfreie Zeit t_0=0) [BL04, S. 45]

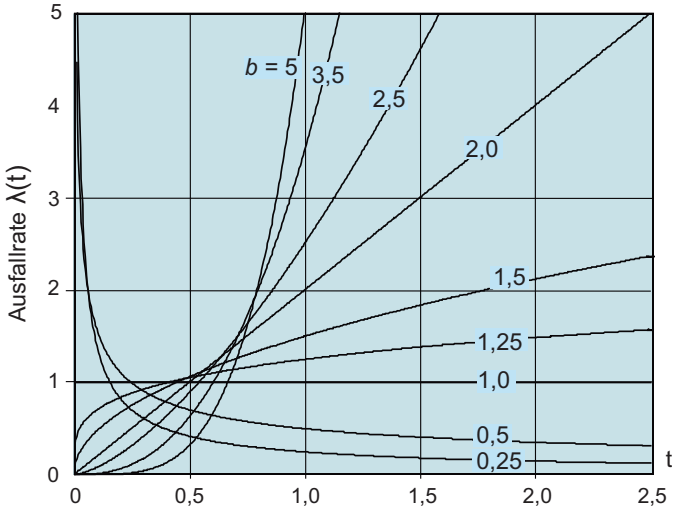


Bild A-12: Verlauf der Ausfallrate der Weibullverteilung für unterschiedliche Formparameter b (charakteristische Lebensdauer T = 1, ausfallfreie Zeit t_0=0) [BL04, S. 45]

A1.4 Exkurs: Ausgewählte Grundlagen der Regelungstechnik

Unter den an der Entwicklung moderner technischer Erzeugnisse beteiligten Domänen nimmt die Regelungstechnik eine besondere Stellung ein [GEK01, S. 219]. Viele Funktionen moderner technischer Erzeugnisse wie der Kraftfahrzeuge, Flugzeuge oder Roboter basieren zunehmend auf regelungstechnischen Konzepten. Die zunehmende Durchdringung technischer Systeme mit Regelungstechnik lässt sich auf steigende Anforderungen zurückführen, die an diese Systeme gestellt werden. Insbesondere geht es hierbei um die Verbesserung der Genauigkeit der durch den Systemnutzer wahrnehmbaren physikalischen Größen (z.B. Verbesserung des Lenkgefühls in einer elektromechanischer Lenkung [PH13, S. 404ff.]) und die Forderung einer automatischen Nachführung im Falle des Eintretens spezieller Ereignisse [GEK01, S. 219].

Die Regelungstechnik ist „die Wissenschaft von der selbsttätigen gezielten Beeinflussung dynamischer Systeme“ [Föl90]. Sie ist nie isoliert anzutreffen, sondern immer im Zusammenhang mit einem zu beeinflussenden System. Im Kontext der vorliegenden Arbeit ist das zu beeinflussende System meist mechanischer Natur. Es wird als Grundsystem oder als (Regel-)Strecke bezeichnet.

Die grundsätzliche Aufgabe jeder Regelung besteht darin, eine physikalische Größe (die Regelgröße) trotz unterschiedlicher Störeinflüsse (Störgröße) auf einem gewünschten Wert (Führungsgröße) zu halten bzw. im Falle einer Änderung der Führungsgröße die Regelgröße möglichst schnell und störungsfrei auf den neuen Wert der Führungsgröße zu bringen. Bild A-13 stellt den allgemeinen Aufbau eines Regelkreises dar; die verwendeten Begriffe sind der Norm DIN 19225 entnommen [DIN19225]:

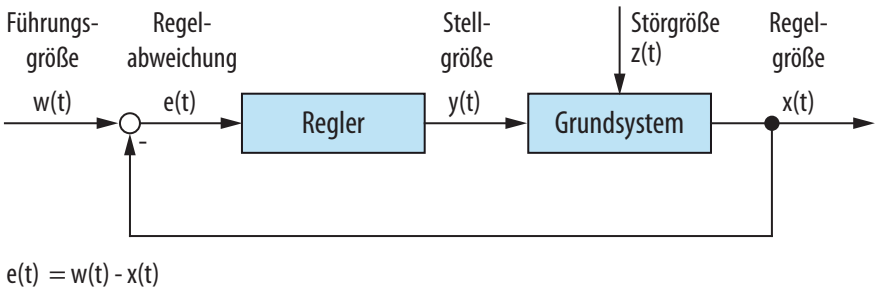


Bild A-13: Grundstruktur eines Regelkreises (klassische, einschleifige Eingangs-/Ausgangsregelung; Vereinfachte Darstellung ohne Stellglied, Messglied etc.) [Lun13a, S. 4], [Sch07, S. 11]

Der Regelkreis besteht aus dem Regler und dem Grundsystem, welches gezielt beeinflusst wird. Die Regelgröße x(t) (Ausgangsgröße des Regelkreises) hängt von der Stellgröße y(t) und der Störgröße z(t) ab. Die Störgröße z(t) ist hierbei nicht beeinflussbar. Ziel ist es, die Regelgröße x(t) der vorgegebenen Führungsgröße w(t) nachzuführen. Idealerweise soll x(t) = w(t) für alle Zeitpunkte t gelten. Folglich ist es die Aufgabe des Reglers die Stellgröße y(t) so vorzugeben, dass der Einfluss der Störgröße kompensiert und die Re-

gelgröße der Führungsgröße angepasst wird. Dem Regler steht hierfür als Eingangsinformation neben den gewünschten Wert w(t) auch der aktuelle Wert x(t) der Regelgröße zur Verfügung. Beide Werte werden einem Vergleichsglied zugeführt, welches graphisch als nicht ausgefüllter Kreis dargestellt wird. Hier wird die Differenz, die sogenannte Regelabweichung, e(t) = w(t) – x(t) berechnet und dem Regler zugeführt. In Abhängigkeit von der Regelabweichung gibt der Regler die Stellgröße zweckmäßig vor. Auch weitere Erweiterungen der grundlegenden Struktur des Regelkreises sind möglich. Z.B. könnte das Messrauschen aus der Messgröße gefiltert werden, bevor die Regel- und Führungsgröße verglichen werden [Lun13a, S. 5]. Für weiterführende Informationen sei auf [Lun13a], [Sch07] verwiesen.

Bild A-14 zeigt eine gegenüber Bild A-13 erweiterte Struktur eines Regelkreises [Lun13a, S. 5]. Zwei zusätzliche Systemelemente Stellglied und Messglied sind zu erkennen. Es wird berücksichtigt, dass bei Regelungen oft zwischen der Regelgröße x(t) und dem Messwert $x_M(t)$ der Regelgröße (Rückführgröße) unterschieden werden muss. Der Grund: das Messglied besitzt nicht selten selbst dynamische Eigenschaften, die dazu führen, dass die gemessene Regelgröße u.U. erheblich von der tatsächlichen abweicht [Lun13a, S. 5]. Ähnlich ist es um die Eingangsseite des Grundsystems bestellt. Der vom Regler vorgegebene Wert y(t) wird durch das Stellglied in den am Grundsystem wirksamen Wert $y_R(t)$ umgesetzt [Lun13a, S. 5]. Auch für das Stellglied gilt, dass dieses typischerweise ein eigenes dynamisches Verhalten aufweist [Lun13a, S. 5].

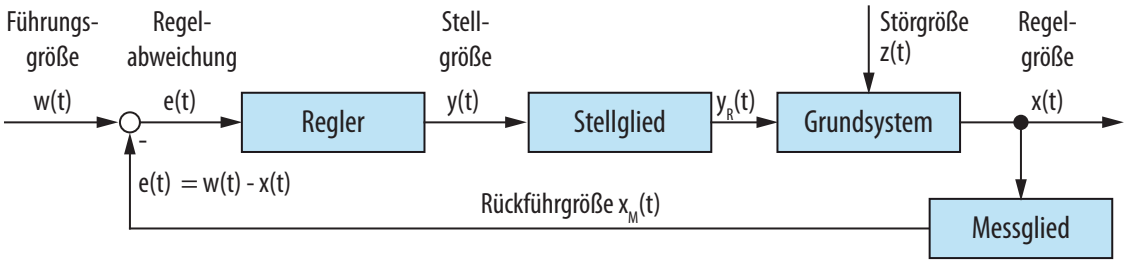


Bild A-14: Erweiterte Struktur eines Regelkreises [Lun13a, S. 5], [GEK01, S. 292]

Zusammenfassend lässt sich die prinzipielle Wirkungsweise einer Regelung als ein Prozess mit folgenden drei wesentlichen Phasen beschreiben [Lun13a, S. 6]:

1) **Messen**: Die Regelgröße wird gemessen. Die Messung erfolgt entweder direkt oder basierend auf anderen Messgrößen.

2) **Vergleichen**: Der Wert der Regelgröße wird hier mit dem Wert der Führungsgröße verglichen und die Regelabweichung ermittelt.

3) **Stellen**: Unter Berücksichtigung der dynamischen Eigenschaften des Grundsystems wird aus der Regelabweichung die Stellgröße bestimmt und das Grundsystem beeinflusst.

Das bisher vorgestellte auf einer Rückführung beruhende Wirkprinzip der Regelungstechnik wird als **Feedback-Control** bzw. **Closed Loop Control** bezeichnet [ADG+09,

S. 27]. Prinzipiell kann ein technisches System auch ohne Rückführung gesteuert werden (Bild A-15) [Lun13a, S. 9]. Man spricht dann von einer Steuerung in der offenen Wirkungskette (kurz Steuerung). Dieses Wirkprinzip wird auch als **Feedforward-Control** bzw. **Open Loop Control** bezeichnet [Sch08, S. 7]. Damit das gewünschte Verhalten durch eine gezielte Beeinflussung erreicht werden kann, müssen bei einer Steuerung zwei wesentliche Voraussetzungen erfüllt werden [Lun13a, S. 9]: Zum einen müssen die auf das Grundsystem wirkenden Einflüsse genau bekannt und modelliert werden können. Zum anderen darf das Grundsystem nicht gestört werden, da bei diesem Wirkprinzip auf Störgrößen nicht reagiert werden kann.

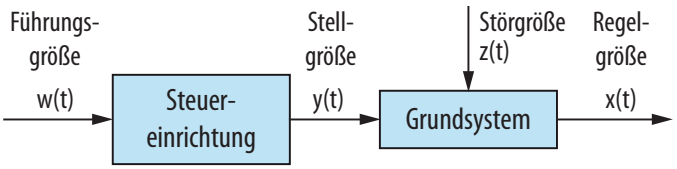


Bild A-15: Steuerung in der offenen Wirkungskette [Lun13a, S. 9]

Beide Arten von Regelungen können miteinander kombiniert werden [Lun13a, S. 11]. Oft wird einer Regelung eine Steuerung vorgeschaltet (Vorsteuerung). Für eine detaillierte Darstellung hierzu sei auf [Lun13a, S. 11ff.] verwiesen.

A1.5 Aufbau der IEC 61508 und der ISO 26262

Tabelle A-1 zeigt den Aufbau der IEC 61508 und der ISO 26262 [IEC61508], [ISO26262], [LPP10, S. 8; S. 119]:

Tabelle A-1: Aufbau der IEC 61508 und der ISO26262

IEC 61508	ISO26262
• **Teil 1:** Allgemeine Anforderungen • **Teil 2:** Anforderungen an sicherheitsbezogene E/E/PE Systeme • **Teil 3:** Anforderungen an Software • **Teil 4:** Begriffe und Abkürzungen • **Teil 5:** Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität • **Teil 6:** Anwendungsrichtlinie für Teil 2 und Teil 3 • **Teil 7:** Anwendungshinweise über Verfahren und Maßnahmen	• **Teil 1:** Glossar (vocabulary) • **Teil 2:** Management der funktionalen Sicherheit (management of functional safety) • **Teil 3:** Konzeptphase (concept phase) • **Teil 4:** Produktentwicklung: Systemebene (product development: system level) • **Teil 5:** Produktentwicklung: Hardwareebene (product development: hardware level) • **Teil 6:** Produktentwicklung: Softwareebene (product development: software level) • **Teil 7:** Produktion und Betrieb (production and operation) • **Teil 8:** Unterstützende Prozesse (supporting processes) • **Teil 9:** ASIL- und sicherheitsorientierte Analysen (ASIL-oriented and safety-oriented analyses) • **Teil 10:** Orientierungshilfe (guideline)

A2 Design-FMEA für das Chamäleon

Tabelle A-2: Design-FMEA für das Chamäleon (Teil 1 von 5; Ausschnitt)

Fehlzustandsart- und -auswirkungsanalyse (FMEA)					
System: Chamäleon **Blatt:** 1 **Bearbeiter:** Dorociak **Stand:** 22. April 2013					
System-element	**Funktion**	**Ausfallmöglichkeit**	**Ausfallauswirkung**	**Ausfallursache**	**...**
Rad	Fahrzeugbewegung erzeugen	Luftaustritt	Verlust vom Kontakt zwischen Rad und Boden	Beschädigung des Reifen z.B. durch Nagel, Glasscherben etc.	...
				Überdruck im Reifen	...
				Überbelastung des Reifen	...
				Alterung des Reifen	...
				Produktionsfehler des Reifen	...
		Zu wenig Profil	Änderung der Kontakteigenschaften zwischen Rad und Boden; das Rad kann weniger Kraft erzeugen	Verschleiß	...
		Verlust vom mechanischen Kontakt zwischen Radträge und Rad	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Schrauben mit zu hohem Drehmoment angeschraubt	...
				Vibration (Schrauben locker, Schraubenbruch)	...
				Bruch der Kontaktplatte	...
Radträger	Lenkkraft übertragen Das Rad festhalten	Radträgerbruch	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Überlastung (z.B. falsche Position der Querlenker zueinander und damit einhergehend eine ungünstige innere Spannungsverteilung)	...
		Verlust vom mechanischen Kontakt zwischen Radträger und Querlenker	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Bruch des Gelenks aufgrund von Korrosion, Überlastung bzw. Vibration.	...
		Verlust vom mechanischen Kontakt zwischen Radträger und Lenkstange	Radeinschlag gegen ein Begrenzungselement. Folglich bewegt sich das Rad frei und lässt sich nicht mehr lenken. Nach mehreren Einschlägen kann sich das Rad vom Fahrzeug weglösen.	Kugelgelenkbruch	...
Querlenker	Radträger festhalten Fahrzeug federn	Verlust vom mechanischen Kontakt zwischen Querlenker und Fahrzeugkörper	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Bruch des Gelenks aufgrund von Korrosion, Überlastung bzw. Vibration	...
		Bruch des Querlenkers	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Überlastung des Querlenkers	...
		Bruch der Kontaktplatte	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Überlastung	...
...	...	...	...	...	...

Tabelle A-3: Design-FMEA für das Chamäleon (Teil 2 von 5; Ausschnitt)

Fehlzustandsart- und -auswirkungsanalyse (FMEA)					
System: Chamäleon **Blatt:** 2 **Bearbeiter:** Dorociak **Stand:** 22. April 2013					
System-element	**Funktion**	**Ausfallmöglichkeit**	**Ausfallauswirkung**	**Ausfallursache**	**...**
Radträger	Lenkkraft übertragen Das Rad festhalten	Radträgerbruch	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Überlastung (z.B. falsche Position der Querlenker zueinander und damit einhergehend eine ungünstige innere Spannungsverteilung)	...
		Verlust vom mechanischen Kontakt zwischen Radträger und Querlenker	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Bruch des Gelenks aufgrund von Korrosion, Überlastung bzw. Vibration.	...
		Verlust vom mechanischen Kontakt zwischen Radträger und Lenkstange	Radeinschlag gegen ein Begrenzungselement. Folglich bewegt sich das Rad frei und lässt sich nicht mehr lenken. Nach mehreren Einschlägen kann sich das Rad vom Fahrzeug weglösen.	Kugelgelenkbruch	... ...
Federmotor	Fahrzeug federn	Bruch der Ausgangswelle des Federmotors	Aktive Federung nicht möglich	Überlastung der Ausgangswelle des Federmotors	...
		Ausfall des elektrischen Teils des Federmotors	Aktive Federung nicht möglich	Kurzschluss	...
				Elektrische Verbindung unterbrochen	...
				Energieversorgung unterbrochen	...
				Überspannung am Frequenzumrichter	...
		Ausgangswelle des Federmotors verklemmt	Alle vertikale Bewegungen des Radmoduls sind blockiert, was fatale Auswirkungen für das Fahrverhalten des Fahrzeug hat.	Bruch eines der Kugellager im Federmotor	...
				Ausfall Getriebe	...
		Verlust vom mechanischen Kontakt zwischen Federmotor und Fahrzeugkörper	Aktive Federung nicht möglich	Bruch des Gelenks aufgrund von Korrosion, Überlastung bzw. Vibration.	...
Torsionsstabfeder	Fehrzeug federn	Bruch der Torsionsstabfeder	Passive Federung nicht möglich. Nur aktive Federung über den Federungsmotor für eine gewisse Zeit möglich bis der Motor überbelastet wird.	Überlastung hins. Gewicht; Elastizität nimmt ab	...
				Sehr niedrige Temperatur, was zu Sprödigkeit und anschließend Bruch führen kann	...
...	...	...	...	...	...

Tabelle A-4: Design-FMEA für das Chamäleon (Teil 3 von 5; Ausschnitt)

Fehlzustandsart- und -auswirkungsanalyse (FMEA)					
System: Chamäleon **Blatt:** 3 **Bearbeiter:** Dorociak **Stand:** 22. April 2013					
System-element	**Funktion**	**Ausfallmöglichkeit**	**Ausfallauswirkung**	**Ausfallursache**	...
Torsions-stabfeder (fortge-setzt)	Fahrzeug federn	Änderung der Steifigkeit der Torsions-stabfeder	Änderung der Steifigkeit (i.d.R. Steigerug) der passiven Fe-derung. Sie führt zu Komforteinschränkungen sowie zu mehr Schwingungen, welche sich negativ auf die Komponenten auswirken.	Überlastung der Torsionsstabfeder	...
				Ermüdung der Torsionsstabfeder	...
				Hohe Temperatur	...
				Sehr niedrige Temperatur, was zu Sprödigkeit und anschlie-ßend Bruch führen kann.	...
Lenkmotor	Fahrzeug lenken	Ausfall des elektrischen Teils des Lenkmotors	Lenkung des Rads nicht mehr möglich. Radeinschlag gegen ein Begrenzungselement. Folglich bewegt sich das Rad frei und lässt sich nicht mehr lenken. Nach mehreren Einschlägen kann sich das Rad vom Fahrzeug weglösen.	Kurzschluss	...
				Elektrische Verbindung unterbrochen	...
				Energieversorgung unterbrochen	...
				Überspannung am Frequenzumrichter	...
		Bruch der Ausgangswelle des Lenk-motors	(wie oben)	Überlastung der Ausgangswelle des Lenkmotors	...
		Ausgangswelle des Lenkmotors verklemmt	Das Rad ist blockiert (keine horizontale Bewegung möglich). Folglich lässt sich der gewünschte Lenkwinkel nicht einstellen und die Fahrdynamik wird beeinträchtigt.	Bruch eines der Kugellager im Federmotor	...
				Ausfall Getriebe	...
		Verlust von mechanischem Kontakt zwischen Lenkmotor und Fahrzeug-körper	Lenkung des Rads nicht mehr möglich. Radeinschlag gegen ein Begrenzungselement. Folglich bewegt sich das Rad frei und lässt sich nicht mehr lenken. Nach mehreren Einschlägen kann sich das Rad vom Fahrzeug weglösen.	Bruch des Gelenks aufgrund von Korrosion, Überlastung bzw. Vibration.	...
Antriebs-motor	Fahrzeug (Rad) antreiben	Ausgangswelle des Antriebsmotors verklemmt	Das Rad dreht sich nicht mehr. Fahrdynamik wird wesentlich beeinträchtigt.	Bruch eines der Kugellager im Antriebsmotor	...
				Ausfall Getriebe	...
		Bruch Ausgangswelle Antriebsmotor	Das zugehörige Rad wird nicht angetrieben	Überlastung der Ausgangswelle des Antriebsmotors	...
		Verlust vom mechanischen Kontakt zwischen Antriebsmotor und Quer-lenker	Fatale Auswirkungen für das Fahrverhalten des Fahrzeugs	Bruch des Gelenks aufgrund von Korrosion, Überlastung bzw. Vibration.	...
...	...	...	...	...	...

Tabelle A-5: Design-FMEA für das Chamäleon (Teil 4 von 5; Ausschnitt)

Fehlzustandsart- und -auswirkungsanalyse (FMEA)					
System: Chamäleon **Blatt:** 4 **Bearbeiter:** Dorociak **Stand:** 22. April 2013					
System-element	**Funktion**	**Ausfallmöglichkeit**	**Ausfallauswirkung**	**Ausfallursache**	...
Antriebs-motor (fortge-setzt)	Fahrzeug (Rad) antreiben	Ausfall des elektrischen Teils des Antriebsmotors	Das zugehörige Rad wird nicht angetrieben	Kurzschluss	...
				Elektrische Verbindung unterbrochen	...
				Energieversorgung unterbrochen	...
				Überspannung am Frequenzumrichter	...
Lenkwin-kelsensor	Lenkwinkel messen	Der Lenkwinkelsensor liefert keinen Messwert.	Regelung nicht möglich: • Lenkmotor wird ausgeschaltet. Lenken wird unmöglich. • Radeinschlag gegen ein Begrenzungselement. Folglich bewegt sich das Rad frei und lässt sich nicht mehr lenken. Nach mehreren Einschlägen kann sich das Rad vom Fahrzeug weglösen.	Bruch des Kabels	...
				Ausfall der Sensorelektronik	
				Ausfall der Sensormechanik	...
		Der Lenkwinkelsensor liefert einen falschen Messwert.	Es wird falsch geregelt: • Lenkwinkel wird falsch eingestellt, wodurch sich die Fahrdynamik verschlechtert. • Lenkmotor bekommt inkorrekte Signale, was zum frühzeitigen Ausfall des Lenkmotors führen kann.	CAN-Bus hat falsche Einstellungen	...
				Ausfall der Sensormechanik	...
Antriebs-motor	Fahrzeug (Rad) antreiben	Der Niveausensor liefert keinen Messwert.	Regelung nicht möglich: • Federmotor ausgeschaltet. Aktive Federung n. möglich. • Falsche vertikale Bewegung (kann durch das Ausschalten des Federmotors durch den Fahrer schnell behoben werden).	Bruch des Kabels	...
				Ausfall der Sensorelektronik	...
				Ausfall der Sensormechanik	...
Niveau-sensor	Niveau zwischen der unteren Platte des Fahrzeugs-körpers und Untergrund (Höhe) messen	Der Niveausensor liefert keinen Messwert.	Regelung nicht möglich: • Federmotor ausgeschaltet. Aktive Federung n. möglich. • Falsche vertikale Bewegung (kann durch das Ausschalten des Federmotors durch den Fahrer schnell behoben werden).	Bruch des Kabels	...
				(Winkel zwischen den Längsträger und den oberen Querlenker wird gemessen)	...
				Ausfall der Sensormechanik	...
...	...	...	...	...	...

Tabelle A-6: Design-FMEA für das Chamäleon (Teil 5 von 5; Ausschnitt)

Fehlzustandsart- und -auswirkungsanalyse (FMEA)					
System: Chamäleon **Blatt:** 5 **Bearbeiter:** Dorociak **Stand:** 22. April 2013					
System-element	**Funktion**	**Ausfallmöglichkeit**	**Ausfallauswirkung**	**Ausfallursache**	**...**
Niveau-sensor (fortge-setzt)	Niveau zwischen der unteren Platte des Fahrzeugs-körpers und Untergrund (Höhe) messen	Der Niveausensor liefert einen falschen Messwert.	Es wird falsch geregelt: • Falsche vertikale Bewegung (kann durch das Ausschal-ten des Federmotors durch den Fahrer schnell behoben werden).	CAN-Bus hat falsche Einstellungen	...
				Ausfall der Sensormechanik	...
				Bruch des Gelenks aufgrund von Korrosion, Überlastung bzw. Vibration.	...
Vertikaler Beschleu-nigungs-sensor	Beschleunigung messen	Beschleunigungsensor liefert keinen Messwert.	Regelung nicht möglich: • Lenkmotor wird ausgeschaltet. Lenken wird unmöglich. • Radeinschlag gegen ein Begrenzungselement. Folglich bewegt sich das Rad frei und lässt sich nicht mehr lenken. Nach mehreren Einschlägen kann sich das Rad vom Fahrzeug weglösen.	Bruch des Kabels	...
				Ausfall der Sensorelektronik	...
				Ausfall der Sensormechanik	...
		Beschleunigungsensor liefert einen falschen Messwert.	Es wird falsch geregelt: • Falsche vertikale Bewegung (kann durch das Ausschal-ten des Federmotors durch den Fahrer schnell behoben werden). • Federmotor bekommt inkorrekte Signale, was zum frühzeitigen Ausfall des Federmotors führen kann.	CAN-Bus hat falsche Einstellungen	...
				Ausfall der Sensormechanik	...
Elastomer	Antriebsmotor halten Bewegung des Motors dämpfen	Bruch des Elastomers	Antriebsmotor wird nicht mehr gehalten	Ermüdung des Materials	...
				Verformung des Materials	...
				Überbelastung des Fahrzeugs	...
		Bewegung des Antriebsmotors dämpfen	Die Bewegungen des Antreibsmotors werden nicht mehr richtig gedämpft. Dies kann dazu führen, dass der Antriebs-motor sehr schnell schwingt und aufgrund der zugehörigen Vibration ausfällt.	Ermüdung des Materials	...
				Dauerbelastung durch hohe Temperatur	...
				Dauerbelastung durch niedrige Temperatur	...

Das Heinz Nixdorf Institut – Interdisziplinäres Forschungszentrum für Informatik und Technik

Das Heinz Nixdorf Institut ist ein Forschungszentrum der Universität Paderborn. Es entstand 1987 aus der Initiative und mit Förderung von Heinz Nixdorf. Damit wollte er Ingenieurwissenschaften und Informatik zusammenführen, um wesentliche Impulse für neue Produkte und Dienstleistungen zu erzeugen. Dies schließt auch die Wechselwirkungen mit dem gesellschaftlichen Umfeld ein.

Die Forschungsarbeit orientiert sich an dem Programm „Dynamik, Mobilität, Vernetzung: Eine neue Schule des Entwurfs der technischen Systeme von morgen“. In der Lehre engagiert sich das Heinz Nixdorf Institut in Studiengängen der Informatik, der Ingenieurwissenschaften und der Wirtschaftswissenschaften.

Heute wirken am Heinz Nixdorf Institut acht Professoren mit insgesamt 200 Mitarbeiterinnen und Mitarbeitern. Etwa ein Viertel der Forschungsprojekte der Universität Paderborn entfallen auf das Heinz Nixdorf Institut und pro Jahr promovieren hier etwa 30 Nachwuchswissenschaftlerinnen und Nachwuchswissenschaftler.

Heinz Nixdorf Institute – Interdisciplinary Research Centre for Computer Science and Technology

The Heinz Nixdorf Institute is a research centre within the University of Paderborn. It was founded in 1987 initiated and supported by Heinz Nixdorf. By doing so he wanted to create a symbiosis of computer science and engineering in order to provide critical impetus for new products and services. This includes interactions with the social environment.

Our research is aligned with the program “Dynamics, Mobility, Integration: En-route to the technical systems of tomorrow.” In training and education the Heinz Nixdorf Institute is involved in many programs of study at the University of Paderborn. The superior goal in education and training is to communicate competencies that are critical in tomorrows economy.

Today eight Professors and 200 researchers work at the Heinz Nixdorf Institute. The Heinz Nixdorf Institute accounts for approximately a quarter of the research projects of the University of Paderborn and per year approximately 30 young researchers receive a doctorate.

Bände der HNI-Verlagsschriftenreihe

Bd. 309 WASSMANN, H.: Systematik zur Entwicklung von Visualisierungstechniken für die visuelle Analyse fortgeschrittener mechatronischer Systeme in VR-Anwendungen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 309, Paderborn, 2013 – ISBN 978-3-942647-28-1

Bd. 310 GAUSEMEIER, J.; RAMMIG, F.; SCHÄFER, W.; TRÄCHTLER, A. (Hrsg.): 9. Paderborner Workshop Entwurf mechatronischer Systeme. HNI-Verlagsschriftenreihe, Band 310, Paderborn, 2013 – ISBN 978-3-942647-29-8

Bd. 311 GAUSEMEIER, J.; GRAFE, M.; MEYER AUF DER HEIDE, F. (Hrsg.): 11. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Band 311, Paderborn, 2013 – ISBN 978-3-942647-30-4

Bd. 312 BENSIEK, T.: Systematik zur reifegradbasierten Leistungsbewertung und -steigerung von Geschäftsprozessen im Mittelstand. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 312, Paderborn, 2013 – ISBN 978-3-942647-31-1

Bd. 313 KOKOSCHKA, M.: Verfahren zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 313, Paderborn, 2013 – ISBN 978-3-942647-32-8

Bd. 314 VON DETTEN, M.: Reengineering of Component-Based Software Systems in the Presence of Design Deficiencies. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 314, Paderborn, 2013 – ISBN 978-3-942647-33-5

Bd. 315 MONTEALEGRE AGRAMONT, N. A.: Immunorepairing of Hardware Systems. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 315, Paderborn, 2013 – ISBN 978-3-942647-34-2

Bd. 316 DANGELMAIER, W.; KLAAS, A.; LAROQUE, C.: Simulation in Produktion und Logistik 2013. HNI-Verlagsschriftenreihe, Band 316, Paderborn, 2013 – ISBN 978-3-942647-35-9

Bd. 317 PRIESTERJAHN, C.: Analyzing Self-healing Operations in Mechatronic Systems. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 317, Paderborn, 2013 – ISBN 978-3-942647-36-6

Bd. 318 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 9. Symposium für Vorausschau und Technologieplanung, Heinz Nixdorf Institut, 5. und 6. Dezember 2013, Berlin-Brandenburgische Akademie der Wissenschaften, Berlin, HNI-Verlagsschriftenreihe, Band 318, Paderborn, 2013 – ISBN 978-3-942647-37-3

Bd. 319 GAUSEMEIER, S.: Ein Fahrerassistenzsystem zur prädiktiven Planung energie- und zeitoptimaler Geschwindigkeitsprofile mittels Mehrzieloptimierung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 319, Paderborn, 2013 – ISBN 978-3-942647-38-0

Bd. 320 GEISLER, J.: Selbstoptimierende Spurführung für ein neuartiges Schienenfahrzeug. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 320, Paderborn, 2013 – ISBN 978-3-942647-39-7

Bd. 321 MÜNCH, E.: Selbstoptimierung verteilter mechatronischer Systeme auf Basis paretooptimaler Systemkonfigurationen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 321, Paderborn, 2014 – ISBN 978-3-942647-40-3

Bd. 322 RENKEN, H.: Acceleration of Material Flow Simulations - Using Model Coarsening by Token Sampling and Online Error Estimation and Accumulation Controlling. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlags-schriftenreihe, Band 322, Paderborn, 2014 – ISBN 978-3-942647-41-0

Bd. 323 KAGANOVA, E.: Robust solution to the CLSP and the DLSP with uncertain demand and online information base. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlags-schriftenreihe, Band 323, Paderborn, 2014 – ISBN 978-3-942647-42-7

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 324 LEHNER, M.: Verfahren zur Entwicklung geschäftsmodell-orientierter Diversifikationsstrategien. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 324, Paderborn, 2014 – ISBN 978-3-942647-43-4

Bd. 325 BRANDIS, R.: Systematik für die integrative Konzipierung der Montage auf Basis der Prinziplösung mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 325, Paderborn, 2014 – ISBN 978-3-942647-44-1

Bd. 326 KÖSTER, O.: Systematik zur Entwicklung von Geschäftsmodellen in der Produktentstehung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 326, Paderborn, 2014 – ISBN 978-3-942647-45-8

Bd. 327 KAISER, L.: Rahmenwerk zur Modellierung einer plausiblen Systemstrukturen mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 327, Paderborn, 2014 – ISBN 978-3-942647-46-5

Bd. 328 KRÜGER, M.: Parametrische Modellordnungsreduktion für hierarchische selbstoptimierende Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 328, Paderborn, 2014 – ISBN 978-3-942647-47-2

Bd. 329 AMELUNXEN, H.: Fahrdynamikmodelle für Echtzeitsimulationen im komfortrelevanten Frequenzbereich. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 329, Paderborn, 2014 – ISBN 978-3-942647-48-9

Bd. 330 KEIL, R.; SELKE, H. (Hrsg):. 20 Jahre Lernen mit dem World Wide Web. Technik und Bildung im Dialog. HNI-Verlagsschriftenreihe, Band 330, Paderborn, 2014 – ISBN 978-3-942647-49-6

Bd. 331 HARTMANN, P.: Ein Beitrag zur Verhaltensantizipation und -regelung kognitiver mechatronischer Systeme bei langfristiger Planung und Ausführung. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 331, Paderborn, 2014 – ISBN 978-3-942647-50-2

Bd. 332 ECHTERHOFF, N.: Systematik zur Planung von Cross-Industry-Innovationen Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 332, Paderborn, 2014 – ISBN 978-3-942647-51-9

Bd. 333 HASSAN, B.: A Design Framework for Developing a Reconfigurable Driving Simulator. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 333, Paderborn, 2014 – ISBN 978-3-942647-52-6

Bd. 334 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 10. Symposium für Vorausschau und Technologieplanung, Heinz Nixdorf Institut, 20. und 21. November 2014, Berlin-Brandenburgische Akademie der Wissenschaften, Berlin, HNI-Verlagsschriftenreihe, Band 334, Paderborn, 2014 – ISBN 978-3-942647-53-3

Bd. 335 RIEKE, J.: Model Consistency Management for Systems Engineering. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 335, Paderborn, 2014 – ISBN 978-3-942647-54-0

Bd. 336 HAGENKÖTTER S.: Adaptive prozessintegrierte Qualitätsüberwachung von Ultraschalldrahtbondprozessen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 336, Paderborn, 2014 – ISBN 978-3-942647-55-7

Bd. 337 PEITZ, C.: Systematik zur Entwicklung einer produktlebenszyklusorientierten Geschäftsmodell-Roadmap. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 337, Paderborn, 2015 – ISBN 978-3-942647-56-4

Bd. 338 WANG, R.: Integrated Planar Antenna Designs and Technologies for Millimeter-Wave Applications. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 338, Paderborn, 2015 – ISBN 978-3-942647-57-1

Bd. 339 MAO, Y.: 245 GHz Subharmonic Receivers For Gas Spectroscopy in SiGe BiCMOS Technology. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 339, Paderborn, 2015 – ISBN 978-3-942647-58-8

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn