Thomas Müller

Integration von Verlässlichkeitsanalysen und -konzepten innerhalb der Entwicklungsmethodik mechatronischer Systeme

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen National-bibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar

Satz und Gestaltung: Thomas Müller

Hersteller: Verlagshaus Monsenstein und Vannerdat OHG
Druck · Buch · Verlag
Münster

Printed in Germany

Geleitwort

Bei der Abwägung zwischen Chancen und Risiken während der Entwicklung mechatronischer Systeme stellt die Verlässlichkeit ein wichtiges Kriterium dar. Insbesondere bei Systemen von hoher Komplexität ist eine methodische Vorgehensweise erforderlich, die jedoch bisher nur ansatzweise verfügbar war. Im Mittelpunkt der VDI-Richtlinie 2206 „Entwicklungsmethodik für mechatronische Systeme" steht die interdisziplinär ausgerichtete Entwicklungsmethodik. Eine systematische Betrachtung der mit dem Thema der Zuverlässigkeit zusammenhängenden Aspekte eines technischen Systems findet bisher nur in Form spezieller Analysen, wie z.B. FMEA oder anderer Risikoanalysen statt, die häufig erst in einer relativ späten Phase des Entwicklungsprozesses eingesetzt werden.

Herr Müller beschreibt in seiner Dissertation, wie Verlässlichkeitsaspekte bereits in den frühen Phasen des Entwicklungsprozesses bei der Synthese berücksichtigt werden können, und wie sie am besten in die Entwicklungsmethodik mechatronischer Systeme integriert werden können. Darüber hinaus gelingt es ihm, universelle Lösungsmuster für Verlässlichkeit zu entwickeln, die als wiederverwertbare Bausteine beim verlässlichkeitsorientierten Entwurf genutzt werden können. Als Basis dafür dient eine systematische Beschreibungsform, mit der von speziellen Lösungen auf die dahinter stehenden universellen Lösungsmuster für Fehlervermeidung, -überwachung und -toleranz verallgemeinert werden kann.

Die Dissertation von Herrn Müller liefert einen wichtigen Beitrag zur systematischen Behandlung der Verlässlichkeit mechatronischer Systeme. Ich wünsche der Arbeit, dass sie die Verbreitung und Beachtung findet, die der hohen Bedeutung des Themas entspricht. Die Arbeit von Herrn Müller entstand im Rahmen des Sonderforschungsbereiches 614 „Selbstoptimierende Systeme des Maschinenbaus", der von der Deutschen Forschungsgemeinschaft gefördert wird.

Paderborn, im Mai 2009

(Prof. Dr.-Ing. Jörg Wallaschek)

Integration von Verlässlichkeitsanalysen und -konzepten innerhalb der Entwicklungsmethodik mechatronischer Systeme

zur Erlangung des akademischen Grades eines

DOKTORS DER INGENIEURWISSENSCHAFTEN (Dr.-Ing.)

der Fakultät für Maschinenbau

der Universität Paderborn

vorgelegte

DISSERTATION

von

Dipl.-Wirt.-Ing. Thomas Müller

aus Herford

1. Referent: Prof. Dr.-Ing. Jörg Wallaschek
2. Referent: Prof. Dr.-Ing. Bernd Bertsche
Tag des Kolloquiums: 13. Mai 2009

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Mechatronik und Dynamik des Heinz Nixdorf Instituts der Universität Paderborn. Da die Arbeit ohne die fachliche und moralische Unterstützung zahlreicher Personen nicht möglich gewesen wäre, möchte ich an dieser Stelle meinen Dank aussprechen.

Mein erster Dank gilt Herrn Prof. Wallaschek für die Möglichkeit zur Promotion. Mit seinem Vertrauen in meine Person, seiner menschlichen Führung und den fachlichen Orientierungshilfen bei Themenfindung und Umsetzung hat er maßgeblichen Anteil an dem Erfolg dieser Arbeit.

Herrn Prof. Bertsche danke ich für das Interesse an meiner Arbeit sowie die Übernahme des Koreferates. Mein Dank gilt ferner für Vorsitz und Beisitz in der Prüfungskommission den Herren Prof. Gausemeier und Prof. Sextro. Herrn Prof. Gausemeier gilt ebenfalls Dank für die Betreuung im SFB614 "Selbstoptimierende Systeme", in dessen Kontext diese Arbeit entstand.

Ein herzlicher Dank gilt allen Kollegen. Sie haben durch fachliche Diskussionen, gemeinsame Forschungen und so manche außerdienstliche Aktivität zum Gelingen dieser Arbeit beigetragen. Stellvertretend seien hier Dr. Hemsel, Dr. Potthast, Herr Walther, Frau Kassühlke, Frau Hille, Dr. Schiedeck und die Herren Twiefel und Liekenbröcker erwähnt. Weiterhin gilt mein Dank allen Studenten, die mich im Rahmen von Studien- oder Diplomarbeiten und SHK-Tätigkeiten unterstützt haben.

Nicht zuletzt richtet sich mein besonderer Dank auch an mein privates Umfeld. Interesse an meiner Arbeit, moralische Unterstützung sowie Ablenkungen in verschiedenster Form halfen mir, das Ziel der Promotion erfolgreich umzusetzen. Meinen Freunden, ebenso wie meiner Verwandschaft gilt hier für viele schöne und abwechlsungsreiche Momente mein herzlichster Dank.

Meiner Freundin Nicole und unserem Hund Maja danke ich für ihre Liebe, Treue, die permanente Unterstützung sowie die wunderschönen privaten Erlebnisse während dieser Zeit. Ihre liebevolle und humorvolle Unterstützung halfen mir auch in anstrengenden Zeiten.

Ein ganz besonderer Dank gilt schließlich meinen Eltern und meinem Bruder, die mich auf meinem bisherigen Lebens- und Bildungsweg stets engagiert unterstützt haben. Sie gaben mir jederzeit moralische Kraft, fachliches Feedback und ihre uneingeschränkte Liebe.

Paderborn, im Juni 2009 Thomas Müller

Inhaltsverzeichnis

1 Einleitung

Mechatronische Systeme vereinen die Vorteile des Maschinenbaus, der Informatik und der Elektrotechnik besonders im Hinblick auf eine innovative Art der Funktionserfüllung. Die Folge sind intelligente, häufig auch komplexe Systeme, deren bemerkenswerte Funktionalität allerdings auch besondere Anforderungen an die Verlässlichkeit stellt. Um dieser Herausforderung adäquat begegnen zu können, müssen bereits in frühen Phasen der Produktentwicklung Ansätze für die direkte und indirekte Steigerung der Verlässlichkeit ihre Anwendung finden. Indirekte Ansätze beinhalten Verlässlichkeitsmethoden, die besonders ihren Fokus auf die Identifikation von Fehlern oder Gefahren, sowie deren Bewertung legen, während direkte Ansätze, wie Diagnosekonzepte oder Fehlertoleranzprinzipen, unmittelbar die Verlässlichkeit mechatronischer Systeme und Produkte erhöhen.
Die indirekten Ansätze nutzen bestehende Verlässlichkeitsmethoden, die bei Bedarf erweitert und verknüpft werden müssen, und integrieren sie in einzelne Phasen der Entwicklungsmethodik mechatronischer Systeme. Für die direkten Ansätze werden generelle Verlässlichkeitskonzepte und -prinzipien gesammelt, strukturiert und im Sinne eines Konstruktionskatalogs in einer Wissensdatenbank bereitgestellt, um den Konstrukteur bei der Entwicklung eines verlässlichen Systementwurfs zu unterstützen. Dabei werden insbesondere innovative Verlässlichkeitskonzepte und -prinzipien verwendet, die erst durch den Einsatz von mechatronischen Strukturen ermöglicht werden [Mül05].

1.1 Motivation

Die Interdisziplinarität der Mechatronik, resultierend aus den Bereichen Maschinenbau, Informatik und Elektronik, eröffnet sowohl Potenziale für höhere Funktionalitäten bestehender Produkte, als auch Möglichkeiten, neue Produktideen zu generieren und umzusetzen. Trotzdem steigt mit der Vernetzung der verschiedenen Disziplinen auch der Umfang für die Integration: Unterschiedliche Herangehensweisen in der Entwicklung, verschiedene Methoden und Lösungsprinzipien treffen aufeinander und sollen im Zusammenspiel zu mechatronischen Systemen integriert werden. Häufig steigt dadurch die Komplexität der Produkte schnell an, die bei ehrgeizigen Zielsetzungen von größeren Projekten oder Systemen, wie z. B. einem innovativem Bahnsystem, noch weiter

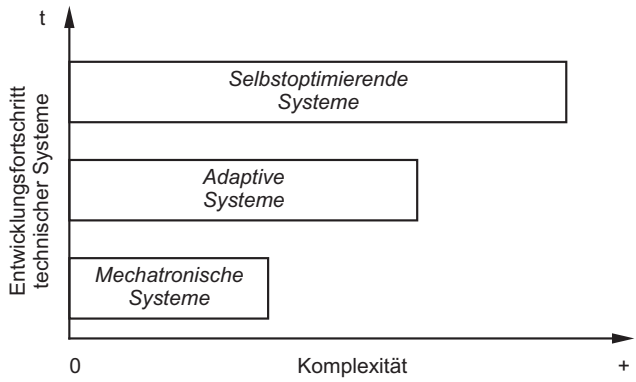


Abbildung 1.1: Qualitativer Zusammenhang von Komplexität und dem Entwicklungsfortschritt mechatronischer Systeme

zunimmt [Mül05]. Eine weitere Entwicklungsstufe hinsichtlich Funktionalität, aber auch Komplexität, stellen *adaptive Systeme* gemäß [ILM92] dar. Diese besitzen die Fähigkeit, Parameter automatisch den statischen und dynamischen Gegebenheiten anzupassen. Auf diese Weise kann das System nicht nur für eine fest definierte Situation, oder im Speziellen für einen Arbeitspunkt, eingestellt werden, sondern es kann sich durch automatische Adaptation auf eine Vielzahl von Situationen, bzw. auf eine Bandbreite von Arbeitspunkten, einstellen. Diese fortschreitende Entwicklung mechatronischer Systeme ist noch immer Gegenstand aktueller Grundlagenforschung, wie z. B. die Aktivitäten zum Wirkparadigma der Selbstoptimierung verdeutlichen: Der in Paderborn im Jahr 2002 gegründete Sonderforschungsbereich *Selbstoptimierende Systeme des Maschinenbaus* betreibt Grundlagenforschung, die den interdisziplinären Ansatz klassischer mechatronischer und adaptiver Systeme erweitert. Selbstoptimierende Systeme besitzen demnach eine inhärente Intelligenz, die es ihnen erlaubt, autonom neue Ziele zu bestimmen oder auch Zielveränderungen vorzunehmen. Teile des Verhaltens selbstoptimierender Systeme werden nichtdeterministisch ablaufen, sodass die Komplexität der resultierenden Systeme und Produkte weiter ansteigen wird [FGK+04]. Abbildung 1.1 verdeutlicht in qualitativer Form den Zusammenhang zwischen dem Entwicklungsfortschritt mechatronischer Systeme und der in der Regel damit einhergehenden steigenden Komplexität.

Diese erhöhte Funktionalität und Komplexität der Systeme beinhaltet bzgl. der Verlässlichkeit sowohl Chancen als auch Risiken. Einerseits existieren häufig mehr potenzielle Fehlerquellen oder Fehlerfortpflanzungsmöglichkeiten in komplexeren Systemen, andererseits können aber auch diese Systeme selbst,

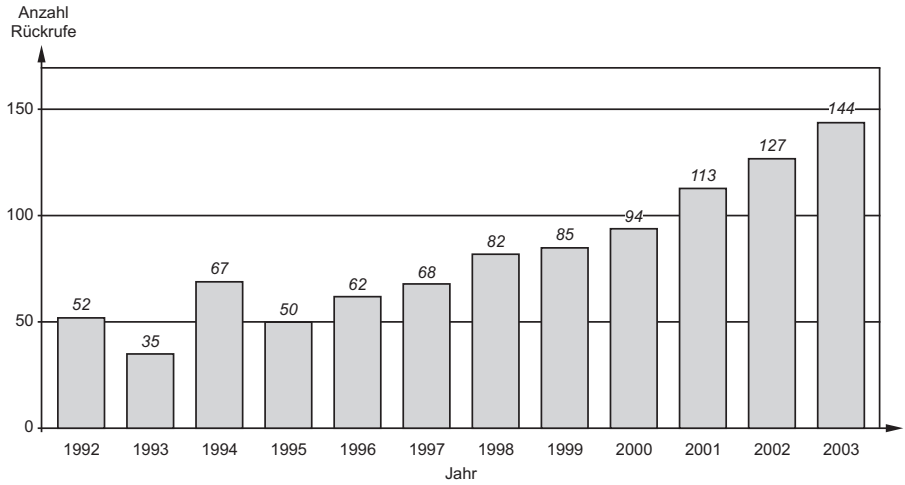


Abbildung 1.2: Rückrufaktionen als Indikator für Verlässlichkeitsdefizite – Statistik des Kraftfahrt-Bundesamts [KB03]

also inhärent, dafür sorgen, verlässlicher zu funktionieren. Neue Möglichkeiten der Fehlerüberwachung oder intelligente Redundanzkonzepte werden erst durch den Einsatz von mechatronischen oder selbstoptimierenden Lösungsmustern möglich.

Der beträchtliche Bedarf von Ansätzen und Lösungen für höhere Verlässlichkeit wird durch die folgenden Aspekte noch weiter unterstützt: Fehlerkosten, z. B. verdeutlicht durch die in Abbildung 1.2 dargestellte Entwicklung der Rückrufaktionen in der Automobilbranche, und der Trend, dass die Kundenforderung *Zuverlässigkeit* mittlerweile als eines der wichtigsten Kriterien beim Neuwagenkauf angesehen wird, zeigen den Bedarf; dieser besteht sowohl aus dem Blickwinkel der Unternehmen, wie auch aus dem der Kunden. Der Imagefaktor von Unternehmen, der auch von der Verlässlichkeit geprägt wird, ist dadurch zu einer Möglichkeit geworden, mit der sich sowohl Geld verdienen, aber auch verlieren lässt [DAT04].

Die Entwicklung in rechtlicher Hinsicht, z. B. bei der Haftung des Herstellers, stellt einen weiteren Motivationsgrund dar, das Thema Verlässlichkeit im Entwicklungsprozess näher zu betrachten: Da absolute Fehlerfreiheit unmöglich zu erreichen ist, müssen zumindest Organisations- und Sorgfaltspflichten beim Entwicklungsprozess für mechatronische Systeme eingehalten und nachgewiesen werden. Ein systematisches und dokumentiertes Vorgehen im Sinne einer um Verlässlichkeitsaspekte erweiterten Entwicklungsmethodik ist daher erforderlich [AFLE04].

Zusammenfassend ist der Bedarf einer verlässlichkeitsorientierten Entwicklungsmethodik unter anderem durch Ausfallstatistiken, Kundenforderungen und Haftungsrisiken motiviert. Demgegenüber existieren zwar zahlreiche Einzelmethoden für Verlässlichkeitsanalysen, die in Kapitel 2 kurz erläutert werden; durchgängige Prozesse innerhalb einer Entwicklungsmethodik bestehen allerdings kaum.

1.2 Zielsetzung

Die Zielsetzung dieser Arbeit besteht in der Erweiterung der Entwicklungsmethodik mechatronischer Systeme um Methoden und Konzepte zur Erhöhung der Verlässlichkeit. Dafür werden ein Verlässlichkeitsprozess und die Methodik der Verlässlichkeitsmuster entwickelt.
Für den Methodenverbund werden die Ansätze und Vorteile bestehender Analysen genutzt und kombiniert, um darauf aufbauend einen effizienten und durchgängigen Prozess zur indirekten Steigerung der Verlässlichkeit zu gestalten. Der Schwerpunkt liegt dabei auf qualitativen Methoden, da primäres Ziel die Identifikation von Fehlern und Gefahren sowie deren Risikobewertung ist. Eine Berechnung oder Vorhersage von quantitativen Werten z. B. für die Zuverlässigkeit wird nur sekundär betrachtet; dennoch werden Anknüpfungspunkte für quantitative Analysen aufgezeigt.
Zur direkten Erhöhung der Verlässlichkeit mechatronischer Systeme wird die Methodik der Verlässlichkeitsmuster inklusive einer Datenbank entwickelt, die im Sinne eines Konstruktionskatalogs generelle Konzepte und Prinzipien in einem Wissensmanagementsystem bereitstellt, um bei der Entwicklung von Lösungen für verlässliches Verhalten zu unterstützen.
Beide Ansätze, der Methodenverbund und die Methodik der Verlässlichkeitsmuster, werden kombiniert und in den Entwicklungsprozess integriert. Orientiert am Inhalt und an der formalen Gestaltung der VDI-Richtlinie 2206 *Entwicklungsmethodik für mechatronische Systeme* wird das Ergebnis sowohl ein generelles Vorgehen mit Phasen auf der Makroebene beschreiben als auch die detaillierte Ausarbeitung wiederkehrender Prozessbausteine, deren Nutzen auch in abgewandelter Form noch besteht.

1.3 Vorgehen

Die dieser Arbeit zugrunde liegende Forschungsmethodik ist die *Design Research Methodology (DRM)* nach [BC02]: DRM stellt einen systematischen Ansatz für wissenschaftliche Arbeiten dar, die einen Beitrag zum Forschungsgebiet der Konstruktions- und Entwicklungsmethodik bereitstellen sollen. DRM ba-

siert auf der Erkenntnis, dass die Forschung in diesem Bereich sowohl Modelle und Theorien für das grundlegende Verständnis von Entwicklungstätigkeiten umfasst, als auch die Entwicklung von neuen Methoden und Werkzeugen einschließt. Die resultierende Forschungsmethodik teilt sich in die folgenden vier Phasen:

Klärung des Forschungsgegenstands: Der Forschungsgegenstand wird innerhalb des Forschungsgebiets eingeordnet, und es werden Erfolgs- und Einflusskriterien definiert.

Deskriptive Studie 1: Das Verständnis von Entwicklungstätigkeiten wird *beschreibend* erforscht, um neue Zusammenhänge und Einflüsse zu identifizieren.

Normative Studie: Aufbauend auf dem erforschten Verständnis, wird ein gewünschtes Soll-Szenario aufgestellt, für das neue Werkzeuge und Methoden entwickelt werden, die die Entwicklungsaktivitäten verbessern sollen.

Deskriptive Studie 2: Die entwickelten Werkzeuge und Methoden werden sowohl hinsichtlich der Funktionalität als auch der messbaren Erfolgskriterien evaluiert.

Die Umsetzung der Forschungsmethodik spiegelt sich in der Gliederung der Arbeit wider: In der Einleitung, im Speziellen in der Motivation, werden Erfolgs- und Einflusskriterien definiert, die den generellen Argumentationspfad für die vorliegende Arbeit darstellen. Der Stand der Technik dient der weiteren Klärung des Forschungsgegenstands, der verlässlichkeitsorientierten Entwicklung mechatronischer Systeme. Einen ersten Forschungsbeitrag zum besseren Verständnis von Entwicklungstätigkeiten bezüglich der Verlässlichkeit leistet das Kapitel *Analyse zur Nutzung von Verlässlichkeitsmethoden und -prozessen.* Dort werden im Sinne der deskriptiven Studie 1 neue Zusammenhänge und Einflüsse identifiziert, die gemeinsam mit Schlussfolgerungen aus dem Stand der Technik zu den Forschungshypothesen dieser Arbeit führen. Darauf aufbauend werden ein Verlässlichkeitsprozess und die Methodik der Verlässlichkeitsmuster entwickelt, die jeweils Beiträge zur Verbesserung der Entwicklungstätigkeiten mit Bezug zur Verlässlichkeit darstellen sollen. Ihre Funktionalitäten werden abschließend gemäß der deskriptiven Studie 2 innerhalb eines Forschungsprojektes evaluiert. Die Evaluation erfolgt dazu durch zwei Perspektiven: *Funktionalität* und *Erfolg* des Einsatzes vom neu entwickelten Prozess und der Methodik der Verlässlichkeitsmuster. Die Evaluation des erfolgreichen Einsatzes kann im Rahmen dieser Arbeit allerdings nur *initial* erfolgen, sodass ein Vergleich von einer Entwicklungsaufgabe, die jeweils mit und ohne den Neuentwicklungen dieser Arbeit bearbeitet wird, nicht realisiert wird. Stattdessen werden die Neuentwicklungen innerhalb eines Forschungsprojektes angewendet

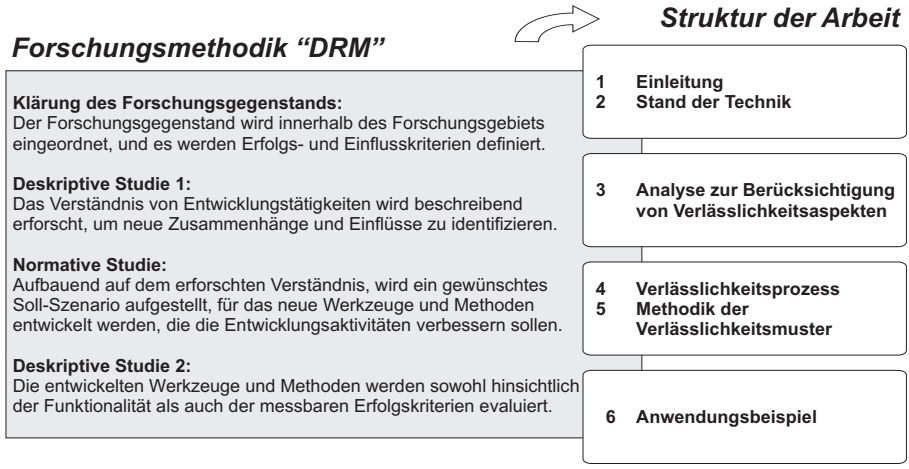


Abbildung 1.3: Aufbau der Arbeit und Bezug zu den Phasen der Forschungsmethodik

und die erzielten Ergebnisse bezüglich der Verlässlichkeitsaspekte diskutiert im Sinne eines Ergebnis-Reviews. Abbildung 1.3 zeigt das Forschungsvorgehen, das den Zusammenhang zwischen der angewendeten Forschungsmethodik und der Umsetzung durch die Struktur der vorliegenden Arbeit enthält.

2 Stand der Technik

In den folgenden Abschnitten wird der Stand der Technik betrachtet, auf dem ein verlässlichkeitsorientiertes Entwicklungsvorgehen basiert. Dazu werden Grundlagen der Verlässlichkeit und angrenzender Begriffe diskutiert, die Entwicklungsmethodik für mechatronische Systeme und gängige Methoden der Verlässlichkeitstechnik werden vorgestellt, und es werden bereits bestehende Ansätze für Verlässlichkeitsprozesse dargestellt und ebenfalls kurz diskutiert.

2.1 Grundlagen der Verlässlichkeit

Begriffe und Definitionen im Kontext der Verlässlichkeit werden sowohl in der Industrie als auch in der Forschung häufig nicht einheitlich verwendet. Zwei verbreitete, sich teilweise aber unterscheidende Sichtweisen, resultierend aus den VDI-Richtlinien und Arbeiten aus der Informationstechnik, werden im Folgenden erläutert und gegenübergestellt. Darüber hinaus werden ebenfalls verschiedene Begriffe bzgl. Fehlerarten, -ursachen und -auswirkungen erörtert.
Die VDI-Richtlinien verwenden überwiegend die *Zuverlässigkeit* als übergeordneten Begriff. Dieser beinhaltet weitere Aspekte wie z. B. die Funktionszuverlässigkeit und die Sicherheit. Trotzdem existieren auch in den Richtlinien teilweise noch geringe Abweichungen in Interpretation und Übersetzung: Gemäß der *Terminologie der Zuverlässigkeit* nach [VDI05] dient die Zuverlässigkeit als zusammenfassender Ausdruck, der die Verfügbarkeit und ihre Einflussfaktoren Funktionsfähigkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft beschreibt. Die englische Übersetzung wird mit *dependability* bezeichnet. Die Richtlinie *Zuverlässigkeitsmanagement* [VDI04b] hingegen erweitert die untergeordneten Faktoren der Zuverlässigkeit und nutzt die Ausdrücke Funktionszuverlässigkeit, Instandhaltbarkeit, Sicherheit und Verfügbarkeit zu deren Begriffsbestimmung. Hier wird die englische Übersetzung mit *reliability* angegeben.
Die Sichtweise der Informationstechnik verwendet im Gegensatz zu den VDI-Richtlinien eine abweichende Begriffswelt mit dem Oberbegriff *Verlässlichkeit*. Dieser wurde detailliert von *Laprie* ausgearbeitet und in zahlreiche Sprachen übersetzt [Lap92]. Er hat mittlerweile eine große Verbreitung auch in anderen Bereichen der Forschung gefunden, wie z. B. in der Mechatronik nach [Koc01]. Analog zum Verständnis des Begriffes Zuverlässigkeit innerhalb der

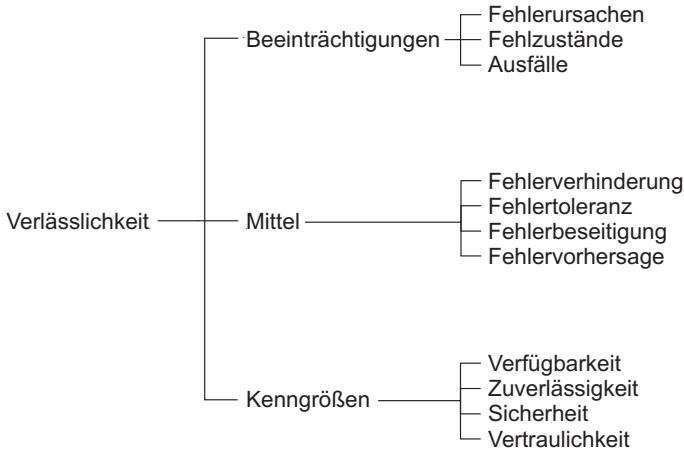


Abbildung 2.1: Verlässlichkeitsbaum nach [Lap92]

VDI-Richtlinien, wird auch die Verlässlichkeit als ein übergeordneter Begriff verstanden. Zu den die Verlässlichkeit beschreibenden Attributen zählen bei dieser Sichtweise die Verfügbarkeit, Zuverlässigkeit, Sicherheit und Vertraulichkeit. Die englische Übersetzung verwendet das Wort *dependability*. Weitere Begriffe, die Mittel und Bedrohungen der Verlässlichkeit beschreiben, vervollständigen das ganzheitliche Konzept, das in Abbildung 2.1 im so genannten Verlässlichkeitsbaum, englisch *dependability tree*, systematisch dargestellt wird. Im Detail werden die genannten Attribute der Verlässlichkeit wie folgt erläutert:

Verfügbarkeit: Verlässlichkeit in Bezug auf das *Bereit sein* zur Benutzung.

Zuverlässigkeit (Funktionsfähigkeit): Verlässlichkeit mit Bezug auf die Kontinuität der Leistung - Überlebenswahrscheinlichkeit.

Sicherheit: Verlässlichkeit mit Bezug auf das Nichtauftreten von kritischen Ausfällen.

Vertraulichkeit: Verlässlichkeit mit Bezug auf die Verhinderung von nicht autorisiertem Zugriff und/oder Behandlung von Informationen [Lap92].

Beide Ansätze verwenden die Struktur eines übergeordneten Begriffs, der durch verschiedene speziellere Aspekte beschrieben werden kann. Die Unterscheidung, Zuverlässigkeit gegenüber Verlässlichkeit, könnte einerseits aus der geringen Verbreitung des Wortes Verlässlichkeit in der deutschen Sprache und

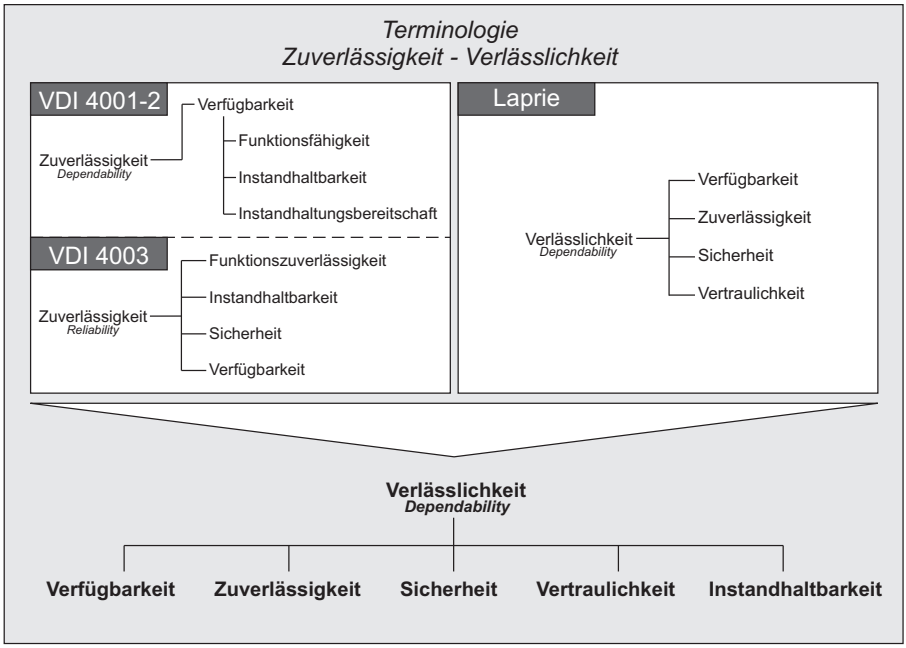


Abbildung 2.2: Terminologie Zuverlässigkeit - Verlässlichkeit

der häufig anzutreffenden Übersetzung *dependability* mit Zuverlässigkeit resultieren und andererseits daraus, dass die Präferenz in den genannten VDI-Richtlinien auf der eigentlichen Zuverlässigkeit im folgenden Sinne liegt:

> Zuverlässigkeit ist die Wahrscheinlichkeit dafür, dass ein Produkt während einer definierten Zeitdauer unter gegebenen Funktions- und Umgebungsbedingungen nicht ausfällt [BL04].

Die Attribute, die der Verlässlichkeit bzw. der Zuverlässigkeit jeweils untergeordnet sind, unterscheiden sich nur geringfügig.
Im Rahmen dieser Arbeit wird der Terminologie der Verlässlichkeit gefolgt, da deutlich werden soll, dass nicht nur die Zuverlässigkeit nach [BL04] im Vordergrund steht, sondern dass ebenso Aspekte z. B. die Sicherheit betreffend von Bedeutung sind. Dieser Argumentation folgt auch die Definition der Verlässlichkeit nach *Kochs*, die als grundlegende Basis dieser Arbeit verstanden werden soll:

> Verlässlichkeit ist ein Maß dafür, wie zuverlässig und/oder sicher eine Betrachtungseinheit (Komponente oder System) ihre Funktion

Abbildung 2.3: Fehlerpropagierung nach [Lap92]

> erfüllt unter Berücksichtigung aller Einwirkungen der Umgebung auf die Betrachtungseinheit (...)[Koc01].

Auch wenn die zitierte Definition nicht explizit darauf eingeht, werden unter der übergeordneten Verlässlichkeit die Attribute Zuverlässigkeit, Verfügbarkeit, Sicherheit, Wartbarkeit und Leistungsfähigkeit verstanden.
Neben der Definition der Verlässlichkeit, inklusive der weiteren Attribute, orientiert sich diese Arbeit im Rahmen der Fehlerbegriffe ebenfalls an den Definitionen nach [Lap92]: Dort wird die Fehlerpropagierung im Sinne eine Fehlerkette definiert, die die wichtigen Unterscheidungen zwischen den Begriffen Fehlerursache, Fehlerzustand, Ausfall und Konsequenz trifft. Die Fehlerursache stellt demnach die verantwortliche Ursache von unerwünschten Ereignissen, z. B. von Gefahren, dar. Eine Aktivierung der Fehlerursache hat einen Fehlerzustand zur Folge, der häufig das Verständnis vom eigentlichen Fehler widerspiegelt. Führt dieser Fehlerzustand dazu, dass die erbrachte Leistung des Systems nicht mehr der Spezifikation, d. h. der erwarteten Funktion entspricht, so spricht man von einem Ausfall des Systems. Dieser Ausfall wiederum kann Konsequenzen außerhalb der Systemgrenzen bewirken.
Eine ähnliche Kette der Fehlerpropagierung wird ebenfalls in [Sto96] beschrieben. Dort wird der Begriff der Auswirkung allerdings nicht mehr hinzugenommen, da die Auswirkungen bereits außerhalb der Systemgrenzen liegen.
Abschließend folgen weitgehend verbreitete und akzeptierte Definitionen für die Begriffe Sicherheit, Gefährdung und Risiko. Bezüglich der Sicherheit werden zwei Definitionen aufgeführt, die sich gegenseitig ergänzen:

> *Sicherheit* ist die Eigenschaft eines Systems, menschliches Leben oder die Umwelt nicht zu gefährden [Sto96].

> *Sicherheit* ist die Freiheit von unvertretbaren Risiken [DIN02].

> *Risiko* ist eine Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens [DIN02].

> Eine *Gefährdung* ist eine Situation, in der tatsächliche oder potenzielle Gefahr für den Menschen oder die Umwelt besteht [Sto96].

Diese Definitionen werden in gleicher oder sehr ähnlicher Form z. B. in [Neu02], [Ben04], [Bom05], [DIN04] und [VDI04b] verwendet und teilweise erweitert.

2.2 Entwicklungsmethodik der Mechatronik

Um innovative Produkte systematisch entwickeln zu können, bedarf es einer Entwicklungsmethodik. Diese sollte einerseits grundlegende Vorgehensschritte beinhalten und andererseits die wesentliche Basis für die Kommunikation und Kooperation der Fachleute darstellen. Aufgrund der Interdisziplinarität der Mechatronik existieren gemäß den spezifischen Domänen verschiedene Entwicklungsmethodiken. Überblicke der Vorgehensweisen des Maschinenbaus/Mechanik, der Elektronik/Mikroelektronik, der Softwaretechnik sowie der Regelungstechnik werden in [GEK01] vorgestellt.
Die als Grundlage der vorliegenden Arbeit dienende VDI-Richtlinie 2206 *Entwicklungsmethodik für mechatronische Systeme* [VDI04a] unterstützt das interdisziplinäre Zusammenwirken der Domänen der Mechatronik und führt die spezifischen Entwicklungsmethodiken zusammen, ohne dabei die bewährten Leitfäden vollständig ersetzen zu wollen. Die Struktur dieser Entwicklungsmethodik folgt einem dreiteiligen Vorgehensmodell und beinhaltet zusätzlich Methoden des modellbasierten Systementwurfs, unterstützende IT-Werkzeuge sowie ausgewählte Aspekte der Organisation. Der Kern der Richtlinie, die dreiteilige Entwicklungsmethodik, enthält die folgenden Elemente, deren Zusammenwirken das Vorgehen zur systematischen Entwicklung mechatronischer Systeme beschreibt:

- Allgemeiner Problemlösungszyklus als Mikrozyklus
- V-Modell als Makrozyklus
- Vordefinierte Prozessbausteine zur Bearbeitung wiederkehrender Arbeitsschritte

Die beiden letztgenannten Aspekte werden im Folgenden kurz erläutert, da sie wichtige Anknüpfungspunkte für Inhalte dieser Arbeit darstellen und darüber hinaus noch die Vorlage für die formale Vorgehensweise beschreiben. Auf eine Erläuterung des allgemeinen Problemlösungszyklus wird verzichtet. Die Begründung dafür liegt darin, dass seine Anwendung weder im Fokus dieser Arbeit liegt, noch eine Veränderung, Erweiterung oder Verknüpfung des in der VDI-Richtlinie dargestellten Problemlösungszyklus notwendig wäre.

2.2.1 V-Modell als Makrozyklus

Gemäß [VDI04a] kann das generische Vorgehen beim Entwurf mechatronischer Systeme durch ein V-Modell beschrieben werden. Dieser Rahmen zum grundsätzlichen Vorgehen wurde aus der Softwaretechnik übernommen und den Anforderungen der Mechatronik folgend adaptiert. Innerhalb des V-Modells werden die wesentlichen Teilschritte in eine logische Abfolge gebracht. Zwischen

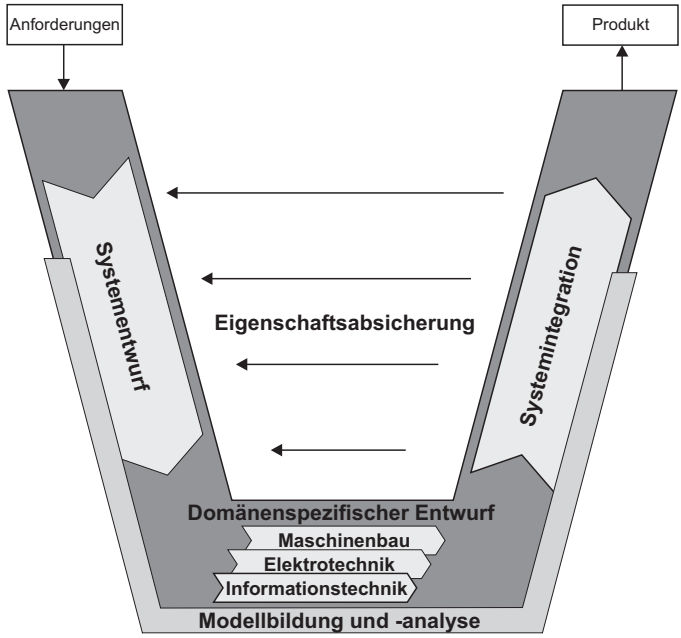


Abbildung 2.4: Makrozyklus des V-Modells nach [VDI04a]

den Anforderungen als Ausgangspunkt und dem Produkt als Ergebnis, das je nach Reifegrad ein Labormuster, Funktionsmuster, Vorserienprodukt, oder Ähnliches sein kann, werden nachfolgende Teilschritte eingeführt:

- Systementwurf
- Domänenspezifischer Entwurf
- Systemintegration
- Eigenschaftsabsicherung
- Modellbildung und -analyse

Die logische Anordnung bzw. die Verknüpfung der Teilschritte werden in der nachstehenden Abbildung ersichtlich. Insbesondere die Eigenschaftsabsicherung verdeutlicht den Nutzen der V-Gestalt, um Anforderungen und Spezifikationen während der Integrationsphase bei unterschiedlichen Realisierungsstufen verifizieren und validieren zu können.

2.2.2 Prozessbausteine für wiederkehrende Arbeitsschritte

Da bei der Entwicklung mechatronischer Systeme teilweise wiederkehrende Arbeitsschritte auftreten, können diese konkreter in Form vordefinierter Prozessbausteine beschrieben werden. Im Folgenden wird daher gemäß [VDI04a] das Vorgehen innerhalb der Teilschritte des V-Modells beschrieben. Neben dem generellen Aufbau eines Prozessbausteins werden anschließend Hauptmerkmale der Phasen Systementwurf, Domänenspezifischer Entwurf, Modellbildung und -analyse; Systemintegration und Eigenschaftsabsicherung dargestellt.

Genereller Aufbau eines Prozessbausteins

Ein Prozessbaustein repräsentiert wiederkehrende Arbeitsschritte, die innerhalb der Phasen des V-Modells liegen. Beschrieben werden die jeweiligen Arbeitsschritte durch

- Phasen/Meilensteine,
- Aufgaben/Tätigkeiten und
- Resultate.

Bei der Verwendung dieser definierten Darstellung ist es notwendig, dass jede Phase, bzw. jeder Meilenstein, zu einem Resultat führt. Abbildung 2.5 zeigt den generellen Aufbau, der auch zur Beschreibung der wiederkehrenden Arbeitsschritte für die verlässlichkeitsorientierte Entwicklungsmethodik angewendet wird.

Systementwurf

Im Prozessbaustein Systementwurf wird, ausgehend von den Anforderungen, eine abstrakte, lösungsneutrale Problemformulierung verfasst. Darauf basierend, wird eine Funktionsstruktur, bestehend aus Gesamtfunktion und hierarchisch geordneten Teilfunktionen aufgestellt. Für die jeweiligen Teilfunktionen werden Wirkprinzipien oder Lösungselemente identifiziert, die zusammengenommen die Wirkstruktur bilden. Beschreibt die Struktur ebenfalls gestalterische oder stützende Aspekte, so wird bereits die Baustruktur realisiert. Abschließendes Resultat ist mindestens eine prinzipielle Lösungsvariante.

Domänenspezifischer Entwurf

Der domänenspezifische Entwurf greift die Wirk- oder Baustruktur des Systementwurfs auf, indem er die getätigte Partitionierung der Struktur nutzt. Häufig beinhaltet sie bereits eine domänenspezifische Trennung, sodass der

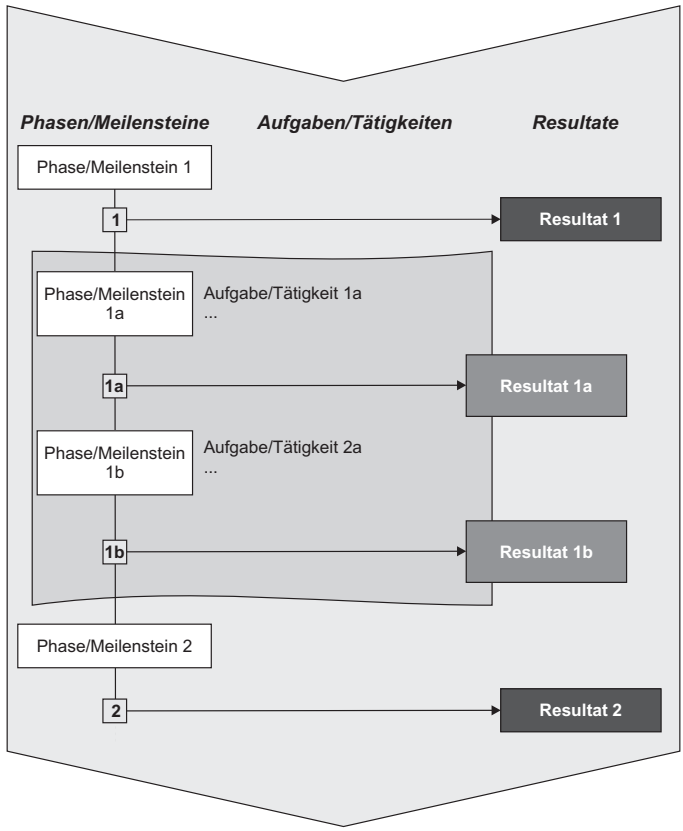


Abbildung 2.5: Genereller Aufbau eines Prozessbausteins

weitere Entwurf, ebenso wie die Ausarbeitung, gemäß der bestehenden spezifischen Entwicklungsmethodiken vollzogen werden kann.

Systemintegration

Der Prozessbaustein Systemintegration führt domänenspezifische und -übergreifende Teillösungen wieder zum Gesamtsystem zusammen. Der Übergang vom Komponentenentwurf zum Gesamtentwurf wird realisiert.

Modellbildung und -analyse

Die zuvor beschriebenen drei Phasen werden vom Prozessbaustein Modellbildung und -analyse begleitet. Die Modellbildung realisiert eine Komplexitätsreduktion des mechatronischen Gesamtsystems bzw. seines Verhaltens. Dies kann domänenübergreifend erfolgen. Die Modelle sind im Rechner darstellbar und analysierbar.

Eigenschaftsabsicherung

Ebenso wie die Modellbildung und -analyse verwendet auch der Prozessbaustein Eigenschaftsabsicherung die Phasen Systementwurf, domänenspezifischer Entwurf und Systemintegration. Die verschiedenen Varianten und Konkretisierungsstufen innerhalb der Entwurfsphasen müssen parallel zu den Integrationsschritten verifiziert und validiert werden.

2.3 Verlässlichkeitsmethoden

Im Folgenden werden einige grundlegende Verlässlichkeitsmethoden dargestellt. Die Strukturierung in Fehleranalysen, Gefahrenanalysen und Risikoanalysen beruht nicht auf Erkenntnissen der verbreiteten aktuellen Literatur, sondern beinhaltet bereits einen ersten Beitrag dieser Arbeit zum Forschungsfeld der Verlässlichkeit.
Dieser besteht in der Zuordnung von Methodenklassen zu den Begriffsdefinitionen Fehler, Gefahr und Risiko, wie sie in Kapitel 2.1 erläutert wurden. Ein exakte Trennung zwischen den Analysen ist häufig durch die Rückführung auf die ursprünglichen Ideen der Methoden möglich. Als Beispiel sei hierzu die Fehler-Möglichkeits- und -Einfluss-Analyse genannt, die ursprünglich ohne den Zusatz einer Risikobewertung entwickelt wurde und daher eindeutig in die Methodenklasse der Fehleranalysen einzuordnen ist. Die Abgrenzung zwischen den Begriffen *Fehler*, *Gefahr* und *Risiko* resultiert aus der Unterscheidung, dass ein Fehler erst in Kombination mit potenziellen Konsequenzen zu einer Gefahr wird, und dass eine Gefahr erst durch die Bewertung von Wahrscheinlichkeit

und Schwere zum Risiko wird. Für jede Methodenklasse bestehen eigene Verfahren, deren Kern entweder die Methodenklasse der Fehler-, Gefahren- oder Risikoanalysen widerspiegeln [MMWW07].
Dieser Gliederung in Fehler-, Gefahren- und Risikoanalysen wird auch bei der späteren Verwendung der Methoden innerhalb des Verlässlichkeitsprozesses gefolgt. Die detaillierten Erläuterungen der Methodenklassen werden innerhalb der folgenden Einzelkapitel dargestellt. Weitere Methoden, die bei der Entwicklung des Verlässlichkeitsprozesses zur Anwendung kommen, werden erst in Kapitel 4 erläutert, wie z. B. Methoden zur Verifikation und Validation.

2.3.1 Fehleranalysen

Fehleranalysen repräsentieren die wahrscheinlich am häufigsten vertretene Methodenklasse. Typische Vertreter sind die Fehler-Möglichkeits- und -Einfluss-Analyse (FMEA), die Fehlerbaumanalyse (FTA - Fault Tree Analysis) und die Verwendung von Checklisten zur Fehlersuche. Letztgenannte können selbstverständlich in verschiedenen Fragestellungen ihre Anwendung finden. Die gemeinsame Basis dieser Methoden zeichnet sich durch die Identifikation von Schwachstellen, potenziellen Fehlern, aus. Der Begriff Fehler muss in diesem Kontext im Sinne der Fehlerursache und dem Fehlerzustand verstanden werden (vgl. Kapitel 2.1), da die Identifikation von beidem in der Aufgabe der Analysen liegen kann. Folglich leisten die Methoden der Fehleranalyse verschiedene systematische Herangehensweisen, um potenzielle Fehlerursachen und Fehlerzustände in Systemen zu identifizieren bzw. bereits in den Systementwürfen. Der jeweilige Fokus, auf den die Fehleranalyse anzuwenden ist, variiert dabei sowohl zwischen den unterschiedlichen Methoden als auch bei der Möglichkeit, die gleiche Methode zu verschiedenen Zwecken zu gebrauchen; z. B. kann eine Anwendung bereits anhand einer sehr allgemein gehaltenen Aufgabenstellung oder erster Hauptfunktionsbeschreibung erfolgen oder auch erst sehr spät im Entwicklungsprozess bei einem fertigen Labormuster. Davon unabhängig werden im Folgenden die Methoden der Fehleranalysen erläutert.

Fehler-Möglichkeits- und -Einfluss-Analyse (FMEA)

Gemäß [DIN90b] ist die Fehler-Möglichkeits- und -Einfluss-Analyse, abgekürzt FMEA, vom Ursprung her eine qualitative Methode, deren Zweck darin besteht, ein System bezüglich potenzieller Ausfälle der Teilkomponenten zu untersuchen und deren Schwachstellen zu identifizieren. Darauf aufbauend werden Maßnahmen getroffen, die zu Verbesserungen des Systems führen.
Die Systematik der Methode besteht darin, dass ausgehend von einer Systemanalyse, das System in Bauelemente oder auch Funktionen strukturiert

dargestellt werden kann. Der Ausfall jedes Bauelements oder jeder Funktion wird anhand von drei Kriterien analysiert:

- Ausfallart
- Ausfallursache
- Ausfallauswirkung

Dieser qualitativen Analyse folgen die zu treffenden Gegenmaßnahmen, die zur Verbesserung des Systems führen sollen.
Eine ergänzende quantitative Bewertung der analysierten Ausfallarten, -ursachen und -auswirkungen erweitert das systematische Vorgehen der ursprünglichen FMEA. Eine verbreitete Bewertung der Fehler bzw. des daraus abzuleitenden Risikos erfolgt durch Einschätzung der Kriterien B für die Bedeutung der Ausfallauswirkung, A für die Auftretenswahrscheinlichkeit der Ausfallursache und E für die Entdeckungswahrscheinlichkeit der aufgetretenen Ausfallursache. Für B, A und E werden jeweils Bewertungszahlen von 1 bis 10 verwendet, wobei 10 jeweils für den höchsten Risikobeitrag vergeben wird. Durch Multiplikation der bewerteten Kriterien ergibt sich die so genannte Risikoprioritätszahl, kurz *RPZ*. Diese spiegelt eine Bewertung des Risikos wieder, das durch den identifizierten Fehler besteht [VDA06].
Neben dieser Quantifizierung der FMEA haben sich darüber hinaus weitere Unterkategorien der Methode gebildet, wie die Konstruktions-, System- und Prozess-FMEA, die jeweils nach dem Anwendungsobjekt der Methode benannt sind [Ben04]. Aktuelle Vorgehensbeschreibungen für die FMEA durch die Automobilindustrie führen diese Unterkategorien wieder etwas näher zusammen, indem nur noch zwischen Produkt- und Prozess-FMEA unterschieden wird [VDA06].
Insbesondere stellt die Richtlinie [VDA06] des Verbands der Automobilindustrie einen detaillierten und weitgehend akzeptierten Stand des heute aktuellen Vorgehens bezüglich der FMEA dar. Ein typisches Formblatt dieser Methode ist in Abbildung 2.6 dargestellt. Weitergehende Erläuterungen und Anwendungsbeispiele, sowohl zur allgemeinen Methode als auch zur FMEA gemäß [VDA06], finden sich bei [BL04].

Fehlerbaumanalyse (FTA)

Die Fehlerbaumanalyse ist eine so genannte *Top-Down-Analyse*, die anhand eines vorgegebenen, unerwünschten Ereignisses nach allen Ursachen sucht, die zu diesem Ereignis führen können. Ursachen sind z. B. Komponenten oder Teilsystemausfälle, die sich selbständig, oder auch durch Verknüpfungen untereinander auswirken können. Unterteilt werden kann die Methode in die ursprüng-

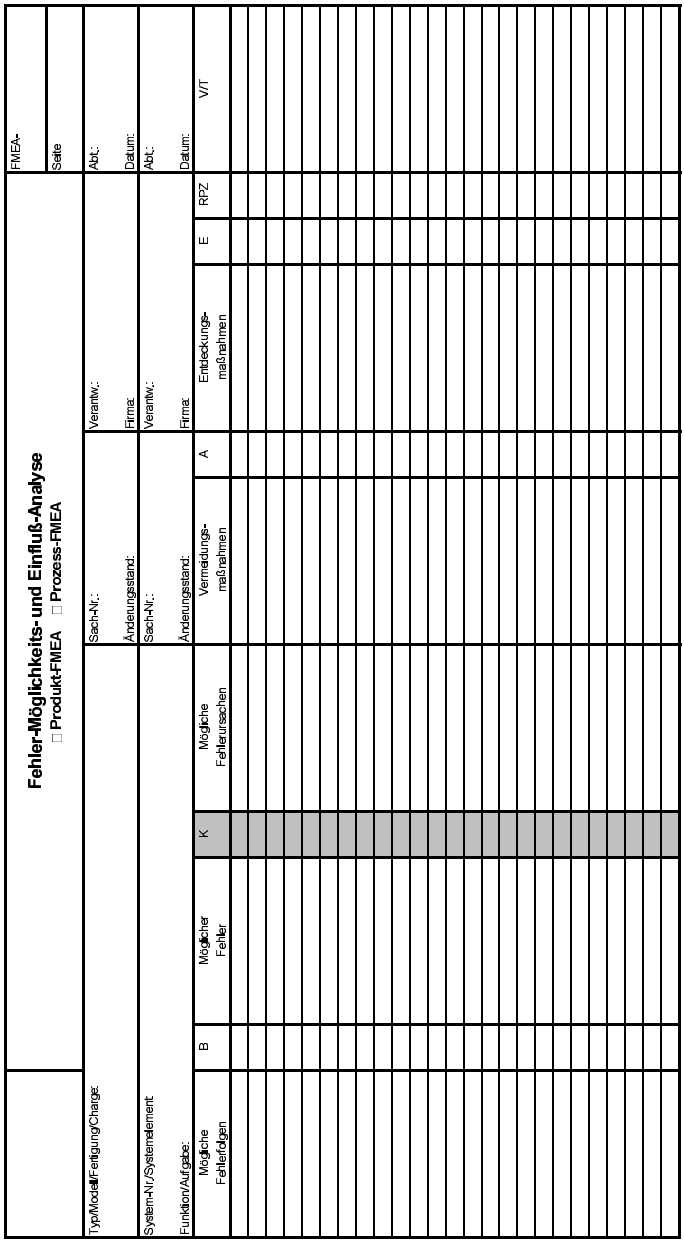


Abbildung 2.6: Formblatt für eine FMEA [VDA06]

liche, qualitative Vorgehensweise gemäß [DIN81] und die zeitlich später eingeführte Erweiterung um die quantitative Auswertung nach [DIN90a]. Weitere Ausführungen zur Methode beschreiben u. a. [Sch99], [BL04] und [Sto96].
Die qualitative Vorgehensweise gemäß [DIN81] beschreibt dabei die eigentliche Erstellung des Fehlerbaums: Das zu analysierende, unerwünschte TOP-Ereignis wird vorgegeben und hinsichtlich möglicher Ursachen analysiert. Dieses unerwünschte Ereignis wird zur oberen Spitze des Fehlerbaums. Darunter werden die identifizierten Ursachen angeordnet, für die wiederum nach Ursachen gesucht wird. Verbunden werden die Ursachen und auch das TOP-Ereignis durch logische UND-, ODER- bzw. NICHT-Verknüpfungen:

UND-Verknüpfung: Sie steht für den logischen Durchschnitt, d. h. die Auswirkung (also die übergeordnete Hierarchiestufe im Fehlerbaum) tritt dann ein, wenn alle direkt angeschlossenen darunter liegenden Ursachen zutreffen.

ODER-Verknüpfung Sie steht für die logische Vereinigung, d. h. die Auswirkung tritt dann ein, wenn mindestens eine direkt angeschlossene darunter liegenden Ursache zutrifft.

NICHT-Verknüpfung Sie steht für die Negation, d. h. die Auswirkung tritt dann ein, wenn die direkt angeschlossene darunter liegende Ursache nicht zutrifft. Diese Verknüpfung hat im Gegensatz zu den vorgenannten nur einen Eingang.

Durch Identifikation von Ursachen verschiedener Hierarchiestufen und deren Verknüpfungen entsteht die Baumstruktur. Abbildung 2.7 zeigt die Darstellung eines Fehlerbaums. Die Funktion der qualitativen Vorgehensweise liegt somit in der systematischen Identifikation und übersichtlichen Darstellung von Ursachen, die zu einem unerwünschten Ereignis führen. Neben den resultierenden Ereignisketten, den einzelnen Ästen des Fehlerbaums, fördert das Aufstellen des Fehlerbaums das Verständnis von Fehlermechanismen und deren Zusammenwirken.
Die quantitative Erweiterung der Methode nach [DIN90a] beinhaltet die Auswertung des Fehlerbaums durch Berechnung von Zuverlässigkeitsgrößen anhand der qualitativen Fehlerbaumstruktur. Mögliche Zuverlässigkeitskenngrößen sind z. B. die Nichtverfügbarkeit bzw. Ausfallwahrscheinlichkeit und die Häufigkeitsdichte für Fehler. Durch Kenntnis der Größen an den jeweiligen Fehlerbaumenden, also den elementaren Ursachen, können durch Anwendung der booleschen Algebra gemäß den Verknüpfungen, die Größen für das Gesamtsystem oder für Teilkomponenten berechnet werden. Neben den dafür anzuwendenen Berechnungsvorschriften gibt [DIN90a] Hinweise zum Vereinfachen

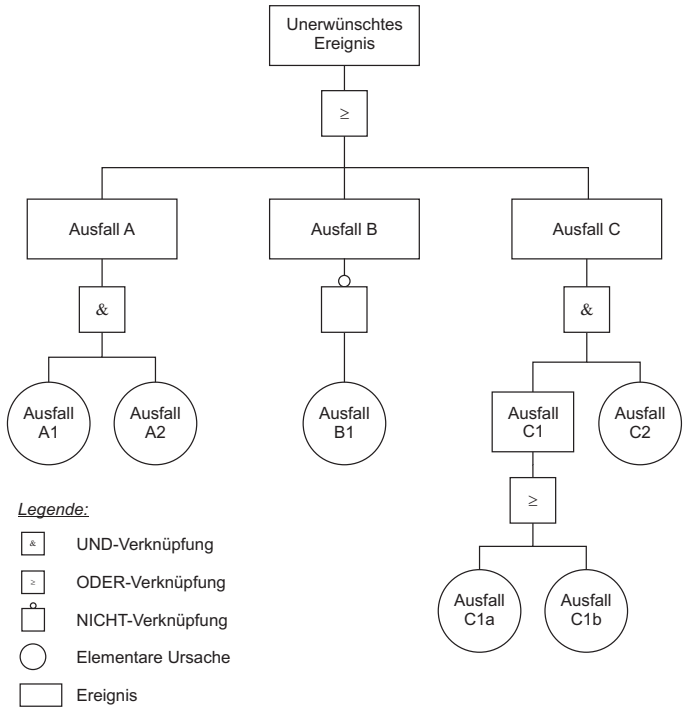


Abbildung 2.7: Darstellung des Fehlerbaums

von Fehlerbäumen, so dass sie auch durch Handrechenverfahren ausgewertet werden können.
Erweiterte oder zumindest verwandte Methoden der Fehlerbaumanalyse, die versuchen, der gesteigerten Komplexität mechatronischer Systeme gerecht zu werden, sind u. a. Methoden mit Entscheidungtabellen gemäß [Bie02] oder die Anwendung der Markoff-Theorie in diesem Kontext nach [BL04] oder [Koc01]. Hier können komplexere Abhängigkeiten zwischen Fehlern berücksichtigt und analysiert werden und der Aspekt in die Methodik integriert werden, dass sich Systeme in verschiedenen Zuständen befinden können und reparabel sind. Die Hauptfunktionen der Fehlerbaumanalyse, die systematischen Darstellung von Fehlermechanismen sowie die Ermittlung von Zuverlässigkeitskenngrößen des Gesamtsystems, stehen auch bei diesen Methoden im Vordergrund.

Checklisten zur Fehleranalyse

Um Fehler und Schwachstellen im Entwurf zu identifizieren, kann die Methode der Checkliste eingesetzt werden, die in anderer Form ebenfalls als Gefahrenanalyse zur Anwendung kommen kann, vgl. Kapitel 2.3.2. Checklisten im Kontext der Fehleranalyse beinhalten einen Satz verschiedener Fragen, die den Benutzer dazu stimulieren sollen, unterschiedliche Aspekte des Systems, kritisch zu betrachten und auf Fehler hin zu analysieren. Die Fragen von Checklisten zur Fehleranalyse sind dabei sehr allgemein formuliert [Sto96]. Eine Auswahl an Beispielfragen aus einer Checkliste nach [Bir91] ist im Folgenden dargestellt:

- Sind Elemente mit beschränkter Lebensdauer vorhanden?
- Wurde der Einfluss von Ein- und Ausschaltvorgängen und von externen Störungen berücksichtigt?
- Liegen Erfahrungsdaten aus ähnlichen Betrachtungseinheiten vor?
- Sind die Umweltbedingungen ausreichend definiert?
- Sind die gegenseitigen Beziehungen und Beeinflussungen der verschiedenen Elemente berücksichtigt worden?

...

Abbildung 2.8: Beispielfragen aus einer Checkliste (Auswahl) nach [Bir91]

Die Anwendung der Checkliste erfolgt durch systematische Abarbeitung der Fragen; immer mit dem Ziel, Fehler und Schwachstellen zu identifizieren, die bisher noch unentdeckt geblieben sind. Ein Problem bei der Fehleranalyse mit

Checklisten liegt darin, dass die Inhalte von Checklisten nicht alle Bereiche abdecken können und sollen, trotzdem aber durch ihren systematischen Aufbau eine Allumfassendheit suggerieren [Neu02].

Antizipierende Fehlererkennung (AFE)

Die Antizipierende Fehlererkennung, kurz AFE, beschreibt gemäß [HHK00] den Einsatz der zahlreichen Werkzeuge der TRIZ-Theorie im Kontext der Fehleranalyse. TRIZ steht dabei für das russische Akronym der *Theorie zum Lösen erfinderischer Aufgaben* und beinhaltet Methoden und Wissen, um systematisch Innovationen zu entwickeln. Dazu werden klassische Kreativitätstechniken, vorhandenes Wissen und Erfahrungen sowie die Logik der widerspruchsorientierten Problemlösung verknüpft, um sie gemeinsam in der TRIZ-Theorie zu verwenden. Die generelle Zielsetzung der Methodenklasse Fehleranalysen, Fehler bzw. deren Ursachen zu identifizieren, kann die Vorteile der TRIZ-Theorie durch die AFE-Methode in zweierlei Hinsicht ausnutzen; nämlich durch Provokation oder Inversion.
Die erste Ausführungsform beschreibt die Idee, das Versagen eines Systems, gezielt zu provozieren. Dazu erhalten die Konstrukteure die abstrakte Aufgabe, das System zum Versagen zu bringen bzw. Fehler zu *erfinden*. Im Gegensatz zur klassischen Vorgehensweise von Fehleranalysen, bei der Fehler die Bedeutung von Schwächen der eigenen Lösung besitzen, können die Konstrukteure mit dieser Aufgabenstellung ihre Kreativität in einer positiven Interpretation einsetzen. Erst im Anschluss an diesen Methodenteil, wird dazu übergangen, anhand der identifizierten Fehlerursachen, das System zu verbessern oder andere Abhilfemaßnahmen zu treffen.
Das zweite Einsatzgebiet der AFE, im Sinne der Inversion, hat die Aufgabe, für bereits bekannte Fehlfunktionen, die unbekannten Ursachen zu identifizieren. Dies erfolgt durch Invertierung des Problems, indem die Fehlfunktion zur gewollten Funktion transformiert wird. Auf dieses invertierte Problem lassen sich dann wiederum die TRIZ-Werkzeuge anwenden, um die Kreativität besser nutzen zu können. Im Anschluss erfolgt dann, ebenso wie bei der ersten Ausführungsform, der Einsatz von Abhilfemaßnahmen.
Beide Ansätze verändern die Aufgabenstellung zur Fehleranalyse insofern, dass der Prozess der Fehleridentifikation von einem negativen in einen positiven Blickwinkel gerückt wird, indem Fehler oder deren Ursachen erfunden werden sollen. Die Werkzeuge der TRIZ-Theorie können mit der einhergehenden systematischen Nutzung der Kreativität auf diese Weise verwendet werden. Abbildung 2.9 zeigt die Systematik der AFE.
Ein Anwendungsbeispiel der AFE wird in [TZZ98] ausführlich behandelt: Neue röhrenförmige Stützen bekommen schwarze Flecken, wobei die Ursache dafür unbekannt ist. Durch Inversion des Problems wird die Aufgabe formu-

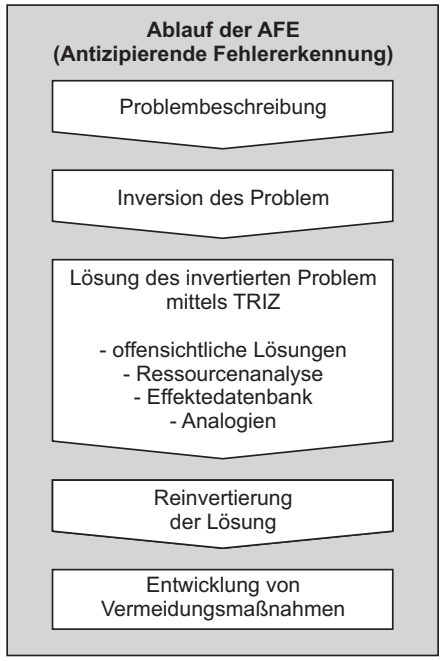


Abbildung 2.9: Ablaufsystematik der AFE [HHK00]

liert, die Rohroberfläche komplett zu schwärzen. Durch Anwendung von TRIZ-Methoden werden anhand der vorhandenen Ressourcen, der ablaufenden Effekte und durch Bildung von Analogien verschiedene Ansätze gefunden, das Rohr komplett zu schwärzen bzw. durch Re-Inversion das Originalproblem zu vermeiden.

2.3.2 Gefahrenanalysen

Gefahrenanalysen beschreiben die Methodenklasse, bei der das Gefahrenpotenzial für den Menschen oder die Umwelt im Analysefokus liegt. Dieses Gefahrenpotenzial kann einerseits aus Fehlern resultieren, für deren Identifikation im vorhergehenden Kapitel einige Methoden erläutert wurden, andererseits kann es durch verschiedene systematische Ansätze neu identifiziert werden. Typische Vertreter für die Methodenklasse Gefahrenanalyse sind die Vorläufige Gefahrenanalyse (Preliminary Hazard Analysis - PHA), die Funktionale Gefahrenanalyse (Functional Hazard Analysis - FHA), die HAZOP-Analyse (Hazard and Operability Study), die Ereignisbaumanalyse (Event Tree Analysis - ETA), sowie die Gefahrenanalyse mittels Normen und Checklisten. Die gemeinsame Basis dieser Methoden liegt in der Identifikation und Analyse von potenzielle Gefahren, die von Systemen ausgehen können. Der jeweilige Fokus, auf den die Gefahrenanalyse anzuwenden ist, variiert dabei, ebenso wie bei den Fehleranalysen, sowohl zwischen den unterschiedlichen Methoden als auch bei der Möglichkeit, die gleiche Methode zu verschiedenen Zwecken zu gebrauchen; z. B. kann eine Anwendung bereits anhand einer sehr allgemein gehaltenen Aufgabenstellung oder erster Hauptfunktionsbeschreibung erfolgen oder auch erst sehr spät im Entwicklungsprozess bei einem fertigen Labormuster. Weiterhin bieten sich selbstverständlich die Ergebnisse der Fehleranalysen als Input für diese Methodenklasse an. Im Folgenden werden ausgewählte Gefahrenanalysen erläutert.

Vorläufige Gefahrenanalyse (PHA)

Die vorläufige Gefahrenanalyse ist im englischsprachigen Raum als Preliminary Hazard Analysis (PHA) bekannt und wird, wie der Name bereits aussagt, zu einem sehr frühen Zeitpunkt im Entwicklungsprozess eingesetzt. In der Literatur gibt es unter diesem Namen abweichende Methodenerläuterungen. Einerseits wird die PHA dort so verstanden, dass sie lediglich ein frühe Anwendung für eine nicht näher festgelegte Methode der Gefahrenanalyse beschreibt [Sto96] [VDI04b], andererseits wird sie als eigenständige Methode verstanden, die auch einer eigenen Systematik folgt [Län03] [MIL93]. Letzterer Sichtweise wird in dieser Arbeit gefolgt.

Die Aufgabe der PHA liegt in der Identifikation von sicherheitskritischen Auswirkungen eines Systemkonzepts, um darauf aufbauend eine erste Bewertung der Gefahren zu treffen sowie notwendige Folgemaßnahmen festzulegen. Dafür soll die PHA bereits mindestens die folgenden Aspekte auf Gefahren hin analysieren [MIL93]:

- Gefährliche Komponenten, z. B. Brennstoffe, Laser, Sprengstoffe, Giftstoffe, gefährliche Konstruktionsmaterialien
- Sicherheitskritische Nahtstellen des Systems, z. B. Mensch-Maschine oder Hardware-Software Schnittstellen, Materialpaarungen, elektromagnetische Verträglichkeit
- Umgebungs- und Betriebsbedingungen, z. B. Stöße, Vibrationen, extreme Temperaturen, Geräusche
- Abläufe im Betrieb, Test, Instandhaltung und Notfall
- Sicherheitsspezifische Ausrüstungen, Schutzvorkehrungen
- Fehlfunktionen des Systems, der Subsysteme oder der Software

Dokumentiert wird die PHA in Form von Tabellenblättern oder Listen. Meist erfolgt für die identifizierten Gefahren innerhalb der PHA-Methodik schon eine Risikobewertung anhand der Häufigkeit und Schwere der Gefahr. Dieser Schritt der PHA-Systematik ist aber eigentlich bereits Teil der Methodenklasse Risikoanalyse.

Funktionale Gefahrenanalyse (FHA)

Die Funktionale Gefahrenanalyse wird im Englischen als Functional Hazard Analysis bzw. Functional Hazard Assessment (FHA) bezeichnet. Sie ist eine systematische Vorgehensweise, bei der die Haupt- und Teilfunktionen eines Systems gezielt auf Gefahren hin analysiert und bewertet werden. Potenzielle Fehlfunktionen und Ausfallzustände sollen identifiziert werden, um sie gemäß ihrer Auswirkungsschwere klassifizieren und Sicherheitsziele auf höheren Systemebenen festlegen zu können. Zur Analyse der Funktionen wird im ersten Schritt der Methode die Aufgabe der Betrachtungseinheit definiert. Diese wird dann im zweiten Schritt in Funktionen und Teilfunktionen beschrieben und zerlegt. Die resultierende Funktionshierarchie wird nun dahingehend analysiert, dass Gefahren identifiziert werden sollen, die aufgrund eines Ausfalls oder einer Fehlfunktion auftreten. Das heißt, dass das Wegfallen jeder Funktion- oder Teilfunktion angenommen wird und die Auswirkungen auf mögliche Gefahren hin überprüft werden. Die identifizierten Gefahren werden dokumentiert und

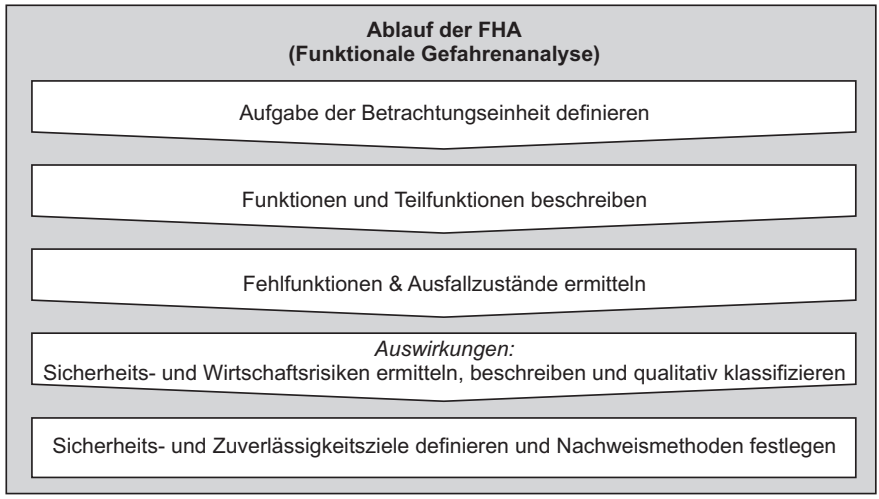


Abbildung 2.10: Ablaufsystematik der FHA [Kne00]

qualitativ klassifiziert. Auf diesen Ergebnissen basierend, werden Sicherheits- und Zuverlässigkeitsziele definiert und Nachweismethoden festgelegt. Abbildung 2.10 zeigt die systematische Vorgehensweise der FHA, die insbesondere in der Luftfahrtindustrie eingesetzt wird [Kne00] [VDI04b] [MG04].

HAZOP-Analyse

Die HAZOP-Analyse steht als Akronym für die englische Bezeichnung Hazard and Operability Study, die ins Deutsche übertragen häufig als PAAG-Verfahren (Prognose von Fehlern, Auffinden der Ursachen, Abschätzen der Wirkungen, Gegenmaßnahmen) beschrieben wird. Trotzdem wird auch in der deutschen Literatur vorwiegend der Name HAZOP verwendet. Entwickelt wurde die HAZOP-Analyse für die Verfahrenstechnik, im Speziellen für die chemische Industrie. Der Ablauf der Methode erfolgt durch eine systematische Suche nach Gefahren, die auf Abweichungen der Aufgabenerfüllung oder von Prozessparametern basieren. Unterstützt wird diese Suche durch einen Katalog mit Leitwörtern (nicht, zu viel, zu wenig, zu früh, zu spät), die die Bearbeiter der HAZOP-Analyse dazu inspirieren sollen, sich Fragen der Art *Was wäre wenn...?* zu stellen. Durch Kombinationen zwischen den Leitwörtern und den System-Attributen, z. B. Prozessparametern oder Funktionen, werden potenzielle Gefahren identifiziert, die in nachfolgenden Schritten, ähnlich dem FMEA-Vorgehen, detailliert analysiert werden [VDI04b] [Sto96] [ONB02]. Abbildung 2.11 zeigt ein beispielhaftes Formblatt, das für die HAZOP-Analyse genutzt

werden kann. Eine Bewertung der identifizierten und analysierten Gefahren kann die HAZOP-Analyse noch im Sinne einer Risikoanalyse erweitern.

Ereignisbaumanalyse (ETA)

Die Ereignisbaumanalyse, im Englischen als Event Tree Analysis (ETA) bezeichnet, ist trotz ihrer großen Ähnlichkeit zur Fehlerbaumanalyse, vgl. Kapitel 2.3.1, eindeutig der Methodenklasse der Gefahrenanalysen zuzuordnen. Der Grund dafür liegt auf dem verschobenen Analysefokus der ETA, der sich anstatt auf die Ursachen eines unerwünschten Ereignisses, auf die potenziellen Systemreaktionen und Folgen richtet. Es werden bei dieser Methode somit nicht die Fehler und ihre Ursachen betrachtet, sondern es werden Gefahren analysiert und teilweise sogar vorher unentdeckte Gefahren identifiziert.
Bei der ETA werden im ersten Schritt Initial-Ereignisse gesucht, die das System schädigen und gefährliche Auswirkungen im Sinne von Gefahren haben können. Jedes identifizierte Initial-Ereignis bildet die Spitze für einen Ereignisbaum. Die Baumstruktur entsteht dadurch, dass die Reaktion des Systems auf das Eintreten eines solchen Initial-Ereignisses analysiert wird und sich verschiedene Ereignis-Pfade ergeben. Jede Reaktion kann ebenfalls unterschiedliche Ereignisverläufe haben, z. B. kann ein spezifiziertes Folgeereignis eintreten oder nicht eintreten. Es entsteht auf diese Weise eine Ereigniskette, die durch die jeweiligen Eintritts-Möglichkeiten zu einem Baum wird. Abbildung 2.12 zeigt ein Beispiel für einen Ereignisbaum. Neben der systematischen Darstellung von Ereignisfolgen kann der Ereignisbaum, ebenso wie der in Kapitel 2.3.1 erläuterte Fehlerbaum, auch quantitativ ausgewertet werden. Dazu werden den Ereignissen jeweils Eintrittswahrscheinlichkeiten zugeordnet. Durch Multiplikation *von oben nach unten* entlang der einzelnen Pfade, kann dann für jedes Ereignisergebnis, die durch die untersten Blätter des Baums repräsentiert werden, die Eintrittswahrscheinlichkeit angegeben werden. Diese Quantifizierung kann selbstverständlich wieder bereits als Teil einer Risikoanalyse verstanden werden [Sto96].

Gefahrenanalyse mittels Normen und Checklisten

Neben den zuvor beschriebenen, systematischen Gefahrenanalysen zur Identifikation von vorher unbekannten Gefahrenpotenzialen, kann selbstverständlich auch auf bereits vorhandenes Wissen zurückgegriffen werden, das aus Projekten oder Produkten resultiert, die bereits in der Vergangenheit durchgeführt bzw. entwickelt wurden. Dieses Wissen ist, insbesondere bei der Entwicklung von Maschinen, z. B. in Form von Normen oder Checklisten vorhanden und kann zur Anfertigung von Gefahrenanalysen verwendet werden. Unabhängig davon, ob das Wissen in Normen oder Checklisten vorhanden ist, stellt das je-

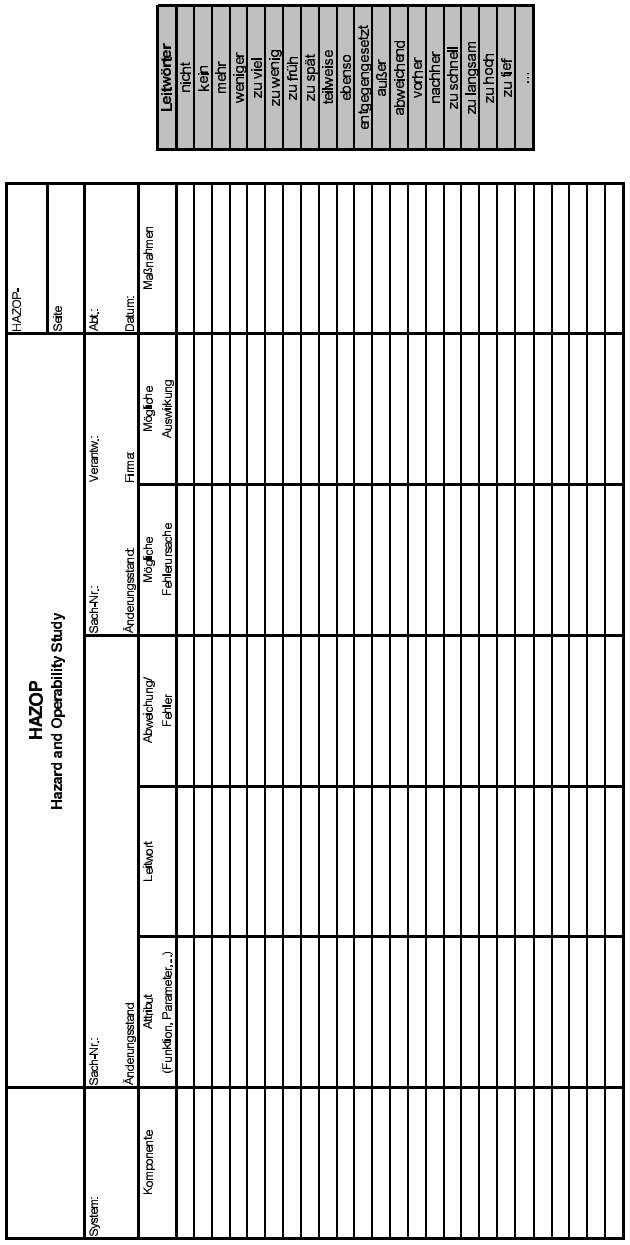


Abbildung 2.11: Formblatt für eine HAZOP-Analyse mit ausgewählten Leitwörtern

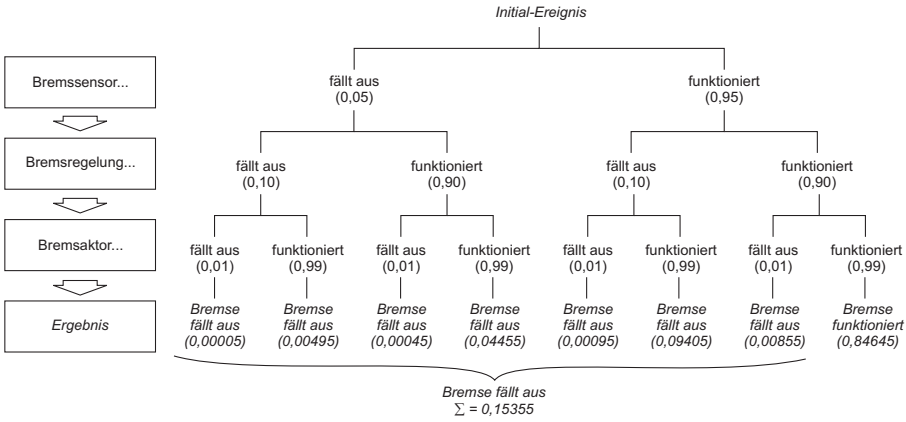


Abbildung 2.12: Darstellung des Ereignisbaums mit Bremsausfall-Beispiel

weilige Medium eine Auflistung von Gefahrenpotenzialen bereit, die analysiert werden müssen. Gemäß [Neu02] kann die Gefahrenanalyse in diesem Kontext als *Verkürzte* oder *Ausführliche Gefahrenanalyse* zur Anwendung kommen:
Die *Verkürzte Gefahrenanalyse* wird dann durchgeführt, wenn die Konstruktion strikt auf einer bestehenden Produktnorm, d. h. auf einer harmonisierten C-Norm, basiert. In diesem Fall muss lediglich überprüft werden, ob die in der Norm aufgelisteten Gefahren auf die Neukonstruktion zutreffen. Die deutlich umfangreicheren Prüfpunkte von allgemeineren Normen, oder auch der EG Maschinenrichtlinie, müssen dann nicht mehr analysiert werden, da sich die Konstrukteure auf die Konformitätsvermutung berufen können. Sie können dann davon ausgehen, dass die Produktnorm bereits die geforderten Sicherheits- und Gesundheitsanforderungen erfüllt.
Da sich Produkt- oder auch Gruppennormen nur auf Standardentwicklungen beziehen können und auch nur für diese vorhanden sind, besteht häufig die Option einer Verkürzten Gefahrenanalyse nicht. In diesen Fällen wird eine *Ausführliche Gefahrenanalyse* gemäß dem Anhang I der EG-Maschinenrichtlinie durchgeführt. Die Systematik dieser Ausführlichen Gefahrenanalysen besteht darin, alle im Anhang der Richtlinie aufgeführten Punkte sorgfältig, aber auch pragmatisch abzuarbeiten. Grundlegende Sicherheits- und Gesundheitsschutzanforderungen, die gemäß der Richtlinie [Eur06] überprüft werden müssen, werden unter den folgenden Oberbegriffen aufgezählt: Allgemeines, Steuerungen und Befehlseinrichtungen, Schutzmaßnahmen gegen mechanische Gefährdungen, Anforderungen an Schutzeinrichtungen, Risiken durch sonstige Gefährdungen, Instandhaltung und Informationen. Im Folgenden werden drei Beispiele für Gefahren genannt, die innerhalb dieser Aspekte aufgezählt werden

[Eur06]:

> Der Bedienungsplatz muss so gestaltet und ausgeführt sein, dass Risiken aufgrund von Abgasen und/oder Sauerstoffmangel vermieden werden.
>
> Die Maschine muss so konstruiert und gebaut sein, dass eine möglicherweise gefährliche elektrostatische Aufladung vermieden oder begrenzt wird, und/oder mit Einrichtungen zum Ableiten solcher Ladungen ausgestattet sein.
>
> Die Maschine muss so konstruiert und gebaut sein, dass Risiken durch Maschinenvibrationen insbesondere an der Quelle so weit gemindert werden, wie es nach dem Stand des technischen Fortschritts und mit den zur Verringerung von Vibrationen verfügbaren Mitteln möglich ist.

Darüber hinaus bietet insbesondere der Anhang A der europäischen Norm DIN EN 1050 [DIN96] eine sehr große Anzahl an überprüfbaren Gefahrenpotenzialen. Diese sind tabellarisch aufbereitet und konkreter formuliert als die in der Maschinenrichtlinie. Daher lassen sie sich im Sinne einer systematischen Abarbeitung besser handhaben. Beispiele für dort aufgelistete Gefahrenpotenziale sind in Tabelle 2.1 aufgeführt. Neben den in Normen zur Verfügung stehenden Auflistungen von Gefahrenpotenzialen, existieren ebenfalls häufig unternehmensinterne Checklisten oder auch kommerziell erhältliche Checklisten, z. B. von Interessensverbänden bestimmter Industrien.

2.3.3 Risikoanalysen

Risikoanalysen repräsentieren die Methodenklasse, deren Ziel die Einschätzung bzw. Bewertung bereits identifizierter Gefahren ist und über deren Vertretbarkeit daraufhin entschieden werden kann [Neu02]. Die Bewertung erfolgt häufig anhand von Kriterien, die unterschiedlichen Risikodefinitionen entsprechen. Ein Beispiel für diese Kriterien ist gemäß der in Kapitel 2.1 verwendeten Risikodefinition die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens [DIN02]. Ähnliche, aber teilweise auch abweichende Kriterien davon stellen ein Unterscheidungsmerkmal für unterschiedliche Methoden der Risikoanalyse dar. Ein anderes Unterscheidungsmerkmal liegt in der Systematik zur Bewertung der Gefahr, z. B. durch Graphen oder durch einfache multiplikative Verfahren. Typische Risikoanalysen dieser Methodenklasse, die auch im weiteren Verlauf dieses Kapitels vorgestellt werden, sind die Methode der Risikoprioritätszahl bzw. das multiplikative Verfahren, die Methode des Risikographen sowie die Methode der

Nr.	Gefährdungen
1	**mechanische Gefährdungen** durch: - Maschinenteile oder Werkstücke - Ansammlung von Energie im Inneren der Maschine
1.1	Gefährdung durch Quetschen
1.3	Gefährdung durch Schneiden oder Abschneiden
2	**elektrische Gefährdungen** durch:
2.1	direkte Berührung von Personen mit von unter Spannung stehenden Teilen
2.2	Berührung von Personen mit Teilen, die durch Fehlzustände spannungsführend geworden sind
3	**thermische Gefährdungen** mit der Folge von
3.1	Verbrennungen und Frostbeulen und andere Verletzungen durch den Kontakt von Personen mit Gegenständen oder Werkstoffen sehr hoher oder niedriger Temperatur, durch Flammen oder Explosionen und auch durch die Strahlung von Wärmequellen
4	**Gefährdungen durch Lärm** mit der Folge von
4.1	Gehörverlust (Taubheit), anderen physiologischen Beeinträchtigungen (z. B. Gleichgewichtsverlust, Nachlassen der Aufmerksamkeit)
5	**Gefährdungen durch Vibration**
5.2	Ganzkörpervibrationen, speziell in Verbindung mit Zwangshaltungen
6	**Gefährdungen durch Strahlungen**
6.1	Strahlungen mit Niederfrequenz, Funkfrequenz Mikrowellen
8	**Gefährdungen durch die Vernachlässigung ergonomischer Grundsätze bei der Gestaltung der Maschine** z. B. Gefährdungen durch
8.1	ungesunde Körperhaltung oder besondere Anstrengung
8.4	unangepasste örtliche Beleuchtung
9	**Kombination von Gefährdungen**
37	**menschliches Fehlverhalten, menschliches Verhalten**

Tabelle 2.1: Gefährdungen gemäß [DIN96] (Auswahl)

Risikomatrix. Darüber hinaus wird die ALARP-Methode erläutert, die einen Abgleich zwischen dem Risiko und dem Aufwand der jeweils entsprechenden Sicherheitsmaßnahmen realisiert.

Risikoprioritätszahl

Die Methode der Risikoprioritätszahl als Risikoanalyse wird allgemeingültiger auch als multiplikatives Verfahren bezeichnet [Neu02]. Der Kern dieser Methode liegt in der Multiplikation von Kriterienbewertungen, die das Risiko beschreiben. Das Produkt liefert eine quantitative Risikogröße, die eine Bewertung von Gefahren darstellt. Häufig wird das Resultat als Risikoprioritätszahl (RPZ) behandelt, das eine Priorisierung der identifizierten Gefahren vornehmen soll. Die Auswahl und Anzahl der verwendeten Kriterien unterscheidet sich allerdings in verschiedenen Ausprägungen der Methode.
Gemäß der Risikodefinition nach [DIN02] kann aus den Bewertungen der Kriterien Schadensausmaß und Eintrittswahrscheinlichkeit das Produkt gebildet werden und als Risikobewertung fungieren [Neu02]. Auch die Verwendung von ähnlichen Kriterien wie z. B. Häufigkeit, Dauer des Aufenthalts im Gefahrenbereich, Schwere der Verletzung oder allgemein die Kritikalität der Konsequenz sind üblich für multiplikative Verfahren. Ein Beispiel zur Umsetzung dieses Verfahrens findet sich in [Ber99]: Dort wird für Druck- und Papierverarbeitende Maschinen eine RPZ anhand von Auftretenswahrscheinlichkeit (AW) und Verletzungsschwere (VS) gebildet. Der Auftretenswahrscheinlichkeit wird dabei ein Wert zwischen 1=Ereignis unmöglich und 5=Ereignis häufig ($>$ 1 x in der Woche) zugeordnet und der Verletzungsschwere ein Wert zwischen 1=kleinere Verletzungen (Quetschung, Abschürfung) und 4=tödliche Verletzung. Das Produkt daraus ergibt die RPZ, die dementsprechend Werte zwischen 1 und 20 einnehmen kann, wobei die akzeptierte RPZ für einen Wert von 8 festgelegt ist.

$$RPZ = AW \times VS$$

Diese zuvor beschriebenen multiplikativen Verfahren orientieren sich dicht an den Kriterien der Risikodefinition. Einen erweiterten Ansatz realisiert ein RPZ-Verfahren, das Kriterien der Risikoentdeckung oder Risikominderung in die Bewertung integriert. Diese Version wird nachfolgend in dieser Arbeit RPZ*-Verfahren genannt, um eine bessere Unterscheidbarkeit zu gewährleisten. Dieses Verfahren wird in vielen heutigen Versionen der FMEA oder auch in HAZOP-Analysen genutzt. Unter anderem verwendet die in Kapitel 2.3.1 vorgestellte FMEA nach [VDA06] eine RPZ*, die die Kriterien Bedeutung der Ausfallauswirkung (B), Auftretenswahrscheinlichkeit der Ausfallursache (A) und Entdeckungswahrscheinlichkeit der aufgetretenen Ausfallursache (E) verwendet.

$$RPZ^* = B \times A \times E$$

		Auswirkung			
		katastrophal	kritisch	begrenzt	geringfügig
Häufigkeit	häufig	I	I	I	II
	wahrscheinlich	I	I	II	III
	gelegentlich	I	II	III	III
	gering	II	III	III	IV
	unwahrscheinlich	III	III	IV	IV
	nicht glaubhaft	IV	IV	IV	IV

Abbildung 2.13: Risikomatrix gemäß [DIN02]

Für B, A und E werden jeweils Bewertungszahlen von 1 bis 10 verwendet, wobei 10 jeweils für den höchsten Risikobeitrag vergeben wird. Trotz quantitativer Werte für das Ergebnis, wird bei diesem Verfahren allerdings keine Grenze für eine akzeptierte RPZ* gesetzt, sondern es werden Interpretationshinweise bezüglich verschiedener Kombinationen gegeben. Das Beispiel, dass sich eine RPZ* von 100 sowohl durch $(10 \times 1 \times 10)$ als auch durch $(10 \times 10 \times 1)$ ergeben kann, verdeutlicht die Problematik, dass die Betrachtung des Absolutwertes einer RPZ* in vielen Fällen irreführend und als Grundlage für weitere Maßnahmen ungeeignet ist [VDA06].

Dennoch realisiert die multiplikative Verknüpfung von Kriterien eine pragmatische Bewertung von Gefahren bzw. den daraus resultierenden Risiken. Je nach Auswahl der Kriterien und nach Interpretation der RPZ variiert die Ausprägung der Methode.

Risikomatrix

Einen ähnlichen Ansatz wie die RPZ-Methode verfolgt auch das Verfahren der Risikomatrix. Gemäß [DIN02] werden die identifizierten Gefahren durch die das Risiko beschreibenden Kriterien *Häufigkeit* und *Auswirkung* bewertet. Die Ausprägungen dieser Kriterien spannen die Risikomatrix auf. Die Bewertung der Gefahr anhand der Kriterien führt dann zu einer Einordnung innerhalb der Risikomatrix und der damit einhergehenden Zuordnung zu einer Risikoklasse. Abbildung 2.13 zeigt eine Risikomatrix, deren Interpretationen der Risikoklassen im Sinne der später beschriebenen ALARP-Methode in Tabelle 2.2 dargestellt ist. Ein weiteres mögliches Vorgehen zur Risikoanalyse mittels einer Matrix ist in [MIL93] beschrieben. Das zuvor erläuterte Vorgehen wird dort noch durch Interpretationstabellen für die Kriterienbewertung von Häufigkeit und Ausmaß erweitert.

Risikoklasse	Interpretation
Klasse I	nicht tolerierbares Risiko
Klasse II	unerwünschtes Risiko, das nur tolerierbar ist, wenn eine Risikominderung nicht durchführbar ist oder die Kosten der Minderung unverhältnismäßig hoch im Vergleich zur erzielten Verbesserung sind
Klasse III	tolerierbares Risiko wenn die Kosten einer Risikominderung die erreichbare Verbesserung übersteigen
Klasse IV	vernachlässigbares Risiko

Tabelle 2.2: Interpretation der Risikomatrixklassen gemäß [DIN02]

Risikograph

Eine weitere Methode der Risikoanalyse wird durch die Erstellung und Anwendung eines Risikographen gegeben, der teilweise auch als Entscheidungsbaum in der Literatur beschrieben wird. Anhand von Kriterien, die das Risiko beschreiben bzw. bewerten, kann ein Zuordnungs- und Klassifizierungsschema erstellt werden, das die Form eines sich verästelnden Risikographen darstellt. Beurteilungskriterien dafür sind z. B. Schadensausmaß, Aufenthaltsdauer, Gefahrenabwendung und Eintrittswahrscheinlichkeit. Je nach Bewertung der einzelnen Kriterien, wird ein Pfad im Risikograph eingeschlagen, der zu einer vorher festgelegten Risiko- bzw. Risikoanforderungsklasse führt. Diese Klassen beschreiben, wie mit dem Risiko bzw. der ursächlichen Gefahr oder dem Fehler umzugehen ist [Neu02].
Auch in [DIN02] wird die Bewertung des Risikos, bzw. die daraus resultierende Notwendigkeit eines klassifizierten Sicherheitssystems, anhand eines Graphen beschrieben, der im Folgenden erläutert und dargestellt wird: Die Verwendung des Graphen dient der Auswahl der Sicherheitsanforderungsklasse, dem so genannten SIL (Sicherheits-Integritätslevel), eines sicherheitsbezogenen Systems. Ein sicherheitsbezogenes Systems ist im Sinne der Norm ein System, das zusätzlich zum Grundsystem verwendet werden muss, um die geforderte Sicherheit zu gewährleisten. Die Basisidee des Graphen beschreibt das Risiko als Produkt aus der Häufigkeit und der Auswirkung des gefährlichen Vorfalls, wobei sich die Häufigkeit weiter in drei beeinflussenden Faktoren aufteilen lässt. Es ergeben sich die folgenden Kriterien für den Risikographen:

- Auswirkung des gefährlichen Vorfalls (C)
- Häufigkeit und Zeit des Aufenthalts im Gefahrenbereich (F)
- Möglichkeit, den gefährlichen Vorfall zu vermeiden (P)

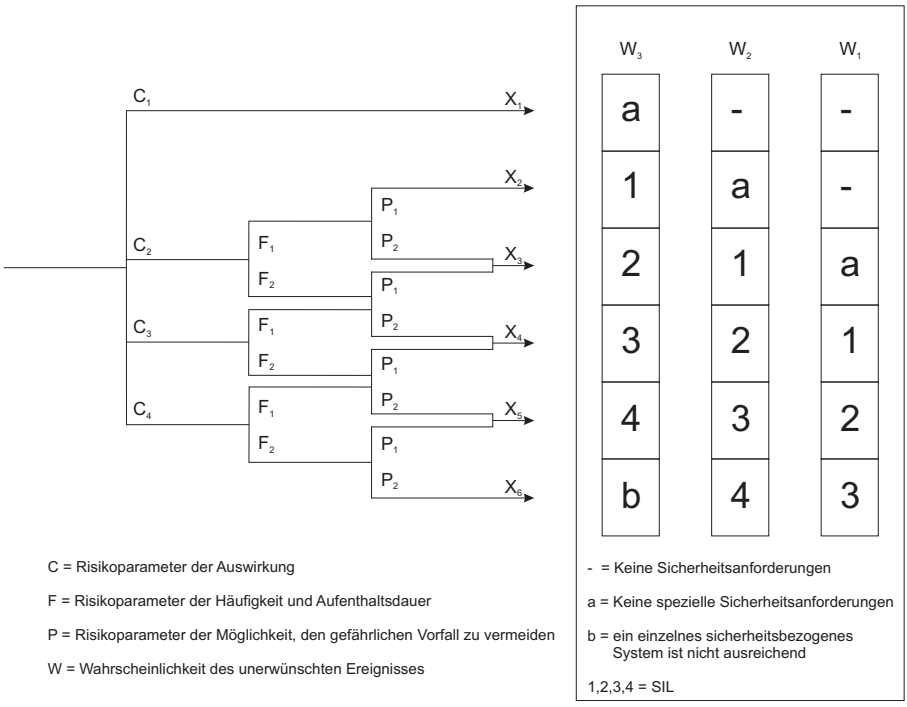


Abbildung 2.14: Beispiel für einen Risikograph gemäß [DIN02]

- Wahrscheinlichkeit des unerwünschten Ereignisses ohne das Vorhandensein eines sicherheitsbezogenen Systems (W)

Durch Kombination der Kriterien lässt sich der Risikograph gemäß Abbildung 2.14 aufstellen. Die Kriterien C, F und P führen zu Verästelungen des Graphen, die zu den Ergebnissen X_1 bis X_6 führen. Diesen sind wiederum verschiedenen Auswahlskalen zugeordnet, deren Verwendung vom Kriterium W abhängig ist. In der Norm wird für die Ausprägungen der Kriterien allgemeingültig lediglich die Ordnung festgelegt:

- $C_A < C_B < C_C < C_D$;
- $F_A < F_B$
- $P_A < P_B$
- $W_1 < W_2 < W_3$

Eine Interpretation dieser Ordnung ist zur Veranschaulichung als Beispiel ebenfalls in der Norm enthalten und in Tabelle 2.3 dargestellt.
Bei der Anwendung des Graphen beginnt man gemäß der Abbildung 2.14 auf der linken Seite und folgt dem jeweiligen Pfad bis zu einem Ergebnis X_n. Daran anschließend erfolgt die Auswahl der Skala anhand der Bewertung von W, nach der sich dann das Endergebnis richtet. Dieses kann dann die Ausprägungen *a=keine speziellen Sicherheitsanforderungen*, *b=ein einzelnes sicherheitsbezogenes System ist nicht ausreichend* oder einen der SIL-Werte zwischen 1 und 4 annehmen. Letztere Ergebnisse lassen dann die Auswahl eines klassifizierten sicherheitsbezogenen Systems zu.
Zusammenfassend erlauben die drei bisher beschriebenen Methoden der Risikoanalyse, sinnvolle Abstufungen für Risikobewertungen anhand verschiedener Schlüsselfaktoren und Vorgehensmodelle zu realisieren. Notwendig zur Durchführung von Risikoanalysen sind jedoch Fehler- und Gefahrenanalysen, die den Input für diese Methodenklasse darstellen.

ALARP-Methode

Neben den zuvor beschriebenen Risikoanalysen, die speziell die Bewertung des Risikos anhand von Kriterien wie Ausmaß und Häufigkeit im Fokus haben, gibt es noch die ALARP-Methode [DIN02], die bei der Bewertung des Risikos auch den Aufwand für Sicherheitsmaßnahmen und den erzielbaren Nutzen berücksichtigt. Gemäß der Bedeutung des Akronoyms ALARP für *as low as reasonably practicable*, das übersetzt *so niedrig wie vernünftigerweise möglich* lautet, wird das Risiko solange reduziert, bis der zusätzliche Aufwand für Maßnahmen den daraus resultierenden Nutzen nicht länger rechtfertigt.
Grundlegend für die Anwendung des ALARP-Prinzips ist eine Bewertung oder Zuordnung der Risiken in die folgenden drei Bereiche, die z. B. auch aus den Risikomatrixklassen resultieren können:

- Das Risiko ist so groß, dass es insgesamt abgelehnt werden muss.
- Das Risiko ist so klein oder soweit verringert worden, dass es unbedeutend ist.
- Das Risiko liegt zwischen den beiden zuvor genannten Bereichen und wurde auf die niedrigste Stufe verringert, die gemäß dem ALARP-Prinzip praktikabel ist.

Aus dem letztgenannten Bereich resultiert nach Anwendung des ALARP-Prinzips das *tolerierbare Risiko*. Dieses muss folglich soweit wie vernünftigerweise möglich reduziert worden sein. Der Begriff *tolerierbar* beinhaltet dabei

Risikoparameter	Klassifizierung
Auswirkung	
C_1	Geringe Verletzung
C_2	Schwere irreversible Verletzung einer oder mehrerer Personen; Tod einer Person
C_3	Tod mehrerer Personen
C_4	Tod sehr vieler Personen
Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich	
F_1	Seltener bis öfterer Aufenthalt im gefährlichen Bereich
F_2	Häufiger bis dauernder Aufenthalt im gefährlichen Bereich
Möglichkeit, den gefährlichen Vorfall zu vermeiden	
P_1	Möglich unter bestimmten Bedingungen
P_2	Beinahe unmöglich
Wahrscheinlichkeit des unerwünschten Ereignisses	
W_1	Eine sehr geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und nur wenige unerwünschte Ereignisse sind wahrscheinlich.
W_2	Eine geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und wenige unerwünschte Ereignisse sind wahrscheinlich.
W_3	Eine relativ hohe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und häufige unerwünschte Ereignisse sind wahrscheinlich.

Tabelle 2.3: Beispiel für eine Kriterienklassifizierung des Risikographs in Abbildung 2.14 [DIN02]

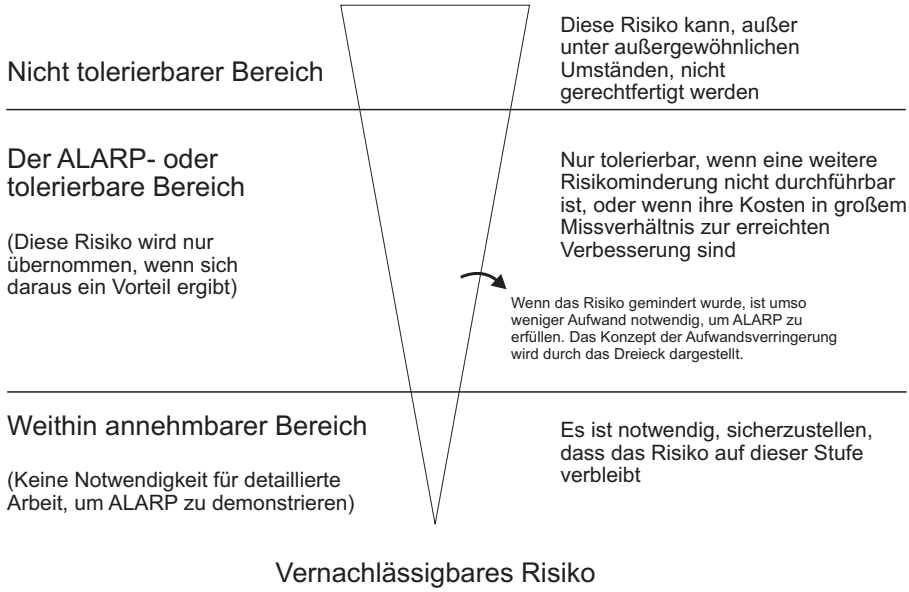


Abbildung 2.15: ALARP-Methode und tolerierbares Risiko [DIN02]

die Bereitwilligkeit, dass mit einem bestimmten Risiko aufgrund des gegenüberstehenden Nutzen gelebt werden kann. Je nachdem, wie hoch das als tolerierbar eingestufte Risiko liegt, kann mehr oder weniger Aufwand erwartet werden, um dieses zu verringern. Am oberen Ende des tolerierbaren Bereichs kann großer Aufwand erwartet werden um bereits unbedeutende Minderungen zu erreichen, während am unteren Ende bereits eine Abwägung zwischen Kosten und Nutzen ausreichend ist. Abbildung 2.15 zeigt die Einteilung der drei Bereiche.

In Verbindung mit den Resultaten der Methode *Risikomatrix*, kann der tolerierbare Bereich durch die Risikoklassen II und III beschrieben werden: Der obere Bereich des tolerierbaren Risikos beinhaltet *unerwünschte Risiken, die nur tolerierbar sind, wenn eine Risikominderung nicht durchführbar ist oder die Kosten der Minderung unverhältnismäßig hoch im Vergleich zur erzielten Verbesserung sind (Klasse II)*; der untere Bereich beinhaltet *tolerierbare Risiken, bei denen die Kosten einer Risikominderung die erreichbare Verbesserung übersteigen (Klasse III)*.

Zusammenfassend gibt es für die Methodenklasse *Risikoanalysen* zahlreiche ähnlich strukturierte Methoden, die auf den das Risiko beschreibenden Kriterien basieren. Darüber hinaus existieren Methoden, die Wirtschaftlichkeits-

aspekte berücksichtigen. Beide Verfahren können komplementär angewendet werden, beinhalten teilweise aber bereits Ansätze des jeweils anderen.

2.4 Ansätze für Verlässlichkeitsprozesse

Neben den zuvor beschriebenen einzelnen Verlässlichkeitsmethoden existieren bereits auch einige Prozessansätze, die die verschiedenen Methoden miteinander kombinieren und teilweise auch in einen Entwicklungsprozess integrieren. Häufig resultieren sie allerdings aus Herausforderungen spezieller Industrien oder sind von einzelnen Unternehmen initiiert. Verschiedene Ansätze für Verlässlichkeitsprozesse werden im Folgenden kurz vorgestellt und anhand von Kriterien analysiert; die ausgewählten Kriterien dafür sind

- Industrie-/Unternehmensfokus,
- System-Fokus,
- Detaillierungsgrad der vorgeschlagenen Inhalte der Prozessbausteine,
- Integration in den Entwicklungsprozess und
- Anwendbarkeit/Übertragbarkeit des Prozesses (resultierend aus den vorigen Kriterien).

Ein übergreifendes Fazit bezüglich der vorgestellten Prozessansätze wird erst in Kapitel 3.2 gegeben, da dort die Erkenntnisse aus einer durchgeführten *Analyse zur Anwendung von Verlässlichkeitsmethoden in der Industrie* mit einfließen können. Einen Beitrag bzgl. der Historie von Verlässlichkeitsanalysen im Entwicklungsprozess wird darüber hinaus in [WR97] gegeben.

2.4.1 Fehlertolerante Systeme nach *Isermann*

Einen Prozessansatz zur Erlangung hoher Systemintegrität mechatronischer Systeme beschreibt [Ise06] mit einem Vorgehen zum Entwurf von fehlertoleranten Systemen. Einige bekannte Entwurfsmethoden für Systemzuverlässigkeit und -sicherheit (z. B. FMEA oder FTA) werden zu einem Prozess kombiniert, dessen Ziel einer hohen Systemintegrität auch durch Verwendung von Konzepten für Fehlertoleranz und Fehlerüberwachung erreicht werden soll. Der Prozess unterscheidet dabei einerseits die Entwurfs- bzw. Testphase und andererseits die Betriebsphase. Abbildung 2.16 zeigt das generelle Vorgehensschema.
Im Detail beginnt der Prozess mit der FMEA, die anhand der Systemstruktur alle Ausfälle, Fehlerursachen und Folgen identifizieren soll. Nach der Durchführung der FMEA unterscheidet der Prozess zwischen dem zuverlässigkeitsorientierten und dem sicherheitsorientierten Vorgehen. Ersteres wir durch die

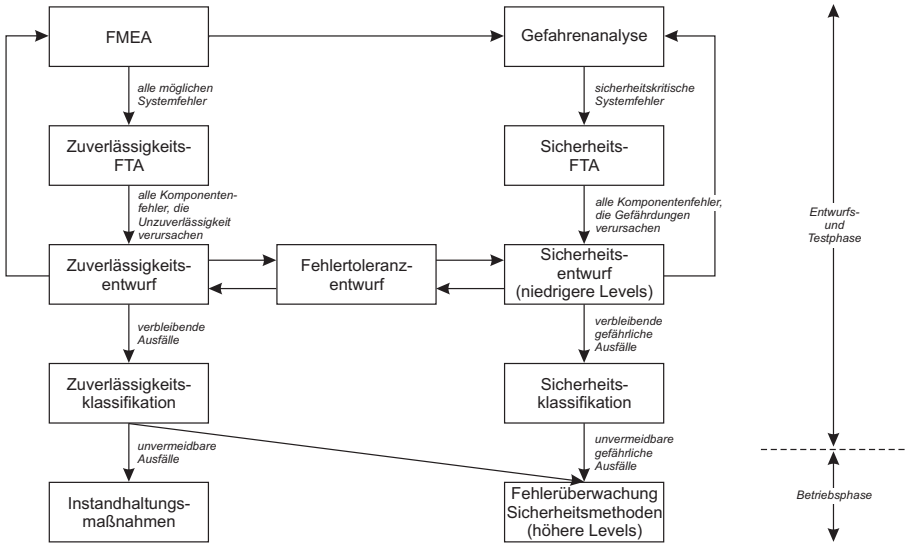


Abbildung 2.16: Integrierte Entwurfsmethoden für Systemzuverlässigkeit und -sicherheit zur Erlangung hoher Systemintegrität nach [Ise06].

linke Seite, letzteres durch die rechte Seite repräsentiert gemäß Abbildung 2.16. Beide Pfade werden parallel durchlaufen und treffen beim fehlertoleranten Systementwurf sowie beim Entwurf von fehlerüberwachenden Konzepten wieder zusammen.

Für das zuverlässigkeitsorientierte Vorgehen werden alle Fehler, die zum Systemausfall führen, durch die Zuverlässigkeits-FTA hinsichtlich logischer Abhängigkeiten analysiert. Anhand der dadurch identifizierten Ursachen bzw. den Komponentenausfällen, kann das System zuverlässigkeitsorientiert entworfen werden und wird dabei durch fehlertolerierende Konzepte unterstützt. Verbleibende Fehler werden identifiziert und anschließend klassifiziert. In der Betriebsphase werden die unvermeidbaren Fehler der Entwurfsphase dann letztendlich behoben durch Instandhaltungsmaßnahmen und durch Fehlerüberwachungskonzepte.

Das sicherheitsorientierte Vorgehen extrahiert durch den Einsatz einer Gefahrenanalyse die sicherheitskritischen Systemausfälle aus der FMEA. Diese werden dann durch die Sicherheits-FTA (reduzierter Umfang im Vergleich zur Zuverlässigkeits-FTA) hinsichtlich logischer Abhängigkeiten analysiert. Alle für Gefährdungen ursächlichen Komponentenfehler, die durch die Sicherheits-FTA identifiziert wurden, sollen möglichst durch den sicherheitsorientierten Entwurf und durch die Nutzung von fehlertolerierenden Konzepten vermieden

werden. Verbleibende Gefahren werden durch eine Risikoklassifikation bewertet und durch Fehlerüberwachung in der Betriebsphase sofort bei ihrem eintreten erkannt.
Zusammenfassend beschreibt der Verlässlichkeitsprozess für fehlertolerante Systeme nach *Isermann* ein Vorgehen, das zwischen zuverlässigkeits- und sicherheitsorientierten Analysen im Entwurf unterscheidet, beide Pfade aber wieder in den Phasen verknüpft, in denen Konzepte für Fehlertoleranz und Fehlerüberwachung eingesetzt werden sollen. Der Grund liegt darin, dass der Einsatz von diesen Konzepten sowohl die Zuverlässigkeit als auch die Sicherheit verbessern kann. Der Fokus dieses Prozessansatzes liegt auf sicherheitskritischen mechatronischen Systemen, deren Funktionalität es erlaubt, Konzepte für Fehlertoleranz und -überwachung in die Informationsverarbeitung des Systems zu integrieren. Die Beschreibung des Prozessansatzes nutzt bekannte Verlässlichkeitsmethoden, deren In- und Outputs miteinander verknüpft werden können und so zu einem durchgängigen Prozess führen. Der Prozessansatz orientiert sich relativ oberflächlich am Entwicklungsvorgehen, dafür beschreibt er aber durch die Integration von Konzepten für Fehlertoleranz und Fehlerüberwachung in einen systematischen Prozess einen neuen Aspekt zur Entwicklung verlässlicher Systeme.
Im Sinne der ausgewählten Kriterien, die einen Vergleich der verschiedenen Prozessansätze realisieren sollen, kann der Entwurfsprozess für fehlertolerante Systeme nach *Isermann* wie folgt bewertet werden: Der Prozess ist auf keine spezielle Industrie oder ein spezielles Unternehmen ausgerichtet, sodass eine Übertragbarkeit bzw. eine Anwendung auf zahlreiche Aufgabenstellungen möglich ist. Allerdings liegt der Fokus bei der Art des betrachteten Systems starr auf sicherheitskritischen mechatronischen Systemen, die fehlertolerante Eigenschaften besitzen können. Eine direkte Verknüpfung zu einem Entwicklungsprozess oder einer Entwicklungsmethodik besteht nicht, wohl aber ein relativ oberflächlicher Bezug zu den Phasen Entwurf, Test und Betrieb. Die Prozessbausteine sind festgelegt mit bekannten und etablierten Methoden. Tabelle 2.4 zeigt die Bewertungen der Kriterien noch einmal im Überblick.

2.4.2 By-Wire-Systeme im Automobil nach *Amberkar*

Ein System-Sicherheitsprozess für By-Wire-Systeme im Automobil wird in [ADM+00] vorgestellt. Anhand von typischen Elementen eines Sicherheitsprozesses wird eine Vorgehensweise vorgeschlagen, die speziell den Fokus auf By-Wire-Systeme für die Automobilindustrie legt und deren Möglichkeiten für systemintegrierte Gefahrenkontrollen verwendet. Der vorgestellte Prozess ist an die wesentlichen Phasen eines Entwicklungsprozesses gebunden und auch direkt mit ihnen verknüpft. Vor dem eigentlichen Sicherheitsprozess wird ein System-Sicherheitsplan aufgestellt, der die relevanten Aufgaben und organisa-

Kriterium	Ausprägung
Industrie-/Unternehmensfokus	Mechatronik allgemein
Systemfokus	sicherheitskritische Systeme mit fehlertoleranten Eigenschaften
Details der Prozessbausteine	festgelegt auf etablierte Methoden
Integration in den Entwicklungsprozess	oberflächlich
Anwendbarkeit/Übertragbarkeit	möglich

Tabelle 2.4: Bewertung des Prozessansatzes nach *Isermann* hinsichtlich ausgewählter Kriterien

torischen Rahmenbedingungen in diesem Kontext definiert. Im Anschluss an den Prozess wird ein umfassender Sicherheitsbericht erstellt, der u. a. die wesentlichen Ergebnisse der Gefahrenanalysen und -kontrollen enthält, ebenso wie Inhalte zum akzeptierten Restrisiko.

Der eigentliche System-Sicherheitsprozess setzt nach dem konzeptionellen Entwurf des Systems an, um darauf aufbauend, eine vorläufige Gefahrenanalyse mit dem Resultat einer Gefahrenliste zu erstellen. Die Identifikation von potenziellen Gefahren kann z. B. mittels Kreativitätstechniken erfolgen, die dann weiterführend durch Risikobewertung gemäß [MIL93] analysiert werden. Daran anschließend werden einerseits generelle Sicherheitsanforderungen definiert und andererseits Forderungen für gezielte Gefahrenkontrollen, die vom System im Betrieb durchgeführt werden. Letztere hängen jeweils direkt mit einer zuvor identifizierten Gefahr zusammen und sollen diese reduzieren oder vermeiden. Insbesondere dieser Aspekt des Prozesses berücksichtigt die Möglichkeiten von By-Wire-Systemen, die relativ einfach softwarebasierte Gefahrenkontrollen sowie Konzepte für Fehlertoleranz bzw. Redundanz im System integrieren können. Beide Anforderungstypen, generelle Sicherheitsanforderungen und Gefahrenkontrollen, werden in der klassischen Anforderungsliste des Entwicklungsprozesses berücksichtigt, der mit der nächsten Phase, dem Architektur-Entwurf, fortgesetzt wird. Die Systemarchitektur ist der Ausgangspunkt für detailliertere Gefahrenanalysen und für die daraus resultierenden Anforderungen, die wiederum in die Entwicklungsprozessphase des Detailentwurfs einfließen. Die detaillierteren Gefahrenanalysen, z. B. FTA, ETA oder FMEA, sollen ein besseres Verständnis sowohl über Zusammenhänge von Fehlern realisieren als auch über Zusammenhänge und Synergien von Gefahrenkontrollen. Letzter Prozessschritt des System-Sicherheitsprozesses ist die Verifikation der Gefahrenkontrollen, die z. B. mittels Fehlerinjektion durchgeführt werden kann. Abbildung 2.17 zeigt den System-Sicherheitsprozess, eingebettet und verbunden

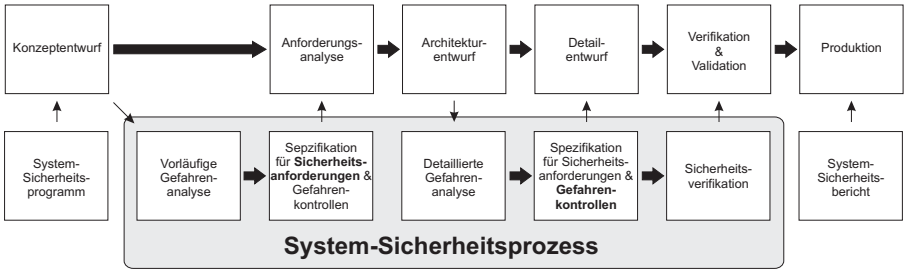


Abbildung 2.17: System-Sicherheitsprozess für By-Wire-Systeme im Automobil nach [ADM+00]

mit den Phasen des Entwicklungsprozesses.
Zusammenfassend beschreibt der Ansatz nach [ADM+00], wie der Rahmen eines Entwicklungsprozesses genutzt werden kann, um darin die typischen Standardelemente eines Sicherheitsprozesses zu integrieren. Die Standardelemente - hier: Gefahrenanalysen, Anforderungen im Kontext der Sicherheit und Verifikation - werden allerdings in ihrer Ausprägung nicht eindeutig festgelegt, sondern es gibt z. B. die Klassen der vorläufigen und der detaillierten Gefahrenanalyse, zu denen dann wiederum zahlreiche Einzelmethoden zählen. Das Vorgehen ist für By-Wire-Systeme ausgelegt, da insbesondere bei diesen Systemen, Möglichkeiten für softwarebasierte Gefahrenkontrollen vorhanden sind. Für die Bewertung hinsichtlich der für die vorliegende Arbeit wichtigen Kriterien ergibt sich, dass der Prozess für die Automobilindustrie und dort speziell für By-Wire-Systeme entwickelt wurde. Trotz dieses eigentlich sehr eingeschränkten Fokus ist eine Übertragbarkeit aber trotzdem sehr gut möglich; zumindest für mechatronische Systeme, die softwarebasierte Gefahrenkontrollen zulassen. Dadurch, dass die Prozessbausteine keine bestimmten Methoden fest vorschreiben, sind die Details der beschriebenen Prozessbausteine zwar eher gering, trotzdem sind sie durch die Verwendung von Methodenklassen und zugehörigen Beispiellisten sehr gut beschrieben. Tabelle 2.5 zeigt die Bewertung im Überblick.

2.4.3 Automobilelektronik nach *Benz*

In [Ben03] und [Ben04] wird eine Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil erläutert. Grundidee ist dabei, die in der Automobilindustrie verbreitete Entwicklungsmethodik, das V-Modell, durch ein zweites V-Modell zu erweitern. Dieses soll die Berücksichtigung von Sicherheit und Zuverlässigkeit auf eine Stufe zur Funktionalen Entwicklung gemäß dem V-Modell stellen. Dieses zweite V-Modell beinhaltet folglich die rele-

Kriterium	Ausprägung
Industrie-/Unternehmensfokus	Automobilindustrie
Systemfokus	By-Wire-Systeme
Details der Prozessbausteine	keine festen Methoden; aber dafür Methodenklassen
Integration in den Entwicklungsprozess	stark vorhanden
Anwendbarkeit/Übertragbarkeit	sehr gut möglich

Tabelle 2.5: Bewertung des Prozessansatzes nach *Amberkar* hinsichtlich ausgewählter Kriterien

vanten Entwicklungstätigkeiten im Kontext der Sicherheit und Zuverlässigkeit und stellt zahlreiche Verknüpfungen mit der klassischen Entwicklungsmethodik dar. Das resultierende Doppel-V-Modell, siehe Abbildung 2.18, gewährleistet die Durchgängigkeit der Methodik. Im Folgenden wird der Prozess anhand der einzelnen Elemente vorgestellt. Kernelemente des zweiten V-Modells sind dabei die Phasen *Funktionale Gefährdungsanalyse* und die beiden *System-Sicherheitsbewertungen*.

Die Entwicklungsmethodik nach *Benz* für sicherheitsrelevante Elektroniksysteme im Automobil startet mit der klassischen *Anforderungsanalyse*, die die allgemeinen Anforderungen für die Systementwicklung sammelt, strukturiert und definiert. Anforderungen können u. a. von Kunden, vom Entwickler selbst, aber auch aus Richtlinien und Normen resultieren. Daran anschließend erfolgt in einem iterativen Zusammenspiel der *Systementwurf*, bei dem das System funktional beschrieben wird, und die *Funktionale Gefährdungsanalyse*. Letztere ermittelt gefährliche Auswirkungen, ausgehend von Fehlerzuständen der Systemfunktionen, und bewertet sie hinsichtlich der Schwere. Anhand der Bewertung werden die Funktionen z. B. in Risikoklassen gemäß [BDM99] eingestuft. Die Ergebnisse der funktionalen Gefährdungsanalyse fließen in eine Liste, die hierarchisch der Funktionsstruktur folgend aufgebaut ist und die eine Vererbung der identifizierten Gefährdungen und Bewertungen erlaubt. Die nächste Phase, das *Designkonzept*, führt die Ergebnisse der zuvor beschriebenen Phasen zusammen: Das System ist funktional beschrieben und in Sub-Systeme bzw. Sub-Funktionen unterteilt. Zu jeder Funktion und Sub-Funktion bestehen identifizierte Gefährdungen und die zugehörigen Bewertungen im Sinne der Risikoklassen. Bei der Phase *Gliederung und Verfeinerung* werden die funktionalen Beschreibungen in einer Systemarchitektur abgebildet, und die einzelnen Systemkomponenten werden entworfen. Dazu zählen u. a. auch strukturelle Redundanzen oder redundante Kommunikationskanäle. Diese Phase wird iterativ zur nachfolgend erläuterten vorläufigen System-Sicherheitsbewertung

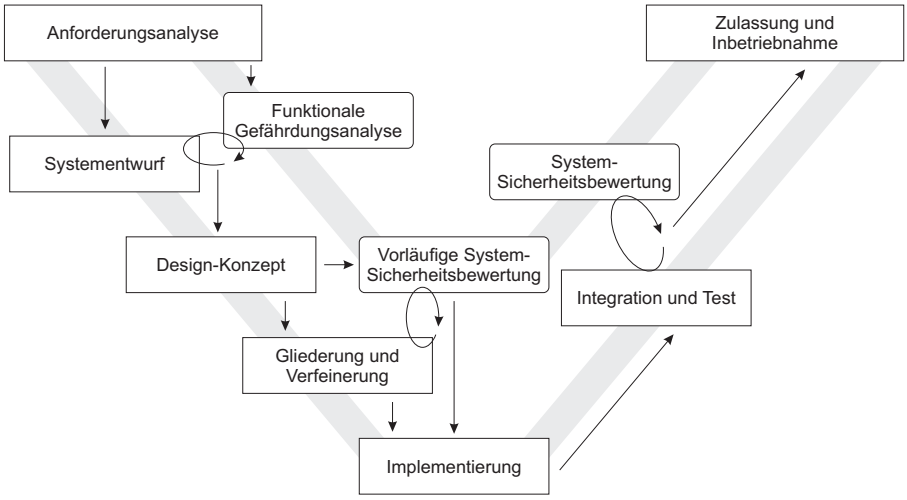


Abbildung 2.18: Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil nach [Ben03]

durchgeführt.

Bei der *Vorläufigen System-Sicherheitsbewertung* werden die jeweiligen entworfenen Architekturvarianten hinsichtlich der Sicherheit bewertet. "Vorläufig" bedeutet in diesem Zusammenhang, dass das System noch nicht physikalisch vorhanden ist, sodass zu diesem Zeitpunkt nur vorläufig bewertet werden kann. Die Bewertung der System-Sicherheit erfolgt durch Identifikation und Bewertung von Fehlern und Fehlerkombinationen der Entwurfsalternativen z. B. mittels etablierter Werkzeuge wie FTA oder FMEA. Anschließend an die beiden zuvor genannten Phasen werden die klassische *Implementierungsphase* sowie die *Integration- und Testphase* durchgeführt. Dafür wird die Hardware konstruiert, der Softwarecode erzeugt, alle Teilsysteme im Gesamtsystem integriert und alles gegen die Spezifikationen getestet.

Parallel zur Implementierungsphase erfolgt die *System-Sicherheitsbewertung*, die nun anhand eines physikalisch vorhandenen Systems durchgeführt werden kann. Die Methoden entsprechen weitestgehend dem Vorgehen bei der vorläufigen Bewertung. Zusätzlich werden für die Verifikation und Validierung noch Methoden des Testens, der Fehlerinjektion oder weitere formale Methoden vorgeschlagen. Abgeschlossen wird der Prozess mit der Phase *Zulassung und Inbetriebnahme*, die die Einhaltung der relevanten Richtlinien im Straßenverkehr überprüft. Dazu gehört bei der Zulassung eines elektronischen Brems- oder Lenksystems eine Dokumentation über das Sicherheitskonzept. Auch das

Kriterium	Ausprägung
Industrie-/Unternehmensfokus	Automobilindustrie/ bestimmter Zulieferer
Systemfokus	Elektroniksysteme/ By-Wire-Systeme
Details der Prozessbausteine	ausführlich; bestimmte Methoden werden vorgeschlagen
Integration in den Entwicklungsprozess	sehr stark vorhanden/ gleichberechtigt
Anwendbarkeit/Übertragbarkeit	möglich

Tabelle 2.6: Bewertung des Prozessansatzes nach *Benz* hinsichtlich ausgewählter Kriterien

korrekte Systemverhalten bei Fehlerinjektion darf durch die Zulassungsstelle überprüft werden.
Zusammenfassend beschreibt der Ansatz nach *Benz* eine sicherheitsorientierte Entwicklungsmethodik, die durch ein zweites, gleichberechtigtes V-Modell den Blickwinkel auf Sicherheit und Zuverlässigkeit bei der Entwicklung auf eine Stufe mit der funktionalen Sicht stellt. Insbesondere die funktionale Strukturierung und Beschreibung der Systeme wird für die Verknüpfungen verwendet. Hinsichtlich der zu bewertenden Kriterien ergibt sich, dass dieser Ansatz den Fokus sehr deutlich auf Elektroniksysteme mit der Vision By-Wire eines bestimmten Automobilzulieferers legt und sich daher auch sehr stark an dessen Entwicklungsvorgehen und den dort verwendeten Methoden orientiert. Die Prozessbausteine sind ausführlich erläutert, legen sich aber dadurch häufig auf bestimmte Methoden zur Durchführung fest. Durch die Verwendung eines Doppel-V-Modells ist der Sicherheitsprozess gleichberechtigt in den funktionalen Entwicklungsprozess integriert. Mit etwas Anpassungsaufwand ist folglich auch eine Übertragbarkeit auf andere Unternehmen oder Systemtypen möglich. Die Bewertungsergebnisse im Überblick zeigt Tabelle 2.6.

2.4.4 Luftfahrt nach *Knepper*

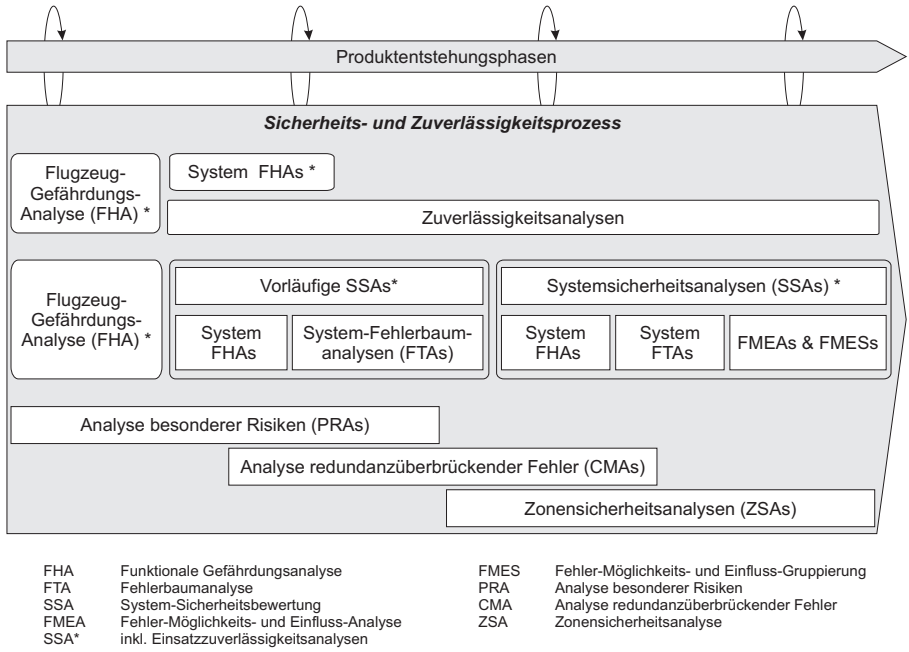
In [Kne00] wird der Sicherheits- und Zuverlässigkeitsprozess für die zivile Luftfahrtindustrie beschrieben, der befolgt werden muss, um den Anforderungen der Luftfahrtbehörden und Luftfahrtgesellschaften entsprechen zu können. Dieser Prozess basiert für Europa auf den Richtlinien der *Joint Aviation Authority*, abgekürzt JAA, und in den USA auf den Richtlinien der *Federal Aviation Association*, kurz FAA. Die Standards *SAE ARP 4754* und *SAE ARP 4754*

beschreiben dafür die umzusetzenden Inhalte bzgl. der Sicherheitsbewertung und des Systementwicklungsprozesses sowie der dazwischen bestehenden Verknüpfungen. Die Kernaufgaben des Prozesses liegen dabei in der Analyse und Optimierung von Sicherheits- und Zuverlässigkeitsaspekten sowie beim Erstellen des Sicherheitsnachweises für die Musterzulassung. Außerdem beschreibt er die engen Wechselbeziehungen zwischen dem Sicherheits- und Zuverlässigkeitsprozess sowie den Phasen der Spezifikation, Verifikation und Validierung. Der Prozess beginnt mit einer *Funktionalen Gefährdungsanalyse (FHA)*, die fokusabhängig für das Flugzeug oder auch für einzelne Flugsysteme durchgeführt wird. Dabei werden anhand der funktionalen Systembeschreibung, Gefährdungen identifiziert und das zugehörige Risiko bewertet. Darauf aufbauend werden Sicherheitsziele definiert, diese werden in die Spezifikation übernommen, und zugehörige Nachweismethoden werden festgelegt. Der Entwurfsprozess setzt sich mit dem Entwickeln von verschiedenen Architekturvarianten fort, die durch die *Vorläufige System-Sicherheitsanalyse (engl. PSSA)* bewertet werden. Außerdem werden durch diese Methode weitere Anforderungen im Kontext der Sicherheit und Zuverlässigkeit abgeleitet. Für die abschließende Verifikation wird die *System-Sicherheitsanalyse (SSA)* verwendet, die überprüft, ob das nun bereits umgesetzte System die zuvor aufgestellten Forderungen erfüllt.

Diese zuvor beschriebenen Prozessphasen werden durch weitere Sicherheits- und Zuverlässigkeitsanalysen unterstützt: Für die Modellierung von Fehlern und deren Abhängigkeiten, wird z. B. die Fehlerbaumanalyse (FTA) angewendet. Die Fehler-Möglichkeits- und Einfluss-Analyse (FMEA) dient der Identifikation von Ausfallarten und Ausfallursachen. Für die Analyse von Abhängigkeiten bzw. im Umkehrschluss für die Verifikation der Unabhängigkeit zwischen Fehlern werden die drei Methoden *Zonensicherheitsanalyse (ZSA)*, *Analyse besonderer Risiken (PRA für engl. Particular Risk Analysis)* und *Analyse redundanzüberbrückender Fehler (CMA für engl. Common Mode Analysis)* angewendet. Selbstverständlich werden auch Methoden für die Analyse von Zuverlässigkeiten der mechanischen Strukturen eingesetzt, um Versagenswahrscheinlichkeiten, auch im Hinblick auf die Risikoeinschätzung, vornehmen zu können.

Abbildung 2.19 zeigt die Prozessphasen sowie die weiteren eingesetzten Methoden im Überblick. Die Integration in die Phasen des Entwicklungsprozesses wird insbesondere durch zwei Verknüpfungstypen realisiert: einerseits aus dem zu analysierenden *Stand des Systementwurfs*, z. B. die funktionale Systembeschreibung oder das Architekturkonzept, und andererseits aus den *sicherheits- und zuverlässigkeitsbezogenen Anforderungen*, die aus den jeweiligen Analysen resultieren.

Zusammenfassend beschreibt *Knepper* einen detailliert ausgearbeiteten und umgesetzten Sicherheits- und Zuverlässigkeitsprozess für die Luftfahrtindus-



FHA	Funktionale Gefährdungsanalyse	FMES	Fehler-Möglichkeits- und Einfluss-Gruppierung
FTA	Fehlerbaumanalyse	PRA	Analyse besonderer Risiken
SSA	System-Sicherheitsbewertung	CMA	Analyse redundanzüberbrückender Fehler
FMEA	Fehler-Möglichkeits- und Einfluss-Analyse	ZSA	Zonensicherheitsanalyse
SSA*	inkl. Einsatzzuverlässigkeitsanalysen		

Abbildung 2.19: Sicherheits- und Zuverlässigkeitsprozess in der zivilen Luftfahrtindustrie nach [Kne00]

Kriterium	Ausprägung
Industrie-/Unternehmensfokus	Luftfahrtindustrie/ bestimmter Hersteller
Systemfokus	Flugzeuge/Flugsysteme
Details der Prozessbausteine	fest vorgegebene Methoden statt allgemeiner Erläuterungen
Integration in den Entwicklungsprozess	stark vorhanden
Anwendbarkeit/Übertragbarkeit	mit Aufwand möglich

Tabelle 2.7: Bewertung des Sicherheits- und Zuverlässigkeitsprozess in der Luftfahrtindustrie nach *Knepper* hinsichtlich ausgewählter Kriterien

trie. Der Prozess erfüllt die Forderungen von Luftfahrtbehörden und Luftfahrtgesellschaften durch Anwendung und Verknüpfung von fest vorgegebenen Methoden. Besondere Aufmerksamkeit wird dabei darauf gelegt, dass die Ergebnisse der verschiedenen Sicherheits- und Zuverlässigkeitsanalysen als Anforderungen in den Entwicklungsprozess zurück fließen und dort für die notwendige Verifikation und Validierung genutzt werden.
Bezüglich der zu bewertenden Kriterien ergibt sich, dass dieser Prozess den Fokus auf die Flugzeugindustrie und evtl. darin auf ein spezielles Unternehmen legt. Die Prozessbausteine werden nicht allgemeingültig erläutert, sondern werden durch fest vorgegebene Methoden repräsentiert. Die Integration in den Entwicklungsprozess ist ausführlich erläutert. Eine Übertragbarkeit des Prozesses ist möglich, bedarf aber eines größeren Aufwands, da der *Weg vom Speziellen zum Allgemeinen und wieder zum Speziellen* gegangen werden muss. Die Bewertungsergebnisse im Überblick zeigt Tabelle 2.7.

2.4.5 Verlässlichkeitsframework nach *Kochs*

In [KP04] und [LGPK05] wird ein Ansatz vorgestellt, der mittels eines wieder kehrenden Frameworks, Wissen über Verlässlichkeit modellbasiert in die Entwicklungsmethodik für mechatronische Systeme (vgl. Kapitel 2.2) integriert. Dies wird durch so genanntes *Verlässlichkeitstracking* realisiert, das von der Spezifikation bis zum Projektabschluss ständig die Eigenschaften im Kontext der Verlässlichkeit analysiert und das Verlässlichkeitsmodell schrittweise erweitert. Kernelement ist dabei das *Verlässlichkeitsframework*, das über den gesamten Entwicklungsverlauf ständig aktualisiert und angepasst wird. Abbildung 2.20 soll diese Vorgehensweise verdeutlichen, die den Baustein des Frameworks immer wieder durchläuft, ausgerichtet an den Phasen des Ent-

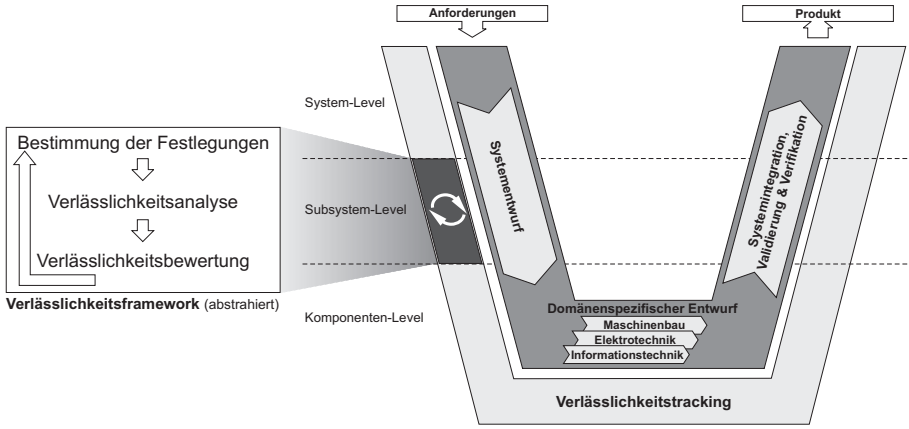


Abbildung 2.20: Modellbasierte Integration von Verlässlichkeitswissen mittels eines Frameworks in die Entwicklungsmethodik der Mechatronik nach [KP04] und [LGPK05]

wicklungsprozesses.
Der Ablauf innerhalb des Frameworks kann untergliedert werden in die Phasen *Bestimmung der Festlegungen*, *Verlässlichkeitsanalyse* und *Verlässlichkeitsbewertung*. Bei der ersten Phase werden Betrachtungseinheit, Betrachtungszeitraum und Anforderungen im Kontext der Verlässlichkeit mit zugehörigen Kriterien und Akzeptanzwerten festgelegt. Die Phase der eigentlichen Verlässlichkeitsanalyse identifiziert Einflusskriterien auf die zuvor bestimmten Festlegungen und modelliert bzw. berechnet einzelne Aspekte. Durch die abschließende Bewertungsphase können dann Entscheidungen zwischen Entwurfsalternativen getroffen werden oder sie können auch zu Veränderungen im Sinne von Iterationsschritten bzgl. der Festlegungen, z. B. der Akzeptanzwerte, führen. Abbildung 2.20 zeigt die Phasen des Verlässlichkeitsframeworks.
In [LGPK05] wird ein Beispiel zur Modellierung des Wissens und der Unsicherheit über eine Ausfallrate eines mechatronischen Systems gegeben, das die Nutzung des Frameworks verdeutlichen soll. Schrittweise wird dort das Wissen bzgl. der Ausfallrate erweitert und die Unsicherheit, diese Informationen betreffend, reduziert. Ausgangspunkt jedes zu durchlaufenden Frameworks ist die *Festlegung* der Ausfallrate als Akzeptanzkriterium. Die Phase *Verlässlichkeitsanalyse* erweitert dann das Wissen bzgl. der Ausfallrate; z. B. durch Expertenwissen, durch den fortgeschrittenen Entwicklungsstand des Systems oder auch durch Anwendung von FMEAs oder Testverfahren. Anhand dieses erweiterten Wissens und der reduzierten Unsicherheiten kann dann die Verlässlichkeit bewertet werden, und es können Entwurfsentscheidungen, z. B. über angedachte

Kriterium	Ausprägung
Industrie-/Unternehmensfokus	Mechatronik
*System*fokus	Fokus liegt auf Modellierung des Wissens über Verlässlichkeit
Details der Prozessbausteine	ein wieder kehrender Baustein
Integration in den Entwicklungsprozess	stark vorhanden
Anwendbarkeit/Übertragbarkeit	sehr gut möglich

Tabelle 2.8: Bewertung des Framework-Ansatzes der modellbasierten Berücksichtigung von Wissen über Verässlichkeit nach *Kochs* hinsichtlich ausgewählter Kriterien

Redundanzstrukturen, getroffen werden.
Zusammenfassend beschreibt der Ansatz nach *Kochs* einerseits eine Möglichkeit, Wissen und zugehörige Unsicherheiten über Verlässlichkeitsaspekte bei der Entwicklung zu modellieren und zu berücksichtigen. Andererseits wird ein schrittweise zu durchlaufender Vorgehensbaustein erläutert, das Verlässlichkeitsframework, um entlang der Phasen der Entwicklungsmethodik für mechatronische Systeme, dem V-Modell, wachsendes Wissen über Verlässlichkeit zu entwickeln und für Entwurfsentscheidungen einzusetzen.
Hinsichtlich der zu bewertenden Kriterien lässt sich dieser Ansatz relativ schwer vergleichen, da der Industriefokus zwar allgemein auf der Mechatronik liegt, der Systemfokus aber eher nicht direkt bewertbar ist. Die Begründung dafür liegt darin, dass bei diesem Ansatz die Modellierung von Wissen über Verlässlichkeit im Vordergrund steht und weniger die Vorgehensweise, wie das Wissen entsteht. Letzteres wird *lediglich* durch die Erläuterungen zum wieder kehrenden Prozessbaustein erfüllt. Demgegenüber ist aber die Integration in einen Entwicklungsprozess durch Anwendung der VDI-Richtline sehr stark vorhanden. Eine Anwendbarkeit des Ansatzes ist durch den allgemeinen Blickwinkel auf mechatronische Systeme zwar sehr gut möglich, betrifft aber größtenteils nur die Modellierung des Wissens.

2.5 Zusammenfassung

Den Stand der Technik zusammenfassend, wurde in diesem Kapitel auf vier grundlegende Bereiche detailliert eingegangen, die einerseits zum Verständnis der weiteren Ausführungen notwendig sind und andererseits den aktuellen Stand der Technik darstellen, der im Kontext einer verlässlichkeitsorientierten Entwicklungsmethodik besteht:

- Verlässlichkeitsgrundlagen
- Entwicklungsmethodik der Mechatronik
- Verlässlichkeitsmethoden
- Ansätze für Verlässlichkeitsprozesse

In den *Verlässlichkeitsgrundlagen* wurde die Terminologie der Verlässlichkeit als Oberbegriff für Verfügbarkeit, Sicherheit, Zuverlässigkeit und Vertraulichkeit diskutiert und deren Verwendung innerhalb der vorliegenden Arbeit erläutert. Darüber hinaus wurden Unterschiede bei der Ausprägung eines Fehlers im Sinne der Fehlerpropagierung (Fehlerursache, Fehlerzustand, Ausfall und Konsequenz) dargestellt.
Die *Entwicklungsmethodik der Mechatronik* wird im Rahmen dieser Arbeit als systematische Basis benutzt, um Aspekte der Verlässlichkeit in den Entwicklungsprozess zu integrieren. Daher wurde neben dem Prozessablauf und den Inhalten der Prozessbausteine auch deren Notation erläutert.
Die Berücksichtigung von Verlässlichkeitsaspekten erfolgt klassischer Weise durch die Anwendung von *Verlässlichkeitsmethoden*. Daher wurde eine Auswahl typischer Methoden vorgestellt, die repräsentativ für die Methodenklassen Fehler- Gefahren- und Risikoanalyse stehen können. Die Gliederung der Methodenklassen, auf die im späteren Kapitel wieder Bezug genommen wird, stellt dabei bereits einen ersten Beitrag dieser Arbeit zum Forschungsfeld von verlässlichkeitsorientierten Entwicklungstätigkeiten dar.
Bestehende relevante Ansätze für die Berücksichtigung von Verlässlichkeitaspekten in der Entwicklung durch *Verlässlichkeitsprozesse* wurden ebenfalls erläutert und bereits initial bewertet. Eine detaillierte Auswertung dazu folgt in Kapitel 3.2. Dargestellt wurden Ansätze nach *Isermann*, *Amberkar*, *Benz*, *Knepper* und *Kochs*, die jeweils verschiedene Industrien oder Systeme betrachtet haben. Eine Übersicht weiterer Ansätze oder Bestandteile für Verlässlichkeitsprozesse, deren Relevanz für die vorliegende Arbeit eher geringer einzuordnen ist, wird in [Ben04] beschrieben.

3 Analyse zur Berücksichtigung von Verlässlichkeitsaspekten

Neben der Aufarbeitung zum Stand der Technik, wird das Verständnis der im Entwicklungsprozess ablaufenden Tätigkeiten und Effekte mit Bezug zur Verlässlichkeit durch Resultate einer eigenen Industrie-Studie [MM06] erweitert. Diese Studie wurde im Rahmen der vorliegenden Arbeit initiiert und durchgeführt: Die im Sinne der deskriptiven Studie 1 durchgeführte Industrie-Befragung soll einerseits die derzeitige Nutzung von Verlässlichkeitsmethoden und -prozessen darstellen und andererseits bestehende Defizite und zukünftigen Bedarf identifizieren. Das Kapitel endet mit einer gemeinsamen Auswertung zum Stand der Technik und zur Industrie-Studie sowie der Definition der Forschungshypothesen dieser Arbeit. Diese basieren folglich sowohl auf den Erkenntnissen, die aus dem Stand der Technik resultieren, als auch auf dem erweiterten Verständnis zur Entwicklung verlässlicher mechatronischer Systeme, das durch die im Folgenden beschriebene Studie entwickelt wurde.

3.1 Industrie-Studie

In Kapitel 1 wurde bereits die Herausforderung erläutert, dass mechatronische Systeme zwar einerseits eine bemerkenswerte Funktionalität ermöglichen, andererseits allerdings auch besondere Anforderungen an die Verlässlichkeit stellen. Industrieunternehmen können auf diese Entwicklung durchaus unterschiedlich reagieren. Die Bandbreite beginnt bei keiner Reaktion bzw. Abwarten und führt über die Einführung vereinzelter Methoden bis hin zu durchgängigen Sicherheitsprozessen, die in bestehende Entwicklungsmethodiken integriert werden. Um diese Reaktionen besser zu verstehen, die Bandbreite und die Einsatzhäufigkeit exakter kennen zu lernen und sie analysieren zu können, wurde die Studie zur Analyse von Verlässlichkeitsmethoden und -prozessen in Unternehmen der Mechatronik-Industrie durchgeführt. Bevor die Ergebnisse der Studie vorgestellt und analysiert werden, wird kurz auf den organisatorischen Rahmen eingegangen.
Eine ähnliche Studie zum zuvor beschriebenen Thema wurde bereits vor einigen Jahren von *Rzepka* durchgeführt und veröffentlicht in [RSB02]. Da einerseits Unsicherheit darüber besteht, ob diese Studie noch den aktuellen Stand

widerspiegelt und andererseits einige weitere Aspekte dort nicht im Fokus stehen, z. B. die Prozessintegration von Methoden, wurde entschieden, eine eigene Analyse durchzuführen. Die Ergebnisse nach [RSB02] werden im Unterkapitel *Zusammenfassende Ergebnisse* kurz diskutiert und haben somit ebenfalls Einfluss auf die vorliegende Arbeit.

3.1.1 Organisatorischer Rahmen der Studie

Im Folgenden werden die Rahmenbedingungen erläutert, unter denen die Studie durchgeführt wurde. Dazu wird sowohl auf die Auswahl der Unternehmen als auch auf die Entscheidung für eine geeignete Befragungsmethodik eingegangen.
Die Studie wurde mit Unternehmen und Instituten durchgeführt, die Mitglieder in einem der beiden nachfolgend beschriebenen Mechatronik-Arbeitskreise sind:

Fachausschuss 4.15 Mechatronik: Der Ausschuss ist Teil der VDI/VDE-Gesellschaft für Mess- und Automatisierungstechnik (GMA). Seine Mitglieder setzen sich sowohl aus Industrieunternehmen als auch aus Forschungsinstituten zusammen. Zielsetzung des Ausschusses ist die Bündelung übergreifender Fragestellungen der Mechatronik und die Ergänzung der Aktivitäten der GMA. Der Fachausschuss ist sowohl Teil des Verbands Deutscher Ingenieure (VDI) als auch des Verbands der Elektrotechnik, Elektronik und Informationstechnik (VDE).

Innovationsnetzwerk OWL Maschinenbau: Das Netzwerk bündelt Interessen von 272 Unternehmen und Instituten der Region Ostwestfalen-Lippe. Die wichtigsten Ziele ihrer Arbeit liegen in der Stärkung der wirtschaftlichen und technologischen Leistungskraft des regionalen mittelständischen Maschinenbaus, der Entwicklung von Standortvorteilen für die Unternehmen im globalen Wettbewerb und der Bestandssicherung von Unternehmen zur Stabilisierung des Arbeitsmarktes. Innerhalb des Innovationsnetzwerks OWL Maschinenbau gibt es wiederum verschiedene, themenbezogene Arbeitskreise.

Für die Studie wurden innerhalb dieser Arbeitskreise Online-Fragebögen via E-Mail verschickt. Gründe für die Auswahl der Befragungsmethodik *Online-Fragebogen* liegen in den geringen Kosten, der hohen Anzahl an Empfängern sowie der Möglichkeit, in relativ kurzer Zeit eine hohe Anzahl an Antworten zu erhalten [TDS03] [Lüt04]. Der über das Internet zur Verfügung gestellte Fragebogen ist im Anhang A hinterlegt, zusammen mit einem Screenshot des Begleittextes zur Befragung.

3.1.2 Ergebnisse der Industrie-Studie

Im Folgenden werden die wichtigsten Ergebnisse der Studie vorgestellt, aus der insgesamt 21 Antworten resultierten; 17 davon kamen von Unternehmen und 4 von Forschungsinstituten. In der Auswertung wird auf die Unterscheidung von Unternehmen und Instituten aufgrund einer besseren Lesbarkeit verzichtet. Den teilnehmenden Unternehmen wurde bei der Befragung Anonymität zugesichert, da sonst eventuell Ergebnisse ungewollt an die Öffentlichkeit gelangen könnten. Daher kann an dieser Stelle nicht detailliert auf die Teilnehmer eingegangen werden. Trotzdem kann angegeben werden, dass sich die teilnehmenden Unternehmen im Zielfokus der Studie, der *Mechatronik-Industrie*, befinden. Vertretene Branchen waren u. a. der Sondermaschinenbau, die Elektronikindustrie und die Automobilindustrie. Da sich neben Unternehmen auch Institute an der Studie beteiligt haben, befinden sich die Objekte für eventuelle Verlässlichkeitsanalysen sowohl in der Forschungs- und Entwicklungsphase als auch in der Produktionsphase. Im Folgenden werden die wichtigsten Ergebnisse der Studie vorgestellt. Sie werden unterteilt in Ergebnisse, die die aktuelle Situation beschreiben und Ergebnisse, die den zukünftigen Bedarf betreffen. Das komplette Datenmaterial der Studie inklusive aller Fragen und Antwortstatistiken ist im Anhang A hinterlegt.

Ergebnisse zur aktuellen Situation

Die wichtigsten Ergebnisse bezüglich der aktuellen Anwendung von verlässlichkeitsorientierten Methoden beim Entwurf mechatronischer Systeme können in drei Bereiche unterteilt werden:

- *Methodenarten*, die zum Einsatz kommen
- *Anwendungszeitpunkt* der Methoden im Entwicklungsprozess
- *Einsatzcharakter und -gründe* für den Methodeneinsatz

Die Frage nach der Art der eingesetzten Methoden, beantworteten 19 Unternehmen. Die detaillierten Ergebnisse sind in Tabelle 3.1 angegeben. Da die Unternehmen teilweise mehrere Methoden anwenden, waren auch mehrfache Antworten möglich. 100% entsprechen der Anzahl von 19 Antworten.
Besonders häufigen Einsatz erfahren die Methoden *FMEA*, *Checkliste* und *Gefahrenanalyse*. Dahinter folgen die Methoden *Funktionale Gefährdungsanalyse* und *Fehlerbaumanalyse*. Gar nicht genannt, und daher auch nicht in der Tabelle aufgeführt, wurden die *Ereignisbaumanalyse*, *HAZOP (Hazard and Operability Study)*, *Markoff-Simulation* sowie die *Weibull-Analyse*. Neben dem Ergebnis, dass die in der Studie am häufigsten genannten Methoden auch die am meisten Verbreiteten sind, läßt das Resultat eine weitere Interpretation zu: Die am

Methode	Anwendende Unternehmen [Antworten]	Prozentsatz [%]
FMEA	13	68
Vorläufige Sicherheitsanalyse Funktionale	1	5
Gefährdungsanalyse	7	37
Gefahrenanalyse	8	42
Fehlerbaumanalyse	6	32
Software Deviation Analysis	1	5
Monte Carlo Simulation	1	5
Checkliste	13	68

Tabelle 3.1: Arten von Verlässlichkeitsmethoden, die in Unternehmen angewendet werden

häufigsten verwendeten Methoden spiegeln zugleich auch die Methoden wider, die sehr allgemeingültig sind und somit ein breites Anwendungsfeld finden. *FMEA*, *Gefahrenanalyse* und *Checkliste* lassen sich für verschiedene Projekte, Produkte und Prozesse anwenden oder zumindest anpassen. Sie könnten daher repräsentativ für Methodenklassen sein.

Auf die Frage nach den hauptsächlichen Anwendungszeitpunkten von Verlässlichkeitsmethoden im Entwicklungsprozess antworteten alle 19 Unternehmen, dass sie die Methoden *in der Konzipierungsphase* und/oder *beim eigentlich fertigen Produkt* einsetzen. Die weiteren Antwortmöglichkeiten, *Bereits bei der Klärung von Anforderungen* und *Sobald Teillösungen bestehen*, wurden demnach nur in Verbindung mit den beiden zuvor genannten Antworten angegeben, sodass festgestellt werden kann, dass diese Möglichkeiten eine Erweiterung des standardisierten Vorgehens darstellen. Einen Einsatz von Sicherheitsmethoden *Bereits bei der Klärung von Anforderungen* realisieren sogar nur drei Unternehmen, sodass diese Vorgehensweise eher der Ausnahme entspricht. Tabelle 3.2 zeigt die Verteilung der Antworten. Bei einer weiteren Frage in diesem Kontext gaben drei Unternehmen an, dass sie einen durchgängigen Sicherheitsprozess befolgen. Nur bei einem dieser Unternehmen startete dieser bereits bei den Anforderungen.

Die weiteren wichtigen Ergebnisse bezüglich der aktuellen Anwendung von verlässlichkeitsorientierten Methoden beim Entwurf mechatronischer Systeme beziehen sich auf den Einsatzcharakter sowie auf die dahinterliegenden Gründe der Anwendung. Dabei sind insbesondere der Nutzen als *Nachweis- und Dokumentationsinstrument* sowie die *systematische Vorgehensweise* bei der Durchführung von Verlässlichkeitsanalysen von sehr hoher Bedeutung. Erstge-

Einsatzzeitpunkt	Anwendende Unternehmen [Antworten]	Prozentsatz [%]
Bereits bei der Klärung von Anforderungen	3	17
Während der Konzipierungsphase	9	50
Sobald Teillösungen bestehen	6	33
Das eigentlich fertige Produkt wird einer Analyse unterzogen	11	61

Tabelle 3.2: Einsatzzeitpunkte von Verlässlichkeitsmethoden im Entwicklungsprozess

nannten Nutzen bestätigten über 75%, während den Zweitgenannten immerhin mehr als 50% auswählten. Die ursprüngliche Idee von Verlässlichkeitsanalysen, das System durch Identifikation und Bewertung von Schwachstellen zu optimieren, wurde lediglich von einem Drittel der Unternehmen als größerer Nutzen genannt.
Die Motivation für den Einsatz von Verlässlichkeitsmethoden, die dem Nutzen vorgelagert ist, verteilte sich relativ gleich auf die zur Auswahl stehenden Optionen *Kundenforderungen*, *Gesetzliche Forderungen* und *Eigeninitiative*.
Weitere Ergebnisse des Einsatzcharakters von Verlässlichkeitsanalysen beziehen sich auf

- die durchschnittliche Einsatzhäufigkeit, die relativ ausgegelichen zwischen dem einmaligen Einsatz und einem entwicklungsbegleitenden Einsatz liegt,
- die überwiegende Verwendung von Analyseergebnissen zur Dokumentation und Archivierung, die kaum die Nutzung von Ergebnissen für den Input weiterer Analysen betrifft (keine Vererbung von Ergebnissen oder ausgeprägte Prozessgedanken) und
- den Fokus der Verlässlichkeitsanalysen, der bei den meisten Unternehmen auf dem Gesamtsystem liegt; eine Perspektive, die auf die Softwarekomponente zielte, war die Ausnahme.

Ergebnisse zur zukünftigen Situation

Nachdem bisher die Ergebnisse der aktuellen Situation dargestellt wurden, werden nun die wichtigsten Ergebnisse bezüglich der zukünftigen Anwendung von

Prognose bzgl. der Methodenanwendung	Unternehmen [Antworten]	Prozentsatz [%]
Steigend	16	76
Sinkend	0	0
Gleich bleibend	5	24

Tabelle 3.3: Erwartungen über die zukünftige Nutzung von Verlässlichkeitsmethoden

verlässlichkeitsorientierten Methoden beim Entwurf mechatronischer Systeme vorgestellt. Sie können ebenfalls in drei Bereiche unterteilt werden:

- *Generelle Prognose* der zukünftigen Anwendung von Verlässlichkeitsmethoden
- *Defizite* aktueller Methoden
- *Spezieller Forschungs- und Entwicklungsbedarf* im Bereich der Verlässlichkeit

Auf die Frage nach der zukünftigen Anwendung von Analysemethoden prognostizierte der Großteil der Unternehmen eine steigende Nutzung, während ein kleinerer Teil eine gleich bleibende Nutzung erwartete. Die Prognose einer sinkenden Anwendung wurde nicht genannt. Tabelle 3.3 zeigt die Verteilung auf die drei Kategorien einer steigenden, sinkenden und gleich bleibenden zukünftigen Nutzung. Neben der Einordung in diese drei Kategorien wurde darüber hinaus auch nach den dahinterliegenden Gründen gefragt. Bei den gegebenen Antworten (komplette Übersicht im Anhang A) traten besonders die folgenden beiden Gründe im- und explizit hervor:

- Steigende Komplexität und *Mechatronisierung* der Systeme
- Erhöhte Sicherheitsforderungen durch Gesetze und Kunden

Ergebnisse auf die Frage nach Defiziten bestehender Methoden verteilten sich gemäß Tabelle 3.4. Insbesondere die Defizite *Abhängigkeit von Fachwissen* und *hoher Aufwand bzw. hohe Kosten bei der Anwendung* wurden sehr häufig ausgewählt. Darüber hinaus wurden auch die Akzeptanzprobleme als verbreitetes Defizit identifiziert.
Neben dem aus den Defiziten abzuleitenden Handlungsbedarf, der Verbesserung der Methoden bzw. des Einsatzes der Methoden, wurde in einer abschließenden offenen Fragestellung der Studie spezieller Forschungs- und Entwicklungsbedarf ermittelt. Die vollständige Übersicht der Antworten ist ebenfalls in

Defizite	Unternehmen [Antworten]	Prozentsatz [%]
Mehrwert der Methoden nur gering	4	20
Sehr starke Abhängigkeit von Fachwissen	13	65
Geringe Akzeptanz der Methoden bei Mitarbeitern	6	30
Hoher Aufwand bzw. hohe Kosten	12	60

Tabelle 3.4: Defizite bestehender Methoden

Anhang A hinterlegt. Drei Aspekte können aus der Vielzahl von Einzelantworten herausgehoben werden, die einen besonders dringenden Forschungs- und Entwicklungsbedarf darstellen:

- Integration von Sicherheitsmethoden
- Vereinfachung von Sicherheitsmethoden
- Bereitstellung von Datenmaterial

Zusammenfassende Ergebnisse

Zusammenfassend vermittelt die Industrie-Studie somit sowohl ein Verständnis bezüglich der aktuellen Situation zur Nutzung von Verlässlichkeitsmethoden und -prozessen als auch eine Prognose zukünftiger Entwicklungen und Bedürfnisse in diesem Bereich. Die wichtigsten Ergebnisse sind im Folgenden noch einmal kurz dargestellt:

- FMEA, Checklisten und Gefahrenanalysen sind die am meisten verbreiteten Verlässlichkeitsmethoden.
- Verlässlichkeitsmethoden werden kaum entwicklungsbegleitend oder innerhalb eines definierten Prozesses eingesetzt, sondern dienen größtenteils als Nachweisinstrument.
- Der typische Einsatzzeitpunkt liegt in der Konzipierungsphase oder beim eigentlich fertig entwickelten Produkt.
- Fehlendes Fachwissen, hohe Kosten und Akzeptanzprobleme sind Defizite bestehender Methoden.
- Es wird eine steigende Nutzung von Verlässlichkeitsmethoden prognostiziert, die in komplexer werdenden Systemen, sowie in erhöhten Sicherheitsforderungen von Gesetzen und Kunden begründet liegt.

- Besonders dringender Forschungs- und Entwicklungsbedarf besteht bei der Integration und Vereinfachung von Verlässlichkeitsmethoden sowie bei der Beschaffung von Datenmaterial.

Aus der anfangs angesprochenen vergleichbaren Studie gemäß [RSB02] resultierten sehr ähnliche Erkenntnisse: Die Umfrage, die den Einsatz von qualitativen und quantitativen Zuverlässigkeitsmethoden in der Industrie untersucht hat, kam ebenfalls zu den Ergebnissen, dass FMEA und Checklisten die verbreitetsten Methoden sind und der Einsatz eher selten bereits in der Planungsphase stattfindet. Die häufigste Anwendungsphase für Zuverlässigkeitsmethoden findet während der eigentlichen Entwicklung und Ausarbeitung statt. Damit decken und bestätigen sich die Ergebnisse der beiden Studien in wesentlichen Aspekten. Wesentliche Widersprüche sind hingegen nicht vorhanden.

3.2 Fazit zum Stand der Technik und zur Industrie-Studie

In den vorangegangenen Kapiteln 2 und 3.1 wurde gemäß der deskriptiven Studie 1 das Verständnis zur verlässlichkeitsorientierten Entwicklung mechatronischer Systeme aufgebaut und erweitert. In diesem Abschnitt werden daraus Schlussfolgerungen gezogen, die die Basis für die normative Studie darstellen sollen, um die Entwicklungstätigkeiten in diesem Kontext verbessern zu können. Fazit und Bewertung wird dabei für jedes der angesprochenen Kapitel erst getrennt betrachtet, bevor dann abschließend das Ergebnis der deskriptiven Studie 1 im Sinne von Forschungshypothesen bzw. Forschungsfragen hergeleitet wird.

3.2.1 Fazit und Bewertung zum Stand der Technik

Der Stand der Technik beschreibt neben den grundlegenden Begriffserläuterungen die Aspekte *Entwicklungsmethodik der Mechatronik*, *Verlässlichkeitsmethoden* und *Ansätze für Verlässlichkeitsprozesse*. Diese werden nachfolgend im Kontext der weiteren Verwendung innerhalb der vorliegenden Arbeit bewertet.

Die *Entwicklungsmethodik der Mechatronik* bietet einen systematischen Entwicklungsleitfaden, der durch seinen generischen Ansatz für viele Entwicklungsaufgaben anwendbar oder zumindest übertragbar ist. Der Prozess beschreibt einen idealtypischen Ablauf als Makroprozess in V-Gestalt sowie die zugehörigen Prozessbausteine als wiederkehrende Prozessphasen. Sowohl die inhaltlichen Aspekte der Entwicklungsmethodik als auch ihr Aufbau und die

Beschreibung der Prozessbausteine lassen sich gut dazu verwenden, Verlässlichkeitsaspekte für die Entwicklung darin zu integrieren und den Beschreibungsstil zu übernehmen. Daher wird die Entwicklungsmethodik der Mechatronik in der vorliegenden Arbeit als Rahmenkonzept verstanden, das einen systematischen Blickwinkel auf die Entwicklungsphasen realisiert und das eine übertragbare Notation zur Beschreibung bereitstellt. Außerdem können Resultate aus den verschiedenen Prozessbausteinen für die Verknüpfungen zwischen dem Verlässlichkeits- und Entwicklungsprozess verwendet werden.
In Kapitel 2.3 wurden ausgewählte *Verlässlichkeitsmethoden* erläutert, die repräsentativ für die Methodenklassen Fehler-, Gefahren- und Risikoanalysen stehen können. Belegt durch die Ergebnisse der Industrie-Studie sind dabei insbesondere die Methoden *FMEA* und *Checkliste* allgemein anwendbar und relativ verbreitet. Durch Rückführung auf die ursprünglichen Anwendungsideen der Methoden konnte die Zuordnung der Methodenklassen eingeführt werden, auf die auch im weiteren Verlauf dieser Arbeit Bezug genommen werden wird. Die Einführung der Methodenklassen erlauben eine klare Beschreibung der durchzuführenden Aktivität innerhalb eines Prozessschrittes, ohne dass dadurch direkt eine spezielle Methode vorgeschrieben wird. Die Auswahl der Methode kann somit bedarfsgerecht erfolgen und der Prozess bleibt für verschiedene Entwicklungsaufgaben anwendbar.
Die verschiedenen *Ansätze für Verlässlichkeitsprozesse* nach *Isermann*, *Amberkar*, *Benz*, *Knepper* und *Kochs* wurden in Kapitel 2.4 erläutert und anhand ausgewählter Kriterien bewertet. Im Folgenden sollen die Ansätze hinsichtlich der Verwendung in der vorliegenden Arbeit analysiert werden:

- Der Ansatz nach *Isermann* beschreibt das Vorgehen zur Entwicklung fehlertoleranter Systeme. Auch wenn die Prozessbeschreibung trotz Anwendung fest definierte Methoden relativ oberflächlich bleibt, so beinhaltet dieser Ansatz einen großen Mehrwert: Er realisiert die Integration von Konzepten zur Fehlerüberwachung und Fehlertoleranz in die Entwicklungstätigkeiten.

- *Amberkar* beschreibt das Vorgehen für einen System-Sicherheitsprozess für By-Wire-Systeme im Automobil. Der Fokus liegt dabei auf Systemen, die softwarebasierte Gefahrenkontrollen ermöglichen. Ein im Rahmen der vorliegenden Arbeit weiter zu verfolgender Ansatz liegt darin, dass den Prozessphasen keine festen Methoden zugewiesen sind, sondern dass diese bedarfsgerecht ausgewählt werden können.

- Die Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme gemäß *Benz* beschreibt einen Ansatz, der speziell für einen Automobilzulieferer entwickelt wurde. Interessant daran ist u. a. die Verwendung der

Entwicklungsmethodik als Rahmenkonzept sowie der daraus resultierenden Grundidee des Doppel-V-Modells.

- Der Sicherheits- und Zuverlässgkeitsprozess nach *Knepper* beschreibt sehr detailliert das Vorgehen in der Luftfahrtindustrie sowie die Einbettung in den dort verwendeten Entwicklungsprozess. Interessant ist dabei u. a. die Realisierung der Verknüpfungen mittels Anforderungen. Die Prozessphasen werden allerdings ausschließlich durch fest definierte Methoden erläutert.

- *Kochs* hat ein Verlässlichkeitsframework entwickelt, das z. B. für die Modellierung von in der Entwicklung anwachsendem Wissen über Verlässlichkeit genutzt werden kann. Hauptmehrwert in Hinblick auf die vorliegende Arbeit ist aber die Verwendung der Entwicklungsmethodik gemäß der VDI-Richtlinie 2206 als Rahmenkonzept.

3.2.2 Fazit und Bewertung zur Industrie-Studie

Die Ergebnisse der Industrie-Studie werden nachfolgend übergreifend analysiert, um Forschungsbedarf daraus ableiten zu können. Dazu werden Resultate des aktuellen Vorgehens in der Industrie zusammenhängend mit den Prognosen und dem ermittelten zukünftigen Bedarf interpretiert. Eine sehr allgemeine Schlussfolgerung, die einerseits aus der Prognose einer steigenden Nutzung von Verlässlichkeitsmethoden und andererseits aus den identifizierten Defiziten resultiert, ist die Aussage, dass überhaupt *Forschungsbedarf im Kontext der verlässlichkeitsorientierten Entwicklung* besteht.
Die weiterführende Frage "Worin dieser Forschungsbedarf besteht?", soll durch einen Vergleich beantwortet werden. Dazu werden das durchschnittlich ermittelte Nutzungsprofil für Verlässlichkeitsmethoden und das ideale Vorgehen (ohne dabei die Effizienz zu betrachten) gegenüber gestellt:

- Das *Durchschnitts-Unternehmen* würde einzelne Verlässlichkeitsmethoden in der Konzipierungsphase und beim eigentlich fertig entwickelten Endprodukt anwenden. Die Gründe dafür würden in der Dokumentation und in einem strukturierten Vorgehen liegen, um die Daten für Nachweise und Neuentwicklungen verwenden zu können.

- Demgegenüber würde das *ideale Unternehmen* jeweils den größtmöglichen Aufwand bei der Nutzung von Verlässlichkeitsmethoden realisieren: Ein durchgängiger Verlässlichkeitsprozess würde entwicklungsbegleitend Anwendung finden und aus untereinander verknüpften Verlässlichkeitsmethoden bestehen. Neben der Dokumentation, dem Nachweis und der

strukturierten Vorgehensweise würde der Mehrwert der Methoden insbesondere im Identifizieren und Optimieren von Schwachstellen bestehen. Fachwissen bzgl. bereits gelöster Probleme würde in wiederverwendbarer Form abgelegt werden. Auch eine höhere Akzeptanz bzgl. der Anwendung der Methoden wäre ein weiterer Bestandteil dieses idealen Profils, ebenso wie das Vorhandensein umfangreichen Datenmaterials.

Aus diesem Profilvergleich resultieren u. a. die nachfolgend aufgelisteten Aspekte, die gemäß der Studie noch größtenteils ungenutzt sind und somit Forschungspotenzial darstellen, um die Entwicklungstätigkeiten im Bereich der Verlässlichkeit zu verbessern:

- Kontinuierliche (d. h. bereits frühzeitig startende) Nutzung von Verlässlichkeitsmethoden
- Verknüpfung von Verlässlichkeitsmethoden zu einem durchgängigen, in die Entwicklung integrierten Prozess
- Akzeptanz der Methoden und Methoden-Kompetenz bei den Mitarbeitern
- Verfügbares Fachwissen und umfassendes Datenmaterial

3.3 Forschungsansatz

Aus den beiden vorausgegangenen Unterkapiteln wird nun der zentrale Forschungsansatz für die vorliegende Arbeit hergeleitet, der das Ergebnis der deskriptiven Studie 1 darstellt. Darauf aufbauend werden dann Ziele und konkrete Anforderungen für die normative Studie abgeleitet.
Gemäß den zuvor interpretierten Ergebnissen der Industrie-Studie wird der Forschungsansatz dieser Arbeit anhand von resultierenden Forschungsfragen hergeleitet. Die für diese Arbeit relevanten Forschungsfragen weisen direkte Zusammenhänge mit den identifizierten Potenzialen der Studie auf und sind nachfolgend aufgezählt:

- Wie können Verlässlichkeitsaspekte kontinuierlich und systematisch in den Entwicklungstätigkeiten berücksichtigt werden?
- Wie kann bestehendes Wissen über Problemlösungen im Kontext der Verlässlichkeit sinnvoll abgelegt und wiederverwendet werden?

Keine bzw. nur geringe Berücksichtigung im Sinne des Forschungsbeitrags dieser Arbeit finden somit die Aspekte bzgl. des Datenmaterials, der Akzeptanz

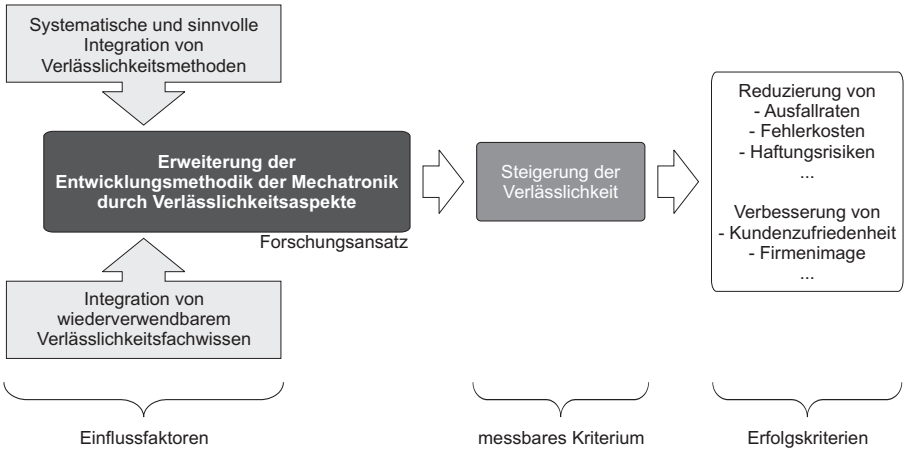


Abbildung 3.1: Forschungshypothese der vorliegenden Arbeit

von Verlässlichkeitsmethoden und der Methoden-Kompetenz der Mitarbeiter. Diese *Vernachlässigung* stellt allerdings keine Wertung bzgl. der Bedeutsamkeit der einzelnen Forschungsaspekte dar, sondern ist Ergebnis einer notwendigen Fokussierung dieser Arbeit auf die beiden zentralen Forschungsfragen.
Aus den beiden Forschungsfragen resultiert die nachfolgende Forschungshypothese der vorliegenden Arbeit, deren Aufbau in Abbildung 3.1 verdeutlicht wird:

> **Die systematische und sinnvolle Integration von Verlässlichkeitsmethoden und die Integration von wiederverwendbarem Verlässlichkeitsfachwissen in die Entwicklungsmethodik der Mechatronik führt zur Steigerung der Verlässlichkeit dieser Systeme.**

Die *Erweiterung der Entwicklungsmethodik der Mechatronik durch Verlässlichkeitsaspekte* stellt demnach den Kern der Hypothese und den wesentlichen Beitrag zu einer verlässlichkeitsorientierten Entwicklung dar. Die gemäß der Hypothese darauf wirkenden Einflussfaktoren werden somit einerseits durch den *systematischen und sinnvollen Einsatz von Verlässlichkeitsmethoden* beschrieben und andererseits durch die *Nutzbarkeit von wiederverwendbarem Verlässlichkeitsfachwissen*. Das messbare Kriterium zur Evaluierung der Hypothese kann durch eine *Steigerung der Verlässlichkeit* dargestellt werden, welche dann dann mittels Annahme einen positiven Einfluss auf die zahlreichen Erfolgskriterien hat.

Aus der Hypothese, im Speziellen aus den Einflussfaktoren und dem messbaren Kriterium, folgt das Vorgehen in den folgenden drei Kapiteln. Im Sinne der normativen Studie werden in Kapitel 4 und 5 die Werkzeuge und Methoden entwickelt, die eine Verbesserung der Entwicklungstätigkeiten gemäß der Einflussfaktoren ermöglichen sollen. Dieses sind einerseits der entwickelte *Verlässlichkeitsprozess für die Entwicklungsmethodik* und andererseits die *Methodik der Verlässlichkeitsmuster*, inklusive der zugehörigen Bereitstellung der Muster. In Kapitel 6 werden anhand eines Anwendungsbeispiels die Funktionalität der entwickelten Werkzeuge und Methoden evaluiert und die Beeinflussung des messbaren Erfolgskriteriums, die *Steigerung der Verlässlichkeit*, bewertet. Dieses Vorgehen entspricht der deskriptiven Studie 2, der verfolgten Forschungsmethodik.
Aus den vorangegangenen Unterkapiteln, Fazit und Bewertung des Standes der Technik und der Industrie-Studie, lassen sich nun weitere Anforderungen ableiten, die größtenteils für die Entwicklung des Verlässlichkeitsprozesses relevant sind: Als systematisches Rahmenkonzept soll die Entwicklungsmethodik der Mechatronik gemäß der VDI-Richtlinie 2206 verwendet werden, was sich in einigen der beschriebenen Ansätze bereits als vielversprechend erwiesen hat. Die verwendeten Verlässlichkeitsmethoden sollen möglichst allgemeingültig, einfach anwendbar sowie relativ verbreitet sein. Die Beschreibung von Prozesschritten mittels Methodenklassen, die auch dem Ansatz nach *Amberkar* mit bedarfsgerechter Methodenauswahl nahe kommt, könnte diese Anforderung erfüllen. Den Ansatz nach *Isermann* aufgreifend, soll auch die Verwendung von vorhandenem Wissen, z. B. über Fehlertoleranzkonzepte, in den Verlässlichkeitsprozess integriert werden, ebenso wie die Prozessverknüpfungen mittels Anforderungen ähnlich zu dem Vorgehen nach *Knepper*.

3.4 Zusammenfassung

Zusammenfassend hat das Kapitel 3 einerseits Erkenntnisse bzgl. der aktuellen *Anwendung von Verlässlichkeitsmethoden in der Industrie* und deren zukünftigen Bedarf entwickelt und andererseits *Schlussfolgerungen aus dieser Studie und dem Stand der Technik* gezogen. Diese Analyseergebnisse wurden dann zusammengeführt in dem vorgestellten *Forschungsansatz* der vorliegenden Arbeit.
Wesentliche Erkenntnisse der Studie zur aktuellen und zukünftigen Anwendung von Verlässlichkeitsmethoden in der Industrie verdeutlichen, dass wichtige Potenziale zur Berücksichtigung von Verlässlichkeit während der Entwicklung bisher noch ungenutzt sind. Dazu gehört neben einer früheren und kontinuierlichen Anwendung von Verlässlichkeitsmethoden auch die Integration innerhalb eines Entwicklungsprozesses und die Wiederverwendung bestehen-

den Verlässlichkeitswissens. Diese Erkenntnisse, kombiniert mit Schlussfolgerungen bezüglich bestehender Ansätze für Verlässlichkeitsprozesse, führte zur zentralen Forschungshypothese der vorliegenden Arbeit: *Die systematische und sinnvolle Integration von Verlässlichkeitsmethoden und die Integration von wiederverwendbarem Verlässlichkeitsfachwissen in die Entwicklungsmethodik der Mechatronik führt zur Steigerung der Verlässlichkeit dieser Systeme.* Diese wird in den weiteren Kapiteln gemäß der verfolgten Forschungsmethodik bearbeitet.

4 Verlässlichkeitsprozess für die Entwicklungsmethodik

Gemäß den aus Kapitel 3 resultierenden Erkenntnissen sowie der aufgestellten Forschungshypothese wird in diesem Kapitel ein Verlässlichkeitsprozess für die Entwicklungsmethodik mechatronischer Systeme entwickelt. Dies entspricht einem von zwei Teilen der normativen Studie der verfolgten Forschungsmethodik. Die Grundlage des Ansatzes stellt der Makroprozess der VDI-Richtlinie 2206 dar, der bereits im Stand der Technik vorgestellt wurde. Dieses V-Modell wird um ein zweites, äußeres V-Modell erweitert, das das Vorgehen für den Verlässlichkeitsprozess darstellt. Diese Grundidee eines Doppel-V-Modells verwendet ebenfalls der bereits vorgestellte Ansatz nach *Benz*. Neben der Makroebene werden entsprechend dem Vorgehen in der VDI-Richtlinie vordefinierte Prozessbausteine zur Bearbeitung wiederkehrender Arbeitsschritte detaillierter betrachtet. Daraus ergibt sich die Unterteilung dieses Kapitels in den eigentlichen Prozess der verlässlichkeitsorientierten Entwicklung mechatronischer Systeme und in die einzelnen Prozessbausteine.

4.1 Prozess der verlässlichkeitsorientierten Entwicklung

Der Makroprozess integriert verschiedene Aktivitäten im Kontext der Verlässlichkeit in einer Prozesskette in V-Gestalt. Insbesondere werden dazu die verschiedenen Klassen von Verlässlichkeitsmethoden verwendet, deren Funktionen und Anwendungen im Stand der Technik identifiziert und erläutert wurden. Der Makroprozess nutzt die Entwicklungsmethodik mechatronischer Systeme, das V-Modell, als systematisches Rahmenkonzept und erweitert die relevanten Prozessmodule Anforderungsanalyse, Systementwurf, Domänenspezifischer Entwurf und Systemintegration. Im Detail beinhaltet der Verlässlichkeitsprozess, dargestellt in Abbildung 4.1, die folgenden Prozessbausteine:

Anforderungsanalyse für Verlässlichkeit: Anforderungen bezüglich der Verlässlichkeit werden identifiziert, analysiert und dokumentiert.

Fehler-, Gefahren- und Risikenanalysen: Potenzielle Fehler und daraus resultierende Gefahren werden identifiziert und das dadurch bestehende Ri-

siko z. B. durch Eintrittswahrscheinlichkeit und Schwere der Konsequenzen bewertet. Fokus der Analysen können sowohl einzelne Funktionen und Teilfunktionen als auch Systemkomponenten bzw. ebenso auch das Gesamtsystem sein.

Konzipierung und Entwurf der Verlässlichkeit: Maßnahmen, mit system- oder prozesstechnischer Ausprägung, werden konzipiert und entworfen, die zur direkten Steigerung der Verlässlichkeit beitragen. Die Methodik der Verlässlichkeitsmuster, anwendbar gemacht durch eine Datenbanklösung, unterstützt dabei.

Verlässlichkeitsanalysen von Kooperation und Integration: Inkompatibilitäten und andere Probleme während der Integration werden aufgedeckt und beseitigt. Die aufgestellten Anforderungen bezüglich der Verlässlichkeit müssen erfüllt werden.

Darüber hinaus werden selbstverständlich die Prozessbausteine der klassischen Entwicklungsmethodik weiterhin angewendet. Dies gilt insbesondere für den Prozessbaustein *Eigenschaftsabsicherung*, der die Verifikation und Validation beinhaltet. Diese Prozessaktivitäten besitzen gerade im Kontext der Verlässlichkeit eine hohe Bedeutung.
Anwendbar ist dieser Prozess sowohl funktionsorientiert, d. h. im Sinne des Verständnisses nach [DIN02], als auch systemorientiert. Letztgenanntes Vorgehen würde nicht mit der abstrakten Funktion den Verlässlichkeitsprozess beginnen, sondern bei einem konkreteren Niveau, z. B. bei bereits ausgewählten Lösungselementen oder Teilkomponenten, starten. Beide Sichtweisen sind mit dem Vorgehen der Entwicklungsmethodik mechatronischer Systeme vereinbar, da die Prozessmodule des Verlässlichkeitsprozesses lediglich auf unterschiedlichem Level auf Ergebnisse des V-Modells zugreifen. Sowohl Funktionsstrukturen als auch Prinziplösungen sind bestehende Teilergebnisse der verwendeten Systematik gemäß VDI-Richtlinie 2206.
Die im Folgenden beschriebene Ausgestaltung des Makroprozesses durch die Prozessbausteine verwendet eine Grundidee des Ansatzes nach *Amberkar*. Dieser definiert die Elemente eines Sicherheitsprozesses nicht absolut durch Vorschriften zur Verwendung fest definierter Methoden, sondern er schlägt jeweils bedarfsgerechte Entscheidungen bezüglich der Auswahl entsprechend detaillierter Sicherheitsanalysen vor.
Durch Verwendung dieses Ansatzes und der Erkenntnisse aus Kapitel 2 dieser Arbeit, der Zuordnung zahlreicher Methoden zu Methodenklassen, können die einzelnen Prozessmodule im Folgenden relativ abstrahiert von Einzelmethoden erläutert werden. Es wird nur auf die jeweiligen Grundfunktionen verschiedener Methodenklassen eingegangen, die durch Beispiele potenzieller Methoden verdeutlicht, aber nicht fest vorgeschrieben werden.

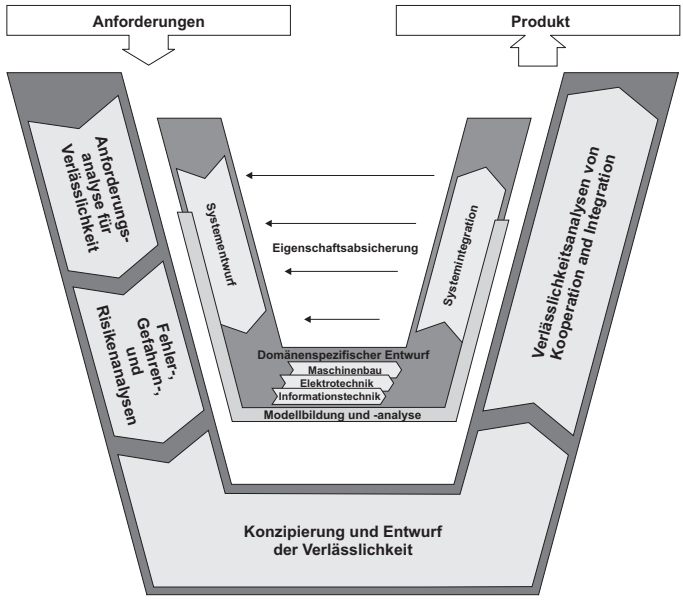


Abbildung 4.1: Doppel-V-Modell als Prozess auf Makroebene der verlässlichkeitsorientierten Entwicklungsmethodik für mechatronische Systeme

Dieser Ansatz eines Verlässlichkeitsprozesses soll die Vorteile der im Stand der Technik genannten Ansätze zusammenführen und erweitern. Der in dieser Arbeit entwickelte Verlässlichkeitsprozess soll somit losgelöst von speziellen Branchen, Produkten oder Systemen anwendbar sein. Somit soll er einen Mehrwert zum breiten Verständnis einer verlässlichkeitsorientierten Entwicklung mechatronischer Systeme bieten und gleichzeitig einen Prozess beschreiben, der direkt umsetzbar ist.

4.2 Prozessbausteine

Im Folgenden werden die einzelnen Prozessbausteine des Verlässlichkeitsprozesses für die Entwicklungsmethodik mechatronischer Systeme erläutert. Dabei wird der Reihenfolge gefolgt, die auch der späteren Anwendung entspricht. Bei der Beschreibung werden jeweils Input, Aufgaben und Ergebnisse dargestellt. Darüber hinaus werden ebenfalls die Verknüpfungen zu den Bausteinen der Entwicklungsmethodik aufgezeigt. Abgeschlossen wird jedes Kapitel mit exemplarischen Methoden der jeweiligen Methodenklasse. Die Auswahl der Methoden berücksichtigt dabei die Erkenntnisse von Kapitel 3, die diejenigen Methoden bevorzugen, die möglichst allgemeingültig, einfach anwendbar sowie relativ verbreitet sind.

4.2.1 Anforderungsanalyse der Verlässlichkeit

Dieser Prozessbaustein beinhaltet die Aufgabe, Anforderungen bezüglich der Verlässlichkeit eines mechatronischen Systems zu identifizieren, zu analysieren und zu dokumentieren. Die Inputs für diesen Prozessbaustein können untergliedert werden in Informationen, die bereits durch die Anwendung der VDI-Richtlinie 2206 als Ergebnisse von Meilensteinen vorhanden sind und in Informationen, die insbesondere durch den Fokus eines Verlässlichkeitsprozesses identifiziert werden. Erstgenannte können die eigentliche Entwicklungsaufgabe, die klassische Anforderungsliste, die abstrakte Problemformulierung sowie die Funktions- oder Wirkstruktur sein. Erweiterungen im Sinne der Verlässlichkeit resultieren von Informationen aus Checklisten, aus Normen und Richtlinien sowie aus Wissen vorangegangener Projekte. Auch die Anwendung bzw. die Ergebnisse von Kreativitätsmethoden zur Identifikation weiterer Verlässlichkeitsanforderungen können als Input genutzt werden.
Nach der Identifikation der Verlässlichkeitsanforderungen, müssen die Informationen zusammengeführt und analysiert werden, sodass sich eine strukturierte Liste von Verlässlichkeitsanforderungen aufstellen lässt. Anhand der Liste können die Anforderungen in quantitativer oder qualitativer Beschreibungsform dokumentiert werden, sollten jedoch unbedingt im Sinne der Verifikation

verwendbar sein. Eine quantitative Anforderung wäre z. B. ein Zielwert für die Zuverlässigkeit eines Systems, einer Funktion oder auch Teilkomponente, während eine qualitative Anforderung z. B. das Erreichen eines so genannten *Safe-State*, eines sicheren Zustands, wäre, der bei einer definierten Situation erreicht werden muss. Das Ergebnis dieses Prozessbausteins ist folglich eine strukturierte Liste, die verifizierbare Anforderungen an die Verlässlichkeit enthält. Auch Festlegungen bzgl. des akzeptablen Risikoniveaus können in dieser Phase getroffen werden.
Methoden, die zur Umsetzung dieses Prozessbausteins eingesetzt werden können, sind neben der klassischen Vorgehensweise zur Anforderungsanalyse, auch Kreativitätsmethoden wie Brainstorming oder Brainwriting sowie weitere Methoden der TRIZ-Systematik (vgl. Kapitel 2), die zur Identifikation weiterer Verlässlichkeitsanforderungen dienen. Eine zur Dokumentation der Ergebnisse relativ einfache, aber sehr effektiv anzuwendende Methode ist die *Checkliste für Verlässlichkeitsanforderungen*. Diese Checkliste sollte als dynamisches Dokument während des gesamten Entwicklungszeitraums gepflegt, erweitert und letztlich bei der Verifikation verschiedener Integrationsstufen erfüllt werden. Die Anwendung von Checklisten entspricht darüber hinaus auch den Ergebnissen aus Kapitel 3, die bereits aktuell eine breite Anwendung der Methode in der Industrie indentifiziert hat.
Zusammenfassend stellt Abbildung 4.2 die Aktivitäten des Prozessbausteins *Anforderungsanalyse der Verlässlichkeit* dar. Eine exemplarische Vorgehensweise davon könnte konkret wie im Folgenden beschrieben ablaufen:

- Eine Entwicklungsaufgabe wurde bereits formuliert und das Dokument der klassischen Anforderungsliste existiert ebenfalls. An dieser Stelle, relativ frühzeitig im Entwicklungsprozess, beginnt der Verlässlichkeitsprozess mit dem Prozessbaustein *Anforderungsanalyse der Verlässlichkeit*.
- Anhand der Entwicklungsaufgabe kann bereits die Anwendung von Normen und Richtlinien geklärt und Aspekte daraus dokumentiert werden, die die Verlässlichkeit betreffen.
- Die vorhandenen Informationen (Entwicklungsaufgabe, klassische Anforderungsliste, Forderungen aus Normen und Richtlinien) werden in einem Experten-Workshop analysiert und durch Wissen vorangegangener Projekte erweitert und strukturiert.
- Die Ergebnisse werden in Form von quantitativen und qualitativen Anforderungen in der um Verlässlichkeitsaspekte erweiterten Anforderungliste oder mittels einer seperaten Checkliste für Verlässlichkeitsanforderungen dokumentiert. Fragen und ggfs. Antworten bzgl. der Verlässlichkeitsanforderungen sollen für die spätere Verifikation eine einfache Handhabung gewährleisten.

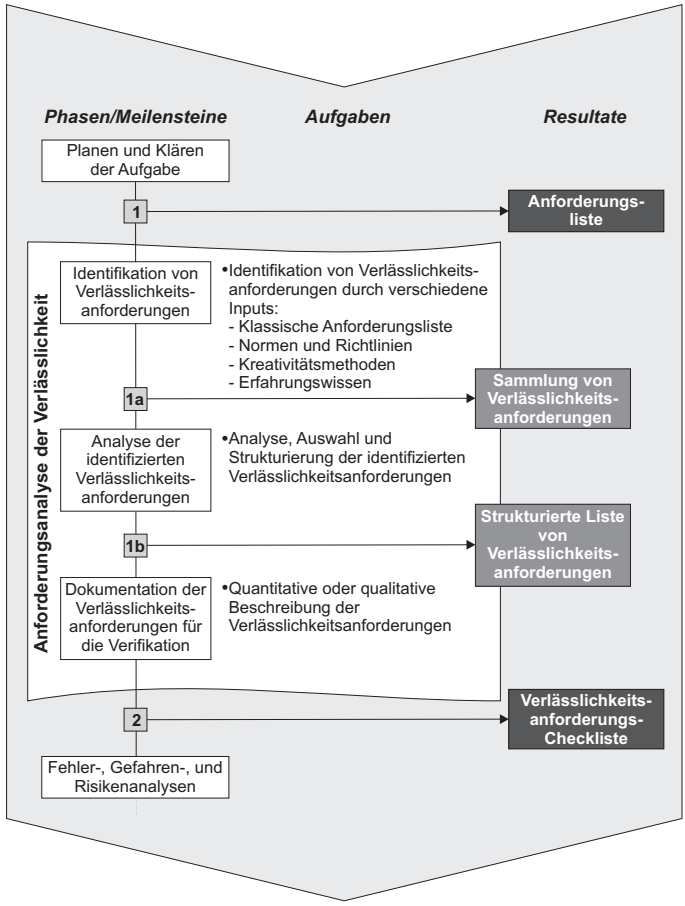


Abbildung 4.2: Aktivitäten im Prozessbaustein *Anforderungsanalyse der Verlässlichkeit*

- Die ersten Schritte des Systementwurfs können nun gemäß der Entwicklungsmethodik der Mechatronik erfolgen, sodass aus einer abstrakten Problemformulierung eine Funktionsstruktur entwickelt wird.

- Die Funktionsstruktur dient nun als Input für den nächsten Schritt: Dabei wird die Funktionsstruktur mit dem Fokus der Verlässlichkeit analysiert, indem die Teilfunktionen, begonnen mit der Hauptfunktion, analysiert werden. Potenzielle Vererbungen von Verlässlichkeitsforderungen höherer Hierarchiebenenen der Funktionsstruktur sollten in diesem Zusammenhang unbedingt genutzt werden.

- Das Ergebnis der Anforderungsanlyse der Verlässlichkeit ist an dieser Stelle des Prozessbausteins bereits nahezu vollständig. Es umfasst die Ergebnisse der Analysen in Form von Checklisten, die die Anforderungen der Verlässlichkeit an das System in unterschiedlichen Leveln gemäß der Funktionsstruktur beschreiben. Die Beschreibungsform wird sowohl durch quantitative als auch qualitative Anforderungen erfüllt. Da diese Checklisten eine dynamische Funktion im Entwicklungsprozess besitzen, können weitere identifizierte Anforderungen kontinuierlich hinzugefügt werden. Diese Aktivitäten werden insbesondere bei der Umsetzung der Funktionsstruktur in eine Wirkstruktur bzw. bei der Umsetzung in Teilkomponenten auftreten.

Eine wichtige Anmerkung und auch eine Begründung zur zusätzlichen Beschreibung des Prozessbausteins in dieser Form ist die, dass die Darstellung des Prozessbausteins zwar eine Reihenfolge von definierten Meilensteinen, Aufgaben und Resultaten beschreibt, diese Reihenfolge allerdings keine Iterationen etc. ausschließen soll. Vielmehr sind Iterationsschleifen sowohl innerhalb der Prozessbausteine als auch zwischen ihnen der Regelfall.

4.2.2 Fehler-, Gefahren- und Risikenanalysen

Der Prozessbaustein *Fehler-, Gefahren,- und Risikenanalysen* beinhaltet die Aktivitäten, die häufig als Kern eines Verlässlichkeitsprozesses verstanden werden. Dieser Sichtweise wird auch in dieser Arbeit gefolgt, mit der Erweiterung, dass der Prozessbaustein durch die Integration in einen durchgängigen Makro-Prozess weiteren Nutzen darstellt. Dieser ist unter anderem dadurch begründet, dass die Verknüpfungen mit Anforderungen bezüglich der Verlässlichkeit sowie der späteren Verifikation sehr wichtig sind und durch den durchgängigen Makroprozess unterstützt werden. Hauptfunktion dieses Prozessbausteins ist die Analyse eines Objektes bezüglich auftretender Fehler, daraus folgender Gefahren sowie der Bewertung des resultierenden Risikos. Objekte dafür können

z. B. das Gesamtsystem, Einzelkomponenten und -module oder auch die Lösungselemente sein, ebenso wie die Elemente der Funktionsstruktur oder auch die abstrakte Entwicklungsaufgabe.
Die Chronologie der Aktivitäten erfolgt entsprechend der Reihenfolge der im Titel genannten Analysen. Die Hauptfunktionen der einzelnen Methodenklassen entsprechen dabei den in Kapitel 2.3 erläuterten unterschiedlichen Aspekten bezüglich Fehler-, Gefahren- und Risikenanalysen:

Fehleranalysen: Identifikation und Analyse von Schwachstellen und potenziellen Fehlern

Gefahrenanalysen: Identifikation und Analyse von Gefahren, die u. a. durch potenzielle Fehler enstehen können

Risikenanalysen: Bewertung der Gefahren, z. B. anhand von Eintrittswahrscheinlichkeiten und Schwere der Konsequenzen

Die Ergebnisse dieses Prozessbausteins sind bewertete Gefahren anhand von Risikokriterien, die auf analysierten Fehlern oder anderweitig identifizierten Gefahren beruhen. Es resultiert somit eine verlässlichkeitsorientierte Bewertung des Systems, die wiederum Einfluss auf die bereits erläuterte Verlässlichkeitsanforderungs-Checkliste hat. Im Folgenden werden die Aktivitäten der drei Phasen innerhalb des Prozessbausteins *Fehler-, Gefahren- und Risikenanalysen* im Detail vorgestellt.

Fehleranalysen

Hauptaufgabe der Fehleranalysen ist die Identifikation von Schwachstellen und potenziellen Fehlern des Systems. Dies können sowohl die eigentlichen Fehlerursachen als auch Fehlerzustände sein, die noch auf tieferliegende Ursachen rückführbar sind (vgl. Kapitel 2.1). Durch systematische Herangehensweisen anhand von Funktionshierarchie, Systemaufbau, Systemzuständen, logischen Abhängigkeiten und auch durch Erfahrung und Kreativität der Entwickler werden potenzielle Fehlerursachen und Fehlerzustände in Systemen bzw. bereits in den Systementwürfen identifiziert.
Abhängig von den vorhandenen Informationen der Ausgangssituation sowie von folgenden Fragestellungen bei bereits identifizierten Fehlern, werden verschiedene Methoden der Fehleranalyse verwendet und kombiniert. Als Grundlage eignen sich insbesondere tabellarische Methoden, die auf einer Systemstruktur basieren, da sie einerseits einem systematischen Ablauf folgen und andererseits das Gesamtsystem im Fokus haben. Dabei kann die *Systemstruktur* z. B. durch Komponenten, Funktionen und Zustände beschrieben werden.

Ein Beispiel dafür wäre etwa die in Kapitel 2.3.1 beschriebene FMEA. Erweitert werden sollte diese Vorgehensweise anhand einer Systemstruktur unbedingt durch Erfahrungswissen über Fehler, die evtl. nicht durch die Analyse von Funktionen, Komponenten oder Zuständen identifiziert worden sind. Auch der Einsatz von Methoden, die die Kreativität der Entwickler nutzen, z. B. die ebenfalls in Kapitel 2.3.1 beschriebene AFE, ist möglich. Beides, Erfahrungswissen und Kreativität, kann verwendet werden, um weitere Fehler zu identifizieren. Diese können dann relativ einfach eingefügt werden, wenn als Grundlage eine tabellarische Methode zur Verfügung steht. Neben dieser so entstandenen Basis können und sollen selbstverständlich weitere Fehleranalysen für Detailuntersuchungen angewendet werden. Unter anderem können dies Analysen bezüglich logischer Abhängigkeiten sein, z. B. die FTA, oder auch Lebensdaueruntersuchungen, die dann in der Regel allerdings ein entsprechend fortgeschrittenes Stadium im Systementwurf benötigen.

Gefahrenanalysen

Nachdem potenzielle Fehler durch den vorangegangenen Prozessschritt identifiziert werden konnten und die Ergebnisse empfohlener Weise in tabellarischer Form zur Verfügung stehen, liegt nun die *Identifikation und die Analyse von Gefahren*, d. h. von gefährlichen Konsequenzen, im Fokus. Die Identifikation von Gefahren basiert dabei auf den gefundenen Fehlern, die durch ihre potenziellen gefährlichen Konsequenzen zu Gefahren werden können. Das Resultat der Identifikation ist eine Fehler- und Gefahrenliste. Diese Vorgehensweise impliziert somit wieder die systematische Herangehensweise anhand von Funktionshierarchie, Systemaufbau oder Ähnlichem.

Zusätzlich können und sollen die auf diese Weise identifizierten Gefahren auch anderweitig ergänzt werden, z. B. durch Erfahrungswissen und die Anwendung von Normenlisten. Insbesondere die Identifikation von Gefahren, die aus dem Umfeld resultieren, d. h. nicht vom System selbst durch eigene Fehler verursacht werden, erweitert in der Regel die Fehler- und Gefahrenliste beträchtlich.

Zur Umsetzung der Gefahrenanalyse sind u. a. die im Stand der Technik beschriebenen Methoden *Vorläufige Gefahrenanalyse*, *Funktionale Gefahrenanalyse* und *HAZOP-Analyse* mögliche Vorgehensweisen, die je nach Stadium im Entwicklungsprozess zu empfehlen sind. Insbesondere die Möglichkeiten von Vererbungen von Gefahren mittels der Funktionshierarchien, detailliert erläutert in [Ben04], verdeutlicht einen Vorteil der funktionsorientierten Sichtweise bei Gefahrenanalysen. Weitere Details, z. B. Abhängigkeiten zwischen Gefahren, könnten u. a. mit der *Ereignisbaumanalyse* untersucht werden.

Risikenanalysen

Der Prozessschritt *Risikenanalysen* beschreibt die Bewertung aller zuvor identifizierten Gefahren mittels Risikoparameter. Dies können z. B. die Eintrittswahrscheinlichkeit und die Schwere der Konsequenzen sein. Weitere Beschreibungen bzgl. verschiedener Risikoparameter finden sich in Kapitel 2. Anhand dieser Bewertung wird auch über die Vertretbarkeit der Risiken entschieden. Fehler und/oder Gefahren, die gemäß den Ergebnissen der Risikoanalyse zu vermeiden sind, werden selbstverständlich in die Verlässlichkeitsanforderungs-Checkliste aus dem vorhergehenden Prozessbaustein übernommen.
Typische Methoden für die Risikoanalyse bzw. -bewertung sind die in Kapitel 2.3.3 beschriebenen Graphen- oder Matrixmethoden sowie das multiplakative Verfahren. Während Letztere, z. B. in der Ausprägung der Methode der Risikoprioritätszahl, anhand von quantitativen Größen das Risiko im Ergebnis durch einen Zahlenwert bewertet, so ermöglichen die Graphen- oder Matrixmethoden intuitivere Entscheidungen durch Klassenzuordnungen.
Zusammenfassend stellt Abbildung 4.3 den Ablauf im Prozessbaustein *Fehler-, Gefahren- und Risikenanalysen* dar. Die *verlässlichkeitsorientierte Bewertung des Systems* beinhaltet neben der risikobewerteten Fehler- und Gefahrenliste auch die Erweiterung der Verlässlichkeitsanforderungs-Checkliste. Nachfolgend ist exemplarisch beschrieben, wie ein konkretes Vorgehen in diesem Prozessbaustein aussehen könnte.

- Der Prozesschritt *Anforderungsanalyse der Verlässlichkeit* wurde durchgeführt und hat als Ergebnis die Verlässlichkeitsanforderungs-Checkliste. Diese beschreibt die Anforderungen der Verlässlichkeit an das System in quantitativer oder qualitativer Form und in unterschiedlichen Leveln gemäß der Funktionsstruktur. Die Checkliste hat eine dynamische Funktion im Entwicklungsprozess, sodass weitere identifizierte Anforderungen kontinuierlich hinzugefügt werden.

- Anhand der Anforderungen (klassisch und verlässlichkeitsorientiert) wurden bereits gemäß der Entwicklungsmethodik der Mechatronik die Funktionshierarchie sowie die Teile des Systementwurfs realisiert. Den Funktionen und Teilfunktionen wurden bereits komponentenbasierte Lösungen zugeordnet.

- Anhand der Funktionen, Zustände und Komponenten werden verschiedene Methoden zur Fehleridentifikation angewendet. Für die Betrachtung der Funktionen und Komponenten wird die Ausfalleffektanalyse im Sinne der FMEA genutzt und für die Zustände die HAZOP-Analyse. Potenzielle Vererbungen zwischen Hierarchiebenen gemäß der Systembeschreibung werden in diesem Zusammenhang ebenfalls genutzt. Um weitere Abhängigkeiten zwischen Fehlern zu identifizieren wird die Fehlerbaumanalyse

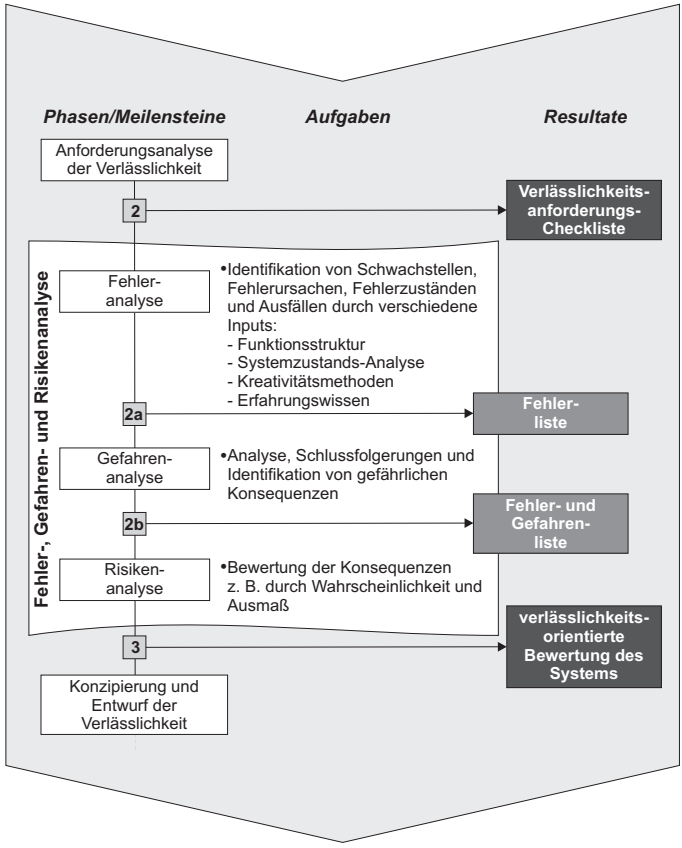


Abbildung 4.3: Aktivitäten im Prozessbaustein *Fehler-, Gefahren- und Risikenanalysen*

durchgeführt. Die Ergebnisse der Analysen werden in einer Fehlerliste dokumentiert.

- Um die systematischen Analyseergebnisse zu erweitern, fließt durch die Durchführung eines Experten-Workshops noch Erfahrungswissen ein.

- Gefahren werden identifiziert und in der Fehler- und Gefahrenliste dokumentiert. Dies erfolgt durch Schlussfolgerungen gefährlicher Konsequenzen aus den identifizierten Fehlern der Fehlerliste, durch identifizierte Gefahren des Umfelds und durch Anwendung von Normenlisten.

- Die identifizierten Fehler und Gefahren werden durch eine Risikomatrix bewertet, deren Achsen die Risikoparameter *Eintrittswahrscheinlichkeit* und *Schwere der Konsequenzen* darstellen. Eine Zuordnung in Risikoklassen erfolgt, die über die Akzeptanz des Risikos bzw. des potenziellen Fehlers oder der Gefahr entscheiden.

- Das Resultat ist einen verlässlichkeitsorientierte Bewertung des Systems, die aus einer risikobewerteten Fehler- und Gefahrenliste besteht und die die Verlässlichkeitsanforderungs-Checkliste des vorangegangenen Prozessbausteins erweitert.

- Das Resultat dient nun als Input für den nächsten Schritt, um das System anhand der Anforderungen weiter zu entwerfen und zu konkretisieren. Für spezielle Anforderungen bzgl. der Verlässlichkeit wird der Prozessbaustein *Konzipierung und Entwurf der Verlässlichkeit* angewendet.

4.2.3 Konzipierung und Entwurf der Verlässlichkeit

Der nachfolgend erläuterte Prozessbaustein beschreibt speziell die Aktivitäten im Entwicklungsprozess, die direkten Einfluss auf die Steigerung der Verlässlichkeit des Systems haben. Die direkte Steigerung beinhaltet folglich Maßnahmen prozess- oder systemtechnischer Art, die das System verlässlicher funktionieren lassen. Im Gegensatz zu den zuvor erläuterten Verlässlichkeitsanalysen, die *lediglich* die Gefährdungen identifizieren können, stellen diese Maßnahmen Lösungen für die resultierenden Anforderungen dar. Die Konzipierung und der Entwurf dieser Maßnahmen zur direkten Steigerung der Verlässlichkeit beschreibt daher die Hauptfunktion dieses Prozessbausteins.
Klassischer Weise könnten die Inhalte dieser Phase auch bereits im Baustein *Domänenspezifischer Entwurf* der Entwicklungsmethodik enthalten sein. Die Konzipierung und der Entwurf von Lösungen im Kontext der Verlässlichkeit werden aber in der vorliegenden Arbeit gesondert betrachtet, da so der hohe Stellenwert dieser Tätigkeiten verdeutlicht werden kann. Der im Stand der

Technik beschriebene Ansatz nach *Isermann* unterstützt ebenfalls die gesonderte Betrachtung der Verlässlichkeitskonzepte beim Entwurf.
Die Beschreibung der einzelnen Aktivitäten des Prozessbausteins *Konzipierung und Entwurf der Verlässlichkeit* basiert auf der *Theorie der Verlässlichkeitsmuster* [MW06], die im nachfolgenden Kapitel umfassend erläutert wird. Ein Verlässlichkeitsmuster ist demnach definiert als wiederverwendbarer Kern einer Lösung für Verlässlichkeit. Die Methodik wurde entwickelt, um den Konstrukteur während der Konzipierungsphase zu unterstützen, indem er, aufbauend auf den Verlässlichkeitsmustern, Lösungen für spezifische Problemstellungen im Rahmen der Verlässlichkeit entwickeln kann. Beispiele für Verlässlichkeitsmuster sind Redundanzstrukturen, ebenso wie Designregeln und verschiedene prinzipielle Diagnosealgorithmen.
Verlässlichkeitsmuster lassen sich in die drei Hauptkategorien *Fehlervermeidung*, *Fehlerüberwachung* und *Fehlertoleranz* unterteilen, die sich daran orientieren, welche Eingriffsmöglichkeiten bestehen, um Verlässlichkeit zu gewährleisten. Diese Eingriffsmöglichkeiten resultieren wiederum aus der in Kapitel 2.1 beschriebenen Fehlerpropagierung nach [Lap92].
Die einzelnen Aktivitäten des Prozessbausteins resultieren aus der Anwendung der Hierarchie der Verlässlichkeitsmuster. Für die identifizierten und risikobewerteten Fehler und Gefahren werden nacheinander Konzepte gesucht, die die Fehler oder Gefahren vermeiden bzw. das Risiko soweit reduzieren können, dass es akzeptabel ist. Nachfolgend sind diese Konzepte im Sinne der Verlässlichkeitsmuster dargestellt:

Anwendung von Konzepten zur Fehlervermeidung: Dies sind Verlässlichkeitsmuster, die die Fehlerursache, also die eigentlichen Fehler, bereits vor oder während der Entstehung verhindern.

Anwendung von Konzepten zur Fehlerüberwachung: Dies sind Verlässlichkeitsmuster, die einen Fehlerzustand erkennen, diagnostizieren und gegebenenfalls daraufhin Maßnahmen einleiten.

Anwendung von Konzepten zur Fehlertoleranz: Dies sind Verlässlichkeitsmuster, die trotz Ausfall von Teilsystemen die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten.

Zusammenfassend zeigt Abbildung 4.4 die Aktivitäten des Prozessbausteins, dessen Resultat ein optimiertes Systemkonzept ist, evtl. mit integrierter Fehlerüberwachung und Fehlertoleranz. Mögliche resultierende Veränderungen der bisherigen Verlässlichkeitsdokumente sowie der Dokumente der klassischen Entwicklungsmethodik sind ebenfalls Resultate dieses Prozessbausteins. Nachfolgend ist wiederum erläutert, wie ein konkreter Ablauf dieses Prozessbausteins aussehen könnte.

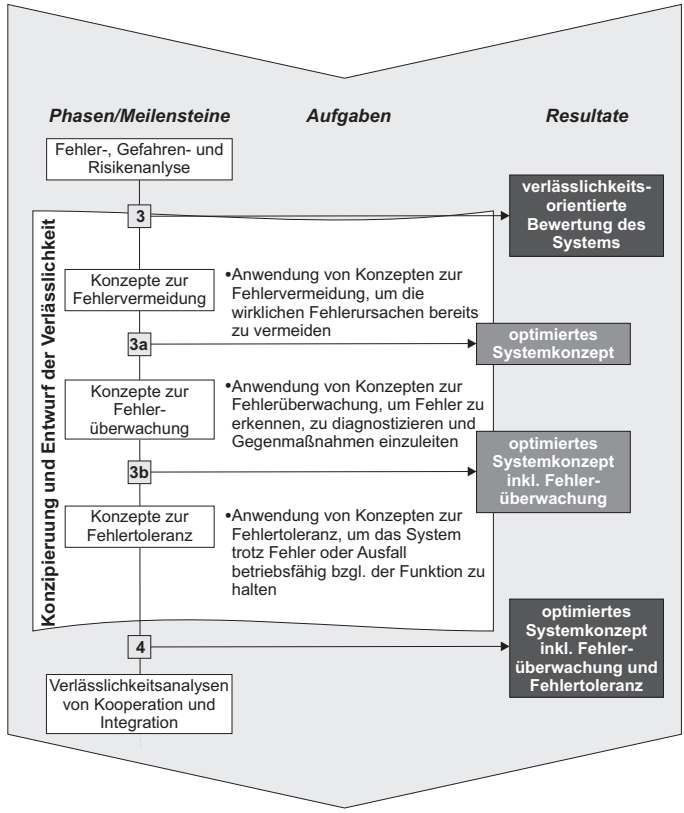


Abbildung 4.4: Aktivitäten im Prozessbaustein *Konzipierung und Entwurf der Verlässlichkeit*

- Eine verlässlichkeitsorientierte Bewertung des Systems im Sinne einer risikobewerteten Fehler- und Gefahrenliste sowie die Verlässlichkeitsanforderungs-Checkliste resultieren aus den vorangegangenen Bausteinen des Verlässlichkeitsprozesses. Ebenso existiert bereits ein relativ konkretes Systemkonzept durch das weitere Vorgehen gemäß der klassischen Entwicklungsmethodik.

- Das aktuelle Systemkonzept erfüllt allerdings noch nicht alle Anforderungen, speziell noch nicht die Anforderungen bzgl. der Verlässlichkeit.

- Es werden konstruktive Veränderungen des Systemskonzepts durchgeführt, um Fehlerursachen oder Fehlerzustände zu vermeiden. Beispielsweise könnten einige Bauteile überdimensioniert werden (Einsatz eines Verlässlichkeitsmusters der Fehlervermeidung).

- Da diese Maßnahme trotzdem noch nicht ausreicht, werden die auf das Bauteil wirkenden Belastungen mittels modellbasierte Diagnose überwacht, um sich anbahnende Fehler erkennen zu können (Einsatz eines Verlässlichkeitsmusters der Fehlerüberwachung).

- Durch das Erkennen ist nicht gewährleistet, dass schnell genug auf den potenziellen Fehler reagiert werden kann, um kritische Gefahren zu vermeiden. Redundante Notfall-Strukturen werden entwickelt, auf die das System notfalls selbständig umschalten kann und die eine Mindestfunktionalität des Systems gewährleisten können (Einsatz eines Verlässlichkeitsmusters der Fehlertoleranz).

- Anhand der Anwendung der Verlässlichkeitsmuster wurde das Systemkonzept bzgl. der Verlässlichkeit optimiert und durch Konzepte zur Fehlerüberwachung und Fehlertoleranz ergänzt. Der weiterentwickelte Systementwurf wird nun gemäß der klassischen Entwicklungsmethodik domänenspezifisch entworfen.

4.2.4 Verlässlichkeitsanalysen von Kooperation u. Integration

Der Prozessbaustein *Verlässlichkeitsanalysen von Kooperation und Integration* beinhaltet Aktivitäten, die Inkompatibilitäten und ähnliche Probleme während der Systemintegration aufdecken und beseitigen bzw. die die korrekte Kooperation von hierarchisch gleichen Komponenten gewährleisten. Darüber hinaus umfasst dieser Baustein ebenfalls im Kontext der Verlässlichkeit die Aktivitäten der Verifikation, d. h. dass die aufgestellten Anforderungen bezüglich der Verlässlichkeit erfüllt werden müssen, sowie die Aktivitäten zur Validation,

d. h. dass anhand der Anforderungen ein korrektes verlässliches System entwickelt worden ist.
Die beiden letztgenannten Aktivitäten könnten klassischer Weise bereits durch die Phase *Eigenschaftsabsicherung* der Entwicklungsmethodik abgedeckt werden. Die Verifikations- und Validationsaktivitäten im Kontext der Verlässlichkeit werden aber aufgrund der hohen Bedeutung dieser Tätigkeiten innerhalb dieser Arbeit und wegen des engen Bezugs zum Prozessbaustein *Anforderungsanalyse der Verlässlichkeit* detailliert dargestellt und sind im aktuell beschriebenen Prozessbaustein integriert.
Input für diesen Prozessbaustein sind Subkomponenten, die gemäß den Anforderungen domänenspezifisch entworfen wurden und die gemäß der *Systemintegration* der Entwicklungsmethodik höhere Hierarchiekomponenten bzw. im letzten Schritt das Gesamtsystem entstehen lassen. Dazu muss einerseits die korrekte Kooperation von verschiedenen Komponenten des gleichen Hierarchielevels gewährleistet werden und andererseits die Integration von Teilkomponenten in höhere Systemlevel. Die Ergebnisse beider Typen, Kooperation und Integration, müssen verifiziert und validiert werden. Für die Verifikation in diesem Kontext kann die systematisch aufgebaute Verlässlichkeitsanforderungs-Checkliste verwendet werden, die wiederum die schon vorher erwähnten Möglichkeiten für Vererbungen zulässt. Die Aktivitäten des Prozessbausteins beziehen sich selbstverständlich auch auf die verwendeten Verlässlichkeitskonzepte, deren Kooperation und Integration in das klassische System abgesichert sein muss.
Zur Realisierung der Aktivitäten des Prozessbausteins bieten sich zahlreiche und sehr unterschiedliche Methoden an. Einen Oberbegriff für die Gesamtheit der Methoden könnte durch *Testmethoden* beschrieben werden, die je nach Testziel dann für die Aktivitäten *korrekte Kooperation* und *Integration*, auch im Sinne der *Verifikation* und *Validation* zur Anwendung kommen. Zusätzlich zu den nachfolgend ausgeführten Testmethoden können aber auch *Formale Methoden*, wie z. B. Therom-Beweise und Model-Checking, genutzt werden [Hed01].
Als übergeordnete Methode für die Verifikation der korrekten Kooperation und Integration wird die Verwendung der Verlässlichkeitsanforderungs-Checkliste empfohlen. Diese ist entsprechend der Funktionshierarchie strukturiert erstellt worden und kann daher das System während der Integrationsphase schrittweise gegen die Anforderungen der verschiedenen Hierarchielevel testen. Um die einzelnen Anforderungen dann evtl. detaillierter zu testen, müssen andere Testverfahren eingesetzt werden. In diesem hierarchieorientierten Kontext können z. B. Fehlerbäume oder Markoff-Analysen die Verifikation von quantitativen Systemzuverlässigkeitszielen realisieren. Die hinterlegten Größen sind dann allerdings, im Unterschied zur Verwendung der Methoden im Prozessbaustein *Fehler-, Gefahren- und Risikenanalysen*, z. B. experimentell am physikalisch

vorhandenen System entstanden und müssen die zuvor aufgestellten Anforderungen erfüllen.
Für die Verifikation einzelner Forderungen, insbesondere im Kontext spezieller Verlässlichkeitsanforderungen, können verschiedene Fehlerinjektionsmethoden genutzt werden, die u. a. zur Untersuchung der Fehlertoleranz eines Systems dienen. Sie sollen das spezifizierte Verhalten eines Systems bei Fehlereintritt überprüfen, z. B. die Aktivierung fehlertoleranter Algorithmen oder Mechanismen. Spezielle Methoden dazu sind die *Physikalische Fehlerinjektion*, die *Softwareimplementierte Fehlerinjektion*, die *Fehlerinjektion in Simulationsmodellen* und *Fehlerinjektion zur Untersuchung der elektromagnetischen Verträglichkeit* [Ben04].
Methoden für die Untersuchung gemeinschaftlicher Fehlerursachen sind insbesondere bei der schrittweisen Integration von Systemen relevant. Beispiele sind die *Zonale Sicherheitsanalyse* für physikalisch getrennt zu betrachtenden Bereiche, die *Analyse Spezieller Risiken* für äußere Einflüsse, sowie die *Common Mode Analyse* für die Betrachtung der Unabhängigkeit von Fehlern [Ben04].
Darüber hinaus könnte zu einer abschließenden Validierung der Verlässlichkeit des Gesamtsystems auch die in Kapitel 2.3.1 erläuterte *Antizipierende Fehlererkennung* angewendet werden.
Um einige der zuvor genannten Testverfahren umsetzten zu können und im Speziellen auch um die Validierung durchzuführen, werden verschiedene Prüfumgebungen verwendet, die realitätsnahe Einsatzumgebungen darstellen oder simulieren sollen. Die Verfahren für *Hardware-in-the-Loop*, *Software-in-the-Loop* und *Modell-in-the-Loop* sind in diesem Kontext hervorzuheben, ebenso die damit verbundenen Testmethoden von Black- bzw. White-Box-Tests [LHD05].
Zusammenfassend zeigt Abbildung 4.5 die Aktivitäten des Prozessbausteins, der neben der Analyse von korrekter Kooperation und Integration auch die Verifikation und Validation im Kontext der Verlässlichkeit realisieren soll. Das Resultat des Bausteins ist ein verifiziertes und validiertes Gesamtsystem. Nachfolgend ist wiederum erläutert, wie ein konkreter Ablauf aussehen könnte.

- Das System ist bereits entsprechend des Systementwurfs der klassischen Entwicklungsmethodik hierarchisch konzipiert, und die Teilsysteme sind domänenspezifisch entworfen.

- Verlässlichkeitsmuster zur Fehlervermeidung, Fehlererkennung und Fehlertoleranz wurden zur Konzipierung verwendet, um den Anforderungen bzgl. der Verlässlichkeit zu entsprechen. Diese wurden ebenfalls domänenspezifisch ausgearbeitet.

- Anhand der Teilsysteme bzw. -komponenten werden entsprechend der klassischen *Systemintegrationsphase* hierarchisch oberlagerte Teilsysteme

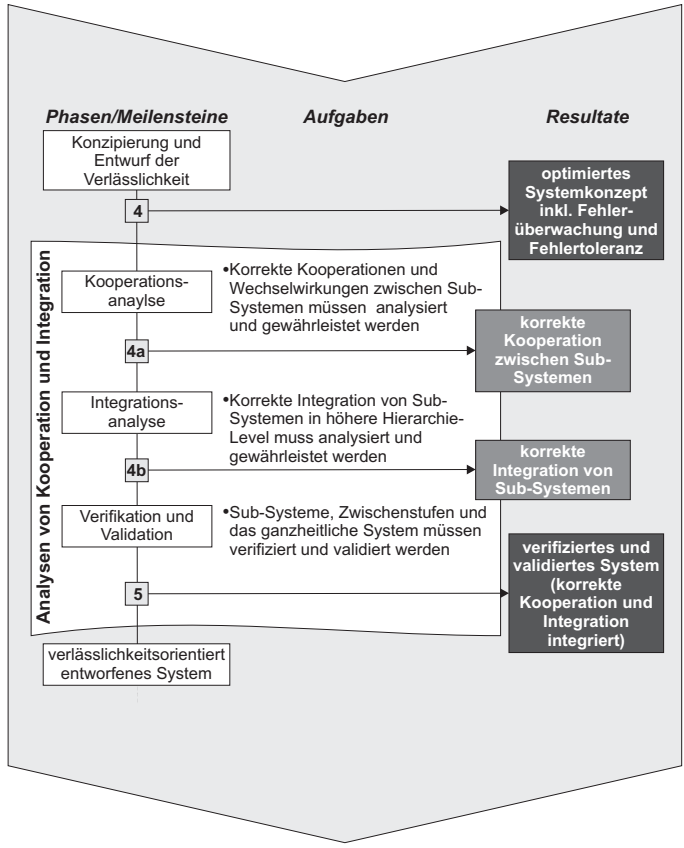


Abbildung 4.5: Aktivitäten im Prozessbaustein *Verlässlichkeitsanalysen von Kooperation und Integration*

bzw. im letzten Schritt das Gesamtsystem realisiert.

- Während dieser klassischen Integration werden bei jedem Schritt sowohl die korrekte Kooperation von hierarchisch gleich einzuordnenden Komponenten analysiert als auch die korrekte Integration von unterlagerten Systemen in übergeordnete. Inkompatibilitäten, z. B. Schnittstellenprobleme, werden erkannt und eliminiert, ebenso wie andere funktionale oder technische Zusammenhänge.

- Parallel dazu wird das System im klassischen Sinne verifiziert. Dazu werden Sub-Systeme und später auch das Gesamtsystem gegen die Spezifikation getestet. Hardware-in-the-Loop-Prüfstande für verschiedene Sub-Systeme unterstützen dabei.

- Außerdem wird das System speziell gegen die Spezifikationen der Verlässlichkeitsanforderungs-Checkliste getestet.

- Für Detailanforderungen werden die Verlässlichkeitsmuster mittels Fehlerinjektionsmethoden verifiziert.

- Die quantitativen Anforderungen der Systemzuverlässigkeit werden einzeln, teilweise experimentell, ermittelt und durch Markoff-Analysen zusammengeführt.

- Neben der Verifikation werden ebenfalls die Anforderungen selbst überprüft, in dem Sinne, ob ein korrektes und verlässliches System entwickelt wurde (Validierung).

- Abschließend wird zusätzlich zur Validierung der Verlässlichkeit des Gesamtsystems die Methode der *Antizipierenden Fehlererkennung* angewendet.

- Resultat des Prozessbausteins und gleichzeitig der verlässlichkeitsorientierten Entwicklungsmethodik ist ein verifiziertes und validertes Gesamtsystem, das alle Anforderungen, also auch den Verlässlichkeitsanforderungen, gerecht wird.

- Die Resultate der jeweiligen Verlässlichkeitsprozessbausteine werden direkt für Dokumentationszwecke verwendet.

4.3 Zusammenfassung

Das Kapitel *Verlässlichkeitsprozess für die Entwicklungsmethodik* beschreibt im Sinne der normativen Studie der verfolgten Forschungsmethodik den An-

satz, durch systematische und sinnvolle Integration von Verlässlichkeitsmethoden in die Entwicklungsmethodik, die Entwicklungstätigkeiten zu verbessern. Gemäß der Forschungshypothese führt diese Verbesserung dann zu einer höheren Verlässlichkeit der zu entwickelnden Systeme.
Der Ansatz zur Integration von Verlässlichkeitsmethoden in den Entwicklungsprozess nutzt die bestehende Systematik der VDI-Richtlinie 2206 *Entwicklungsmethodik für mechatronische Systeme* als Rahmenkonzept. Dabei wird sowohl das inhaltliche Vorgehen verwendet als auch die formale Beschreibung der Methodik durch Makroprozess und Prozessbausteine: Um das bestehende V-Modell herum legt der Ansatz ein zweites V-Modell, das den Verlässlichkeitsprozess darstellt, der selbstverständlich zahlreiche Verknüpfungen zur klassischen Entwicklungsmethodik aufweist. Die Phasen, und damit gleichzeitig die Prozessbausteine des Verlässlichkeitsprozesses sind nachfolgend aufgeführt:

- Anforderungsanalyse für Verlässlichkeit
- Fehler-, Gefahren- und Risikenanalysen
- Konzipierung und Entwurf der Verlässlichkeit
- Verlässlichkeitsanalysen von Kooperation und Integration

Die Prozessbausteine wurden jeweils durch Input, Aktivitäten und Resultate beschrieben, sowie die Tätigkeiten anhand von Methodenbeispielen verdeutlicht. Abschließend wurde das Vorgehen jedes Prozessbausteins mittels eines erdachten exemplarischen Ablaufs konkretisiert.

5 Methodik der Verlässlichkeitsmuster

Nachdem im vorangegangen Kapitel der Prozess einer verlässlichkeitsorientierten Entwicklungsmethodik erläutert wurde, der größtenteils die Möglichkeiten zur indirekte Steigerung der Verlässlichkeit im Fokus hatte, wird nun beschrieben, dass allgemeine Verlässlichkeitsmuster bestehen, die direkt zu einem verlässlicheren Verhalten von Systemen führen. Diese können wiederverwendbares Verlässlichkeitsfachwissen repräsentieren und entsprechen so dem zweiten Forschungsaspekt, der durch die normative Studie gemäß der verfolgten Forschungsmethodik betrachtet wird. Integriert ist diese *Methodik der Verlässlichkeitsmuster* in den in Kapitel 4.2.3 erläuterten Prozessbaustein *Konzipierung und Entwurf der Verlässlichkeit*.
Verlässlichkeitsmuster basieren auf dem Verständnis, dass spezifische Lösungen für verlässliches Verhalten von Systemen auf den Lösungskern reduziert werden können. Aus diesem Kern kann dann das lösungsneutrale Verlässlichkeitsmuster formuliert werden, das eine Wiederverwendung, auch bei geänderten Randbedingungen oder in einem anderen Umfeld, gewährleisten kann. Die Verlässlichkeitsmuster unterstützen den Entwickler somit insbesondere während der beschriebenen Konzipierungsphase, indem Lösungen für spezifische Problemstellungen im Rahmen der Verlässlichkeit entwickelt werden, die auf den Verlässlichkeitsmustern aufbauen können. Beispiele dafür sind Redundanzstrukturen, ebenso wie Designregeln und verschiedene prinzipielle Diagnosealgorithmen.
Im Folgenden wird dazu zunächst der Begriff des Verlässlichkeitsmusters im Detail definiert. Darauf aufbauend werden Hauptkategorien und ausgewählte Beispiele erläutert, und abschließend wird die Nutzung der Muster im Rahmen eines Wissensmanagementsystems, der Datenbank für Verlässlichkeitsmuster, dargestellt.

5.1 Definition des Verlässlichkeitsmusters

Der Begriff des Verlässlichkeitsmusters ist kein verbreitetes Paradigma in der wissenschaftlichen Literatur, sondern stellt vielmehr einen neu entwickelten Beitrag dieser Arbeit zum Forschungsgebiet der Verlässlichkeit dar. Der Begriff

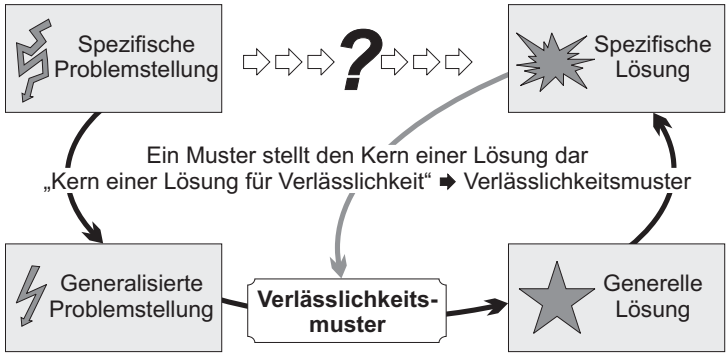


Abbildung 5.1: Begriffsentwicklung des Verlässlichkeitsmusters

setzt sich aus den beiden Teilen Muster und Verlässlichkeit zusammen, deren Verknüpfung die Ursächlichkeit verdeutlichen soll, die das Muster besitzt, um eine erhöhte Verlässlichkeit von Systemen zu erreichen. Das Wissen, das durch das lösungsneutrale Verlässlichkeitsmuster repräsentiert wird, basiert u. a. auf Erfahrungswissen und Recherchearbeiten.
Der Begriff des Musters wird dabei gemäß [FGK+04] verwendet und beschreibt den Kern einer Lösung für eine spezifische Problemstellung. Das Muster resultiert folglich aus bereits zuvor erfolgreichen Lösungen und lässt sich in analogen Problemsituationen wiederholt verwenden. Ähnliche Begriffe stellen Entwurfsmuster aus dem Bereich der Informationsverarbeitung und Wirkprinzipien aus den Domänen Maschinenbau und Elektrotechnik dar. Der verwendete neutrale Musterbegriff soll die übergeordnete Ebene darstellen, die die beiden zuvor genannten Begriffe integriert.
In dem Fall, dass ein Muster die Lösung für ein Verlässlichkeitsproblem darstellt, kann folglich von einem Verlässlichkeitsmuster gesprochen werden. Aus bereits erfolgten erfolgreichen Lösungen für Problemstellungen der Verlässlichkeit können somit die Kernelemente extrahiert werden, die eine Übertragbarkeit zu lassen. Auf die so entstehenden Verlässlichkeitsmuster, kann dann bei ähnlichen Herausforderungen wieder zurückgegriffen werden [MW07] [MW06].

5.2 Strukturierungskonzept für Verlässlichkeitsmuster

Die Verlässlichkeitsmuster lassen sich in drei Hauptkategorien unterteilen, die sich daran orientieren, welche Eingriffsmöglichkeiten bestehen, um Verlässlichkeit zu gewährleisten. Diese Eingriffsmöglichkeiten resultieren aus der in

Kapitel 2 vorgestellten Fehlerpropagierung. Die Fehlerpropagierung wird im Sinne eine Fehlerkette definiert, die die wichtigen Unterscheidungen zwischen den Begriffen *Fehlerursache*, *Fehlerzustand*, *Ausfall* und *Konsequenz* trifft. Die Fehlerursache stellt demnach die verantwortliche Ursache von unerwünschten Ereignissen, z. B. von Gefahren, dar. Die Fehlerursache für sich hat aber nicht zwangsläufig einen Fehlerzustand zur Folge, da sie sich theoretisch während der gesamten Lebensdauer passiv verhalten könnte. Erst eine Aktivierung der Fehlerursache hat einen Fehlerzustand zur Folge, der häufig das Verständnis des eigentlichen Fehlers widerspiegelt. Führt dieser Fehlerzustand dazu, dass die erbrachte Leistung des Systems nicht mehr der Spezifikation, d. h. der erwarteten Funktion entspricht, so spricht man von einem Ausfall des Systems. Dieser Ausfall wiederum kann Konsequenzen bzw. Auswirkungen außerhalb der Systemgrenzen besitzen. Daran angelehnt ergeben sich, wie in Abbildung 5.2 dargestellt, die drei Hauptkategorien für Verlässlichkeitsmuster. Diese repräsentieren verschiedene Eingriffsmöglichkeiten entsprechend der Fehlerkette, um den jeweils nachfolgenden Fehlertyp zu vermeiden bzw. den aktuellen zu beheben:

Fehlervermeidung beschreibt Verlässlichkeitsmuster, die die Fehlerursache bereits vor oder während der Entstehung verhindern.

Fehlerüberwachung beschreibt Verlässlichkeitsmuster, die einen Fehlerzustand erkennen, diagnostizieren und gegebenenfalls daraufhin Maßnahmen einleiten.

Fehlertoleranz beschreibt Verlässlichkeitsmuster, die trotz Ausfall von Teilsystemen die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten.

Diese drei Hauptkategorien werden im Folgenden detailliert betrachtet, in weitere Subtypen untergliedert und mit Beispielen erweitert. Dabei gilt es zu beachten, dass sie keine vollständige Auflistung darstellen können und sollen. Sie bieten vielmehr eine Basis, die im Sinne der Datenbank für Verlässlichkeitsmuster dynamisch erweitert werden muss [MW07].

5.2.1 Fehlervermeidung

Verlässlichkeitsmuster der Fehlervermeidung verhindern die Fehlerursache bereits vor oder während der Entstehung. Damit sind es diese Konzepte, deren Umsetzung primär verfolgt werden sollte. Zu den typischen Mustern der Fehlervermeidung zählen neben der wünschenswerten, aber leider unrealistischen Perfektion, die zahlreichen *Designprinzipien zur Vermeidung von stochastischen*

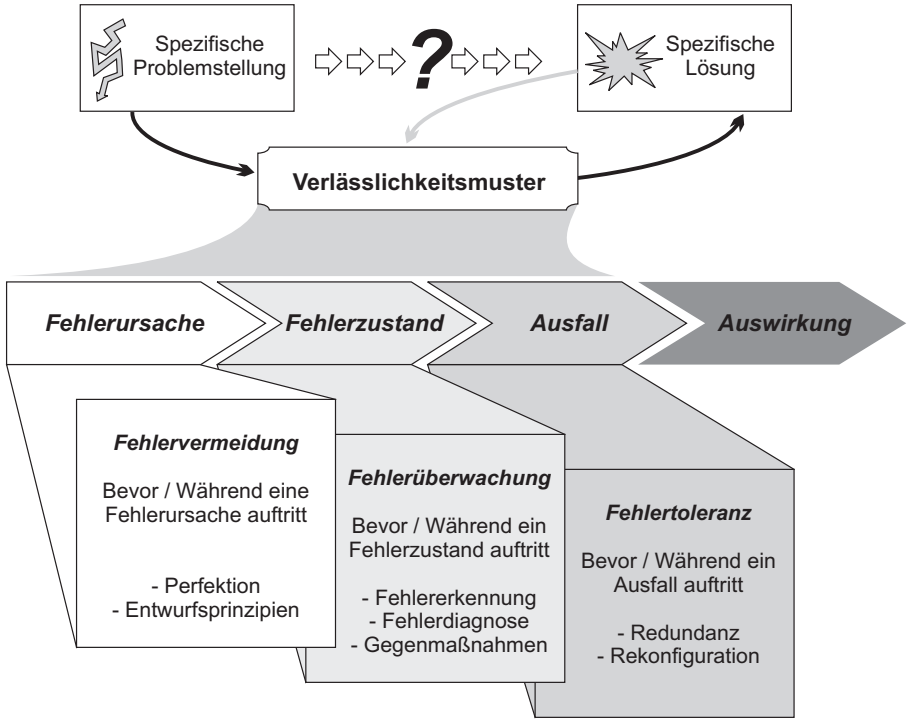


Abbildung 5.2: Hauptkategorien der Verlässlichkeitsmuster, resultierend aus der Fehlerkette

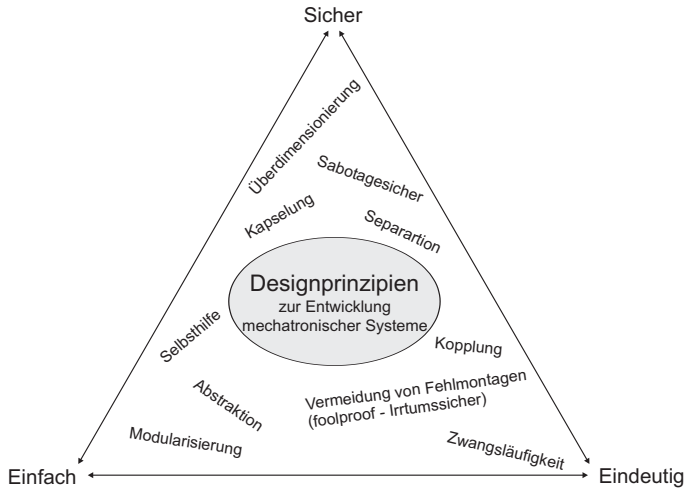


Abbildung 5.3: Designprinzipien für die Entwicklung mechatronischer Systeme

Fehlern. Beispiele sind Überdimensionierung, Zwangsläufigkeit und Sabotagesicherheit [Pah01]. Auch die *Vermeidung von deterministischen Gefahren* durch bewährte Maßnahmen der unmittelbaren, mittelbaren und hinweisenden Sicherheitstechnik [Neu02], z. B. durch trennende Sicherheitsbarrieren, sind dieser Kategorie zuzuordnen. Weitere Unterkategorien für Verlässlichkeitsmuster der Fehlervermeidung sind selbstverständlich denkbar, werden an dieser Stelle allerdings nicht betrachtet.

Designprinzipien

Die Designprinzipien, oder auch Gestaltungsprinzipien genannt, werden in der Domäne des Maschinenbaus z. B. durch [Pah01] unter den drei Oberbegriffen eindeutig, einfach und sicher subsumiert. *Eindeutigkeit* beschreibt dabei die klare Zuordnung und Erfüllung der technischen Funktion, *Einfachheit* die übersichtliche und möglichst elementare Gestaltung und *Sicherheit* die Haltbarkeit, Zuverlässigkeit, Unfallfreiheit und den Schutz für Mensch und Umwelt. Diese übergeordneten Gestaltungsprinzipien sind vollständig übertragbar auf die Mechatronik. Innerhalb dieser Kategorien lassen sich weitere, teilweise abstrakte Designprinzipien einordnen, die jedoch häufig Bezüge zu mehr als einer Kategorie aufweisen. Abbildung 5.3 zeigt eine Übersicht ausgewählter Designprinzipien. Außerdem sollen zwei Sammlungen für Designprinzipien diesen Bereich der Verlässlichkeitsmuster verdeutlichen:
Für den Entwurf der Funktionsarchitektur von verteilten Regelaufgaben im

Automobil sind nachfolgend exemplarische Designprinzipien aufgezählt. Diese wurden im Rahmen der offenen Architektur *CARTRONIC* eines Automobilzulieferers entwickelt für vernetzende Steuergeräte in Fahrzeugen [BDM99]:

- Jedes System/Jede Komponente besteht aus eigenständigen unabhängigen Komponenten mit einer minimalen Anzahl an physischen Schnittstellen.
- Jedes System/Jede Komponente erfüllt autonom die eindeutig definierte Aufgabe durch Beschaffen von Informationen und Einleiten von Befehlen.
- Übergeordnete Entscheidungskomponenten koordinieren Systeme/Komponenten; diese sind z. B. dafür verantwortlich, dass aus konkurrierenden Abfragen eine einzelne Information hergeleitet wird.
- Befehle werden hierarchisch vom Initiator zum Aktuator/Auslöser propagiert.
- Die Schnittstellen von jedem System/jeder Komponente sind so vielen anderen wie notwendig bekannt und so wenigen wie möglich.

Die zweite dargestellte Sammlung enthält Entwicklungs- und Konstruktionsrichtlinien für die Zuverlässigkeit elektronischer Bauteile nach [Bir91]:

- Elektrische/Thermische *Unterlastung* elektronischer Bauteile wird mittels Belastungsfaktoren zwischen 0 und 1 beim Entwurf berücksichtigt, da die Belastung einen großen Einfluss auf die Ausfallrate besitzt.
- Die Chiptemperatur der Halbleiterbauteile muss möglichst niedrig gehalten werden. Sie setzt sich zusammen aus der Umgebungstemperatur und der durch eigene Verlustleistung verursachten Temperaturerhöhung. Einfluss darauf besitzen Konstruktion und Gehäuse des Bauteils sowie evtl. vorhandene Kühlkörper und -mittel.
- Feuchtigkeit soll möglichst vermieden werden. Dabei ist weniger der Wasserdampf störend, sondern die in ihm aufgelösten Verunreinigungen und Gase können durch Korrosion und Elektrolyse metallische Kontakte und Leiterbahnen angreifen und sind daher kritisch. Daher ist besonders eine Tau- oder Eisbildung direkt auf den Bauteilen zu vermeiden. Mögliche Schutzmechanismen: Kühlung durch trockene Luft oder inerte Stoffe, Verhinderung galvanischer Materialpaarungen z. B. durch Schutzlackierungen.
- Äußeren elektromagnetischen Störungen soll widerstanden werden und der Pegel der eigenen Störung nach Außen soll unterhalb gegebener

Grenzwerte gehalten werden. Je energiereicher und kürzer die entsprechenden Anstiegszeiten, desto gefährlicher sind die elektromagnetischen Störungen. Wichtige Störverursacher sind Schaltvorgänge, elektrostatische Entladungen und Emissionen. Für die Reduzierung der Störungen existieren wiederum zahlreiche detailliertere Regeln wie z. B. *Möglichst breite Speiseleiter verwenden* oder *Öffnungen in schirmenden Gehäusen vermeiden*.

Vermeidung deterministischer Gefahren

Verlässlichkeitsmuster zur Vermeidung deterministischer Gefahren repräsentieren die klassischen *unmittelbaren*, *mittelbaren* und *hinweisenden Konzepte der Sicherheitstechnik*. Strukturiert dargestellt werden sie z. B. in [Neu02].Bei der Anwendung dieser Muster wird gemäß Abbildung 5.4 vorgegangen, sodass die identifizierten Gefahren zuerst durch Konzepte der unmittelbaren Sicherheitstechnik vermieden werden sollen. Erst wenn dies nicht möglich ist, werden mittelbare Sicherheitskonzepte umgesetzt, um gegen Gefahren zu sichern, bevor nicht zu vermeidende Restgefahren durch hinweisende Muster angezeigt werden. Neben den umgesetzten Sicherheitskonzepten verbleibt dann das akzeptierte Restrisiko. Nachfolgend werden einige Beispiele und Ausführungen zu den drei zuvor angesprochenen Verlässlichkeitsmustern gegeben:

- Verlässlichkeitsmuster der *unmittelbaren Sicherheitstechnik* beschreiben Konzepte, die der Vermeidung und Minimierung von Gefahren dienen und nicht manipulierbar sind. Dies kann durch geometrische und energetische Gestaltungsmaßnahmen erfolgen. Beispiele der ersten Kategorie sind Mindest- und Sicherheitsabstände oder anderweitige Beschränkungen der Zugänglichkeit von Gefahrenstellen, die durch die geometrischen Abmaße des Systems oder der Maschine festgelegt sind. Beispiele für energetische Gestaltungsmaßnahmen sind eine Begrenzung der wirksamen Energie oder eine gezielte elastische Verformung von Bauteilen.

- Verlässlichkeitsmuster der *mittelbaren Sicherheitstechnik* werden verwendet, wenn die Gefahren mit unmittelbaren Konzepten nicht zu beseitigen sind. Diese Muster sichern gegen Gefahren. Sie umfassen Konzepte mittels ruhender und bewegter Sperren sowie Konzepte, die durch steuerungstechnische Maßnahmen realisiert werden. Diese mittelbaren Konzepte sind im Gegensatz zu den unmittelbaren allerdings manipulierbar. Beispiele für ruhende Sperren sind fangende oder trennende Schutzeinrichtungen wie Fanghauben und Verkleidungen; für steuerungstechnische Maßnahmen können z. B. ortsbindende Zweihandschaltungen oder Schutzeinrichtungen mittels Annäherungsreaktion genannt werden. Au-

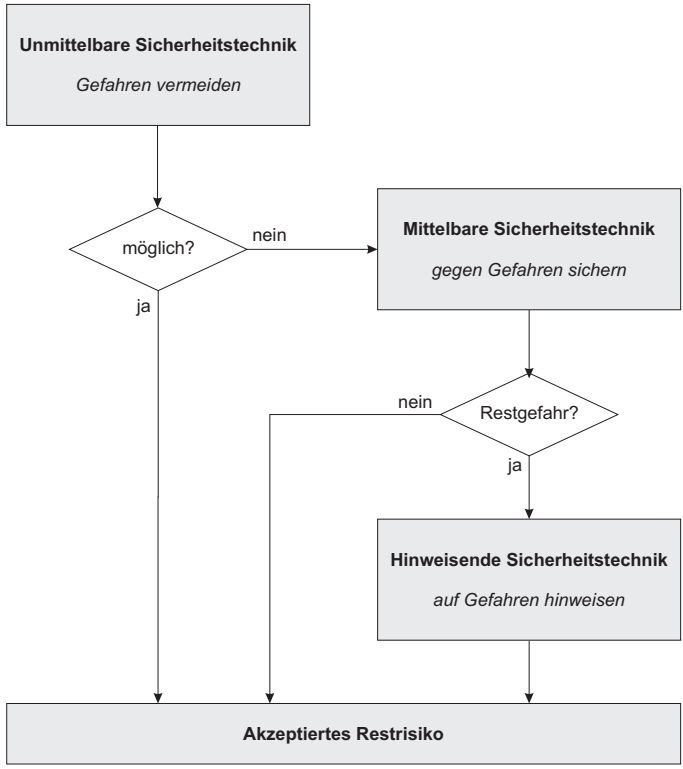


Abbildung 5.4: Ablaufhierarchie zur Nutzung der Verlässlichkeitsmuster für unmittelbare, mittelbare und hinweisende Sicherheitstechnik [Neu02]

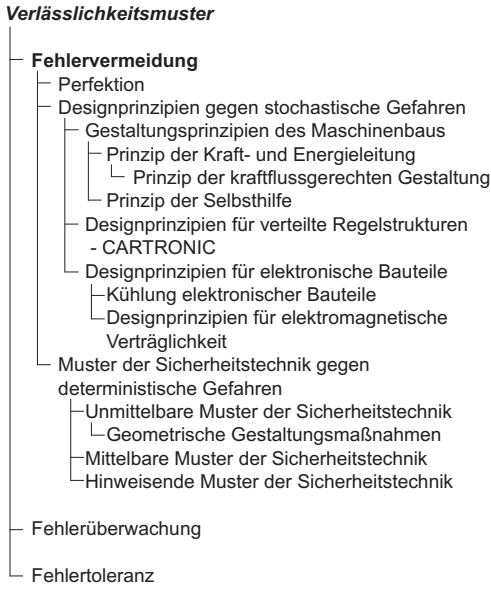


Abbildung 5.5: Verlässlichkeitsmuster zur Fehlervermeidung

ßerdem gehören auch Verriegelungen und andere Zuhaltungsmechanismen zu den mittelbaren Konzepten.

- Erst wenn die zuvor beschriebenen Konzepte nicht umzusetzen sind, werden Verlässlichkeitsmuster der *hinweisenden Sicherheitstechnik* verwendet. Diese informieren in statischer oder dynamischer Form über die verbliebenen Gefahren. Statische Muster der hinweisenden Sicherheitstechnik sind z. B. Bedienungsanleitungen, Schilder und Markierungen, während Beispiele für dynamische Muster in diesem Kontext Licht- oder akustische Signale sein können.

Abbildung 5.5 zeigt eine Baumstruktur aller im Anhang hinterlegten Verlässlichkeitsmuster zur Fehlervermeidung. Selbstverständlich erhebt diese Darstellung keine Ansprüche auf Vollständigkeit, sondern stellt lediglich eine exemplarische Auswahl dar.

5.2.2 Fehlerüberwachung

Die Verlässlichkeitsmuster der Fehlerüberwachung erkennen und diagnostizieren Fehlerzustände und leiten gegebenenfalls erste Maßnahmen ein. Sie unterteilen sich daher in die Kategorien *Fehlererkennung*, *Fehlerdiagnose* und

Fehlerbehandlung. Die Fehlererkennung beinhaltet dabei *nur* die Möglichkeit, Abweichungen vom Soll-Wert zu identifizieren, z. B. durch klassischen Parametervergleich, Paritätsgleichungen oder Plausibilitäts-Checks. Kommt neben dem Wissen um Abweichungen noch Wissen über das Fehlerverhalten hinzu, so kann die Abweichung durch Muster der Fehlerdiagnose, z. B. durch beschreibende und modellbasierte Diagnoseverfahren, analysiert werden [Hei99]. Im Falle eines identifizierten Fehlers oder einer Abweichung vom Soll-Wert können Verlässlichkeitsmuster zur Fehlerbehebung oder -eingrenzung im Sinne resultierender Maßnahmen angewendet werden; ein Neustart des Systems, eine Reparatur oder ein Austausch sind Beispiele dafür. Ein Muster in diesem Bereich ist ebenfalls die Systemdegradation, die das Einschränken der Funktionalität des Systems oder einzelner Komponenten beschreibt. Nachfolgend werden die drei genannten Unterkategorien für Verlässlichkeitsmuster der Fehlerüberwachung tiefergehend erläutert.

Fehlererkennung

Verässlichkeitsmuster der *Fehlererkennung* beschreiben die Möglichkeit, Fehler durch Abweichungen von Soll-Werten zu identifizieren, ohne dabei Wissen über das Fehlerverhalten zu besitzen oder zu benutzen. Resultat der Fehlererkennung ist somit die Beantwortung der Frage, "Liegt ein Fehler vor?", nicht aber die Beantwortung der Frage "Was für ein Fehler liegt vor?". Notwendig ist dafür folglich neben dem Ist-Verhalten lediglich das Wissen über das korrekte Soll-Verhalten, sodass durch Vergleich von diesen (mindestens) zwei Werten, vorgegebene Zusammenhänge geprüft werden können. Abweichende oder unzulässige Zusammenhänge gelten als Fehler. Gute Übersichten verschiedener Fehlererkennungsverfahren sind u. a. in [Mün06], [Ise06], [Ger98] und [LA90] beschrieben. Insbesondere die Möglichkeiten der modellbasierten Fehlererkennung werden anschließend weiter verdeutlicht. Beispiele und nachfolgend erläuterte Verlässlichkeitsmuster der *Fehlererkennung* sind daher Parametervergleich, Parameterschätzverfahren, Paritätsgleichungen und Plausibilitäts-Checks. Abbildung 5.6 zeigt das grundsätzliche Prinzip der Fehlererkennung.
Das Verlässlichkeitsmuster *Parametervergleich* stellt dabei die einfachste Form einer Fehlererkennung dar. Ein gemessener Parameter, der Ist-Wert, wird mit dem bekannten Parameter bei korrekter Funktion, dem Soll-Wert, verglichen. Es wird daher teilweise auch von *Fremdüberprüfung* bei diesem Muster gesprochen. Weichen diese Werte voneinander ab, Toleranzen können selbstverständlich berücksichtigt werden, so liegt ein Fehler vor. Stimmen sie überein, so funktioniert das System korrekt. Dieses Verlässlichkeitsmuster wird auch als *1v2 Voting* bezeichnet in dem Falle, dass der Soll-Wert durch einen zweiten redundanten Sensor ermittelt wird [Mah00].
Wird der gemessenen Wert nicht mit einem anderen fremden Wert verglichen,

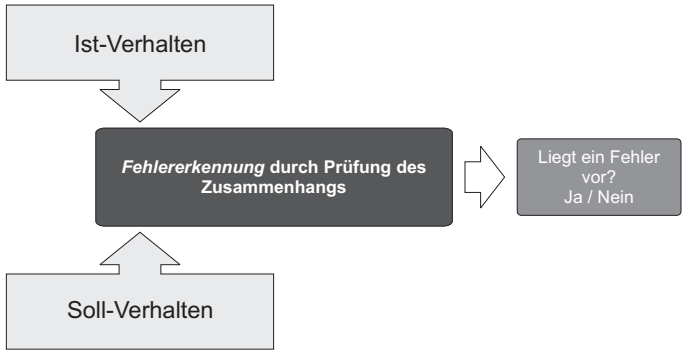


Abbildung 5.6: Prinzip der Fehlererkennung

sondern mittels *Eigenüberprüfung*, so beschreibt dieses Vorgehen bereits den Kernaspekt des Verlässlichkeitsmusters *Plausibilitäts-Check*, das auch *Sanity-Check* genannt wird. Dabei kann im Sinne der Fehlererkennung z. B. überprüft werden, ob sich der gemessene Wert innerhalb *plausibler* Grenzen befindet oder er im Vergleich zu anderen ermittelten Parametern *plausibel* ist. Die Ausprägung bzw. das Vorgehen für Plausibilitäts-Checks kann sich selbstverständlich in der Praxis wesentlich komplexer darstellen. Ein Beispiel für den Einsatz von Plausibilitäts-Checks ist das Sicherheitskonzept der elektrohydraulischen Bremse für ein Kraftfahrzeug nach [BK01].

Ein weiteres Verlässlichkeitsmuster, das den zuvor beschriebenen Parametervergleich erweitert, ist das *Parameterschätzverfahren* [FA04] [Ise06]. Hier kann der bzw. können die zu vergleichende(n) Parameter nicht direkt bestimmt oder gemessen werden. Daher werden z. B. die Ein- und Ausgangsgrößen des Systems oder Teilsystems bestimmt und deren Zusammenhang in einem parametrischen mathematischen Systemmodell nachgebildet. Diese *geschätzten Parameter* des Modells werden mit den Nominalwerten verglichen. Bei Abweichung wird auch bei diesem Muster ein Fehler unterstellt. Ausführliche Beschreibungen verschiedener Parameterschätzverfahren sind in [Ise06] erläutert. Ein Anwendungsbeispiel für die Überwachung einer linearen hydraulischen Servo-Achse ist in [Mün06] beschrieben.

Das Verlässlichkeitsmuster *Paritätsgleichungen* verwendet für die Fehlererkennung als Grundlage ein mathematisches Systemmodell mit bereits bekannten Parametern. Durch Einsetzen der gemessenen Ein- und Ausgangsgrößen kann ein Residuum zwischen gemessenen Parametern und den resultierenden Nominalwerten des Modells gebildet werden, das im Fehlerfall signifikant von 0 abweicht. Insbesondere für additive Fehler ist dieses Verfahren gut anwendbar [Ise06]. Weitere Ausprägungen dieses Verlässlichkeitsmuster sind ebenfalls in

[Ise06] dargestellt. Ein Anwendungsbeispiel anhand eines elektromechanischen Radbremsaktors wird in [FA04] erläutert, das die modellbasierte Fehlererkennung durch ein zweistufiges Konzept, bestehend aus Paritätsgleichungen und rekursiver Parameterschätzverfahren, realisiert.
Nachfolgend sind zur Konkretisierung der Verlässlichkeitsmuster zur *Fehlererkennung* exemplarisch spezielle Verfahren aufgezählt, die Fehler bei der Kommunikation und Vernetzung von Steuergeräten im Kraftfahrzeug erkennen sollen [BDM99]:

- Empfangsbestätigung bei der Kommunikation
- Vergleich durch redundante Architekturen
- Referenz-Checks, realisiert durch das Stellen einer Frage mit vorher bekannter Antwort
- Paritäts-Checks, realisiert durch Prüfung auf Geradzahligkeit
- Überwachung physikalischer Eigenschaften der Steuergeräte, wie z. B. der Temperatur
- Logische oder zeitliche Überwachung der Programmausführung
- Dynamische Kommunikation – ein eigentlich gleich bleibender Output wird in verschiedenen Arten zu verschiedenen Zeiten ausgegeben; z. B. wird jeder zweite Wert mit einem negativen Vorzeichen ausgegeben, obwohl der Wert gleich geblieben sein kann.

Fehlerdiagnose

Verlässlichkeitsmuster der *Fehlerdiagnose* beschreiben die Möglichkeit, die zur Fehlererkennung führenden Abweichungen als Symptome zu verstehen und darauf aufbauend den vorliegenden Fehler zu diagnostizieren. Wissen über das Fehlerverhalten ist im Gegensatz zur zuvor beschriebenen Fehlererkennung zusätzlich notwendig, um die Frage "Was für ein Fehler liegt vor?" beantworten zu können. Abbildung 5.7 zeigt das grundsätzliche Prinzip der Fehlerdiagnose, das Wissen über Ist-, Soll- und Fehlerverhalten benötigt. Der Vergleich von Ist- und Soll-Wert führt zur Fehlererkennung, während die Zuordnung einer potenziellen Abweichung, des so genannten Symptoms oder auch Residuums, zur Fehlerzuordnung und somit zur Fehlerdiagnose führt.
Die Fehlerdiagnose bzw. Fehlerzuordnung kann durch Interpretations- und Klassifikationsverfahren erfolgen, um den Fehler z. B. zu lokalisieren, zu bewerten oder sogar exakt zu identifizieren. Unterschieden wird bei wissensbasierter Diagnose z. B. zwischen beschreibenden und modellbasierten Verfahren

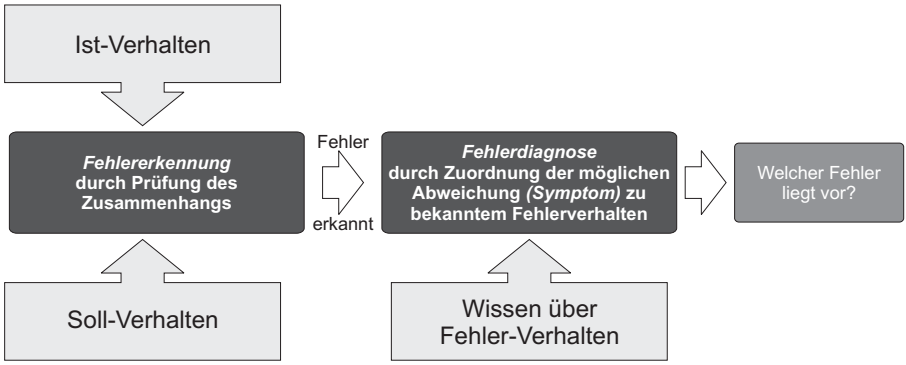


Abbildung 5.7: Prinzip der Fehlerdiagnose

gemäß [Hei99], siehe dazu auch Abbildung 5.8. Weitere Übersichten verschiedener Fehlerdiagnoseverfahren, teilweise inklusive Anwendungsbeispielen, sind in [Mün06], [Ise06] und [Ger98] beschrieben. Nachfolgend werden exemplarisch zwei Diagnoseverfahren kurz erläutert:

Regelbasierte Diagnoseverfahren [Hei99] gehören zur Kategorie der beschreibenden Methoden. Sie versuchen durch Anwendung geeigneter Regeln im detektierten Fehlerfall, eine Fehlerdiagnose zu erstellen. Dafür soll Wissen eines menschlichen Diagnoseexperten nachgebildet werden. Es werden Regeln angegeben, die theoretisches Wissen aber auch Erfahrungen und Daumenregeln widerspiegeln. Durch Anwendung dieser Regeln versucht nun das regelbasierte Diagnosesystem das beobachtete Systemverhalten zu erklären. Bei einer Vorwärts-Verkettung werden die Regeln auf die Anfangssymptome angewendet um eine so genannte Verdachtsdiagnose zu erstellen; bei der Rückwärts-Verkettung werden sie auf mögliche Ursachen angewendet um Symptome zu erklären.

Modellbasierte Diagnoseverfahren mit dem Prinzip der Widerspruchsfreiheit [Hei99] überprüfen Widersprüche zwischen Modell und technischem System. Die modellbasierte Diagnose allgemein betrachtet, vergleicht den tatsächlichen Zustand eines Systems mit dem Sollzustand eines Verhaltens- oder Strukturmodells. Treten Widersprüche auf, so beinhaltet diese Erkenntnis bereits das Wissen, dass ein Fehler vorliegt. Für die Fehlerdiagnose kann dann auf das Prinzip der Widerspruchsfreiheit zurück gegriffen werden, indem versucht wird, das Modell so anzupassen, dass beide Zustände wieder gleich sind; durch die Kenntnis bzgl. der Anpassung des Modells kann dann auf die Fehlerursache geschlossen werden. Das Prinzip der Widerspruchsfreiheit versucht somit eine Fehlerdiagnose zu erstellen, in dem es durch Anpassung des Modells Wider-

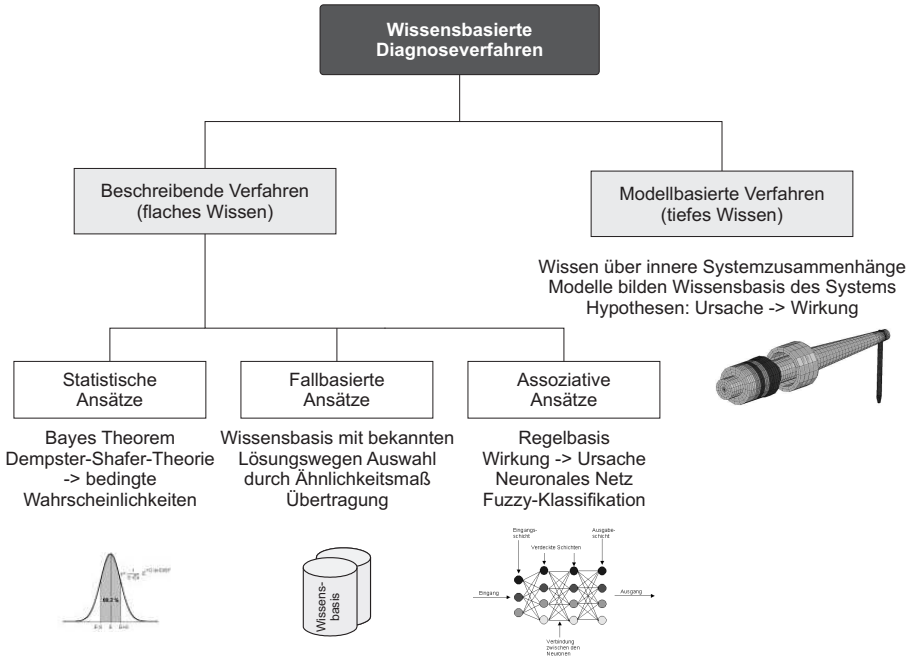


Abbildung 5.8: Strukturierung und Beispiele für Diagnoseverfahren

sprüche auflöst und damit erklären kann.

Resultierende Maßnahmen

Nachdem Fehler erkannt und evtl. auch diagnostiziert werden konnten, dienen Verlässlichkeitsmuster für *Resultierende Maßnahmen* dazu, Fehler zu beheben oder zumindest einzugrenzen und damit beherrschbarer zu machen; z. B. durch Systemdegradation, Neustart, Reparatur oder den Austausch von Komponenten. Theoretisch könnten auch die Muster der Fehlertoleranz unter diesem Aspekt subsumiert werden, da sie teilweise Muster darstellen, die automatisch die resultierenden Maßnahmen einleiten und somit fehlertolerantes Verhalten gewährleisten. Die Unterscheidung im Sinne der vorliegenden Arbeit basiert demgegenüber darauf, dass bei den Verlässlichkeitsmustern der Fehlerbehebung der Funktionsausfall zumindest zeit- oder teilweise durchaus eintritt. Diese Ausfallzeiten resultieren sowohl aus Instandhaltungs-, Neustart- und Reparaturdauern als auch aus Zeiten, in denen der funktionale Systemumfang bewusst reduziert wird und somit nicht vollständig zur Verfügung steht. Da ein Verständnis der Verlässlichkeitsmuster z. B. für Instandhaltung, Systemneustart oder Reparatur vorausgesetzt werden kann, wird nachfolgend lediglich das Muster der Systemdegradation inkl. der unterlagerten Degradationsstufen dargestellt.
Das Verlässlichkeitsmuster *Systemdegradation* beschreibt das Einschränken der Funktionalität des Systems oder einzelner Komponenten. Je nach Umfang der Degradation kann zwischen den Konzepten *Fehlerpassiv*, *Fehlersicher* und *Fehleroperativ* unterschieden werden, wobei der Aufwand, um sichere Systemzustände zu erreichen, mit der angegebenen Reihenfolge ansteigt [Ise06]:

- Das Degradationskonzept *Fehlerpassiv*, englisch mit Fail-silent bezeichnet, beschreibt die resultierende Maßnahme, dass ein Teilsystem oder eine Komponente nach einer Fehlererkennung in einen passiven Zustand versetzt wird. Dieses passiv geschaltete Teilsystem reduziert zwar die Funktion des Gesamtsystems, beeinflusst in diesem Zustand aber keine anderen Komponenten negativ, sodass die Gesamtsystemsicherheit gewährleistet bleibt.

- Das Degradationskonzept *Fehlersicher*, im Englischen und häufig auch im Deutschen mit Fail-safe bezeichnet, beschreibt die resultierende Maßnahme, dass direkt nach der Erkennung eines Fehlers ein sicherer Zustand für das Gesamtsystem erreicht werden muss. Kann dieses direkte Erreichen eines sicheren Zustands nur durch eine besondere Aktion realisiert werden, eine Aktion die über ein normales Abschalten der Energie hinaus geht, so ist diese Maßnahme zwar noch Inhalt dieses Konzepts, wird aber durch den erweiterten Begriff *Aktives Fail-safe* kenntlich gemacht.

Bekannte Beispiele für Fail-safe-Systeme im Kraftfahrzeug sind gemäß [Ise02] u. a. das Anti-Blockier-System und das Elektronische Stabilitätssystem.

- Das Degradationskonzept *Fehleroperativ*, englisch mit Fail-operational bezeichnet, beschreibt die resultierende Maßnahme, die Betriebsfähigkeit des Systems nach einer Fehlererkennung zu gewährleisten. Dies ist dann erforderlich, wenn kein sicherer Zustand existiert, der direkt erreicht werden könnte, wie z. B. bei einem sich in der Luft befindenden Flugzeug. Diese Degradationsstufe kann selbstverständlich auch bereits als Bestandteil der Verlässlichkeitsmuster für Fehlertoleranz angesehen werden.

Abschließend und zur weiteren Verdeutlichung von Verlässlichkeitsmustern für *Resultierende Maßnahmen* folgt eine Aufzählung von Fehlerbehandlungsverfahren, die bei der Kommunikation und Vernetzung von Steuergeräten im Kraftfahrzeug verwendet werden nach [BDM99]:

- Redundanz (siehe Fehlertoleranzmuster)
- Herunterfahren von Systembestandteilen
- Herunterfahren des gesamten Elektroniksystems
- Sicheren Park-Status erreichen
- Im Fehlerstatus bleiben (kein Konzept, sondern es dient der Vollständigkeit der Aufzählung)
- Fehlerbehebung durch Reset
- Fehlerbehebung durch Reparatur oder Wartung, z. B. durch das Abschleifen von Kontakten um den elektrischen Widerstand zu reduzieren
- Strategieänderung

Abbildung 5.9 zeigt eine Baumstruktur aller im Anhang hinterlegten Verlässlichkeitsmuster zur Fehlerüberwachung. Ebenso wie bei den Mustern der Fehlervermeidung erhebt diese Darstellung keine Ansprüche auf Vollständigkeit, sondern stellt lediglich eine exemplarische Auswahl dar.

5.2.3 Fehlertoleranz

Die Verlässlichkeitsmuster der *Fehlertoleranz* beschreiben Konzepte, die trotz eines Fehlers die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten und damit Ausfälle vermeiden [VDI88]. Die Aussage, dass alle Methoden der Fehlertoleranz auf Redundanz basieren, gemäß

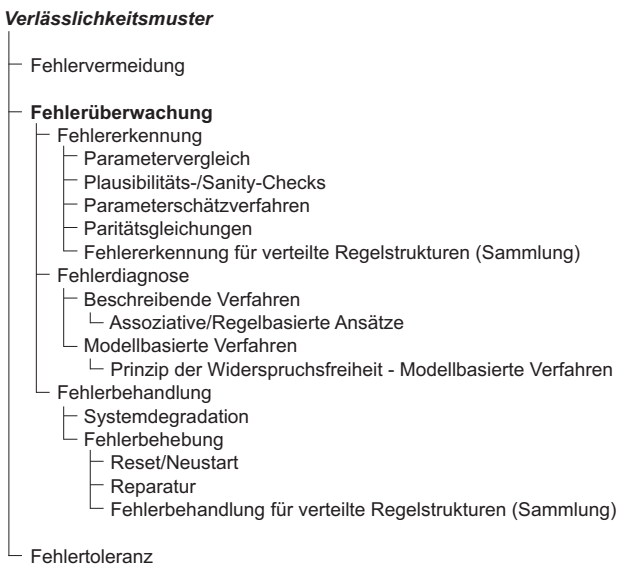


Abbildung 5.9: Verlässlichkeitsmuster zur Fehlerüberwachung

[Sto96], beschreibt das Verständnis von Redundanz innerhalb dieser Arbeit: Das System wird durch Redundanz komplexer, als es zur einfachsten Funktionsausübung erforderlich wäre, mit dem Ziel Fehler zu tolerieren. Die Art, in der das System komplexer entwickelt wird, beschreibt den Redundanztyp, der in verschiedensten Formen realisiert werden kann.

Diese Sichtweise wird auch durch [VDI00] unterstützt, in dem das Vorhandensein von mehr als für die geforderte Funktion notwendigen Mitteln als Redundanz bezeichnet wird. Außerdem werden Redundanzkonzepte so beschrieben, dass durch ihre Anwendung eine Betrachtungseinheit die geforderte Funktion auch bei einer begrenzten Anzahl von Ausfällen weiterhin ausführen kann; sie ist dann als ausfalltolerant zu bezeichnen. Anhand der dafür verwendeten Mittel, z. B. zusätzliche Verfahren, Maßnahmen und technische Einrichtungen, bestimmt sich die Art der Redundanz.

Der Redundanz-Typ, bzw. die Strukturierung dieser Verlässlichkeitsmuster in der vorliegenden Arbeit, basiert auf zwei Sichtweisen: Zum einen lassen sich die Konzepte anhand der Struktur der redundanten Einheiten oder Mechanismen unterscheiden und zum anderen anhand des Typs der verwendeten Diversität. Während erstgenannte Sichtweise Muster wie Duplex-, Triplex- und Duo-Duplex-Strukturen betrachtet, unterscheidet die Diversität Muster durch die Unterschiedlichkeit der zu vergleichenden oder redundant auftretenden Kom-

ponente o. Ä.; z. B. durch Hardware-, Software-, Informations- oder Temporale Redundanz. Weitere Möglichkeiten zur Strukturierung von Fehlertoleranzmustern werden in [AHKSC02] erläutert.

Redundanzstrukturen

Verlässlichkeitsmuster durch *Redundanzstrukturen* gewährleisten fehlertolerantes Verhalten dadurch, dass Einheiten mehrfach vorhanden sind, diese sich gegenseitig kontrollieren können und sich das System im Fehlerfall durch Mehrheitsvotum oder Rekonfiguration weiterhin korrekt verhält. Nachfolgend sind einige Beispiele verschiedener redundanter Strukturen erläutert, deren exemplarischen Architekturkonzepte in Abbildung 5.10 dargestellt sind.

- *Statische Redundanz* bedeutet, dass die redundante Einheit dauernd als aktive Reserveeinheit mitläuft; eine identifizierte fehlerhafte Einheit kann entweder nicht oder nur am Ein- oder Ausgang abgeschaltet werden. Häufig wird durch *Mehrheitsvotum* die fehlerhafte Einheit nicht berücksichtigt [Ise06]. Dieses Konzept wird auch als *Funktionsbeteiligte Redundanz* bezeichnet, bei der alle Mittel an der Erfüllung der geforderten Funktion beteiligt sind [VDI00].

- *Dynamische Redundanz* bedeutet, dass die redundante Einheit im fehlerfreien Fall keine Aufgabe hat; sie ist also eine passive Reserveeinheit. Erst im Fehlerfall erfolgt eine Umschaltung auf die fehlerfreie Einheit. Dabei wird dieses Muster weiter unterteilt in *Hot-stand-by*, d. h. dass die passive Reseerveeinheit für sich selbst aktiv ist, und in *Cold-stand-by*, d. h. dass die passive Reserveeinheit im fehlerfreien Fall nicht selbst aktiv ist. Zur Verdeutlichung: Bei einer Hot-stand-by-Struktur ist die Reserveeinheit selbst zwar aktiv, jedoch im fehlerfreien Systemzustand nicht an der Systemfunktionalität beteiligt; bei einer Cold-stand-by-Struktur ist die Reserveeinheit selbst nicht aktiv und ebenfalls nicht an der Systemfunktionalität beteiligt [Ise06]. Das Konzept der Dynamischen Redundanz wird auch als *Nicht funktionsbeteiligte Redundanz* bezeichnet, bei der die zusätzlichen Mittel erst bei Störung bzw. Ausfall die geforderte Funktion übernehmen [VDI00].

- Die *Duplex-Redundanzstruktur* entspricht dem Parametervergleich zweier Komponenten zur Fehlererkennung, siehe Kapitel 5.2.2. Sie hat allerdings den Zusatz, dass *harte Fehler*, z. B. ein Kurzschluss, bereits durch den Vergleich lokalisiert werden können. Dadurch kann die Duplex-Struktur fehlertolerantes Verhalten erreichen, wenn sie gemäß der zuvor erläuterten dynamischen Redundanz entworfen wird [Stö00] [Ise06].

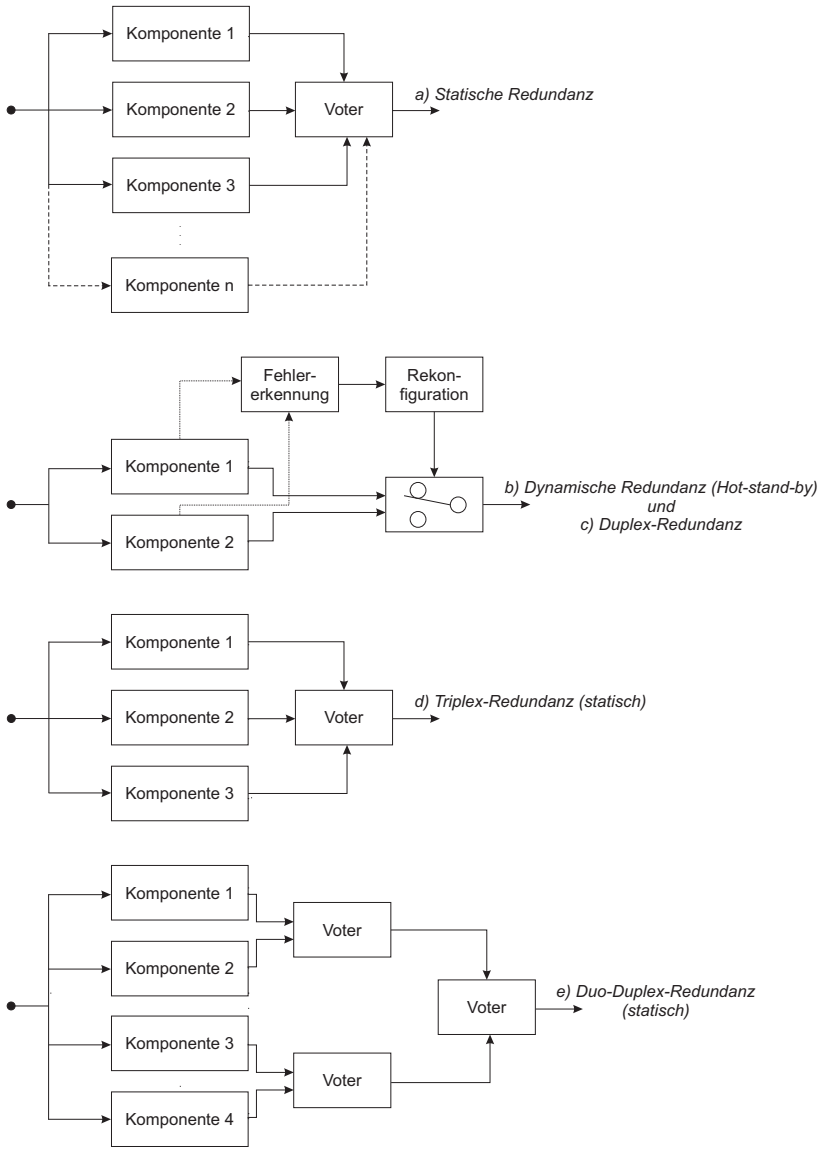


Abbildung 5.10: Architekturkonzepte verschiedener Redundanzstrukturen nach [Ise06]

- Die Redundanzstruktur *Triplex*, die auch als *3v2 Voting* und international als *Triple Modular Redundancy* bekannt ist, bezeichnet eine dreikanalige Struktur redundanter Komponenten, deren Outputs von einem Voter nach dem Mehrheitsprinzip verglichen werden. Im Fehlerfall einer Komponente kann der Fehler erkannt, lokalisiert und die fehlerhafte Komponente aus der Struktur durch Rekonfiguration ausgeschlossen werden. Durch den Ausschluss bleibt eine zweikanalige Struktur bestehen, die die Funktionsfähigkeit des Systems gewährleisten kann und Fehler weiterhin erkennt. Lediglich die fehlertolerante Eigenschaft ist dann nicht mehr, bzw. nur noch im Sinne der Duplex-Struktur vorhanden [Stö00] [Mah00] [LA90]. Je nach implementierter Rekonfigurations-Strategie kann die Triplex-Redundanz statisch oder dynamisch realisiert werden.
- Die *Duo-Duplex-Redundanz* beinhaltet vier redundante Komponenten, die jeweils zwei Duplex-Systeme bilden. Im Falle der Abweichung innerhalb einer Duplex-Einheit, wird diese als fehlerhaft betrachtet. Das fehlertolerante Verhalten entspricht der Triplex-Struktur [Stö00]. Gemäß [Ise06] sind die Wahrscheinlichkeiten eines Totalausfalls von Triplex- und Duo-Duplex-Systemen annähernd gleich.

Beispiele für die Umsetzung unterschiedlicher Redundanzkonzepte sind in [BK01] erläutert: Für das *Anti-Blockier-System* dient die konventionelle Bremse als redundante Rückfallebene, die als statische bzw. funktionsbeteiligte Redundanz fungiert; diese Rückfallebene ist allerdings nicht so sicher wie die usprüngliche Funktionsebene. Bei der *Elektro-Hydraulischen Bremse* wird im Fehlerfall eine direkte hydraulische Verbindung zwischen Bremspedal und den Bremsaktoren aktiviert; d. h. dass dann der Kraftfluss hierüber geleitet wird. Diese Anordnung entspricht der dynamischen bzw. nicht funktionsbeteiligten Redundanz in der Cold-stand-by-Ausprägung. Das *Elektro-Mechanische Bremssystem* besitzt keine mechanische Rückfallebene mehr, sondern besitzt u. a. eine fehlertolerante Duo-Duplex-Architektur.

Diversitäre Redundanz

Die *Diversitäre Redundanz* beschreibt die Redundanz nicht durch strukturelle Darstellungen, sondern mittels der Ungleichartigkeit der verwendeten Mittel. Diese können z. B. andere physikalische Prinzipien, andere Lösungswege der gleichen Aufgabe oder andere Aufbauweisen sein [VDI00]. Anhand der Ausprägung der Diversität bestimmt sich die Art der diversitären Redundanz. Nachfolgend werden exemplarisch für diese Kategorie der Verlässlichkeitsmuster die Hardware-, Software-, Informations-, Temporale und Kinematische Redundanz erläutert.

- Die *Hardware-Redundanz* beschreibt den Typus Redundanz, der wahrscheinlich dem verbreitetsten Verständnis von Redundanz entspricht. Zusätzliche diversitäre Hardware, häufig in Komponentenform, wird eingesetzt, um im Fehlerfall die Funktionalität weiterhin gewährleisten zu können [Sto96]; z. B. durch zusätzliche Sensoren mit anderem Funktionsprinzip, Zwillingsreifen bei Lastkraftwagen, auf die unterschiedliche Belastungen wirken, oder auch dem zweiten vorhandenen Leuchtmittel in Tageslichtprojektoren, das die Hardware-Diversität durch Einsatz- und Herstellungsunterschiede vorweisen kann.

- Bei der *Software-Redundanz* gewährleistet zusätzliche Software die Fehlertoleranz. Dies kann einerseits dadurch realisiert werden, dass Softwarebausteine für Fehlererkennung, -diagnose und -behebung hinzugefügt werden; andererseits dadurch, dass Softwarekomponenten der eigentlich gleichen Funktionalität eingesetzt werden, die allerdings *unterschiedlich*, d.h. auch möglichst unabhängig, entworfen wurden. Dieses unterschiedliche Entwerfen wird auch N-Version-Programmieren genannt und kann verschiedene Ausprägungen dadurch annehmen, dass z. B. unterschiedliche Entwicklungswerkzeuge, Spezifikationssprachen, Entwicklungsteams etc. eingesetzt werden [LA90] [Sto96].

- Die *Informationsredundanz* bedeutet das Verwenden zusätzlicher Informationen zur Gewährleistung der Fehlertoleranz. Diese zusätzlichen Informationen sind dann z. B. durch Verwendung von Checksummen und Korrektur-Codes anstelle der ursprünglichen Informationen diversitär. Häufigen Einsatz findet dieses Muster bei der Kommunikationtechnik [Sto96].

- Die *Temporale Redundanz* gewährleistet durch zusätzliche Zeit fehlertolerantes Verhalten. Zeitliche Redundanz ermöglicht z. B. das Wiederholen und Vergleichen von Berechnungen oder unterstützt auch bei der Kommunikation [Sto96].

- Die *Kinematische Redundanz* ermöglicht fehlertolerantes Verhalten dadurch, dass z. B. eine Ziel-Position von einem mehrgelenkigen Greifer durch unterschiedliche Gelenkstellungen erreichbar ist. Fällt ein Gelenk aus, d. h. wird eine kinematische Bewegung fixiert, so kann die Funktion trotzdem noch größtenteils erfüllt werden [Koc01].

In [DGOS03] ist ein Umsetzungsbeispiel für diversitäre Redundanz an einem Lenkwinkelgeber erläutert. Dieses verdeutlicht noch einmal die Anwendung der Diversitätskonzepte ebenso wie das Zusammenwirken mit den zuvor erläuterten Redundanzstrukturen. Abschließend zeigt Abbildung 5.11 wiederum

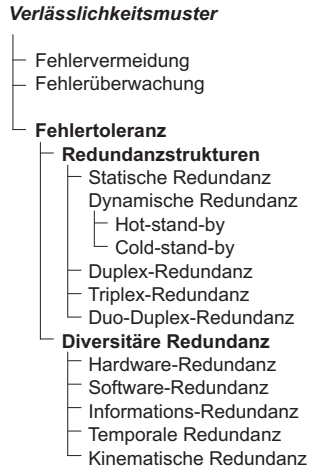


Abbildung 5.11: Verlässlichkeitsmuster für Fehlertoleranz

eine Baumstruktur exemplarischer Verlässlichkeitsmuster der Fehlertoleranz, die im Anhang hinterlegt sind.

5.3 Datenbank für Verlässlichkeitsmuster

Zur Verwendung der Verlässlichkeitsmuster in der Konzipierungsphase wird eine Datenbank entwickelt, die die klassische Idee der Konstruktionskataloge, siehe [Rot94], erweitert. Die Idee systematischer Lösungssammlungen bzw. der dahinter stehenden Muster, wird mit den Möglichkeiten verknüpft, die die Informationstechnologie durch Datenbanken bereitstellt. Dies sind zur Umsetzung der *Methodik der Verlässlichkeitsmuster* insbesondere die Vorteile bzgl. ständiger Erweiterungsmöglichkeiten, veränderbarer Darstellungen und mehrerer Suchfunktionalitäten; letztere z. B. mittels der hierarchischen Baumstruktur der Verlässlichkeitsmuster, der Volltextsuche oder direkt ausführbarer Verweise auf verwandte Muster. Vergleichbare Ansätze für Sammlungen von Mustern bzw. Maßnahmen beschreiben z. B. [AHKSC02] oder [Göh05]. Nachfolgend werden die Entwicklung bzw. Architektur und die Funktionalität der Datenbank erläutert.

5.3.1 Architektur der Datenbank

Für die Umsetzung der *Datenbank für Verlässlichkeitsmuster* wurde das relationale Datenbanksystem *MySQL* ausgewählt, auf das mittels der entwickel-

ten Benutzersoftware, realisiert durch die *Java 2 Plattform, Standard Edition (J2SE)*, zugegriffen werden kann. Die Datenbank-Architektur und die entwickelte Benutzersoftware, die allgemein auch als Datenbank-Client bezeichnet wird, werden im Folgenden nur kurz dargestellt, da die eigentliche Umsetzung des Systems selbst keinen Forschungscharakter besitzt und daher auch nicht im Fokus der vorliegenden Arbeit steht.
MySQL ist ein freies Datenbanksystem (Open-Source-Lizenz), das zwar nicht die Funktionsfülle kommerzieller Datenbanksysteme erreicht, dafür aber zuverlässig und schnell funktioniert und daher für die Ziele der vorliegenden Arbeit gut geeignet ist. Die Daten von MySQL Systemen werden in Tabellen strukturiert; die Tabellen wiederum haben Verweismöglichkeiten untereinander. Diese Verknüpfungen werden als *Relationen* bezeichnet, sodass man bei MySQL von einem *relationalen Datenbanksystem* spricht. Weitere relationale Datenbanken wären z. B. Oracle und IBM DB2 [Kof01].
Für die Datenbank für Verlässlichkeitsmuster werden fünf Tabellen angelegt, die die nachfolgend beschriebenen Datensätze beinhalten:

- Tabelle *"muster"* beinhaltet die für jedes Muster unbedingt notwendigen Daten. Dies sind der Primärschlüssel (id), den das Datenbanksystem fortlaufend vergibt, der Name des Verlässlichkeitsmusters (name) und die zugehörige Kurzbeschreibung (beschreibung_kurz). Der Primärschlüssel wird für die Relationen mit allen anderen Tabellen verwendet und wird daher nur an dieser Stelle erwähnt sowie bei der nachfolgenden Erstellung der Baumstruktur. Bei den anderen Tabellen wird er als Fremdschlüssel bezeichnet.

- Tabelle *"baumstruktur"* beschreibt die Verbindungen zwischen ober- und unterlagerten Verlässlichkeitsmustern, die bei Datenbankrelationen auch anschaulich als Eltern und Kinder beschrieben werden. Umgesetzt wird dies dadurch, dass dem Fremdschlüssel (id) ein Vorgängermuster (parentid) zugewiesen wird. Die Relationen in dieser Tabelle führen letztendlich zur Baumhierarchie der Verlässlichkeitsmuster, da mehreren Mustern dasselbe Vorgängermuster zugeordnet werden kann.

- Tabelle *"info"* beinhaltet weitere optionale Beschreibungen, die das Verlässlichkeitsmuster näher erläutern. Im Detail sind das eine ausführliche Beschreibung (beschreibung_lang), Literaturhinweise (lesenswert) sowie Autor (autor) und Eingabedatum (datum).

- Tabelle *"images"* beinhaltet ebenfalls weitere optionale Beschreibungen; allerdings in Form von Bildern (image), die mittels einzutragendem Link hochgeladen werden können.

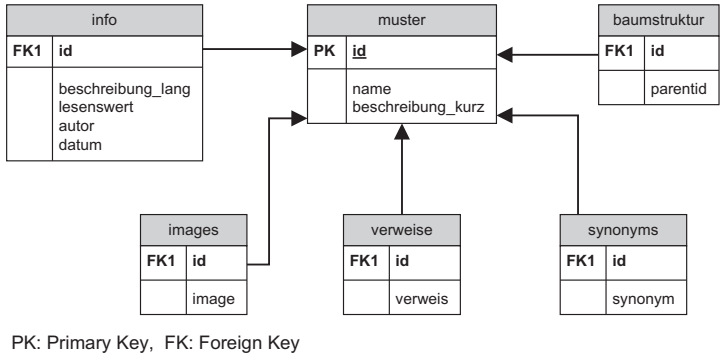


Abbildung 5.12: Schema der Datenbank für Verlässlichkeitsmuster, bestehend aus Tabellen und Relationen

- Tabelle *"verweise"* beinhaltet Verbindungen (verweis) zu assoziierten Verlässlichkeitsmustern.
- Tabelle *"synonyms"* beinhaltet Synonyme (synonym), die bei Bedarf eingetragen werden können, damit Doppeleinträge möglichst vermieden werden.

Das zugrunde liegende Datenbankschema für die *Datenbank für Verlässlichkeitsmuster* zeigt zusammenfassend noch einmal Abbildung 5.12.
Die Benutzersoftware für die Datenbank wurde, wie zuvor bereits erwähnt, mittels J2SE entwickelt. J2SE, mit Java als Programmiersprache, ist eine Ablaufumgebung und Sammlung von Programmierschnittstellen, um einerseits den Zugriff auf das Datenbanksystem zu realisieren und andererseits das Erstellen von Komponenten einer grafischen Benutzeroberfläche, engl. Graphical User Interface (GUI), zu unterstützen. Eine mögliche Oberflächen-Bibliothek in dieser Sammlung ist das hier verwendete Paket *Swing* [wik]. Das grafische Ergebnis der entwickelten Benutzeroberfläche zeigen die Screenshots in Abbildung 5.13.
Um die Verbindung von der Benutzersoftware zur Datenbank aufzubauen und diese zu verwalten wird die Datenbankschnittstelle der Java-Plattform, die *Java Database Connectivity (JDBC)* genutzt. Sie leitet die SQL-Anfragen von der Benutzersoftware an die Datenbank weiter, wandelt die Ergebnisse der Datenbank-Abfrage wiederum in eine für Java nutzbare Form um und stellt sie dem Programm zur Verfügung. JDBC bietet eine einheitliche Schnittstelle zu Datenbanken verschiedener Hersteller und ist speziell auf relationale Datenbanken wie MySQL ausgerichtet [wik]. Zusammenfassend zeigt Abbildung 5.14 die Umsetzung der Datenbank für Verlässlichkeitsmuster.

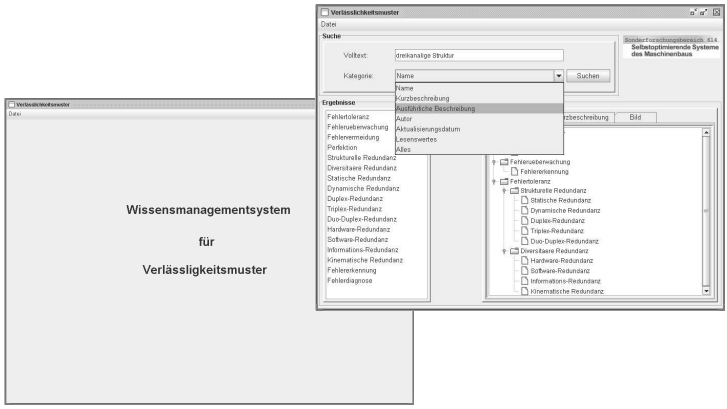


Abbildung 5.13: Screenshots der Benutzeroberfläche (GUI) der Datenbank für Verlässlichkeitsmuster

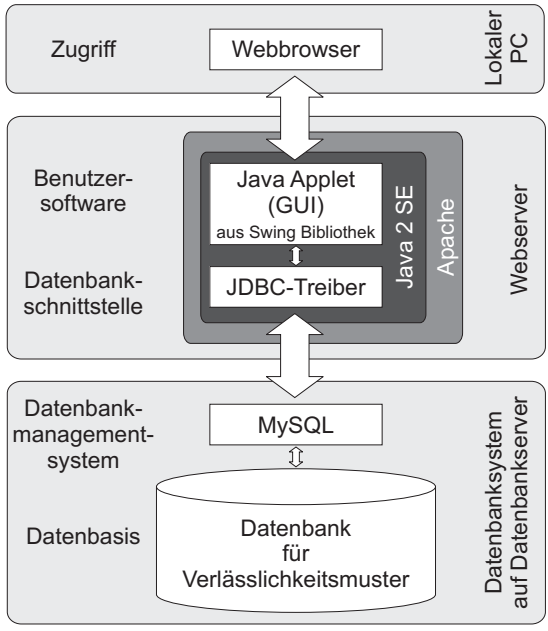


Abbildung 5.14: Umsetzung der Datenbank für Verlässlichkeitsmuster

5.3.2 Funktionalität der Datenbank

Die Funktionalität der *Datenbank für Verlässlichkeitsmuster* teilt sich auf in das *Erfassen bzw. Ändern von Verlässlichkeitsmustern* und in das *Suchen von Verlässlichkeitsmustern*. Letzteres durch die Navigation innerhalb der Datenbank mittels Strukturansicht (Darstellung der Datenbank bzw. der Verlässlichkeitsmuster in einer Baumansicht), Volltextsuche oder durch das Aufrufen der angegebenen Verweise zu assoziierten Verlässlichkeitsmustern. Um diese Funktionalitäten zu verdeutlichen, werden die nachfolgend beschriebenen Anwendungsfälle bzw. *Use Cases* verwendet. Ein Anwendungsfall, auch im Deutschen mit dem englischen Begriff Use Case bekannt, beschreibt die Interaktion zwischen Akteuren und dem betrachteten System [wik].

Use Cases für das *Erfassen bzw. Ändern von Verlässlichkeitsmustern*:

- *Verlässlichkeitsmuster erzeugen:* Um ein Verlässlichkeitsmuster neu zu erzeugen, vergibt der Benutzer einen Namen. Der entsprechende Eintrag wird in der Datenbank erfasst. Zusätzlich ist die Eingabe einer Kurzbeschreibung verpflichtend.

- *Beschreibungen eingeben:* Wurde ein Verlässlichkeitsmuster erzeugt oder auch ein bereits vorhandenes ausgewählt, kann der Benutzer verschiedene Beschreibungen zusätzlich eingeben. Die Beschreibung kann aus Text und gegebenenfalls einer hochladbaren Grafik bestehen. Sie unterteilt sich im Detail in die Kategorien Ausführliche Beschreibung, Grafik, Lesenswertes, Verweise, Synonyme, Autor und Aktualisierungsdatum.

- *Hierarchie anordnen:* Die Verlässlichkeitsmuster sind hierarchisch strukturiert. Die Einordnung des Verlässlichkeitsmusters in die Hierarchie wird durch Ziehen in das entsprechende Baumsteuerelement realisiert.

Use Cases für das *Suchen von Verlässlichkeitsmustern*:

- *Suche mittels Strukturansicht nach Verlässlichkeitsmustern:* Die Suche erfolgt durch Auswählen eines Verlässlichkeitsmusters aus der Baumstruktur.

- *Volltextsuche nach Verlässlichkeitsmustern:* Die Suche erfolgt durch Eingabe eines Textes, Wortes oder auch Datums. Dabei kann ausgewählt werden innerhalb welcher Kategorien gesucht werden soll (Name, Kurzbeschreibung, Ausführliche Beschreibung, Grafikennamen, Lesenswertes, Verweise, Synonyme, Autor, Aktualisierungsdatum). Die Suchergebnisse werden in alphabetischer Reihenfolge angezeigt.

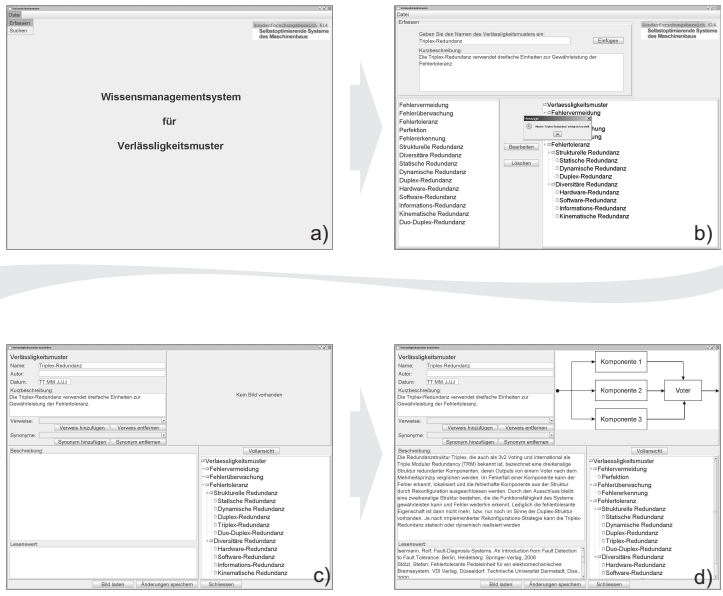
- *Suche mittels Verweisen nach Verlässlichkeitsmustern:* Die Suche erfolgt durch Auswählen eines Verweises, der selbst Bestandteil der Beschreibungskategorien eines anderen Musters sein kann.

- *Beschreibung anzeigen:* Nach dem Auswählen eines Verlässlichkeitsmusters in der hierarchischen Struktur, in der Liste der Suchergebnisse oder eines Verweises wird die Beschreibung des ausgewählten Verlässlichkeitsmusters in Form des Namens und der weiteren Beschreibungen (Kurzbeschreibung, Ausführliche Beschreibung, Grafik, Lesenswertes, Verweise, Synonyme, Autor und Aktualisierungsdatum) angezeigt.

Die Umsetzung dieser beiden Gruppen von Use Cases und damit auch die Funktionalität der *Datenbank für Verlässlichkeitsmuster* ist nachfolgend in den Abbildungen 5.15 und 5.16 exemplarisch verdeutlicht. Während die Abbildung 5.15 die Schritte des Erfassens eines neuen Verlässlichkeitsmusters beschreibt, zeigt Abbildung 5.16 das Recherchieren innerhalb der bestehenden Sammlung mittels Volltextsuche. Zusammenfassend bietet die Umsetzung der entwickelten Methodik für Verlässlichkeitsmuster durch ein Datenbanksystem einen schnellen und intelligenten Zugriff auf die bestehende Mustersammlung und eine einfache Möglichkeit, diese zu erweitern.

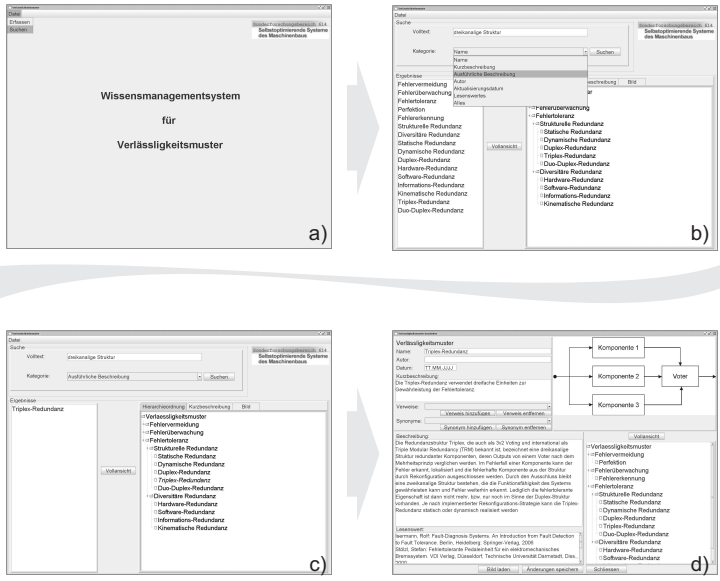
5.4 Zusammenfassung

Das Kapitel *Methodik der Verlässlichkeitsmuster* beschreibt im Sinne der normativen Studie der verfolgten Forschungsmethodik den Ansatz, durch Integration von wiederverwendbarem Verlässlichkeitsfachwissen in die Entwicklungsmethodik, die Entwicklungstätigkeiten zu verbessern. Gemäß der Forschungshypothese führt diese Verbesserung dann zu einer höheren Verlässlichkeit der zu entwickelnden Systeme.
Die Methodik beschreibt die Definition, Strukturierung und Wiederverwendung von Verlässlichkeitsmustern, die zur direkten Steigerung der Verlässlichkeit von mechatronischen Systemen genutzt werden können. Ein Verlässlichkeitsmuster beschreibt in diesem Sinne den Kern einer etablierten Lösung für gesteigerte Verlässlichkeit, der wiederum für spezifische Problemstellungen, teilweise in adaptierter Form, umgesetzt werden kann. Diese möglichst lösungsneutral beschriebenen Verlässlichkeitsmuster sind z. B. Designprinzipien, Diagnosealgorithmen oder Redundanzstrukturen. Sie repräsentieren vorhandenes Wissen, das u. a. durch eigene Entwicklungen oder auch Recherchetätigkeiten erlangt werden kann. Eine innerhalb dieser Arbeit entwickelte Strukturierung der Verlässlichkeitsmuster orientiert sich an den Eingriffsmöglichkeiten im Sinne der Fehlerkette (Fehlerursache – Fehlerzustand – Ausfall):



a) Der Menüpunkt "Erfassen" wird ausgewählt.
b) Im Fenster "Erfassen" wird durch Eingabe von Name und Kurzbeschreibung ein neues Verlässlichkeitsmuster erstellt.
c) Das Muster wird in die Baumhierarchie eingegliedert.
d) Weitere Beschreibungen, eine Abbildung, Literaturhinweise etc. werden hinzugefügt.

Abbildung 5.15: Screenshot-Abfolge zum Erfassen eines neuen Verlässlichkeitsmusters



a) Der Menüpunkt "Suchen" wird ausgewählt.
b) Im Fenster "Suche" wird durch Eingabe eines Textes und durch die Angabe, in welcher Beschreibungskategorie gesucht werden soll, eine Volltextsuche ausgelöst.
c) Das Sucherergebnis wird dargestellt.
d) Das Fenster der Vollansicht des Verlässlichkeitsmusters wird geöffnet.

Abbildung 5.16: Screenshot-Abfolge zum Recherchieren

- *Fehlervermeidung* beschreibt Verlässlichkeitsmuster, die die Fehlerursache, also den eigentlichen Fehler, bereits vor oder während der Entstehung verhindern.
- *Fehlerüberwachung* beschreibt Verlässlichkeitsmuster, die einen Fehlerzustand erkennen, diagnostizieren und gegebenenfalls daraufhin Maßnahmen einleiten.
- *Fehlertoleranz* beschreibt Verlässlichkeitsmuster, die trotz Ausfall von Teilsystemen die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten.

Neben dem Strukturierungskonzept dient die Entwicklung einer *Datenbank für Verlässlichkeitsmuster* dazu, eine Wiederverwendung der Muster innerhalb der Konzipierungsphase zu ermöglichen und die bestehende Sammlung zu erweitern. Die Funktionalität der auf MySQL basierenden Datenbank teilt sich daher in das *Erfasssen neuer Verlässlichkeitsmuster* anhand von Titel, Kurzbeschreibung, ausführlicher Beschreibung, Verweise und Grafiken und in das *Suchen von Verlässlichkeitsmustern* mittels der Baumstruktur, der Volltextsuche und Verweise.

6 Anwendungsbeispiel

In den beiden vorhergehenden Kapiteln wurde einerseits der entwickelte Verlässlichkeitsprozess dargestellt und andererseits die Methodik der Verlässlichkeitsmuster. Beide Ergebnisse stellen gemäß der verfolgten Forschungsmethodik aus Kapitel 1.3 Methoden dar, die entwickelt wurden, um Tätigkeiten im Entwicklungsprozess bzw. die Entwicklung selbst zu verbessern. Sie erfüllen daher das Vorgehen der Phase *Normative Studie*. Darauf aufbauend folgt die Phase *Deskriptive Studie 2*, die eine Evaluierung der Methoden hinsichtlich *Funktionalität* und *messbarem Erfolg* realisieren soll. Dies soll im vorliegenden Kapitel erreicht werden durch die Umsetzung an einem Entwicklungsprojekt mit Forschungscharakter. Zur Evaluierung der Funktionalität werden der Verlässlichkeitsprozess und die Methodik der Verlässlichkeitsmuster zur Entwicklung eines Spurführungsmoduls für ein autonomes Bahnfahrzeug angewendet und diese Anwendung daran anschließend analysiert. Die Evaluierung eines messbaren Erfolgs des Einsatzes erfolgt darauf aufbauend durch kritische Diskussion im Sinne eines Ergebnis-Reviews. Dort soll diskutiert werden, in wie weit das zu Beginn definierte messbare Erfolgskriterium *Verlässlichkeit steigern* erreicht wurde.

6.1 Spurführungsmodul des RailCabs

Das ausgewählte Anwendungsbeispiel bezieht sich auf die Entwicklung des Spurführungsmoduls eines neuen Bahnsystems namens *RailCab*, das auch bekannt ist unter dem Namen der *Neuen Bahntechnik Paderborn* [Lüc00] [Trä06a]: Das RailCab ist ein modulares Bahnsystem, das innovative Fahrwerkstechnologien der Mechatronik mit den Vorteilen des Transrapids und der Nutzung bestehender Bahntrassen vereint. Kleine führerlose RailCabs fahren bedarfsgesteuert ohne Zwischenstopps von individuell gewünschten Startpunkten zu individuell gewünschten Zielen. Abbildung 6.1 zeigt den modularen Aufbau eines RailCabs, inklusive des im Folgenden detaillierter betrachteten Spurführungsmoduls.
Die Hauptfunktion des Spurführungsmoduls ist das komfortable und richtungsgebende Führen des RailCabs, insbesondere bei der Durchfahrt einer *passiven Weiche*, die für einen Konvoibetrieb notwendig ist. Darüber hinaus realisiert das Modul noch die klassischen Fahrwerksfunktionen *Tragen des Fahrzeugs (in-*

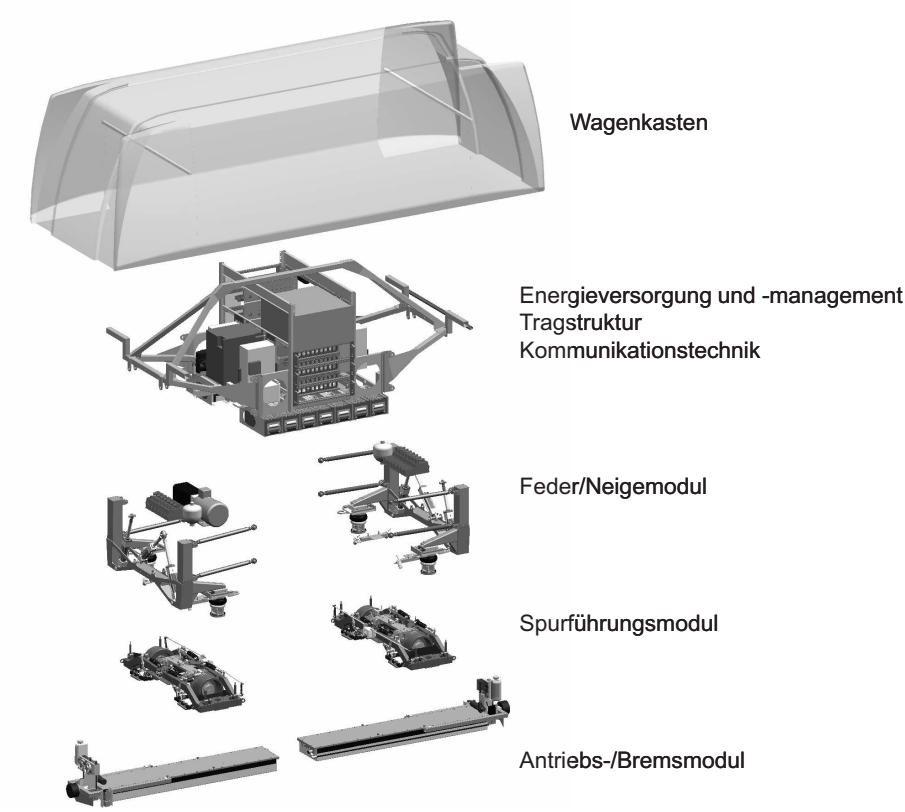


Abbildung 6.1: Modularer Aufbau des RailCabs [WMW06]

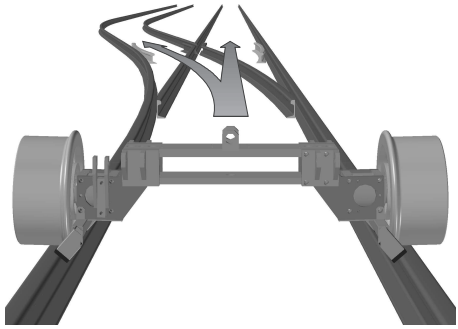


Abbildung 6.2: Passive Weiche, die den Konvoibetrieb von RailCabs ermöglicht [WMW06]

kl. der Spurführungskomponenten) und *Führen entlang der Schiene*, die durch Fahrwerksrahmen, Achse und Räder realisiert werden. Anstelle von klassischen Drehgestellen mit Starrachsen und konischem Radprofil werden beim RailCab Losradachsen mit zylindrischem Profil und eine aktive Spurführung eingesetzt. Die aktive Spurführung wird durch lenkbare Achsen und in einer Weiterentwicklung durch Verstellung des Radsturzes realisiert. In einem direkten Zusammenhang zur aktiven Spurführung steht die zuvor genannte *passive Weiche*, die für einen Konvoibetrieb notwendig ist, zusätzlich aber auch für die klassische Bahntechnik eine Alternative zur aktiven, umschaltbaren Weiche darstellt. In einer passiven Weiche erfolgt der Gleiswechsel durch aktive Lenkbewegung des RailCabs bzw. des Spurführungsmoduls. Die Richtungsentscheidung ist folglich von der Schiene auf das Fahrzeug verlagert worden. Abbildung 6.2 zeigt die passive Weiche, die keine beweglichen Teile mehr enthält [Trä06a] [WMW06].

Der konstruktive Aufbau des Spurführungsmoduls, sowie die Explosionsdarstellung der wichtigsten Baugruppen ist in Abbildung 6.3 dargestellt. Die Lenkbewegung der Achse gegenüber dem Tragrahmen wird durch einen Hydraulikzylinder realisiert, während Wirbelstromsensoren die Informationen zur Positionsbestimmung gegenüber dem Gleis ermitteln [MWEW05].

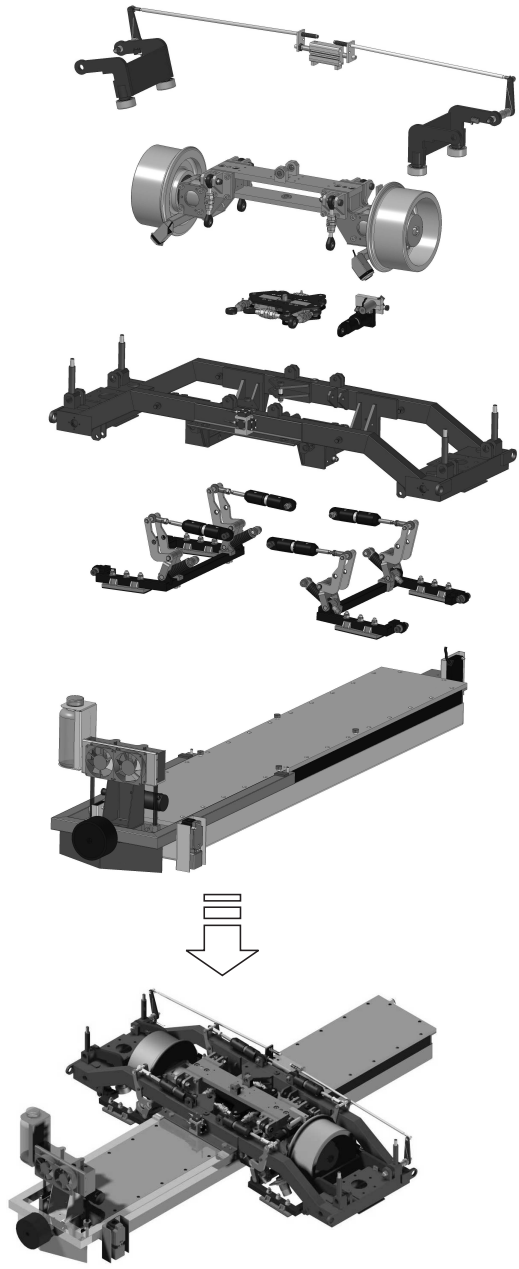


Abbildung 6.3: Spurführungsmodul in kompletter und in Explosionsdarstellung [WMW06] [Trä06a]

6.2 Anwendung des Verlässlichkeitsprozesses auf die Spurführung

Die Evaluierung des entwickelten Verlässlichkeitsprozesses und der darin integrierten Methodik der Verlässlichkeitsmuster wird im aktuellen Kapitel anhand des Spurführungsmoduls des RailCabs realisiert. Dazu werden neben den kurz dargestellten Ergebnissen der *Systemanalyse* gemäß des klassischen Entwicklungsvorgehens, insbesondere die Aktivitäten und Ergebnisse der einzelnen Prozessbausteine des Verlässlichkeitsprozesses erläutert. Dies sind im Detail *Anforderungsanalyse für Verlässlichkeit*, *Fehler-, Gefahren- und Risikenanalysen*, *Konzipierung und Entwurf der Verlässlichkeit* und *Verlässlichkeitsanalysen von Kooperation und Integration*. Der Fokus der vorliegenden Arbeit liegt dabei nicht auf der eigentlichen Entwicklung des Systems, sondern auf einer erfolgreichen Anwendung der verlässlichkeitsorientierten Entwicklungsmethodik.

6.2.1 Systemanalyse

Die notwendige Basis zur Durchführung des Verlässlichkeitsprozesses ist die *Systemanalyse*, die das zu entwickelnde System mindestens durch Funktionen beschreibt und strukturiert. Darüber hinaus ist die Beschreibung mittels Attributen und in späteren Realisierungsphasen auch mittels Komponenten sinnvoll. Daher sind nachfolgend diese drei Systembeschreibungen für das Spurführungsmodul des RailCabs dargestellt.

Funktionsbeschreibung

Die Hauptfunktion des Spurführungsmoduls kann durch *Komfortables Führen des Fahrzeugs in der Schiene, sowie richtungsgebendes und komfortables Führen in der passiven Weiche* beschrieben werden. Mit dem Begriff *komfortabel* ist die auf Fahrgäste oder Güter wirkende Kraft z. B. durch Stöße oder Fliehkräfte gemeint, dessen Reduzierung eine Hauptfunktion des Spurführungsmodul darstellt. Der Begriff *richtungsgebend* ist direkt mit dem Begriff der Weiche verknüpft und beinhaltet die Entscheidung, das Fahrzeug in der Weiche nach rechts oder links zu führen.
Von der Hauptfunktion ausgehend lassen sich einerseits die beiden klassischen Fahrwerksfunktionen *Tragen von Fahrzeug und Modulkomponenten* und *Führen entlang der Strecke* ableiten; andererseits können die im Sinne der aktiven Spurführung und des Konvoibetriebs relevanten Funktionen *Komfortables Führen in der Schiene und Weiche* und *Richtungsgebendes Führen in der passiven Weiche* bestimmt werden. Für das Forschungsvorhaben einer aktiven Spurführung sind die beiden letztgenannten Funktionen von hervorgeho-

bener Bedeutung und erfahren daher auch in den folgenden Ausführungen eine detaillierte Betrachtung. Die weiter unterteilten und konkretisierten Sub-Funktionsbeschreibungen zeigt Abbildung 6.4 durch die Funktionshierarchie des Spurführungsmoduls.

Komponentenbeschreibung

Da sich das Entwickungsvorhaben des aktiven Spurführungsmoduls bereits in einem fortgeschrittenem Stand befindet, kann das System neben der Funktionshierarchie auch durch die Komponenten beschrieben werden. Dazu wurde mittels des konstruktiven Entwurfs und der Architektur der Informationsverarbeitung bzw. der Kommunikationsstruktur eine Tabelle erstellt, die das System in dieser Hinsicht beschreibt. Zusätzlich wurden ebenfalls die zuvor identifizierten Funktionen zugeordnet. Tabelle 6.1 zeigt einen Ausschnitt des Ergebnisses der Komponentenbeschreibung inkl. der zugeordneten Funktionen. Die vollständige Übersicht ist im Anhang hinterlegt.

Attributsbeschreibung

Neben den beiden zuvor dargestellten Beschreibungsformen, die die Struktur eines Systems gut darstellen, kann zusätzlich noch eine Attributsbeschreibung weitere Informationen zur Verfügung stellen. Diese ermöglicht insbesondere für Verlässlichkeitsanalysen einen weiteren Blickwinkel auf das zu analysierende System. Attribute sind in diesem Kontext veränderbare Größen wie z. B. Drücke, Temperaturen oder auch Signale. Tabelle 6.2 zeigt die identifizierten Attribute des Spurführungsmoduls.

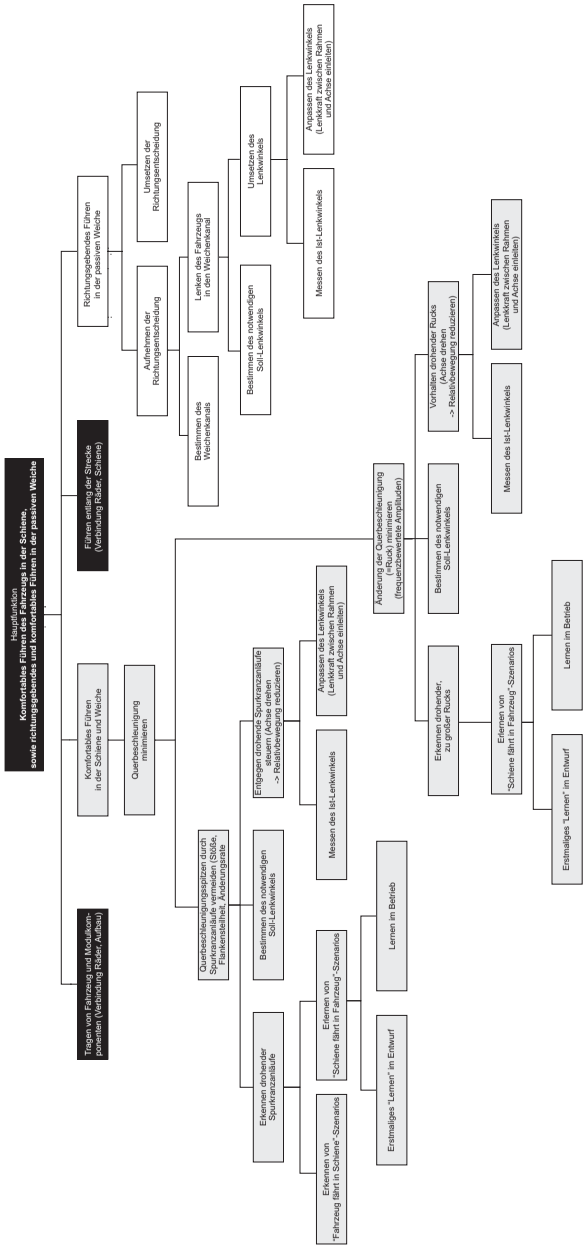


Abbildung 6.4: Funktionshierarchie des Spurführungsmoduls

Hauptkomponenten	Subkomponenten	Merkmal	Funktionen
Fahrwerkrahmen			Tragen von Fahrzeug und Modulkomponenten (Verbindung Räder, Aufbau)
		Tragstruktur	Tragen und Befestigung der Komponenten (inkl. Kraftaufnahme)
			Tragen des Aufbaus
		Druckluftspeicher	Zusatzvolumen für Luftfedern, da der Fahrwerkrahmen als Druckluftspeicher genutzt wird
Verbindungsgelenke			Tragen von Fahrzeug und Modulkomponenten (Verbindung Räder, Aufbau)
	Kugelgelenk (8x)		Kräfte übertragen; translatorische Bewegungen unterbinden
			Momente nicht übertragen; rotatorische Bewegungen ermöglichen
	Querfeder		Drehbewegung der Achse zulassen
	Verbindungsmutter inkl. Schraubensicherungslack		Kräfte übertragen
Achsmodul			Tragen von Fahrzeug und Modulkomponenten (Verbindung Räder, Aufbau)
			Führen entlang der Strecke (Verbindung Räder, Schiene)
	Tragstruktur Achse		Tragen und Befestigung der Komponenten (inkl. Kraftaufnahme)
		Neigungswinkel 1:40	Selbstzentrierung
	Räder	zylindr. Lauffläche	Tragen des Aufbaus
			Führen entlang der Strecke (Verbindung Räder, Schiene); Ermöglichen der translatorischen Bewegung (Fahrtrichtung)
		Spurkranz	Begrenzung der Querbewegung des Fahrzeugs (oder Räder) gegenüber den Schienen
	Lager		Axiales Fixieren der Räder
			Rotation der Räder ermöglichen

Tabelle 6.1: Resultat der Komponentenbeschreibung des Spurführungsmoduls (Ausschnitt)

Attribute
Kraft im Fahrwerksrahmen
Luftdruck in Feder
Kraft im Kugelgelenk
Translatorische Bewegungen im Kugelgelenk
Rotatorische Bewegungen im Kugelgelenk
Normalkraft auf Räder
Querkraft und -schlupf bei Rädern
Längskraft und -schlupf bei Rädern
Lagerreibung in Rädern
Rotation der Räder
Kraft des Lenkaktors
Weg des Lenkaktors
Signal der Spurführungssensoren
Öldruck
Geschwindigkeit Fahrzeug
Querbeschleunigung im Fahrwerk
Drehrate Fahrwerk
Gewicht Aufbau
Gewichtsverteilung
Reibbeiwert Rad-Schiene Kontakt
Seitenwind
Streckensteigung
Kurvenradius
Gleisüberhöhung
Temperatur
Luftfeuchtigkeit
Verschmutzungen
Abbiegewunsch (j/n)
Soll-Zustand (Lenkwinkel)
Ist-Zustand (Lenkwinkel)
Sensorsignal (Lenkzylinderlänge)
Fehlerinformationen
Position des Fahrzeugs (Querposition)
Position des Fahrzeugs (Längsposition)
Geschwindigkeit (virtueller Sensor)
Zylinderlänge Soll-Wert
Zylinderlänge Ist-Wert
Signal Längsposition
Signal Drehratensensor
Signal Querbeschleunigungssensor

Tabelle 6.2: Attribute des Spurführungsmoduls

6.2.2 Anforderungsanalyse

Da es sich beim RailCab um ein Forschungsprojekt handelt, existieren entsprechend auch keine direkt anwendbaren Normen. Trotzdem bietet z. B. die *Eisenbahn-Bau- und Betriebsordnung*, kurz EBO, eine Grundlage, um erste Anforderungsbereiche zu identifizieren [Bun06]: Die grundlegende Anforderung darin beinhaltet, dass Bahnanlagen und Fahrzeuge den detaillierteren Vorschriften der EBO entsprechen müssen sowie den anerkannten Regeln der Technik. Davon darf lediglich abgewichen werden, wenn mindestens die gleiche Sicherheit nachgewiesen wird. Exemplarisch sind nachfolgend ausgewählte Anforderungen aus der EBO aufgezählt, die einen direkten Bezug zur Funktionalität des Spurführungsmoduls besitzen:

- 18 t maximal zulässige Radsatzlast (Anteil des Gesamtgewichts des Fahrzeugs auf einen Radsatz)
- 5,6 t/m maximal zulässiges Fahrzeuggewicht je Längeneinheit
- Räder müssen Gleisbogen mit einem minimalen Radius von 150 m und einer Spurweite von 1 435 mm einwandfrei durchfahren können
- Räder dürfen auf der Radsatzwelle seitlich nicht verschiebbar sein (Ausnahmen für Spurwechselräder)

Eine weitere Quelle zur Identifikation von Anforderungen bzgl. der Verlässlichkeit stellt z. B. die *DIN EN 50126 "Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)"* dar. Durch die weiteren Aktivitäten dieses Prozessschrittes, der Analyse bzw. Strukturierung der identifizierten Anforderungen sowie der verifizierbaren Dokumentation, entsteht die erste und damit vorläufige Version der Verlässlichkeitsanforderungs-Checkliste, dargestellt in Tabelle 6.3. Diese wird kontinuierlich im Verlauf des Verlässlichkeitsprozesses erweitert; insbesondere im Anschluss an den Prozessbaustein *Fehler-, Gefahren- und Risikenanalysen.*

Komponente	Anforderungen
Spurführungsmodul	- Modul muss der *EBO* oder den anerkannten Regeln der Technik entsprechen; andernfalls Nachweis der mindestens gleichen Sicherheit - 18 t maximal zulässige Radsatzlast muss ermöglicht werden - 5,6 t/m maximal zulässiges Fahrzeuggewicht je Längeneinheit muss ermöglicht werden - Gleisbogen mit 150 m Radius und 1 435 mm Spurweite muss einwandfrei durchfahren werden - Kenntnisse über realistisch auftretende Betriebsbelastungen sind für Bahnfahrzeuge nicht bekannt; insbesondere stoßartigen Belastungen in wenigen Komponenten muss das Modul standhalten
Fahrwerksrahmen	- Überschlagsrechnungen bzgl. der Belastungen ergaben das Auftreten bis zur 50-fachen Erdbeschleunigung - Größere Löcher sollen erkannt werden (Funktion: Druckluftspeicher)
Verbindungsgelenke	- Dauerfeste Auslegung - Ausfall eines Kugelgelenks soll toleriert aber angezeigt werden; bei einem zweiten Ausfall soll eine Fail-Safe Aktion durchgeführt werden
Achsmodul	- Dauerfeste Auslegung der Achse; evtl. mit Wartungsintervallen kontrollieren - erwarteter Verschleiß der Radlaufflächen; größere Risse oder Brüche dürfen nicht toleriert werden bzw. sind schnell zu erkennen - Dauerfeste Auslegung der Spurkränze der Räder; Mindestdicke ist zu kennzeichnen - Räder dürfen nicht seitlich verschiebbar sein auf der Radsatzwelle - Dauerfeste Auslegung der Radlager; trotzdem sollte mögliches schleichendes Versagen erkannt werden - Fehlertolerante Auslegung des Inkrementalgebers durch Redundanz - Lenkaktor darf nicht dauerhaft ausfallen, ein Ausfall sollte sich ankündigen und der Aktor sollte austauschbar sein
Spurführungssensoren	- Ausfälle sollen erkannt werden
Informationsverarb.	- Ausfall darf nicht erfolgen

Tabelle 6.3: Vorläufige Verlässlichkeitsanforderungs-Checkliste des Spurführungsmoduls

6.2.3 Fehler-, Gefahren- und Risikenanalysen

Der Prozessschritt teilt sich auf in die Fehleranalysen zur Identifikation von Fehlern, in die Gefahrenanalyse zur Identifkation von gefährlichen Konsequenzen und in die Bewertung durch Risikenanalyse. Daher sind nachfolgend sowohl die Resultate als auch die gewählten Vorgehensweisen dazu erläutert.

Fehleranalysen

Für die Aktivitäten bzgl. der Fehleranalysen im Sinne der Fehleridentifikation wurden drei Vorgehensweisen bzw. Methoden ausgewählt und angewendet, deren Beschreibung bereits in Kapitel 2.3 enthalten sind: Zuerst wurde eine *Ausfallanalyse* entsprechend dem FMEA-Vorgehen anhand von Funktionsstruktur und Komponentenstruktur durchgeführt, woran sich eine *HAZOP-Analyse* anhand der Attributsbeschreibung des Systems anschloss. Danach wurde eine *Fehlerbaumanalyse* angefertigt, die neben der Identifikation von weiteren Fehlern, auch bereits Zusammenhänge zwischen bereits zuvor identifizierten Fehlern erkennen konnte. Ergebnis der Prozessaktivität *Fehleranalysen* ist eine Fehlerliste, die gemeinsam mit den aufgestellten Fehlerbäumen in Anhang C hinterlegt ist. Ein Ausschnitt der Fehlerliste ist in Tabelle 6.4 dargestellt.

Fehlerausfall/Fehlerzustand	Fehlerursache
Ausfall der Tragfunktion	Materialfehler, Auslegungsfehler, Missbrauch, Fertigungsfehler
Ausfall Tragstruktur	Materialfehler, Auslegungsfehler, Fertigungsfehler Überbelastung im Fahrwerksrahmen oder anderer Missbrauch
Ausfall Rad (tragende Funktion)	Materialfehler, Auslegungsfehler, Fertigungsfehler zu hohe Normalkraft auf Räder oder anderer Missbrauch
Ausfall Kugelgelenk	Verschleiß zu hohe Kraft im Kugelgelenk (Missbrauch) translatorische Bewegungen im Kugelgelenk (Missbrauch)
Ausfall Querfeder	Missbrauch, Materialfehler und -ermüdung
Ausfall Verbindungsmutter	mechanischer Missbrauch, Materialfehler,...
Ausfall Lager	Verschleiß, Schmutz, Missbrauch
Ausfall/Fehler der Sensorik	
Ausfall/Fehler Inkrementalgeber	Ausfälle in der Signalverarbeitungskette,... Falsches Signal Kein Signal Zu schlechtes Signal
Ausfall/Fehler Lenkaktorsensor	Ausfälle in der Signalverarbeitungskette,... Falsches Signal Kein Signal Zu schlechtes Signal
Ausfall/Fehler Wirbelstromsensor	Ausfälle in der Signalverarbeitungskette,... Falsches Signal Kein Signal Zu schlechtes Signal

Tabelle 6.4: Ausschnitt aus der Fehlerliste des Spurführungsmoduls als Resultat verschiedener zusammengeführter Fehleranalysen

Gefahrenanalyse

Die identifizierten Fehler werden bzgl. gefährlicher Konsequenzen analysiert. Tabelle 6.5 zeigt einen Ausschnitt des Ergebnisses der weiter reduzierten Gefahrenanalyse. Die Fehler- und Gefahrenliste ist im Anhang als Bestandteil der Tabellen C.5 bis C.8 abgebildet.

Fehlerausfall/-zustand/-ursache	Gefahren
Ausfall der Tragfunktion	
Ausfall Tragstruktur	
- Material-, Auslegungs-, Fertigungsfehler	Entgleisung, Umkippen des Fahrzeugs
Ausfall Rad (tragende Funktion)	
- Material-, Auslegungs-, Fertigungsfehler	Entgleisung, Umkippen des Fahrzeugs
Ausfall Kugelgelenk	
- Verschleiß	Schlingern, bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung
- zu hohe Kraft im Kugelgelenk	bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung
Ausfall Querfeder	
- Missbrauch, Materialfehler,...	leichtes Schlingern
Ausfall Verbindungsmutter	
- mech. Missbrauch, Materialfehler,...	Schlingern
Ausfall Lager	
- Verschleiß, Schmutz, Missbrauch	Blockieren des Rads
Ausfall/Fehler der Sensorik	
Ausfall/Fehler Lenkaktorsensor	
- Falsches Signal	Falsches Lenken und unkomfortables Führen
- Kein Signal	Lenken und komfortables Führen wird unmöglich
- Zu schlechtes Signal	Lenken und komfortables Führen eingeschränkt

Tabelle 6.5: Ausschnitt aus der Gefahrenliste des Spurführungsmoduls

Risikenanalyse

Für die nächste Prozessaktivität, die Risikobewertung wird die Methode der Risikomatrix angewendet, die bereits in Kapitel 2.3.3 vorgestellt wurde. Anhand von zwei Kriterien, die das Risiko beschreiben bzw. bewerten, kann ein Zuordnungs- und Klassifizierungsschema in Form einer Matrix erstellt werden. Die für die Achsen verwendeten Beurteilungskriterien, die dann durch Zuordnung zu den Risikoanforderungsklassen führen, sind die Häufigkeit (H) und die Auswirkung(A). Abbildung 6.5 zeigt die resultierende Risikomatrix inkl. der Kriterienausprägungen, während Tabelle 6.6 die Interpretationen der Risikoklassen bzw. den Umgang mit den Risiken beschreibt. Die verwendete Matrix als auch die Klasseninterpretationen entsprechen dem Vorgehen nach [DIN02], das bereits in Kapitel 2.3.3 beschrieben wurde.

		Auswirkung			
		katastrophal	kritisch	begrenzt	geringfügig
Häufigkeit	häufig	I	I	I	II
	wahrscheinlich	I	I	II	III
	gelegentlich	I	II	III	III
	gering	II	III	III	IV
	unwahrscheinlich	III	III	IV	IV
	nicht glaubhaft	IV	IV	IV	IV

Abbildung 6.5: Risikomatrix für das Spurführungsmodul gemäß [DIN02]

Risikoklasse	Interpretation
Klasse I	nicht tolerierbares Risiko
Klasse II	unerwünschtes Risiko, das nur tolerierbar ist, wenn eine Risikominderung nicht durchführbar ist oder die Kosten der Minderung unverhältnismäßig hoch im Vergleich zur erzielten Verbesserung sind
Klasse III	tolerierbares Risiko wenn die Kosten einer Risikominderung die erreichbare Verbesserung übersteigen
Klasse IV	vernachlässigbares Risiko

Tabelle 6.6: Interpretation der Risikomatrixklassen für das Spurführungsmodul gemäß [DIN02]

Das eigentliche Vorgehen dieser Prozessaktivität beinhaltet die Analyse jedes Fehlers bzw. der zugehörigen Gefahr anhand der gewählten Kriterien *Häufigkeit* und *Auswirkung* sowie anhand der dadurch resultierenden Zuordnung zu einer Risikoklasse. Letzteres bedeutet, dass zusätzlich zu der Bewertung der einzelnen Kriterien noch eine Überprüfung stattfindet, ob die resultierende Klasse und der damit empfohlene Umgang mit dem Risiko, auch tatsächlich plausibel sind. Anhand dieser Ergebnisse wird auch die Verlässlichkeitsanforderungs-Checkliste, siehe Kapitel 6.2.2, entsprechend erweitert. Das Resultat der Phase *Fehler-, Gefahren- und Risikenanalysen* ist als Ausschnitt in Tabelle 6.7 dargestellt, während sie im Anhang in den Tabellen C.5 bis C.8 hinterlegt ist. Bei einigen Fehlern oder Gefahren erfolgte keine eigene Risikobewertung mittels der Kriterien, sondern die jeweils kritischste Risikoklasse wurde der überlagerten Hierarchieebene vererbt.

Fehlerausfall/-zustand/-ursache	Gefahren	Häufigkeit	Auswirkung	Risiko
Ausfall der Tragfunktion				II
Ausfall Tragstruktur				III
- Material-, Auslegungs-, Fertigungsfehler	Entgleisung, Umkippen des Fahrzeugs	unwahrsch.	katastrophal	III
- zu hohe Kraft im Fahrwerksrahmen	Entgleisung, Umkippen des Fahrzeugs	unwahrsch.	katastrophal	III
Ausfall Rad (tragende Funktion)				II
- Material-, Auslegungs-, Fertigungsfehler	Entgleisung, Umkippen des Fahrzeugs	gering	katastrophal	II
- zu hohe Normalkraft auf Räder	Entgleisung, Umkippen des Fahrzeugs	gering	katastrophal	II
Ausfall Kugelgelenk				III
- Verschleiß	Schlingern, bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung	gering	begrenzt	III
- zu hohe Kraft im Kugelgelenk	bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung	unwahrsch.	katastrophal	III
- translat. Bewegung im Gelenk	bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung	gering	gering	III
Ausfall Querfeder				IV
- Missbrauch, Materialfehler,...	leichtes Schlingern	gering	geringfügig	IV
Ausfall Verbindungsmutter				IV
- mech. Missbrauch, Materialfehler,...	ungleichmäßige Krafteinleitung, Schlingern	unwahrsch.	begrenzt	IV
Ausfall Lager				III
- Verschleiß, Schmutz, Missbrauch	Blockieren des Rads	gelegentlich	begrenzt	III
Ausfall/Fehler der Sensorik				III
Ausfall/Fehler Lenkaktorsensor				III
- Ausfall Signalverarbeitungskette,...	Lenken unmöglich und unkomfortables Führen	gering	begrenzt	III
- Falsches Signal	Falsches Lenken und unkomfortables Führen	gering	begrenzt	III
- Kein Signal	Lenken und komfortables Führen wird unmöglich	gering	begrenzt	III
- Zu schlechtes Signal	Lenken und komfortables Führen eingeschränkt	gering	geringfügig	IV

Tabelle 6.7: Ausschnitt aus der Risikenanalyse, dem Resultat der Phase *Fehler-, Gefahren- und Risikenanalysen* des Spurführungsmoduls

6.2.4 Konzipierung und Entwurf der Verlässlichkeit

Im Prozessschritt *Konzipierung und Entwurf der Verlässlichkeit* werden nun Maßnahmen durchgeführt, die zur direkten Steigerung der Verlässlichkeit des Systems beitragen. Dieses wird erreicht bzw. unterstützt durch die Nutzung der entwickelten *Methodik der Verlässlichkeitsmuster*, die mittels der Datenbanklösung anwendbar gemacht wurde. Basis zur Konzipierung und zum Entwurf für Fehlervermeidung, Fehlerüberwachung und Fehlertoleranz sind die Erkenntnisse der vorhergehenden Phase, die kritische Fehler oder Gefahren identifiziert und bewertet hat. Nachfolgend werden ausgewählte Konzepte dargestellt, die exemplarisch für die drei Hauptkategorien der Verlässlichkeitsmuster stehen.

Fehlervermeidung

Der Ausfall der Tragstruktur, der zum Ausfall der Tragfunktion führen würde, wurde im Prozessschritt *Fehler-, Gefahren- und Risikenanalysen* mit der *Risikoklasse III* klassifiziert. Das bedeutet, dass es sich hierbei um ein tolerierbares Risiko handelt, wenn die Kosten einer Risikominderung die erreichbare Verbesserung übersteigen. Durch Abschätzungen bzgl. der auftretenden Belastungen im Betrieb während der gesamten Lebensdauer, kann das Verlässlichkeitsmuster der Überdimensionierung mittels eines Sicherheitsfaktors bei der Auslegung der Struktur verwendet werden. Die Anwendung dieses Musters ist bereits Bestandteil für die resultierende Bewertung der *Risikoklasse III* gewesen. Eine zusätzliche Online-Kontrolle der tatsächlichen Belastungen (würde bereits der Kategorie Fehlerüberwachung entsprechen) ist beim derzeitigen System dagegen gemäß der Klassen-Definition nicht zwangsläufig notwendig. Im Falle intelligenter werdender Systeme mit mehr verfügbaren Informationen könnte aber eine Auswertung dieser vorhandenen Informationen im Sinne einer Online-Kontrolle der Belastungen durchaus nötig werden bzw. sinnvoll sein, da die Kosten relativ gering wären und sie evtl. nicht mehr die erreichbare Verbesserung übersteigen würden.
Ein weiteres genutztes Konzept der Fehlervermeidung ist das ständige Vorhandensein eines *Zwangwertes* für die Lenkvorgabe bei der Informationsverarbeitung der Bahnsteuerung. Im vorhergehenden Prozessschritt wurde der Ausfall bzw. Fehler der Bahnsteuerung durch das Fehlen eines Abbiege-Sollwerts mit der *Risikoklasse II* bewertet. Das bedeutet, dass dieses ein unerwünschtes Risiko sei, das nur tolerierbar ist, wenn eine Risikominderung nicht durchführbar ist oder die Kosten der Minderung unverhältnismäßig hoch im Vergleich zur erzielten Verbesserung sind. Der identifizierte Fehler kann aber relativ einfach vermieden werden durch das Vorgeben eines zwangsläufig immer vorhandenen Abbiege-Sollwerts. Es kann dann zwar wiederum bedeuten, dass die Vorgabe vorhanden aber falsch ist; dieser Fehler ist allerdings als weniger kritisch be-

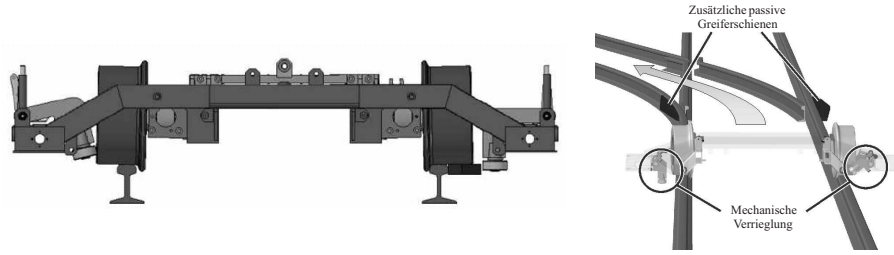


Abbildung 6.6: Mechanische Verriegelung für sicheres Durchfahren einer passiven Weiche - Aufbau (links) und Funktionsweise (rechts) [MWEW05] [WMW06]

wertet worden, sodass gesamtheitlich betrachtet eine Risikominderung durchgeführt werden konnte.
Das Verlässlichkeitsmuster eines Zwangwertes für die Lenkvorgabe in der Weiche ist auch in mechanischer Hinsicht umgesetzt: Eine ständig ausgerichtete mechanische Verriegelung im Sinne einer Wippe sorgt ebenfalls dafür, dass bei der Weichendurchfahrt eine eindeutige Richtung eingestellt und verfolgt wird [MWEW05] [WMW06]. Die Argumentation, der dieses Verlässlichkeitsmuster folgt, lautet: *Besser in die falsche Richtung abbiegen, als gar nicht wissen, dass abgebogen werden soll.* Abbildung 6.6 zeigt Aufbau und Funktionsweise der mechanischen Verriegelung im Detail. Durch eine mechanische Kopplung kann immer nur eine der Führrollen die Verriegelung realisieren.

Fehlerüberwachung

Ein falsches Signal eines Wirbelstromsensors ist zwar *nur* mit der *Risikoklasse III* bewertet worden, trotzdem kann mittels Plausibilitätschecks das Risiko durch relativ geringen Aufwand reduziert werden. So können einige Fehler, z. B. ein Kabelabriss, bereits durch den Einsatz einfacher Signal-Bereichsgrenzen erkannt werden. Werden diese Grenzen im Betrieb überschritten, so wird das Signal als fehlerhaft eingestuft und in der weiterführenden Informationsverarbeitung quasi nicht berücksichtigt. Umgesetzt wird dieses Vorgehen durch eine *Vertrauensbewertung* des Signals, die zwischen 0,01 und 1 liegt, wobei die Bereiche außerhalb der definierten Grenzen den Wert 0,01 zur Folge haben während der plausible Bereich den Vertrauenswert 1 zuweist. In der weiteren Signalverarbeitung wird die Multiplikation von Sensorwert und Vertrauenswert verwendet. Bei der Nutzung von mehreren Signalen z. B. durch Mittelwertbil-

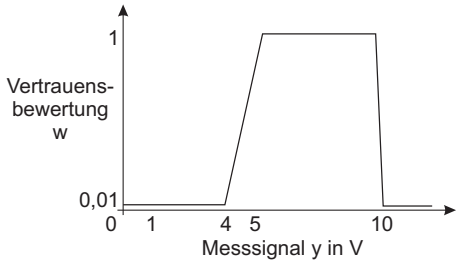


Abbildung 6.7: Plausibilitätsgrenzen werden *überwacht* durch die Anwendung einer Vertrauensbewertung bzgl. des Sensorsignals

dung, kommt dann dem plausiblen Signal ein deutlich höherer Wert zu. Auf diese Weise werden quasi nur noch plausible Werte berücksichtigt. In Abbildung 6.7 ist die Zuordnungsvorschrift für die Vertrauenswerte dargestellt.
Neben der zuvor beschriebenen Fehlererkennung und der direkt implementierten Nicht-Berücksichtigung fehlerhafter Werte, besteht auch die Möglichkeit, die Abweichung vom Sollbereich oder von Sollverläufen mittels Residuen-Generierung zu analysieren. Durch Interpretation der Residuen mittels verschiedener Klassifikationsverfahren könnten die Fehler diagnostiziert werden. Dieses Muster wurde aufgrund des unverhältnismäßigen Aufwandes gegenüber dem reduzierbaren Risiko nicht umgesetzt.
Bei der Erkennung von sehr kritischen Fehlern oder auch bei nicht erklärbaren kritischen Zuständen des Systems, wird das Verlässlichkeitsmuster einer fehlersicheren Degradationsstufe (engl. Fail-safe) eingesetzt. Sie beschreibt eine Notfallmaßnahme, die direkt einen sicheren Systemzustand herstellt; in diesem Fall mittels einer mechanischen Notbremsung. Abbildung 6.8 zeigt die Konstruktionszeichnung der mechanischen Notbremse beim RailCab.

Fehlertoleranz

Obwohl die Risikobewertung mit *Klasse III* für einen Ausfall oder Fehler der Wirbelstromsensoren durchaus tolerierbar wäre, so führen höhere Anforderungen an die zuverlässige Funktionserfüllung für komfortables Führen zur Konzipierung von fehlertolerantem Verhalten durch Sensor-Redundanz: Zur einfachen Funktionserfüllung genügen bereits zwei Wirbelstromsensoren, die unterschiedliche Signale messen. Für eine sicherere Fehlererkennung als durch die zuvor angesprochenen Plausibilitätschecks, wird ein dritter Sensor hinzugenommen. Fehlertolerantes Verhalten wird allerdings erst durch die Nutzung eines vierten Wirbelstromsensors erreicht, da so der fehlerhafte Sensor identifiziert und aus der Struktur ausgeschlossen werden kann. Erst dadurch kann

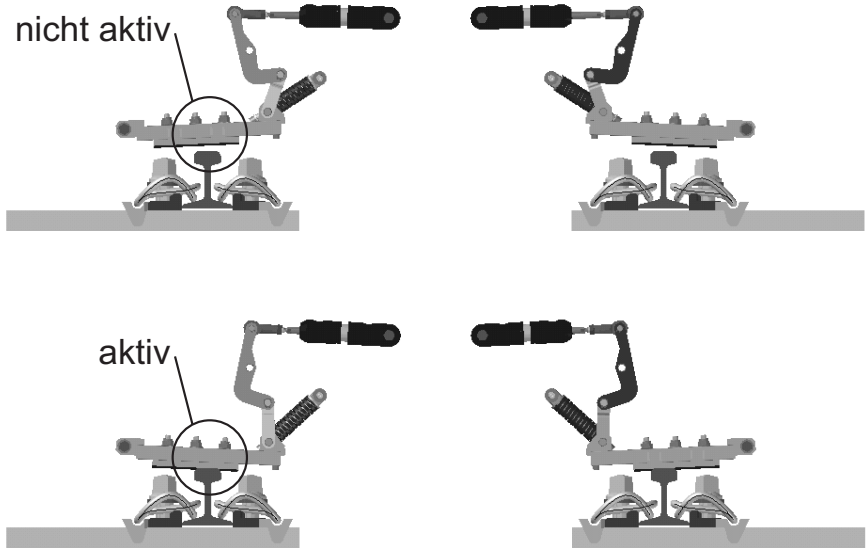


Abbildung 6.8: Mechanische Notbremse als fehlersicheres Degradationskonzept beim RailCab

Fehlertoleranz realisiert werden. Abbildung 6.9 zeigt die vier Wirbelstromsensoren des Spurführungsmoduls, von denen jeweils zwei als Sensorpaar genügen, um die Funktion der Positionsermittlung zu erfüllen.

6.2.5 Verlässlichkeitsanalysen von Kooperation u. Integration

Dieser Prozessschritt analysiert im Sinne von Verifikation und Validierung die korrekte Kooperation von hierarchisch gleich einzuordnenden Komponenten als auch die korrekte Integration von unterlagerten Modulen in oberlagerte Systemebenen. Sowohl die Teil- und Hauptfunktionen müssen dazu erfüllt werden als auch die Anforderungen der Verlässlichkeitsanforderungs-Checkliste. Zur Überprüfung werden daher verschiedene Testmethoden und Prüfumgebungen angewendet, die realitätsnahe Einsatzumgebungen darstellen oder simulieren. Für das gesamte RailCab-Projekt existieren sowohl *Hardware-in-the-Loop*-Prüfstände zum Testen verschiedener Einzelmodule [FGK+04] als auch eine Versuchsanlage mit 600m Strecke und zwei Fahrzeugen im Maßstab 1:2,5 [Trä06a], die die Module zum Gesamtkonzept integrieren. Zusätzlich können die Funktionen der Informationsverarbeitung rechnerintern simuliert und ana-

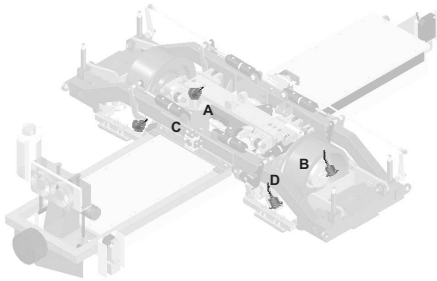


Abbildung 6.9: Fehlertoleranz der vier Wirbelstromsensoren (A,B,C und D) durch Sensor-Redundanz [MWEW05][WMW06]

lysiert werden. Angewendete Testmethoden sind bei den Prüfständen die physikalische Fehlerinjektion, z. B. ein absichtlich durchgeführter Kabelabriss, sowie bei der Informationsverarbeitung die Fehlerinjektion in Simulationsmodellen, z. B. durch die Manipulation eines Sensorsignals. Methoden zur Untersuchung gemeinschaftlicher Fehlerursachen oder auch kritischer Wechselwirkungen werden aktuell noch bearbeitet. Experimentelle Tests zum Bestimmen von quantitativen Zuverlässigkeitswerten sind bisher nicht notwendig gewesen. Der Grund dafür liegt darin, dass das Ziel des RailCab-Projekts nicht das marktreife Seriensystem ist, sondern dass *lediglich* die Machbarkeit des Technologiekonzepts dargestellt werden soll. Die Abbildungen 6.10 und 6.11 zeigen Prüfstände sowie die Versuchsanlage mit einem Fahrzeug. Weitere Aktivitäten bzgl. Verlässlichkeitsanalysen von Kooperation und Integration sind derzeit noch nicht abgeschlossen, sind aber für die angestrebte initiale Evaluierung der Funktionalität des Prozesses auch nicht unbedingt notwendig.

6.3 Ergebnis-Review

Die Evaluierung des Einsatzes der entwickelten Methodiken bzgl. eines messbaren Erfolgs erfolgt durch kritische Diskussion der Prozessresultate im Sinne eines *Ergebnis-Reviews*. Dies stellt im Sinne der verfolgten Forschungsmethodik die initiale Erfolgsvalidierung dar. Es soll diskutiert werden, in wie weit das zu Beginn definierte messbare Erfolgskriterium *Verlässlichkeit steigern* erreicht werden konnte. Dazu werden im Folgenden die einzelnen Prozessbausteine bzw. deren Ergebnisse betrachtet und dem zuvor vorhandenen Entwicklungsvorge-

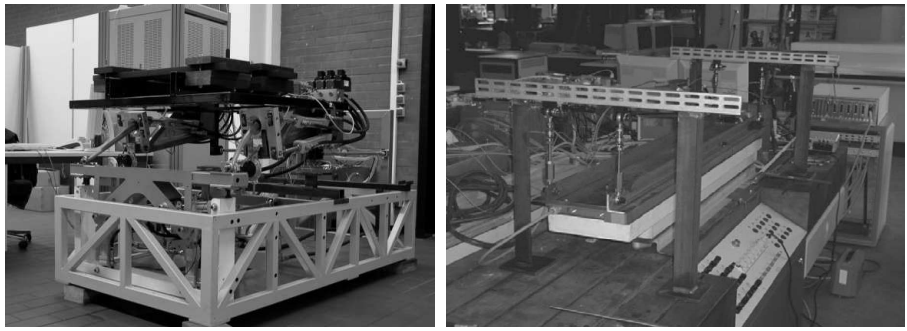


Abbildung 6.10: RailCab-Prüfstände für das Feder-Neige-Modul [Trä06b] und für Wechselwirkungen zwischen Antriebs- und Spurführungsmodul [Sch04]

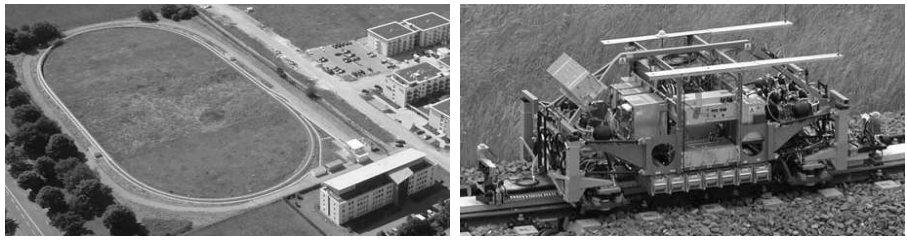


Abbildung 6.11: RailCab-Versuchsstrecke und -fahrzeug im Maßstab 1:2,5 [Trä06a]

hen gegenüber gestellt.
Obwohl das Forschungsprojekt RailCab bereits seit einiger Zeit bearbeitet wird, waren kaum detaillierte oder vollständige Systembeschreibungen dokumentiert worden oder zumindest nicht verfügbar. Da zur Durchführung des Verlässlichkeitsprozesses die *Systemanalyse* eine notwendige Basis darstellt, wurde diese in einem ersten Schritt für das Spurführungsmodul angefertigt. Dazu wurde das System durch Funktionen, Komponenten und Attribute beschrieben und strukturiert. Diese Systembeschreibungen sind bereits der erste Mehrwert, der durch die Anwendung der verlässlichkeitsorientierten Entwicklungsmethodik realisiert werden konnte.
Darauf aufbauend wurde eine Anforderungsanalyse im Kontext der Verlässlichkeit angefertigt, die bisher ebenfalls noch nicht bestand, ebenso wie alle folgenden Resultate des Verlässlichkeitsprozesses. Diese *Verlässlichkeitsanforderungsanalyse* ist jedoch nur in einer ersten vorläufigen Version angefertigt worden und steigert die Kenntnisse daher nur in einer relativ geringen Form.
Der Prozessschritt *Fehler-, Gefahren- und Risikenanalyse* generierte hingegen ein sehr großen Mehrwert, der sogar noch in untergliederter Form betrachtet werden soll: Vorher unbekannte Fehler wurden identifiziert durch die Anwendung verschiedener Methoden und Herangehensweisen, deren Ergebnisse wieder zu einer Fehlerliste zusammengeführt wurden. Daraus konnten Gefahren ermittelt werden, die zwar auch im Vorfeld bereits größtenteils bekannt waren, die aber durch die Aktivität der Risikobewertung eine Priorisierung erfahren haben, die den Handlungsbedarf verdeutlichen. Erweiterte Kenntnisse über mögliche Fehler und deren Zusammenhänge sowie eine Klassifizierung bzgl. der Kritikalität von Fehlern und Gefahren sind relevante Resultate, die durch Anwendung des entwickelten Vorgehens erreicht werden konnten.
Die Anwendung der Methodik der Verlässlichkeitsmuster in der Phase *Konzipierung und Entwurf der Verlässlichkeit* führte dazu, dass sich strukturiert, detailliert und fokussiert damit auseinander gesetzt wurde, wie die identifizierten Risiken reduziert werden könnten. Dazu wurden verschiedene Ansätze aus der Datenbank für Verlässlichkeitsmuster genutzt, bzw. es wurden neue Lösungen entwickelt und als Muster abgelegt. Aufgrund der Parallelität der Arbeiten zur Systementwicklung und dem Füllen der Datenbank, konnte noch nicht in vollem Umfang der Mehrwert genutzt werden, sodass weiteres Steigerungs-Potenzial vorhanden ist.
Der Prozessschritt *Verlässlichkeitsanalyse von Kooperation und Integration* führte bisher nur geringfügig zu weiteren Kenntnissen oder Verbesserungen im Kontext der Verlässlichkeit gegenüber dem bisherigen Entwicklungsvorgehen. Die Begründung dafür liegt darin, dass die Testumgebungen bereits vorher vorhanden waren und die Aktivitäten in dieser Prozessphase noch weiter geführt werden.
Neben den zuvor erläuterten Resultaten der einzelnen Prozessschritte, war ein

weiterer großer Mehrwert des angewendeten Prozessmodells, die eigentliche Dokumentation des Entwicklungsvorgehens. Dokumente über Systembeschreibungen sowie die Systemhierarchisierung fehlten vorher nahezu vollständig und auch eine Dokumentation über teilweise vorhandenes Wissen bzgl. Fehler und Gefahren existierte nicht.
Tabelle 6.8 zeigt die erreichten Mehrwerte nochmals in der Übersicht und bewertet sie mit einem, zwei oder drei Sternen, wobei eine höhere Anzahl einen größeren Nutzen widerspiegelt. Bereits diese initiale Erfolgsvalidierung zeigt, dass die Verlässlichkeit des Systems *Spurführungsmodul* gesteigert werden konnte und Grundlagen geschaffen wurden, diese auch weiter analysieren und steigern zu können. Darüber hinaus wurden wichtige Ergebnisse dokumentiert, sodass auch im Kontext der Verlässlichkeit nun notwendige Entwicklungsunterlagen vorhanden sind.
Entsprechend den Bewertungen in Tabelle 6.8 kann das Fazit gezogen werden, dass einerseits der Erfolg der entwickelten Methodiken festgestellt werden konnte, andererseits aber in einigen Bereichen bisher *nur* das Potenzial dargestellt aber noch nicht endgültig validert wurde. Der Hinweis auf den initialen Charakter der Erfolgsvaliderung rechtfertigt dieses Vorgehen und das Ergebnis ebenso, wie es auch dem möglichen Kritikpunkt entgegensteht, dass beim Vergleich ein Entwicklungsvorgehen gegenüber gestellt wurde, dass nicht unbedingt dem industriellen Standard entsprechen würde. Die Forschungshypothese, dass die Verlässlichkeit durch den Einsatz der entwickelten Methodiken gesteigert werden kann, wurde bereits mit diesem initialen Vorgehen validiert.

6.4 Zusammenfassung

Das Kapitel *Anwendungsbeispiel* beschreibt im Sinne der deskriptiven Studie 2 der verfolgten Forschungsmethodik den Ansatz, durch Anwendung der entwickelten Methodiken der vorangegangenen Kapitel, eine steigenden Verlässlichkeit zu erreichen und damit die aufgestellte Forschungshypothese zu validieren. Dies geschieht durch Anwendung der verlässlichkeitsorientierten Entwicklungsmethodik und der darin integrierten Methodik der Verlässlichkeitsmuster anhand eines Forschungsprojekts. Dieses bezieht sich auf die Entwicklung eines Spurführungsmoduls, das das aktive Fahrwerk eines innovativen autonomen Bahnfahrzeugs namens *RailCab* darstellt.
Die Evaluierung der Methodiken soll dabei sowohl die *Funktionalität* als auch den *messbaren Erfolg* zeigen. Während die Funktionalität bereits durch die reibungslose Anwendung der auf einander folgenden Prozessbausteine sowie der Umsetzung verschiedener Verlässlichkeitsmuster nachgewiesen wurde, konnte der messbare Erfolg durch einen Ergebnis-Review dargestellt werden. Zusammenfassend konnte also die Forschungshypothese validiert werden, dass die

Prozessphase	Erfolgs-bewertung	Anmerkungen
Systemanalyse	***	Systembeschreibungen und -strukturierungen durch Funktionen, Komponenten und Attribute sind nicht vorhanden gewesen
Anforderungsanalyse	*	Anforderungslisten sind nicht vorhanden gewesen, auch nicht im Kontext der Verlässlichkeit; derzeit haben sie aber nur einen relativ geringen Mehrwert erbracht
Fehleranalyse	***	Fehleridentifikation durch den Einsatz verschiedener Methoden erzielten wichtige neue Erkenntnisse
Gefahrenanalyse	*	Gefahren waren größtenteils bereits bekannt, aber nicht dokumentiert
Risikobewertung	**	Priorisierung von Fehlern und Gefahren identifizierte detaillierten Handlungsbedarf
Konzipierung der Verlässlichkeit	**	Fokussierung auf Verlässlichkeitskonzipierung führte direkt zu Risikominderungen; wegen Parallelität von System- und Datenbankentwicklung besteht noch weiteres Potenzial
Verlässlichkeitsanalyse von Kooperation und Integration	*	Testumgebungen waren bereits vorhanden; Aktivitäten werden fortgesetzt
Entwicklungs-dokumentation	***	Dokumentation fehlte vorher nahezu vollständig

Tabelle 6.8: Bewertetes Resultat der Erfolgsvalidierung im Sinne eines Ergebnis-Reviews

Verlässlichkeit durch die systematische und sinnvolle Integration von Verlässlichkeitsmethoden und die Integration von wiederverwendbarem Verlässlichkeitsfachwissen in die Entwicklungsmethodik gesteigert werden kann.

7 Zusammenfassung und Ausblick

Die Vernetzung mehrerer technischer Domänen durch die Mechatronik führt zu intelligenteren, häufig auch komplexeren Systemen. Nicht selten stellt die Gewährleistung der Verlässlichkeit dabei eine große Herausforderung dar, deren positive Erfüllung sich durch verschiedene Aspekte motivieren lässt: Dazu gehören u. a. das Reduzieren von Ausfallraten und damit verbundenen Kosten, das Entsprechen von Kundenwünschen bzgl. eines hohen Sicherheitsbedürfnisses oder das Vermeiden von Haftungsrisiken und Imageverlusten.
Nach Klärung des Forschungsgegenstands durch die Darstellung des Standes der Technik, wurde im Rahmen dieser Arbeit eine Industrie-Befragung durchgeführt. Diese verbesserte das Verständnis von Entwicklungstätigkeiten im Kontext der Verlässlichkeit sowohl bzgl. der derzeitigen Nutzung von Verlässlichkeitsmethoden und -prozessen als auch bzgl. bestehender Defizite und zukünftiger Bedürfnisse. Wesentliche Erkenntnisse der Studie verdeutlichen, dass einige Potenziale zur Berücksichtigung von Verlässlichkeit während der Entwicklung bisher noch ungenutzt sind. Dazu gehört neben einer früheren und kontinuierlichen Anwendung von Verlässlichkeitsmethoden auch die Integration innerhalb eines Entwicklungsprozesses und die Wiederverwendung bestehenden Verlässlichkeitswissens. Diese Erkenntnisse, kombiniert mit Schlussfolgerungen bezüglich bestehender Ansätze für Verlässlichkeitsprozesse, führte zur zentralen Forschungshypothese der vorliegenden Arbeit:

> **Die systematische und sinnvolle Integration von Verlässlichkeitsmethoden und die Integration von wiederverwendbarem Verlässlichkeitsfachwissen in die Entwicklungsmethodik der Mechatronik führt zur Steigerung der Verlässlichkeit dieser Systeme.**

Der *Verlässlichkeitsprozess für die Entwicklungsmethodik* beschreibt den Teil des Forschungsansatzes, der durch systematische und sinnvolle Integration von Verlässlichkeitsmethoden in die Entwicklungsmethodik, die Entwicklungstätigkeiten verbessern soll. Der neu entwickelte Ansatz nutzt die bestehende Systematik der VDI-Richtlinie 2206 *Entwicklungsmethodik für mechatronische Systeme* als Rahmenkonzept. Dabei wird um das bestehende V-Modell ein zweites

V-Modell gelegt; der eigentliche Verlässlichkeitsprozess. Im Detail besteht er aus den folgenden Prozessbausteinen:

- Anforderungsanalyse für Verlässlichkeit
- Fehler-, Gefahren- und Risikenanalysen
- Konzipierung und Entwurf der Verlässlichkeit
- Verlässlichkeitsanalysen von Kooperation und Integration

Der weitere Teil des Forschungsansatzes, die Integration von wiederverwendbarem Verlässlichkeitswissen in die Entwicklungsmethodik, wurde durch die entwickelte *Methodik der Verlässlichkeitsmuster* bearbeitet. Die Methodik beschreibt die Definition, Strukturierung und Wiederverwendung von Verlässlichkeitsmustern, die zur direkten Steigerung der Verlässlichkeit von mechatronischen Systemen genutzt werden können. Ein Verlässlichkeitsmuster beschreibt in diesem Sinne den Kern einer etablierten Lösung für gesteigerte Verlässlichkeit, der wiederum für spezifische Problemstellungen, teilweise in adaptierter Form, umgesetzt werden kann. Diese möglichst lösungsneutral beschriebenen Verlässlichkeitsmuster sind z. B. Designprinzipien, Diagnosealgorithmen oder Redundanzstrukturen. Sie repräsentieren vorhandenes Wissen, dass u. a. durch eigene Entwicklungen oder auch Recherchetätigkeiten erlangt werden kann. Wiederverwendbar gesammelt werden die Muster durch die *Datenbank für Verlässlichkeitsmuster*, die den Entwickler in der Konzipierungsphase unterstützt. Die neu entwickelte Strukturierung der Verlässlichkeitsmuster ist nachfolgend dargestellt:

- *Fehlervermeidung* beschreibt Verlässlichkeitsmuster, die die Fehlerursache, also den eigentlichen Fehler, bereits vor oder während der Entstehung verhindern.
- *Fehlerüberwachung* beschreibt Verlässlichkeitsmuster, die einen Fehlerzustand erkennen, diagnostizieren und gegebenenfalls daraufhin Maßnahmen einleiten.
- *Fehlertoleranz* beschreibt Verlässlichkeitsmuster, die trotz Ausfall von Teilsystemen die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten.

Abschließend wurden die entwickelten Methodiken anhand eines Anwendungsbeispiels, dem Forschungsprojekt *RailCab*, hinsichtlich Funktionalität und Erfolg evaluiert. Im Detail wurde die verlässlichkeitsorientierte Entwicklungsmethodik und die darin integrierte Methodik der Verlässlichkeitsmuster bei der

Entwicklung eines Spurführungsmoduls für ein innovatives Bahnsystem angewendet. Während die Funktionalität bereits durch die reibungslose Anwendung der auf einander folgenden Prozessbausteine sowie der Umsetzung verschiedener Verlässlichkeitsmuster nachgewiesen wurde, konnte der messbare Erfolg durch einen Ergebnis-Review dargestellt werden.

Ausgehend von diesem Ergebnis eröffnen sich weiterführende Fragestellungen für zukünftige Forschungs- und Entwicklungsaktivitäten auf diesem Gebiet. Sie betreffen z. B. die Umsetzbarkeit der Ergebnisse in einem Unternehmen, die weitere Vervollständigung und Vertiefung der Sammlung von Verlässlichkeitsmustern und die Übertragung des Vorgehens auf eine andere Forschungsebene. Nachfolgend werden diese Potenziale für weitere Aktivitäten kurz erläutert.
Um den Verlässlichkeitsprozess und die Methodik der Verlässlichkeitsmuster in einem Unternehmen umsetzen und etablieren zu können, müssen selbstverständlich weitere Arbeiten verrichtet werden: Das durch diese Arbeit vorliegende konzeptionelle Vorgehen muss an den Entwicklungsprozess des jeweiligen Unternehmens und an die Unternehmenskultur angepasst werden. Neben der formalen Einführung der einzelnen Prozessphasen, müssen Verantwortlichkeiten sinnvoll verteilt und eine hohe Akzeptanz für das Vorgehen geschaffen werden.
Die Sammlung der Verlässlichkeitsmuster besitzt weder derzeit noch zukünftig einen Anspruch auf Vollständigkeit. Trotzdem besteht weiterer Arbeitsbedarf darin, z. B. durch Recherchen die Sammlung zu Erweitern. Damit könnte ein größere Raum für Lösungsmöglichkeiten abgebildet werden. Neben dieser Erweiterung bzgl. der Breite könnten auch Aktivitäten mit dem Fokus der Vertiefung betrachtet werden. Vertiefung bedeutet in diesem Zusammenhang, dass die unteren Ebenen der Struktur der Verlässlichkeitsmuster weiter befüllt werden; evtl. sogar auch durch konkrete Umsetzungbeispiele.
Einen weiteren potenziellen Aspekt für zukünftige Aktivitäten in diesem Bereich stellt die Übertragung des Verlässlichkeitsprozesses auf andere Forschungsebenen dar; z. B. auf Technologie-Betrachtungen [MS07]: Das fehlende Vertrauen in die verlässliche Funktionalität neuer Technologien stellt häufig ein Hindernis für deren Nutzung dar. Die Herausforderung, bereits das physikalische Wirkprinzip der Technologie bzw. dessen Integration mit Hilfe eines sinnvollen Prozesses hinsichtlich der Verlässlichkeit analysieren zu können, bietet weitere Nutzenpotenziale der erreichten Ergebnisse.

Zusammenfassend konnte in der vorliegenden Arbeit die Forschungshypothese validiert werden, dass die Verlässlichkeit durch die systematische und sinnvolle Integration von Verlässlichkeitsmethoden und die Integration von wiederverwendbarem Verlässlichkeitsfachwissen in die Entwicklungsmethodik gesteigert werden kann. Umgesetzt und validiert wurde der Forschungsansatz durch

einen *Verlässlichkeitsprozess für die Entwicklungsmethodik* und die *Methodik der Verlässlichkeitsmuster*, die abschließend an einem Forschungsprojekt evaluiert wurden.

Literaturverzeichnis

[ADM+00] Amberkar, Sanket; D´Ambrosio, Joseph; Murray, Brian T.; Wysocki, Joseph; Czerny, Barbara J.: A System-Safety Process For By-Wire Automotive Systems. In: *SAE 2000 World Congress*. Detroit, Michigan, 2000

[AFLE04] Amsler, Klaus-Jürgen; Fetzer, Joachim; Lederer, Dieter; Erben, Meinhard: Sicherheitsgerechte Entwicklungsprozesse. Alles neu geregelt? In: *Aktive Sicherheit durch Fahrerassistenzsysteme*. München, 2004

[AHKSC02] Auerswald, Marko; Herrmann, Martin; Kowalewski, Stefan; Schulte-Coerne, Vincent: Entwurfsmuster für fehlertolerante softwareintensive Systeme. In: *at - Automatisierungstechnik* Bd. 8, 2002

[BC02] Blessing, Lucienne; Chakrabati, Amaresh: DRM: A Design Research Methodology. In: *Proceedings of Les Sciences de la Conception*. Lyon, 2002

[BDM99] Bertram, Torsten; Dominke, Peter; Müller, Bernd: The Safety-Related Aspect of CARTRONIC. In: *SAE International Congress & Exposition, March 1999, Detroit (USA), Session: Intelligent Transportation Systems: Vehicle Navigation Systems*, 1999

[Ben03] Benz, Stefan: Eine Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil. In: *15th Workshop Testmethods and Reliability of Circuits and Systems*. Timmendorfer Strand, 2003

[Ben04] Benz, Stefan: *Eine Entwicklungsmethodik für sicherheitskritische Elektroniksysteme im Automobil*. Bosch, Universität Karlsruhe, Diss., 2004

[Ber99] Berufsgenossenschaft Druck und Papierverarbeitung: *Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitenden Maschinen*. 1999

[Bie02] Biegert, Uwe: *Ganzheitliche modellbasierte Sicherheitsanalyse von Prozessautomatisierungssystemen*, Institut für Automatisierungs- und Softwaretechnik der Universität Stuttgart, Diss., 2002

[Bir91] Birolini, Allessandro: *Qualität und Zuverlässigkeit technischer Systeme*. Berlin: Springer-Verlag, 1991

[BK01] Binfett-Kull, Maria: *Entwicklung einer Steer-by-Wire-Architektur nach zuverlässigkeits- und sicherheitstechnischen Vorgaben*, Bergische Universität - Gesamthoschschule Wuppertal, Diss., 2001

[BL04] Bertsche, Bernd; Lechner, Gisbert: *Zuverlässigkeit im Fahrzeug- und Maschinenbau. Ermittlung von Bauteil- und System-Zuverlässigkeiten*. Berlin: Springer-Verlag, 2004

[Bom05] Bommer, Marc: *Ein wissensbasiertes Informations- und Entscheidungshilfesystem für fahrzeugbezogenes Online-Sicherheitsmanagement in bestimmten Ausnahmesituationen des Schienenverkehrs*. Culliver Verlag Göttingen, Technische Universität Ilmenau, Diss., 2005

[Bun06] Bundesministerium der Justiz: *Eisenbahn-Bau- und Betriebsordnung (EBO)*. 2006

[DAT04] DAT-Veedol-Report 2004 / Deutsche Automobil Treuhand GmbH. Vogel Auto Medien GmbH, Würzburg, 2004. – Forschungsbericht

[DGOS03] Dilger, E.; Gulbins, M.; Ohnesorge, T.; Straube, B.: Redundanter diversitärer Lenkwinkelgeber. In: *15. GI/ITG/GMM Workshop "Testmethoden und Zuverlässigkeit von Schaltungen und Systemen"*, 2003

[DIN81] *DIN 25424 Teil 1 Fehlerbaumanalyse*. 1981

[DIN90a] *DIN 25424 Teil 2 Fehlerbaumanalyse - Handrechenverfahren zur Auswertung eines Fehlerbaums*. 1990

[DIN90b] *DIN 25448: Ausfalleffektanalyse – (Fehler-Möglichkeits- und –Einfluss-Analyse)*. 1990

[DIN96] *DIN EN 1050: Sicherheit von Maschinen - Leitsätze zur Risikobeurteilung*. 1996

[DIN02] *DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbar elektronischer Systeme.* 2002

[DIN04] *DIN EN ISO 12100: Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze.* 2004

[Eur06] Europäisches Parlament und Rat: *Maschinenrichtlinie 2006/42/EG.* 2006

[FA04] Fritz, M.; Albers, A.: Fehlererkennung an einem elektromechanischen Radbremsaktor mittels modellbasierter Methoden. In: *AUTOREG*, 2004

[FGK+04] Frank, Ursula; Giese, Holger; Klein, Florian; Oberschelp, Oliver; Schmidt, Andreas; Schulz, Bernd; Vöcking, Henner; Witting, Kathrin; Gausemeier, Jürgen (Hrsg.): *Selbstoptimierende Systeme des Maschinenbaus. Definitionen und Konzepte.* Paderborn: HNI Verlagsschriftenreihe, 2004

[GEK01] Gausemeier, Jürgen; Ebbesmeyer, Peter; Kallmeyer, Ferdinand: *Strategische Planung und Entwicklung der Produkte von morgen.* München: Carl Hanser Verlag, 2001

[Ger98] Gertler, Janos J.: *Fault Detection and Diagnosis in Engineering Systems.* New York: Marcel Dekker, Inc., 1998

[Göh05] Göhner, Peter: Zuverlässigkeitsmethoden für frühe Entwicklungsphasen programmierbarer mechatronischer Systeme auf Basis qualitativer Modelle. In: Bertsche, Bernd (Hrsg.): *Workshop der Forschergruppe DFG 460: Entwicklung von Konzepten und Methoden zur Ermittlung der Zuverlässigkeit mechatronischer Systeme in frühen Entwicklungsphasen.* Universität Stuttgart, 2005

[Hed01] Hedenetz, Bernd: *Entwurf von verteilten fehlertoleranten Elektronikarchitekturen in Kraftfahrzeugen*, Eberhard-Karls-Universität Tübingen, Diss., 2001

[Hei99] Heinzelmann, Andreas: *Produktintegrierte Diagnose komplexer mobiler Systeme*, Universität Paderborn, Diss., 1999

[HHK00] Herb, Rolf; Herb, Thilo; Kohnhauser, Veit: *TRIZ - Der systematische Weg zur Innovation: Werkzeuge, Praxisbeispiele, Schritt-für-Schritt-Anleitungen.* Landsberg/Lech: mi, Verlag Moderne Industrie, 2000

[ILM92] Isermann, Rolf; Lachmann, Karl-Heinz; Matko, Drago: *Adaptive Control Systems*. Prentice Hall, 1992

[Ise02] Isermann, Rolf: Fehlertolerante Komponenten für Drive-by-Wire-Systeme. In: *ATZ - Automobiltechnische Zeitschrift* Bd. 4, 2002

[Ise06] Isermann, Rolf: *Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance*. Berlin, Heidelberg: Springer-Verlag, 2006

[KB03] Kraftfahrt-Bundesamt: Pressebericht 2003/2004. Flensburg, 2003. – Forschungsbericht

[Kne00] Knepper, R.: Der Sicherheits- und Zuverlässigkeitsprozess in der zivilen Luftfahrtindustrie. In: *VDI Berichte 1546: Sicherheit komplexer Verkehrssysteme*. Düsseldorf: VDI Verlag, 2000

[Koc01] Kochs, Hans-Dieter: Verlässlichkeitsanalyse mechatronischer Systeme / Fachgruppe "Fehlertolerierende Rechensysteme" der Gesellschaft für Informatik. 2001. – Forschungsbericht

[Kof01] Kofler, Michael: *MySQL – Einführung, Programmierung, Referenz*. München: Addison-Wesley Verlag, 2001

[KP04] Kochs, Hans-Dieter; Petersen, Jörg: A Framework for Dependability Evaluation of Mechatronic Units. In: *ARCS 2004: Organic and Pervasive Computing (GI-Edition)*. Augsburg, 2004

[LA90] Lee, P. A.; Anderson, T.: *Fault Tolerance*. Wien: Springer-Verlag, 1990

[Lap92] Laprie, Jean-Claude et a.; Laprie, Jean-Claude (Hrsg.): *Dependable Computing and Fault-Tolerant Systems*. Bd. 5: *Dependability: Basic Concepts and Terminology - in English, French, German, Italian and Japanese*. Wien: Springer Verlag, 1992

[Lüc00] Lückel, Joachim: Systemkonzept Neue Bahntechnik Paderborn. In: *4. Internationales Heinz Nixdorf Symposium - Auf dem Weg zu den Produkten für die Märkte von morgen...* Paderborn: HNI-Verlagsschriftenreihe, 2000

[LGPK05] Limbourg, Philipp; Germann, Daniel; Petersen, Jörg; Kochs, Hans-Dieter: Integration von Verlässlichkeitsbetrachtungen in die VDI 2206: Entwicklungsmethodik für mechatronische Systeme - Ein Anwendungsbeispiel. In: *VDI Berichte 1892: Mechatronik 2005*. Düsseldorf: VDI Verlag, 2005

[LHD05] Liu-Henke, X; Duym, S: Modellgestützte Funktionsabsicherung des vernetzten mechatronischen Kraftfahrzeugs. In: *VDI Berichte 1892: Mechatronik 2005*. Düsseldorf: VDI Verlag, 2005

[Län03] Längst, Wolfgang: *Formale Anwendung von Sicherheitsmethoden bei der Entwicklung verteilter Systeme*, Universität Karlsruhe, Diss., 2003

[Lüt04] Lüttgers, Holger: *Online-Marktforschung: Eine Positionsbestimmung im Methodenkanon der Marktforschung unter Einsatz eines webbasierten Analytic Hierarchy Process (webAHP)*, Freie Universität Berlin, Diss., 2004

[Mah00] Mahmoud, Rachad: *Sicherheits- und Verfügbarkeitsanalyse komplexer Kfz-Systeme*, Universität-Gesamthochschule Siegen, Diss., 2000

[MG04] Milius, Birgit; Gayen, Jan-Tecker: Functional Hazard Assessment der Luftfahrt im Vergleich zu Risikoanalysen der Eisenbahn. In: *SIGNAL + DRAHT* Bd. 10, 2004

[MIL93] *MIL-STD-882C: System safety program requirements*. 1993

[Mül05] Müller, Thomas: Sicherheit als Herausforderung in der mechatronischen Produktentwicklung. In: *Tagungsband Internationales Forum Mechatronik*. Augsburg, 2005

[MM06] Müller, Thomas; Manga, Karine: Analyse von Sicherheitsmethoden und -prozessen in Unternehmen der Mechatronik-Industrie. 2006. – Forschungsbericht

[MMWW07] Müller, Thomas; Manga, Karine; Walther, Michael; Wallaschek, Jörg: Results of an Industry Survey on the Application of Dependability Oriented Design Methods. In: *The Future of Product Development. Proceedings of the 17th CIRP Design Conference*. Berlin: Springer-Verlag, 2007

[Mün06] Münchhof, Marco: *Model-Based Fault Detection for a Hydraulic Servo Axis*, Technische Universität Darmstadt, Diss., 2006

[MS07] Müller, Thomas; Schiedeck, Florian. *Verlässlichkeitsorientierte Technologiebewertung innovativer Aktortechnologien am Beispiel von Antrieben mit Formgedächtnislegierungen*. Forschungsbericht. 2007

[MW06] Müller, Thomas; Wallaschek, Jörg: General Concepts of Dependability in the Design of Mechatronic Systems. In: *Research and Education in Mechatronics*. Stockholm, 2006

[MW07] Müller, Thomas; Wallaschek, Jörg: Musterdatenbank zur Konzipierung verlässlicher mechatronischer Systeme. In: *VDI-Berichte 1984: TTZ 2007 - Tagung Technische Zuverlässigkeit*. Düsseldorf: VDI Verlag, 2007

[MWEW05] Müller, Thomas; Walther, Michael; Ettingshausen, Clemens; Wallaschek, Jörg: Dependability oriented Design of Self-Optimizing Mechatronic Systems. In: *REM - 6th International Workshop on Research and Education in Mechatronics*. Annecy, France, 2005

[Neu02] Neudörfer, Alfred: *Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG Maschinenrichtlinie, 2. Auflage*. Berlin: Springer Verlag, 2002

[ONB02] O'Connor, Patrick D.; Newton, David; Bromley, Richard: *Reliability Engineering*. Fourth Edition. Chichester, West Sussex: John Wiley & Sons, Ltd., 2002

[Pah01] Pahl, Gerhard: F - Grundlagen der Konstruktionstechnik - Grundlagen technischer Systeme und des methodischen Vorgehens. In: Beitz, Wolfgang (Hrsg.); Grote, Karl-Heinz (Hrsg.): *Dubbel - Taschenbuch für den Maschinenbau, 20. Auflage*, Springer-Verlag, 2001

[Rot94] Roth, Karlheinz: *Konstruieren mit Konstruktionskatalogen Band I und II, 2. Auflage*. Berlin: Springer Verlag, 1994

[RSB02] Rzepka, Bettina; Schröpel, Heydrun; Bertsche, Bernd: Studie zur Anwendung von Zuverlässigkeitsmethoden in der Industrie. In: *VDI-Berichte Nr. 1713: TTZ 2002 - Tagung Technische Zuverlässigkeit*, VDI Verlag, 2002

[Sch99] Schneeweiss, Winfried G.: *The fault tree method: from the field of reliability and safety technology*. Hagen: LiLoLe-Verlag, 1999

[Sch04] Schulz, Andreas; Fröhleke Norbert; Böcker J.: Modelling of Influences to a Linear-Drive-System. In: *11th International Power Electronics and Motion Control Conferences (EPE-PEMC 2004)*. Riga, Lettland, 2004

[Stö00] Stölzl, Stefan: *Fehlertolerante Pedaleinheit für ein elektromechanisches Bremssystem.* VDI Verlag, Düsseldorf, Technische Universität Darmstadt, Diss., 2000

[Sto96] Storey, Neil: *Safety-Critical Computer Systems.* Essex: Prentice Hall, 1996

[TDS03] Theobald, Axel; Dreyer, Marcus; Starsetzki, Thomas: *Online-Marktforschung, 2. Auflage.* Gabler Verlag, 2003

[Trä06a] Trächtler, Ansgar: Railcab - mit innovativer Mechatronik zum Schienenverkehrssystem der Zukunft. In: *VDE Kongress.* Aachen, 2006

[Trä06b] Trächtler, Eckehard; Vöcking H.: Iterative Learning and Self-Optimization Techniques for the Innovative RailCab-System. In: *32nd Annual Conference of the IEEE Industrial Electronics Society (IECON'06).* Paris, France, 2006

[TZZ98] Terninko, John; Zlotin, Boris; Zusman, Alla; Herb, Rolf (Hrsg.): *TRIZ - der Weg zum konkurrenzlosen Erfolgsprodukt.* Landsberg/Lech: mi, Verlag Moderne Industrie, 1998

[VDA06] *VDA: Qualitätsmanagement in der Automobilindustrie - Band 4 - Sicherung der Qualität vor Serieneinsatz - System FMEA.* 2006

[VDI88] *VDI 2244: Konstruieren sicherheitgerechter Erzeugnisse.* 1988

[VDI00] *VDI/VDE Richtlinie 3542 - Blatt 1: Sicherheitstechnische Begriffe für Automatisierungssysteme. Qualitative Begriffe.* 2000

[VDI04a] *VDI 2206: Entwicklungsmethodik für mechatronische Systeme.* 2004

[VDI04b] *VDI 4003-ENTWURF: Zuverlässigkeitsmanagement.* 2004

[VDI05] *VDI 4001-BLATT 2-ENTWURF: Terminologie der Zuverlässigkeit.* 2005

[wik] Wikimedia Foundation Inc.: *Verschiedene Webseiten der Kategorie "'Programmiersprache Java"'.* Website. – `http://www.wikipedia.de` zuletzt besucht am 10.08.2007

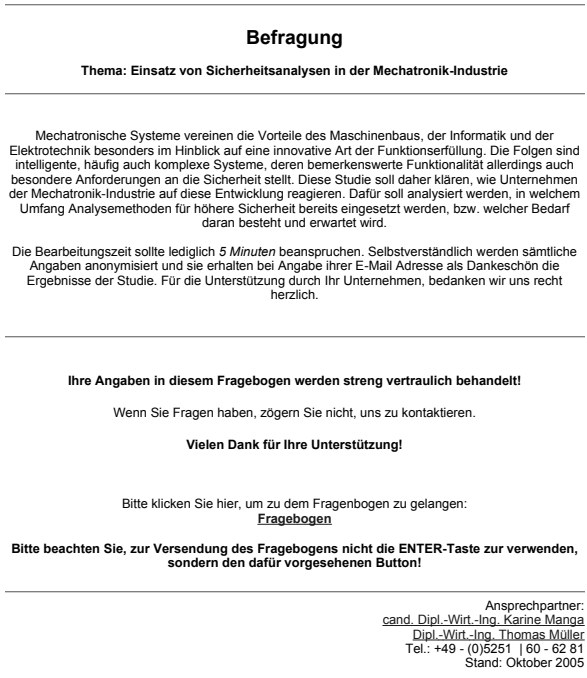
[WMW06] Walther, Michael; Müller, Thomas; Wallaschek, Jörg: Optimisation of mechatronic systems using dependability oriented design methods. In: *MSM - Mechatronic Systems and Materials*. Krakau, Polen, 2006

[WR97] Wang, J.; Ruxton, T.: Design for Safety. In: *Journal of American Society of Safety Engineers*, 1997

Anhang A

Datenmaterial zur Industrie-Studie

Das im Folgenden hinterlegte Material erweitert die Erläuterungen bzgl. der Industriestudie in Kapitel 3.1. Dies erfolgt neben eines Screenshot des Eröffungsbildschirms einerseits durch die Darstellung des verwendeten Fragebogens und andererseits durch das resultierende Datenmaterial.



Befragung

Thema: Einsatz von Sicherheitsanalysen in der Mechatronik-Industrie

Mechatronische Systeme vereinen die Vorteile des Maschinenbaus, der Informatik und der Elektrotechnik besonders im Hinblick auf eine innovative Art der Funktionserfüllung. Die Folgen sind intelligente, häufig auch komplexe Systeme, deren bemerkenswerte Funktionalität allerdings auch besondere Anforderungen an die Sicherheit stellt. Diese Studie soll daher klären, wie Unternehmen der Mechatronik-Industrie auf diese Entwicklung reagieren. Dafür soll analysiert werden, in welchem Umfang Analysemethoden für höhere Sicherheit bereits eingesetzt werden, bzw. welcher Bedarf daran besteht und erwartet wird.

Die Bearbeitungszeit sollte lediglich *5 Minuten* beanspruchen. Selbstverständlich werden sämtliche Angaben anonymisiert und sie erhalten bei Angabe ihrer E-Mail Adresse als Dankeschön die Ergebnisse der Studie. Für die Unterstützung durch Ihr Unternehmen, bedanken wir uns recht herzlich.

Ihre Angaben in diesem Fragebogen werden streng vertraulich behandelt!

Wenn Sie Fragen haben, zögern Sie nicht, uns zu kontaktieren.

Vielen Dank für Ihre Unterstützung!

Bitte klicken Sie hier, um zu dem Fragenbogen zu gelangen:
Fragebogen

Bitte beachten Sie, zur Versendung des Fragebogens nicht die ENTER-Taste zur verwenden, sondern den dafür vorgesehenen Button!

Ansprechpartner:
cand. Dipl.-Wirt.-Ing. Karine Manga
Dipl.-Wirt.-Ing. Thomas Müller
Tel.: +49 - (0)5251 | 60 - 62 81
Stand: Oktober 2005

Abbildung A.1: Screenshot des Eröffungsbildschirms zur Industrie-Studie

Fragebogen über den Einsatz von Sicherheitsanalysen und -prozessen

in Unternehmen der Mechatronik-Industrie

Nutzen Sie in Ihrem Unternehmen Analysemethoden um die Sicherheit zu erhöhen?

Ja ☐ Nein ☐ (Falls "Nein", können Sie bei Frage 8 fortfahren.)

Frage 2: Welche Methoden werden eingesetzt?

☐ FMEA (Fehlermöglichkeits- und Einflussanalyse)

☐ Vorläufige Sicherheitsanalyse (PHA)

☐ Funktionale Gefährdungsanalyse

☐ Gefahrenanalyse

☐ Fehlerbaumanalyse

☐ Ereignisbaumanalyse

☐ HAZOP (Hazard and Operability Study)

☐ SDA (Software Deviation Analysis)

☐ Markoff Simulation

☐ Monte Carlo Verfahren

☐ Weibullanalysen

☐ Checklisten

☐ Weitere: _____

Frage 3: Wie würden Sie die Einsatzhäufigkeit der Methoden charakterisieren?

Einmaliger Einsatz ☐ ☐ ☐ ☐ ☐ Entwicklungsbegleitend mit kontinuierlicher Aktualisierung

Abbildung A.2: Fragebogen (Teil 1/4)

Frage 4: ***Welche Kriterien treffen bei der Nutzung von Sicherheitsanalysen in Ihrem Unternehmen zu?***

- ☐ Analyseergebnisse werden dokumentiert und gespeichert
- ☐ Analyseergebnisse werden zur Dokumentation für den Kunden genutzt
- ☐ Bestehende Analysen werden bei nachfolgenden Neu- oder Variantenentwicklungen wieder verwendet
- ☐ Verschiedene Sicherheitsmethoden „kooperieren“ untereinander
- ☐ Sicherheitsmethoden sind innerhalb eines Entwicklungsprozesses integriert
- ☐ Ein durchgängiger Sicherheitsprozess existiert
- ☐ Weitere Anmerkungen: _____

Frage 5: ***Wer steht hinter der Motivation zum Einsatz von Sicherheitsmethoden?***

- ☐ Eigeninitiative
- ☐ Gesetzliche Forderungen
- ☐ Kundenforderungen
- ☐ Weitere Gründe: _____

Frage 6: ***Zu welchem Zeitpunkt der Produktentwicklung setzen Sie Sicherheitsanalysen ein?***

- ☐ Bereits bei der Klärung von Anforderungen
- ☐ Während der Konzipierungsphase
- ☐ Sobald Teillösungen bestehen
- ☐ Das eigentlich fertige Produkt wird einer Sicherheitsanalyse unterzogen
- ☐ Weitere Anmerkungen: _____

Abbildung A.3: Fragebogen (Teil 2/4)

Frage 7: Worauf liegt bei den von Ihnen genutzten Analysen der Fokus?

- ☐ Gesamtsystem
- ☐ Mechanik
- ☐ Elektrotechnik / Elektronik
- ☐ Software
- ☐ Menschliche Bedienung
- ☐ Weitere Anmerkungen: _____

Frage 8: Worin sehen Sie einen größeren Nutzen von Sicherheitsanalysen?

- ☐ Dokumentation von Fachwissen
- ☐ Strukturiertes Vorgehen
- ☐ Vorher unbekannte Aspekte werden aufgedeckt
- ☐ Nachweis, dass an Sicherheit gedacht wurde
- ☐ Nachweis, dass eine geforderte Sicherheit gewährleistet wird
- ☐ Sonstige (Welche?): _____

Frage 9: Welche Defizite zeigen diese Methoden?

- ☐ Hoher Aufwand bzw. hohe Kosten
- ☐ Geringe Akzeptanz der Methoden bei Mitarbeitern
- ☐ Sehr starke Abhängigkeit von Fachwissen
- ☐ Mehrwert der Methoden nur gering
- ☐ Sonstige (Welche?): _____

Abbildung A.4: Fragebogen (Teil 3/4)

Frage 10: ***Wie schätzen Sie die Nutzung von Sicherheitsanalysen in der Zukunft ein?***

- ☐ steigend
- ☐ sinkend
- ☐ gleich bleibend
- ☐ Begründung: _____

Frage 11: ***Wo sehen Sie speziellen oder besonders dringenden Forschungs- und Entwicklungsbedarf?***

_____

_____

_____

Unternehmensdaten:

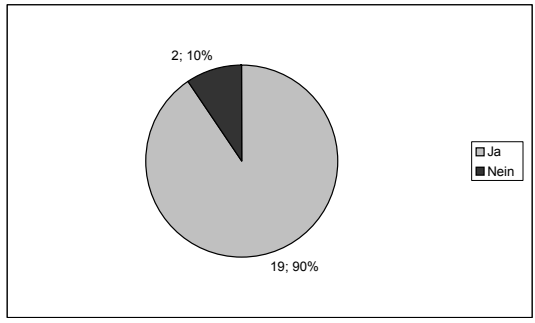
Name	
Branche	
Email	

Abbildung A.5: Fragebogen (Teil 4/4)

Frage 1 *Nutzen Sie in Ihrem Unternehmen Analysemethoden um die Sicherheit zu erhöhen?*

Antworten: 21

Ja	19	90%
Nein	2	10%



Frage 2 *Welche Methoden werden eingesetzt?*

Antworten: 19

FMEA (Fehlermöglichkeits- und Einflussanalyse)	13	68,4%
Vorläufige Sicherheitsanalyse (PHA)	1	5,3%
Funktionale Gefährdungsanalyse	7	36,8%
Gefahrenanalyse	8	42,1%
Fehlerbaumanalyse	6	31,6%
Ereignisbaumanalyse	0	0,0%
HAZOP (Hazard and Operability Study)	0	0,0%
SDA (Software Deviation Analysis)	1	5,3%
Markoff Simulation	0	0,0%
Monte Carlo Verfahren	1	5,3%
Weibullanalysen	0	0,0%
Checklisten	13	68,4%
Weitere	0	0,0%

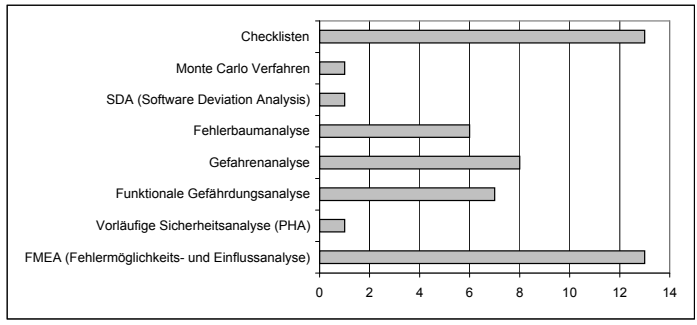


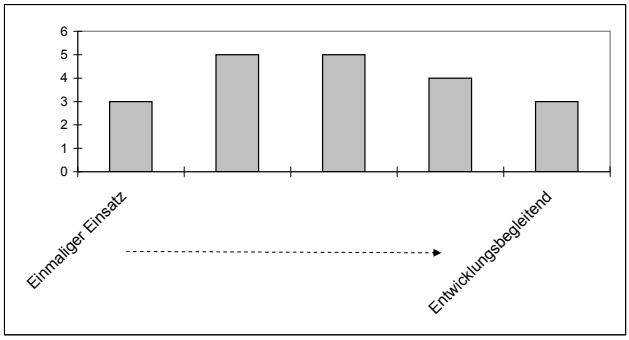
Abbildung A.6: Datenmaterial zur Industrie-Studie (Teil 1/6)

Frage 3 *Wie würden Sie die Einsatzhäufigkeit der Methoden charakterisieren?*

Antworten: 20

Einmaliger Einsatz	1	3	15%
	2	5	25%
	3	5	25%
	4	4	20%
Entwicklungsbegleitend	5	3	15%

Mittelwert 2,95



Frage 4 *Welche Kriterien treffen bei der Nutzung von Sicherheitsanalysen in Ihrem Unternehmen zu?*

Antworten: 19

Analyseergebnisse werden dokumentiert und gespeichert	16	84%
Analyseergebnisse werden zur Dokumentation für den Kunden genutzt	10	53%
Bestehende Analysen werden bei nachfolgenden Neu- oder Variantenentw. wieder verwendet	10	53%
Sicherheitsmethoden sind innerhalb eines Entwicklungsprozesses integriert	8	42%
Ein durchgängiger Sicherheitsprozess existiert	3	16%
Verschiedene Sicherheitsmethoden „kooperieren“ untereinander	1	5%

Weitere Anmerkungen:
Ein durchgängiger Sicherheitsprozess befindet sich im Aufbau.

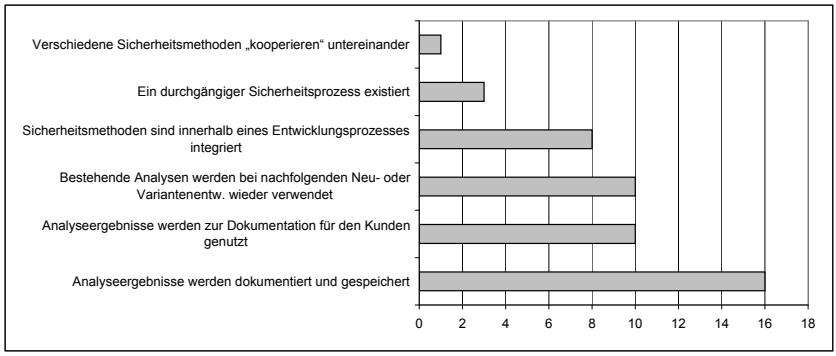


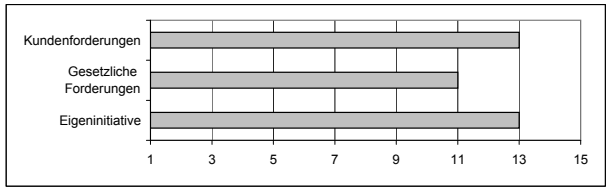
Abbildung A.7: Datenmaterial zur Industrie-Studie (Teil 2/6)

Frage 5 ***Wer steht hinter der Motivation zum Einsatz von Sicherheitsmethoden?***

Antworten: 19

Eigeninitiative	13	68%
Gesetzliche Forderungen	11	58%
Kundenforderungen	13	68%

Weitere Gründe (je einmal genannt - 5,3%):
"Masterarbeit"
"Zum einen Funktionen, die verstärkt die Betrachtung auf die Sicherheit erfordern. Zum anderen Erhöhung der Qualität
"Senkung der Garantiekosten"



Da mehrere Antworten möglich waren, sind nachfolgend die exakten Kombinationen dargestellt:

Eigeninitiative	3	16%
Gesetzliche Forderungen	2	11%
Eigeninitiative und Kundenforderungen	5	26%
Gesetzliche Forderungen und Kundenforderungen	4	21%
Eigeninitiative und Gesetzliche Forderungen	1	5%
Eigeninitiative, Kunden- und Gesetzliche Forderungen	4	21%

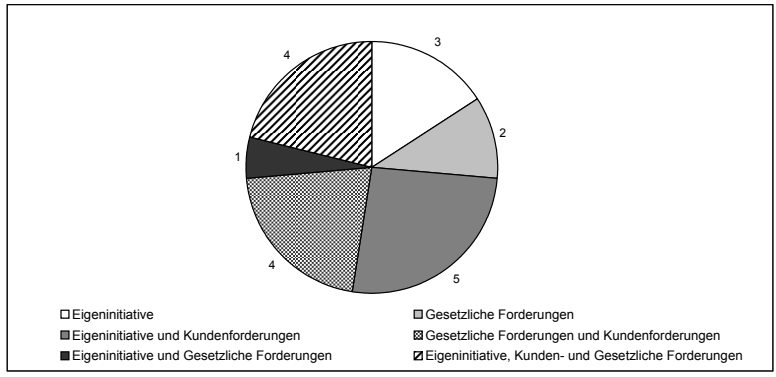


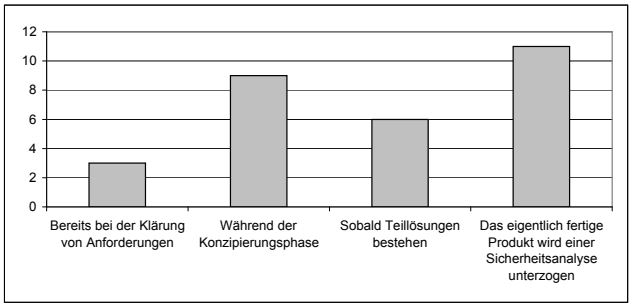
Abbildung A.8: Datenmaterial zur Industrie-Studie (Teil 3/6)

Frage 6 ***Zu welchem Zeitpunkt der Produktentwicklung setzen Sie Sicherheitsanalysen ein?***

Antworten: 18

Bereits bei der Klärung von Anforderungen	3	17%
Während der Konzipierungsphase	9	50%
Sobald Teillösungen bestehen	6	33%
Das eigentlich fertige Produkt wird einer Sicherheitsanalyse unterzogen	11	61%

Weitere Anmerkungen:
eine Erläuterung zu -Bereits während der Klärung der Anforderungen-:
"Konkret: nachdem die Produktanforderungen spezifiziert sind wird eine Riskoanalyse durchgeführt und die Sicherheitsanforderungen für das System festgelegt. Danach geht es in die Konzipierungsphase mit dem Systementwurf."



Frage 7 ***Worauf liegt bei den von Ihnen genutzten Analysen der Fokus?***

Antworten 19

Gesamtsystem	11	58%
Mechanik	6	32%
Elektrotechnik / Elektronik	6	32%
Software	2	11%
Menschliche Bedienung	6	32%

Weitere Anmerkungen:

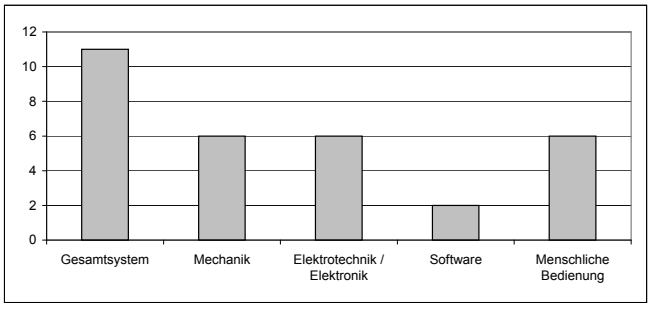


Abbildung A.9: Datenmaterial zur Industrie-Studie (Teil 4/6)

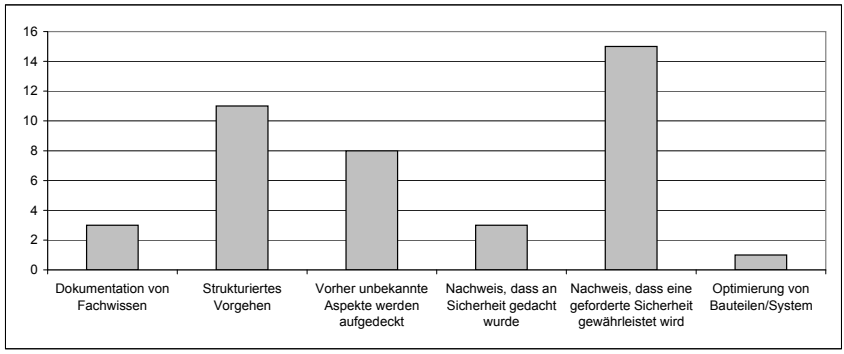
Frage 8 ***Worin sehen Sie einen größeren Nutzen von Sicherheitsanalysen?***

Antworten: 21

Dokumentation von Fachwissen	3	14%
Strukturiertes Vorgehen	11	52%
Vorher unbekannte Aspekte werden aufgedeckt	8	38%
Nachweis, dass an Sicherheit gedacht wurde	3	14%
Nachweis, dass eine geforderte Sicherheit gewährleistet wird	15	71%

Sonstige (Welche?)

Optimierung von Bauteilen/System	1	5%



Frage 9 ***Welche Defizite zeigen diese Methoden?***

Antworten: 20

Hoher Aufwand bzw. hohe Kosten	12	60%
Geringe Akzeptanz der Methoden bei Mitarbeitern	6	30%
Sehr starke Abhängigkeit von Fachwissen	13	65%
Mehrwert der Methoden nur gering	4	20%

Sonstige (Welche?)

Geringe Akzeptanz im Management	1	5%

...weil es länger dauert bis die ersten Ergebnisse in Form von Funktionen sichtbar sind und das obowohl das Verfahren dem Schutz des Management vor eventuellen Produkthaftungsfällen dient.

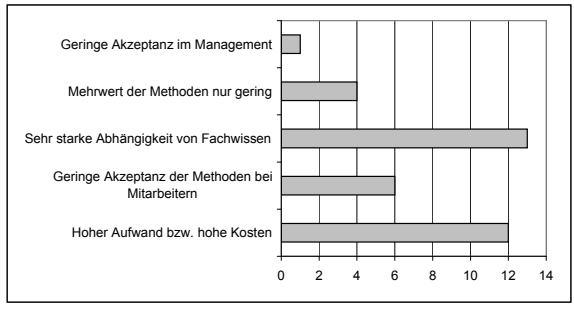


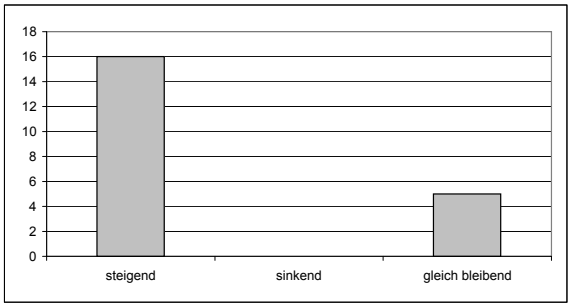
Abbildung A.10: Datenmaterial zur Industrie-Studie (Teil 5/6)

Frage 10 *Wie schätzen Sie die Nutzung von Sicherheitsanalysen in der Zukunft ein?*

Antworten: 21

steigend	16	76%
sinkend	0	0%
gleich bleibend	5	24%

Begründung (wurde wenn, dann nur bei steigend angegeben):
"Der Funktionsnachweis von mechatronischen Bauelementen unter Einwirkung möglichst beliebiger Randbedingungen wird in Zukunft noch wichtiger. Besonders die stabile Funktion im Gesamtsystem wird weiter in den Vordergrund der Betrachtung rücken."
"Sicherheitsstandards im Personenverkehr (Schienenverkehr) werden international steigen und nachgewiesene Sicherheit entscheidend für die Auftragsvergabe"
"Die zunehmende Anzahl von Funktionen, die statt bisher rein mechanisch mehr mechatronisch oder rein elektronisch realisiert werden. Dadurch wird es wichtiger systematisch insbesondere in der Software-Entwicklung vorzugehen und klare Strukturen zu schaffen."
"Die gesetzlichen Bestimmungen fordern in vielen Fällen eine Gefahrenanalyse"
"Steigende Sicherheitsanforderungen, einhergehend mit einer steigenden Systemkomplexität."
"Die Methode mit ihren Vorteilen wird sich stetig durchsetzen"
"Unsere Produkte werden immer komplexer; Für den Einsatz in der Prozesstechnik müssen die Produkte der EN 61508 entsprechen. Um die Produkte nach dieser Norm verkaufen zu können, müssen weitere Sicherheitsbetrachtungen und Analysen erstellt werden."



Frage 11 *Wo sehen Sie speziellen oder besonders dringenden Forschungs- und Entwicklungsbedarf?*

Antworten: 11

"Bislang sind zur Entwicklung von Komponenten mit sicherheitskritischer Funktion spezielle Kenntnisse über die Einsatzumgebung sowie über viele unterschiedliche Entwicklungswerkzeuge notwendig. Hier sind Entwicklungskonzepte gefragt, die die Zusammenhänge zeigen."
"Integration der Methoden für Hardware-/Softwaresysteme"
"Die einheitliche Europa-Norm wird in den Ländern unterschiedlich ausgelegt"
"in Tools zur wirtschaftlichen Softwareanalyse"
"Bessere Erforschung von Ausfallraten von Komponenten und beispielhaften Systemen. Entwicklung von praxisnahen Standardverfahren zur einfachen Realisierung von sicherheitsrelevanten Entwicklungen."
"Vereinheitlichung von Sicherheitsforderungen (Länder, Personen etc.)"
"Vereinfachung der Methoden Herstellen einer größeren Transparenz"
"Langzeitverhalten von Werkstoffen, hier Techn. Kunststoffe"
"Integration der Sicherheitsmethoden in den Produktentwicklungsprozess."
"Sicherheitsrelevante Betriebe, aber auch Verkehr und Haushalt"
"Ohne das Vorhandensein von statistischen Daten eine Ausfallwahrscheinlichkeit hervor sagen zu können. (EN 61508, EN 61511)"

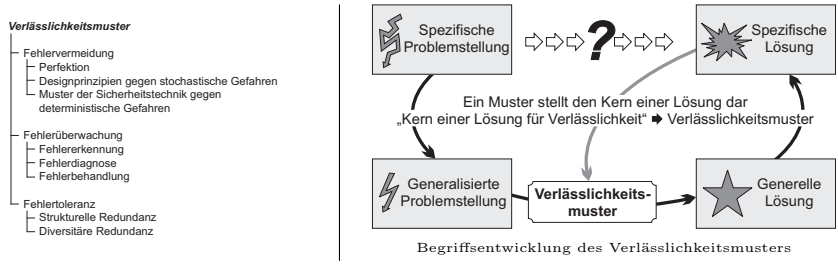
Abbildung A.11: Datenmaterial zur Industrie-Studie (Teil 6/6)

Anhang B

Katalog der Verlässlichkeitsmuster

Verlässlichkeitsmuster (Definition)

Verlässlichkeitsmuster repräsentieren den Kern von Lösungen, die die Verlässlichkeit von Systemen gewährleisten.



Begriffsentwicklung des Verlässlichkeitsmusters

Verlässlichkeitsmuster basieren auf dem Verständnis, dass spezifische Lösungen für verlässliches Verhalten von Systemen auf den Lösungskern reduziert werden können. Aus diesem Kern kann dann das lösungsneutrale Verlässlichkeitsmuster formuliert werden, das eine Wiederverwendung, auch bei geänderten Randbedingungen gewährleisten kann. Die Verlässlichkeitsmuster unterstützen den Entwickler während der Konzipierungsphase, indem Lösungen für spezifische Problemstellungen im Kontext der Verlässlichkeit entwickelt werden, die auf den Verlässlichkeitsmustern aufbauen. Beispiele dafür sind Redundanzstrukturen, Designregeln und prinzipielle Diagnosealgorithmen.

Der Begriff setzt sich aus den beiden Teilen Muster und Verlässlichkeit zusammen, deren Verknüpfung die Ursächlichkeit verdeutlichen soll, die das Muster besitzt, um eine erhöhte Verlässlichkeit von Systemen zu erreichen. Das Wissen, das durch das lösungsneutrale Verlässlichkeitsmuster repräsentiert wird, basiert u. a. auf Erfahrungswissen und Recherchearbeiten.

Die Verlässlichkeitsmuster lassen sich in drei Hauptkategorien unterteilen:
Fehlervermeidung beschreibt Verlässlichkeitsmuster, die die Fehlerursache, also den eigentlichen Fehler, bereits vor oder während der Entstehung verhindern.
Fehlerüberwachung beschreibt Verlässlichkeitsmuster, die einen Fehlerzustand erkennen, diagnostizieren und gegebenenfalls daraufhin Maßnahmen einleiten.
Fehlertoleranz beschreibt Verlässlichkeitsmuster, die trotz Ausfall von Teilsystemen die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten.

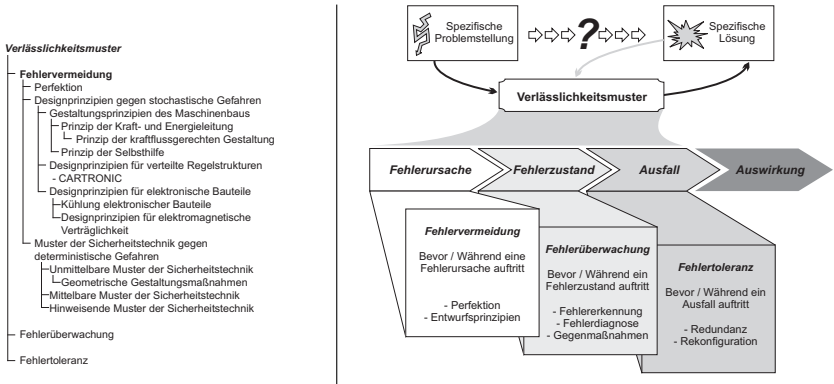
Weiterführende Informationen:

Müller, Thomas; Wallaschek, Jörg: General Concepts of Dependability in the Design of Mechatronic Systems. In: Research and Education in Mechatronics. Stockholm, 2006

Müller, Thomas; Wallaschek, Jörg: Musterdatenbank zur Konzipierung verlässlicher mechatronischer Systeme. In: VDI-Berichte 1984: TTZ2007 - Tagung Technische Zuverlässigkeit. Düsseldorf: VDI Verlag, 2007

Fehlervermeidung

Fehlervermeidung beschreibt Verlässlichkeitsmuster, die die Fehlerursache, also den eigentlichen Fehler, bereits vor oder während der Entstehung verhindern.



Def. und Kategorien für Verlässlichkeitsmuster

Verlässlichkeitsmuster der Fehlervermeidung verhindern den Fehler, bzw. die Fehlerursache, bereits vor oder während der Entstehung. Damit sind es diese Konzepte, deren Umsetzung primär verfolgt werden sollte. Zu den typischen Mustern der Fehlervermeidung zählen neben der wünschenswerten, aber leider unrealistischen Perfektion, die zahlreichen *Designprinzipien zur Vermeidung von stochastischen Fehlern.* Beispiele sind Überdimensionierung, Zwangsläufigkeit und Sabotagesicherheit [Pahl2001]. Auch die *Vermeidung von deterministischen Gefahren* durch bewährte Maßnahmen der unmittelbaren, mittelbaren und hinweisenden Sicherheitstechnik [Neudörfer2002], z. B. durch trennende Sicherheitsbarrieren, sind dieser Kategorie zuzuordnen. Weitere Unterkategorien für Verlässlichkeitsmuster der Fehlervermeidung sind selbstverständlich denkbar, werden an dieser Stelle allerdings nicht betrachtet.

Weiterführende Informationen:

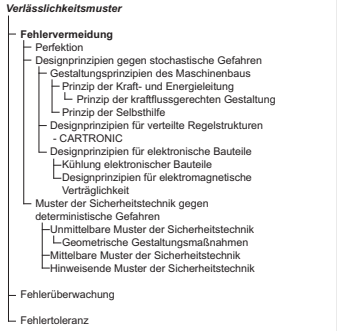
Pahl, Gerhard: Dubbel - Taschenbuch für den Maschinenbau: Kap.F: Grundlagen der Konstruktionstechnik. Grundlagen technischer Systeme und des methodischen Vorgehens. Springer-Verlag, 2001 [Pahl2001]

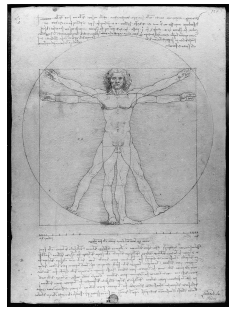
Neudörfer, Alfred: Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG Maschinenrichtlinie. Berlin: Springer-Verlag, 2002 [Neudörfer2002]

Müller, Thomas; Wallaschek, Jörg: Musterdatenbank zur Konzipierung verlässlicher mechatronischer Systeme. In: VDI-Berichte 1984: TTZ2007 - Tagung Technische Zuverlässigkeit. Düsseldorf: VDI Verlag, 2007

Perfektion

Perfektion beschreibt das wünschenswerte aber unrealistische Verlässlichkeitsmuster, Fehler dadurch zu vermeiden, dass das System zu 100% auf die tatsächlich auftretenden Belastungen ausgelegt ist.





Auch das Proportionsschema der menschlichen Gestalt nach Vitruv von Leonardo da Vinci ist nicht perfekt; es entspricht nur mit einer Abweichung von 1,7% dem Goldenen Schnitt [wikipedia2007]

Beim Muster der Perfektion wird versucht, von vornherein ein verlässliches System zu entwickeln, das exakt auf die tatsächlich auftretenden Belastungen abgestimmt ist. Leider ist diese Umsetzung zwar wünschens- und erstrebenswert, aber auch unrealistisch. Häufig wird das Prinzip der Perfektion im Systementwurf daher wie folgt umgesetzt: Das Streben nach Perfektion erfordert neben einer umfangreichen Spezifikation unter anderem ein planmäßiges Vorgehen, die Einhaltung von Normen und Standards, Formale Verifikation, Vermeidung von Nebeneffekten, Konsistenz des Systems und der Einzelkomponenten sowie Qualitätssicherungs-Maßnahmen. Je komplexer ein System wird, desto aufwendiger werden die zu ergreifenden Maßnahmen. Perfektion ist das Grundprinzip der Fehlervermeidung, da ein perfektes System keine Fehler aufweist. Da es aber sehr kostenintensiv ist und es immer Fehler gibt, deren Auftreten unvorhersehbar ist, kann man Perfektion zwar anstreben aber niemals erreichen.

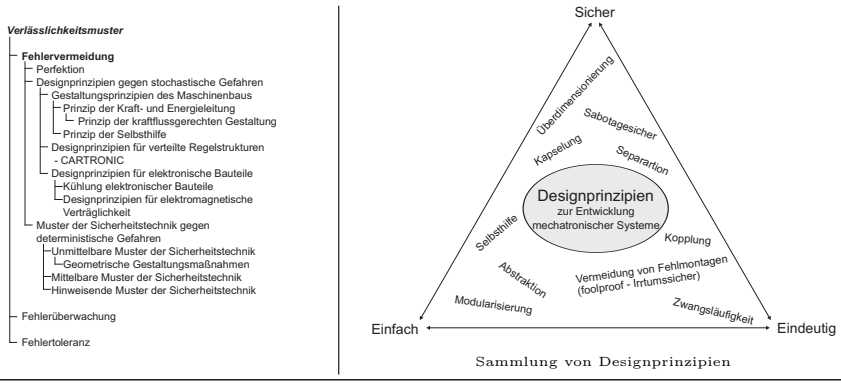
Weiterführende Informationen:

VDI Richtlinie 3780: Technikbewertung: Begriffe und Grundlagen, VDI Verlag, 1991

Wikimedia Foundation Inc.: Goldener Schnitt. Website - http://www.wikipedia.de - zuletzt besucht am 15.10.2007 [wikipedia2007]

Designprinzipien gegen stochastische Gefahren

Designprinzipien gegen stochastische Gefahren dienen zur Vermeidung von Fehlern, die während der Lebensdauer eines Systems mit unterschiedlicher Wahrscheinlichkeit auftreten. Die übergeordneten Prinzipien sind einfach, eindeutig und sicher.



Sammlung von Designprinzipien

Designprinzipien werden in der Domäne des Maschinenbaus z. B. durch [Pahl2001] unter den drei Oberbegriffen eindeutig, einfach und sicher subsumiert. *Eindeutigkeit* beschreibt dabei die klare Zuordnung und Erfüllung der technischen Funktion, *Einfachheit* die übersichtliche und möglichst elementare Gestaltung und *Sicherheit* die Haltbarkeit, Zuverlässigkeit, Unfallfreiheit und den Schutz für Mensch und Umwelt. Diese übergeordneten Gestaltungsprinzipien resultieren zwar aus der Maschinenbaudomäne, sind aber übertragbar auf andere Domänen oder interdisziplinäre Bereiche wie die Mechatronik. Innerhalb dieser Kategorien lassen sich weitere, teilweise abstrakte Designprinzipien einordnen, die jedoch häufig Bezüge zu mehr als einer Kategorie aufweisen. Die Abbildung zeigt eine Auswahl von Designprinzipien. Beispiele für unterlagerte Designprinzipien gegen stochastische Gefahren sind Überdimensionierung und Zwangsläufigkeit [Pahl2001].

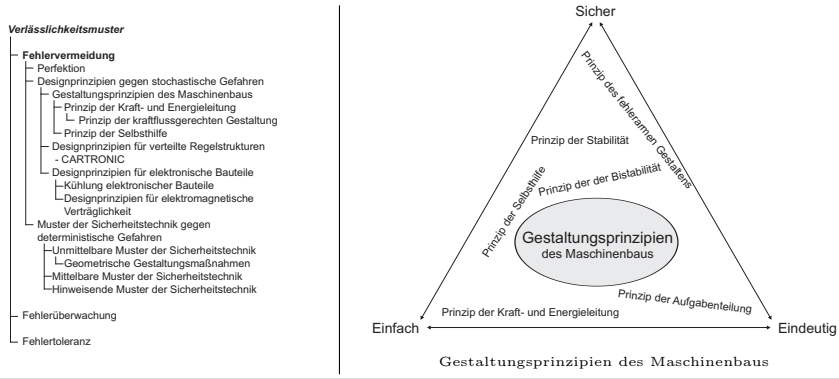
Weiterführende Informationen:

Pahl, Gerhard: Dubbel - Taschenbuch für den Maschinenbau: Kap.F: Grundlagen der Konstruktionstechnik. Grundlagen technischer Systeme und des methodischen Vorgehens. Springer-Verlag, 2001 [Pahl2001]

Leyer, A.: Maschinenkonstruktionslehre. Birkhäuser Verlag, 1963

Gestaltungsprinzipien des Maschinenbaus

Die übergeordneten Enwturfsregeln des Maschinenbaus (einfach, eindeutig und sicher) werden dadurch erfüllt, dass verschiedene *Gestaltungsprinzipien* befolgt werden, wie z. B. Prinzipien der Kraft- und Energieleitung.



Gestaltungsprinzipien des Maschinenbaus

Designprinzipien werden in der Domäne des Maschinenbaus durch den Einsatz verschiedener Gestaltungsregeln erfüllt. Eine Auswahl davon ist nachfolgend aufgeführt, wobei diese sich teilweise weiter untergliedern lassen [Pahl2001]:

- Prinzip der Kraft- und Energieleitung
- Prinzip der Aufgabenteilung
- Prinzip der Selbsthilfe
- Prinzip der Stabilität
- Prinzip der Bistabilität
- Prinzip des fehlerarmen Gestaltens

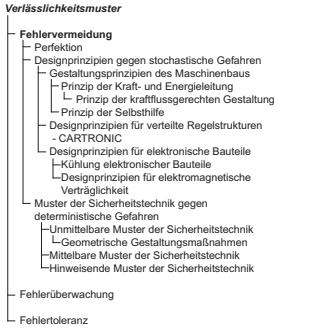
Weiterführende Informationen:

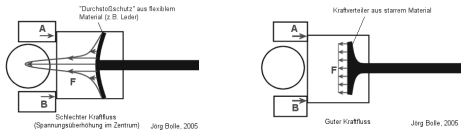
Pahl, Gerhard: Dubbel - Taschenbuch für den Maschinenbau: Kap.F: Grundlagen der Konstruktionstechnik. Grundlagen technischer Systeme und des methodischen Vorgehens. Springer-Verlag, 2001 [Pahl2001]

Leyer, A.: Maschinenkonstruktionslehre. Birkhäuser Verlag, 1963

Prinzip der Kraft- und Energieleitung

Prinzipien der Kraft- und Energieleitung sind Gestaltungsprinzipien des Maschinenbaus, um Fehler zu vermeiden, die z. B. auf falscher Kraftflussplanung oder -verteilung basieren. Sie unterstützen bei der Aufgabe, Kräfte und Momente fehlerfrei aufzunehmen und zu leiten.





Kraftflussgerechte Gestaltung als exemplarisches Prinzip der Kraft- und Energieleitung am Beispiel eines Pfeils [Bolle2005]

Prinzipien der Kraft- und Energieleitung vermeiden Fehler zu hoher Biege- oder Torsionsbelastungen und schließen auch die Vermeidung ungewollter Verformungen mit ein. Folgende Prinzipien beschreiben das oberlagerte Prinzip der Kraft- und Energieleitung [Pahl2001]:

- Prinzip der kraftflussgerechten Gestaltung
- Prinzip der gleichen Gestaltfestigkeit
- Prinzip der direkten und kurzen Krafteinleitung
- Prinzip der abgestimmten Verformung
- Prinzip des Kraftausgleichs

Weiterführende Informationen:

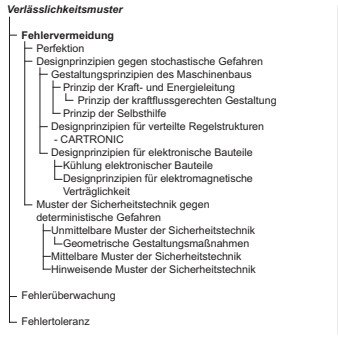
Pahl, Gerhard: Dubbel - Taschenbuch für den Maschinenbau: Kap.F: Grundlagen der Konstruktionstechnik. Grundlagen technischer Systeme und des methodischen Vorgehens. Springer-Verlag, 2001 [Pahl2001]

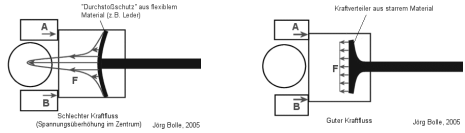
Leyer, A.: Maschinenkonstruktionslehre. Birkhäuser Verlag, 1963

Jörg Bolle: Sicherheit beim Bogenschießen im LARP. Website - http://www.section32.de/fantasy/larppfeilsicherheit/index.html - zuletzt besucht am 15.10.2007 [Bolle2005]

Prinzip der kraftflussgerechten Gestaltung

Das *Prinzip der kraftflussgerechten Gestaltung* unterstützt den konstruktiven Entwurf mit Hilfe eines anschaulichen Vorstellungsbildes des Kraftflusses.





Kraftflussgerechte Gestaltung eines Larppfeil [Bolle2005]

Die anschauliche Größe des Kraftflusses beschreibt das Leiten von Kräften, ist aber physikalisch nicht begründbar [Pahl2001]. Im Querschnitt eines Bauteils stellt man sich durchgeleitete Kräfte und Momente im Fluss vor, die den folgenden Forderungen entsprechen müssen:

- Der Kraftfluss muss stets geschlossen sein.
- Scharfe Umlenkungen des Kraftflusses sind zu vermeiden.
- Änderungen der Kraftflussdichte infolge schroffer Querschnittsänderungen sind zu vermeiden.

Bei komplexen Kraftleitungssituationen hilft die Definition einer Kraftfluss-Hüllfläche. Außerhalb dieser Hüllfläche treten keine weiteren Kräfte auf.

Weiterführende Informationen:

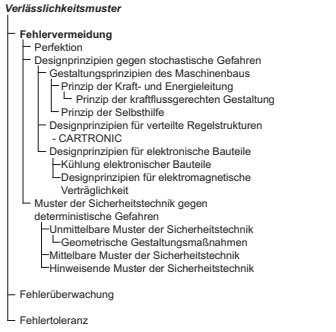
Pahl, Gerhard: Dubbel - Taschenbuch für den Maschinenbau: Kap.F: Grundlagen der Konstruktionstechnik. Grundlagen technischer Systeme und des methodischen Vorgehens. Springer-Verlag, 2001 [Pahl2001]

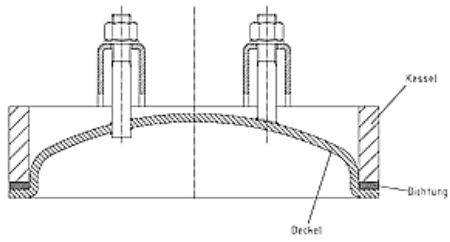
Leyer, A.: Maschinenkonstruktionslehre. Birkhäuser Verlag, 1963

Jörg Bolle: Sicherheit beim Bogenschießen im LARP. Website - http://www.section32.de/fantasy/larppfeilsicherheit/index.html - zuletzt besucht am 15.10.2007 [Bolle2005]

Prinzip der Selbsthilfe

Prinzipien der Selbsthilfe erzielen im System sich gegenseitig unterstützende Wirkungen, die zur besseren Funktionserfüllung und Fehlervermeidung genutzt werden.





Selbsthilfe am Beispiel eines Dampfkessels, der bei innerem Überdruck zusätzlich selbstdichtend wirkt [idt-dichtungen.de]

Das Prinzip der Selbsthilfe versucht, im System eine sich gegenseitig unterstützende Wirkung zu erzeugen. Diese soll eine bessere Funktionserfüllung erzielen und bei Überlast helfen, Schäden zu vermeiden. Die Gesamtwirkung eines Selbsthilfe-Prinzips resultiert somit aus einer Ursprungswirkung und einer Hilfswirkung. Sub-Prinzipien der Selbsthilfe sind nachfolgend dargestellt und kurz erläutert [Pahl2001]:

- *Selbstverstärkende Lösungen:* Die Gesamtwirkung wird durch sich gegenseitig verstärkende Prinzipien erzeugt; z. B. bei einer sich selbstverstärkenden Seilklemme.
- *Selbstausgleichende Lösungen:* Die Gesamtwirkung kann dadurch erhöht werden, dass die Hilfswirkung der Ursprungswirkung entgegenwirkt und damit einen Ausgleich schafft. Einsatz findet dieses Prinzip z. B. bei der Anordnung von Schaufeln in Strömungsmaschinen.
- *Selbstschützende Lösungen:* Zum Schutz vor Überlast kann die Hilfswirkung einen zusätzlichen Kraftleitungsweg durch Umverteilung oder Veränderung der Beanspruchungsart realisieren. Ein Beispiel ist das Fließen von Bauteilen an Stellen zu hoher Spannung.

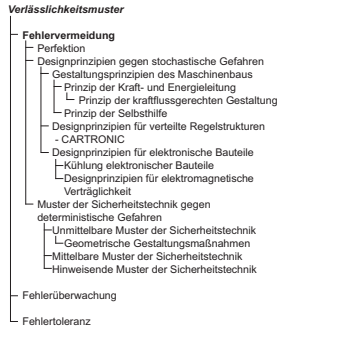
Weiterführende Informationen:

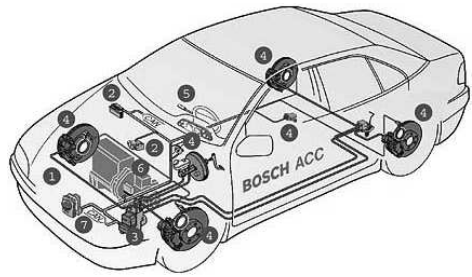
Pahl, Gerhard: Dubbel - Taschenbuch für den Maschinenbau: Kap.F: Grundlagen der Konstruktionstechnik. Grundlagen technischer Systeme und des methodischen Vorgehens. Springer-Verlag, 2001 [Pahl2001]

Kühnpast, R.: Das System der selbsthelfenden Lösungen in der maschinenbaulichen Konstruktion. Diss., Darmstadt, 1968

Designprinzipien für verteilte Regelstrukturen - CARTRONIC

Sammlung von exemplarischen Designprinzipien für den Entwurf der Funktionsarchitektur von verteilten Regelaufgaben im Automobil.





Verteilte Regelaufgaben im Automobil [www.offis.de]

Für den Entwurf der Funktionsarchitektur von verteilten Regelaufgaben im Automobil sind nachfolgend exemplarische Designprinzipien aufgezählt. Diese wurden im Rahmen der offenen Architektur *CARTRONIC* eines Automobilzulieferers entwickelt für vernetzende Steuergeräte in Fahrzeugen [Bertram1999]:

- Jedes System/Jede Komponente besteht aus eigenständigen unabhängigen Komponenten mit einer minimalen Anzahl an physischen Schnittstellen.
- Jedes System/Jede Komponente erfüllt autonom die eindeutig definierte Aufgabe durch Beschaffen von Informationen und Einleiten von Befehlen.
- Übergeordnete Entscheidungskomponenten koordinieren Systeme/Komponenten; diese sind z. B. dafür verantwortlich, dass aus konkurrierenden Abfragen eine einzelne Information hergeleitet wird.
- Befehle werden hierarchisch vom Initiator zum Aktuator/Auslöser propagiert.
- Die Schnittstellen von jedem System/jeder Komponente sind so vielen anderen wie notwendig bekannt und so wenigen wie möglich.

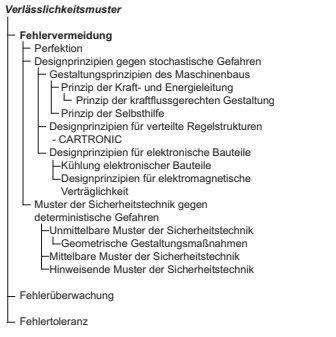
Weiterführende Informationen:

Bertram, Torsten; Dominke, Peter; Müller, Bernd: The Safety-Related Aspect of CARTRONIC. In: SAE International Congress & Exposition, Detroit(USA), 1999 [Bertram1999]

Hedenetz, B.: Entwurf von verteilten fehlertoleranten Elektronikarchitekturen in Kraftfahrzeugen. Diss., Tübingen, 2001

Designprinzipien für elektronische Bauteile

Sammlung von exemplarischen Designprinzipien für den Entwurf elektronischer Bauteile.



keine Abbildung vorhanden

Die nachfolgend dargestellte Sammlung enthält Entwicklungs- und Konstruktionsrichtlinien für die Zuverlässigkeit elektronischer Bauteile nach [Birolini1991]:

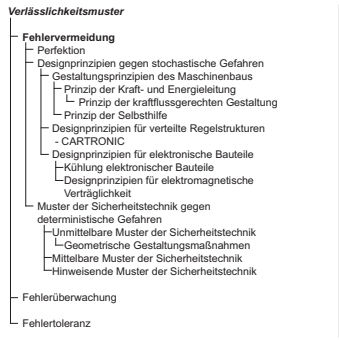
- Elektrische/Thermische *Unterlastung* elektronischer Bauteile wird mittels Belastungsfaktoren zwischen 0 und 1 beim Entwurf berücksichtigt, da die Belastung einen großen Einfluss auf die Ausfallrate besitzt.
- Die Chiptemperatur der Halbleiterbauteile muss möglichst niedrig gehalten werden. Sie setzt sich zusammen aus der Umgebungstemperatur und der durch eigene Verlustleistung verursachten Temperaturerhöhung. Einflüsse: Konstruktion und Gehäuse des Bauteils, vorhandene Kühlkörper und -mittel
- Feuchtigkeit soll möglichst vermieden werden. Dabei ist weniger der Wasserdampf störend, sondern die in ihm aufgelösten Verunreinigungen und Gase können durch Korrosion und Elektrolyse metallische Kontakte und Leiterbahnen angreifen und sind daher kritisch: Tau- oder Eisbildung auf den Bauteilen vermeiden; mögliche Schutzmechanismen: Kühlung, Verhinderung galvanischer Materialpaarungen z. B. durch Schutzlackierungen.
- Äußeren elektromagnetischen Störungen soll widerstanden werden und die eigene Störung nach Außen soll unterhalb einer Grenze bleiben. Je energiereicher und kürzer die Anstiegszeiten, desto gefährlicher sind die elektromagnetischen Störungen. Wichtige Störverursacher sind Schaltvorgänge, elektrostatische Entladungen und Emissionen. Für die Reduzierung der Störungen existieren wiederum zahlreiche detailliertere Regeln wie z. B. *Möglichst breite Speiseleiter verwenden* oder *Öffnungen in schirmenden Gehäusen vermeiden.*

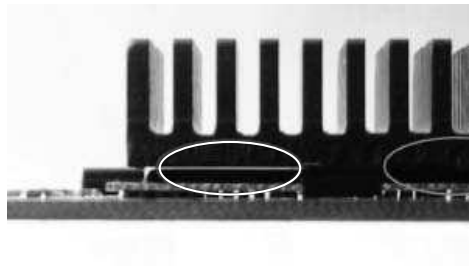
Weiterführende Informationen:

Birolini, Allessandro: Qualität und Zuverlässigkeit technischer Systeme. Berlin: Springer-Verlag, 1991 [Birolini1991]

Kühlung elektronischer Bauteile

Überschüssige Verlustleistung (Wärme) wird zum Schutz einer Schaltung und zur Aufrechterhaltung eines sicheren Betriebs abgeleitet.





Passives Kühl-Prinzip von elektronischen Bauteilen; Luftspalt zwischen Kühlkörper und Bauteil kann trotzdem zum Ausfall führen [Lehnberger2004]

Die Temperatur elektronischer Bauteile, z. B. die Chiptemperatur eines Halbleiterbauteils, muss möglichst gering gehalten werden. Sie setzt sich aus der Umgebungstemperatur und der Temperaturerhöhung aus der eigenen Verlustleistung zusammen. Es gibt generell zwei Arten, ein Bauteil vor temperaturbedingten Beschädigungen zu schützen:

- *Passive Kühlung:* Die Dimensionierung der Kühlflächen sowie der thermische Widerstand zwischen den Kühlflächen ist zu beachten; z. B. realisiert durch Kühlkörper, Gehäuse und Leiterplattendesign.
- *Aktive Kühlung:* Der Luftstrom und das Umwälzvolumen sind zu beachten; z. B. realisiert mittels eines Lüfters.

Auch die Kühlung von LED sind ein weiteres Beispiel für dieses Muster. Im KFZ-Scheinwerfer werden dafür sogar eigens Lüfter eingebaut.

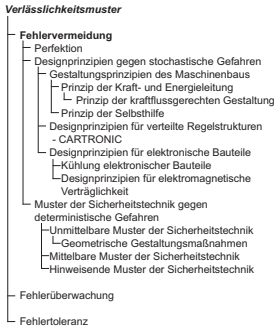
Weiterführende Informationen:

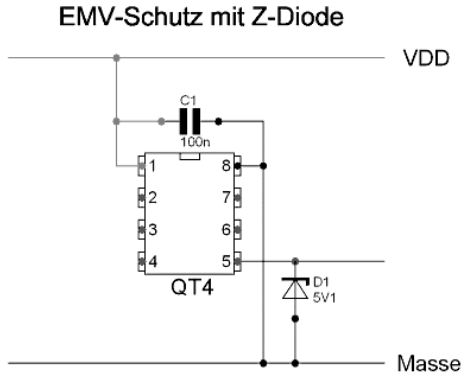
Birolini, Allessandro: Qualität und Zuverlässigkeit technischer Systeme. Berlin: Springer-Verlag, 1991

Lehnberger, C.; Oberender L.: Über die Entwärmung von elektronischen Baugruppen - Strategien zur Elektronikkühlung. 2004 [Lehnberger2004]

Designprinzipien für elektromagnetische Verträglichkeit

Designprinzipien, um äußeren elektromagnetischen Störungen zu widerstehen und um den Pegel eigener Störungen nach außen unterhalb gegebener Grenzwerte zu halten.





EMV-Schutz mit Z-Diode [om.dharlos.de]

Als elektromagnetische Verträglichkeit, abgekürzt EMV, bezeichnet man die Fähigkeit eines Systems, in der elektromagnetischen Umwelt zufriedenstellend zu arbeiten, ohne dabei selbst elektromagnetische Störungen zu verursachen. Dies bedeutet, dass die entsprechenden Baugruppen so zu gestalten sind, dass Störungen durch Schaltvorgänge mit galvanischer, kapazitiver oder induktiver Kopplung, statische Entladung und Emissionen eliminiert bzw. reduziert werden, sowie das Eindringen dieser Störgrößen in die Baugruppe vermieden wird. Einige Lösungsansätze zum Erreichen von EMV sind nachfolgend aufgelistet [Birolini1991]:

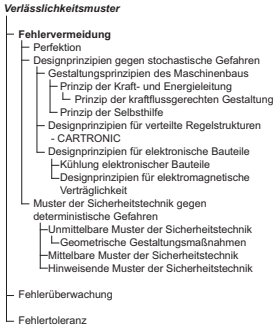
- Möglichst große Masseflächen verwenden
- Bei galvanisch nicht getrennten Systemen, Logikmasse und Masse der Leistungselektronik getrennt verdrahten
- Breite Speiseleiter verwenden
- Induktivitätsarme Stützkondensatoren verwenden
- Bei größerer Impulsbelastung, Spannungsregler direkt auf der Leiterplatte montieren
- Störverursacher in unmittelbarer Nähe entstören
- Keine schnellere Logik als notwendig verwenden
- Wellenanpassung bei langen Signalleitungen
- Signal- und Rückführleitungen verdrillen, Kabelschirme beidseitig auf Masse legen
- Leistungsreiche Störimpulse am Anfang und Ende von Leitungen eliminieren
- Dynamische Belastung der Bauteile beachten, transiente Laufzeiten berücksichtigen
- Öffnungen in schirmenden Gehäusen vermeiden
- Definierte Ableitpfade für elektrostatische Entladung einführen
- Äußere Störungen durch Absorption und/oder Reflexion bekämpfen
- Netzfilter mit eigener Abschirmung verwenden
- Große Gleichtaktunterdrückung anstreben

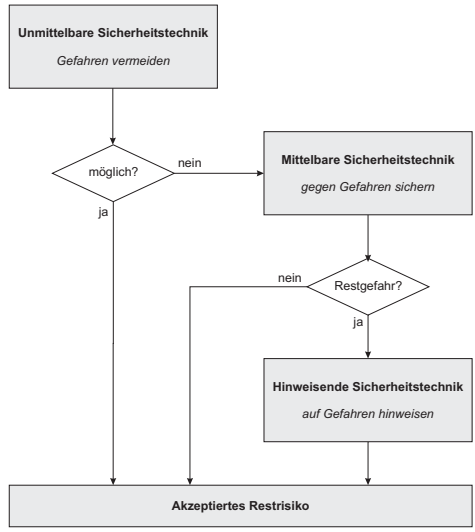
Weiterführende Informationen:

Birolini, Allessandro: Qualität und Zuverlässigkeit technischer Systeme. Berlin: Springer-Verlag, 1991 [Birolini1991]

Muster der Sicherheitstechnik gegen deterministische Gefahren

Verlässlichkeitsmuster zur Vermeidung deterministischer Gefahren repräsentieren die klassischen *unmittelbaren*, *mittelbaren* und *hinweisenden Konzepte der Sicherheitstechnik*.





Ablaufhierarchie zur Nutzung der Verlässlichkeitsmuster für unmittelbare, mittelbare und hinweisende Sicherheitstechnik [Neudörfer2002]

Strukturiert dargestellt werden die Muster der Sicherheitstechnik gegen deterministische Gefahren z. B. in [Neudörfer2002]: Bei der Anwendung dieser Muster wird gemäß der Abbildung vorgegangen, sodass die identifizierten Gefahren zuerst durch Konzepte der unmittelbaren Sicherheitstechnik vermieden werden sollen. Erst wenn dies nicht möglich ist, werden mittelbare Sicherheitskonzepte umgesetzt, um gegen Gefahren zu sichern, bevor nicht zu vermeidende Restgefahren durch hinweisende Muster angezeigt werden. Neben den umgesetzten Sicherheitskonzepten verbleibt dann das akzeptierte Restrisiko.

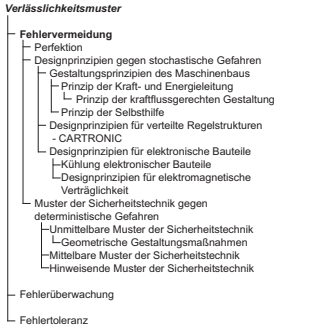
Weiterführende Informationen:

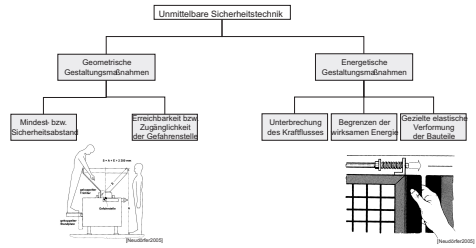
Neudörfer, Alfred: Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG Maschinenrichtlinie. Berlin: Springer-Verlag, 2002 [Neudörfer2002]

VDI Richtlinie 2244: Konstruieren sicherheitsgerechter Erzeugnisse, VDI Verlag, 1988

Muster der unmittelbaren Sicherheitstechnik

Verlässlichkeitsmuster der *unmittelbaren Sicherheitstechnik* beschreiben Konzepte, die der Vermeidung und Minimierung von Gefahren dienen und nicht manipulierbar sind.





Unmittelbare Sicherheitstechnik [Neudörfer2002]

Umgesetzt werden die Muster der unmittelbaren Sicherheitstechnik durch geometrische und energetische Gestaltungsmaßnahmen. Beispiele der ersten Kategorie sind Mindest- und Sicherheitsabstände oder anderweitige Beschränkungen der Zugänglichkeit von Gefahrenstellen, die durch die geometrischen Abmaße des Systems oder der Maschine festgelegt sind. Beispiele für energetische Gestaltungsmaßnahmen sind eine Begrenzung der wirksamen Energie oder eine gezielte elastische Verformung von Bauteilen.

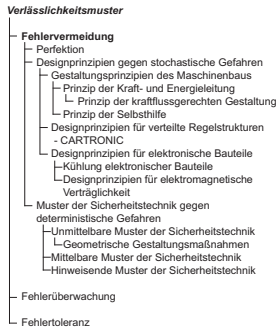
Weiterführende Informationen:

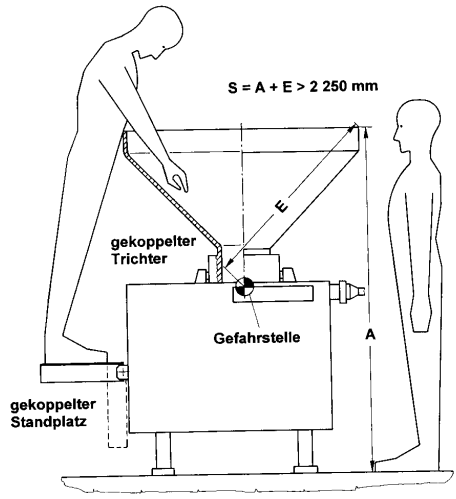
Neudörfer, Alfred: Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG Maschinenrichtlinie. Berlin: Springer-Verlag, 2002 [Neudörfer2002]

VDI Richtlinie 2244: Konstruieren sicherheitsgerechter Erzeugnisse, VDI Verlag, 1988

Geometrische Gestaltungsmaßnahmen

Geometrische Gestaltungsmaßnahmen sind Verlässlichkeitsmuster der unmittelbaren Sicherheitstechnik, die versuchen, das Enstehen oder die Zugänglichkeit von Gefahrenstellen oder das Auftreten von Gefahrensituationen durch intelligente räumliche Gestaltung des Systems oder der Umgebung zu vermeiden.





Geometrische Gestaltungsmaßnahmen verhindern die Zugänglichkeit von Gefahrenstellen [Neudörfer2002]

Geometrische Gestaltungsmaßnahmen funktionieren durch formgebende Gestaltung und Werkstoffauswahl. Zugänglichkeit, Mindest- und Sicherheitsabstände zu Gefahrenstellen werden dafür nicht manipulierbar konstruiert. Besonders relevant ist hier der Zusammenhang zwischen den Abmessungen von Maschinen und den Körpergrößen von Menschen. Unterlagerte Prinzipien sind *Abstand*, *Abmessungen von Bauteilen* und *Zugänglichkeit* [Neudörfer2002].

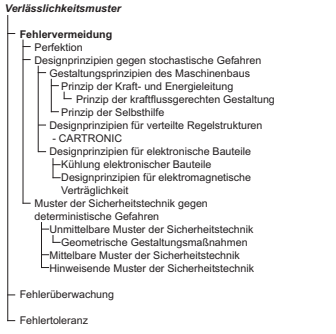
Weiterführende Informationen:

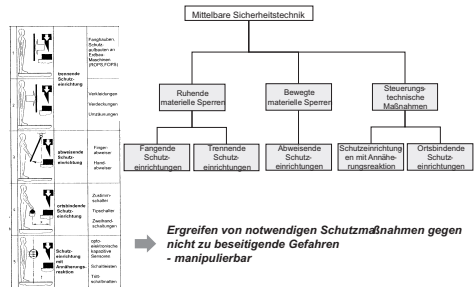
Neudörfer, Alfred: Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG Maschinenrichtlinie. Berlin: Springer-Verlag, 2002 [Neudörfer2002]

VDI Richtlinie 2244: Konstruieren sicherheitsgerechter Erzeugnisse, VDI Verlag, 1988

Muster der mittelbaren Sicherheitstechnik

Verlässlichkeitsmuster der *mittelbaren Sicherheitstechnik* werden verwendet, wenn die Gefahren mit unmittelbaren Konzepten nicht zu beseitigen sind. Diese Muster sichern gegen Gefahren und müssen zusätzlich konzipiert werden.





Mittelbare Sicherheitstechnik [Neudörfer2002]

Verlässlichkeitsmuster der *mittelbaren Sicherheitstechnik* umfassen Konzepte mittels ruhender und bewegter Sperren sowie Konzepte, die durch steuerungstechnische Maßnahmen realisiert werden. Diese mittelbaren Konzepte sind im Gegensatz zu den unmittelbaren allerdings manipulierbar. Beispiele für ruhende Sperren sind fangende oder trennende Schutzeinrichtungen wie Fanghauben und Verkleidungen; für steuerungstechnische Maßnahmen können z. B. ortsbindende Zweihandschaltungen oder Schutzeinrichtungen mittels Annäherungsreaktion genannt werden. Außerdem gehören auch Verriegelungen und andere Zuhaltungsmechanismen zu den mittelbaren Konzepten [Neudörfer2002].

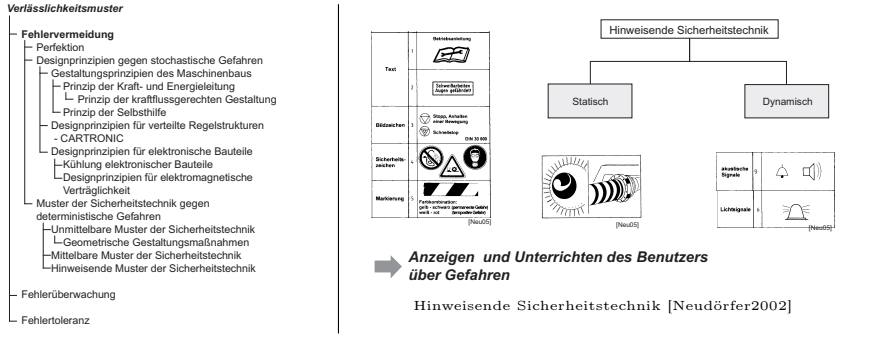
Weiterführende Informationen:

Neudörfer, Alfred: Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG Maschinenrichtlinie. Berlin: Springer-Verlag, 2002 [Neudörfer2002]

VDI Richtlinie 2244: Konstruieren sicherheitsgerechter Erzeugnisse, VDI Verlag, 1988

Muster der hinweisenden Sicherheitstechnik

Verlässlichkeitsmuster der *hinweisenden Sicherheitstechnik* werden verwendet, wenn unmittelbare und mittelbare Konzepte nicht umzusetzen sind.



Hinweisende Sicherheitstechnik [Neudörfer2002]

Die Muster der hinweisenden Sicherheitstechnik informieren in statischer oder dynamischer Form über die verbliebenen Gefahren nach Anwendung der unmittelbaren und mittelbaren Sicherheitstechnik. Sie sollten als letztes Mittel eingesetzt werden, da sie keinen direkten Einfluss auf eine Gefahrensituation nehmen können, sondern nur auf das Sicherheitsbewusstsein der handelnden Person abzielen. Es werden somit Verhaltensrichtlinien im Umgang mit gefährlichen Teilen sowie in Gefahrensituationen gegeben und es wird auf Gefahrenstellen hingewiesen.
Hinweisende Muster der Sicherheitstechnik teilen sich in statisch hinweisende Muster und dynamisch hinweisende Muster der Sicherheitstechnik. Statische Muster der hinweisenden Sicherheitstechnik sind z. B. Bedienungsanleitungen, Schilder und Markierungen, während Beispiele für dynamische Muster in diesem Kontext Licht- oder akustische Signale sein können [Neudörfer2002].

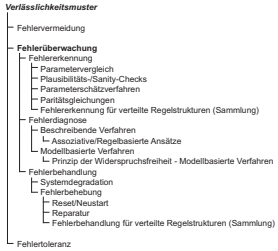
Weiterführende Informationen:

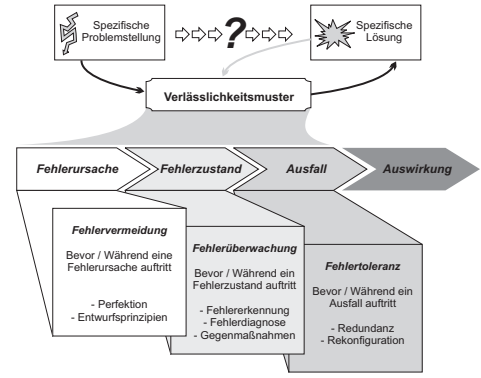
Neudörfer, Alfred: Konstruieren sicherheitsgerechter Produkte - Methoden und systematische Lösungssammlungen zur EG Maschinenrichtlinie. Berlin: Springer-Verlag, 2002 [Neudörfer2002]

VDI Richtlinie 2244: Konstruieren sicherheitsgerechter Erzeugnisse, VDI Verlag, 1988

Fehlerüberwachung

Fehlerüberwachung beschreibt Verlässlichkeitsmuster, die einen Fehlerzustand erkennen, diagnostizieren und gegebenenfalls daraufhin Maßnahmen einleiten.





Def. und Kategorien für Verlässlichkeitsmuster

Verlässlichkeitsmuster der Fehlerüberwachung erkennen und diagnostizieren Fehlerzustände und leiten gegebenenfalls erste Maßnahmen ein. Sie unterteilen sich daher in die Kategorien *Fehlererkennung*, *Fehlerdiagnose* und *Fehlerbehandlung*. Die Fehlererkennung beinhaltet dabei *nur* die Möglichkeit, Abweichungen vom Soll-Wert zu identifizieren, z. B. durch klassischen Parametervergleich, Paritätsgleichungen oder Plausibilitäts-Checks. Kommt neben dem Wissen um Abweichungen noch Wissen über das Fehlerverhalten hinzu, so kann die Abweichung durch Muster der Fehlerdiagnose, z. B. durch beschreibende und modellbasierte Diagnoseverfahren, analysiert werden. Im Falle eines identifizierten Fehlers oder einer Abweichung vom Soll-Wert können Verlässlichkeitsmuster zur Fehlerbehebung oder -eingrenzung im Sinne resultierender Maßnahmen angewendet werden; ein Neustart des Systems, eine Reparatur oder ein Austausch sind Beispiele dafür. Ein Muster in diesem Bereich ist ebenfalls die Systemdegradation, die das Einschränken der Funktionalität des Systems oder einzelner Komponenten beschreibt.

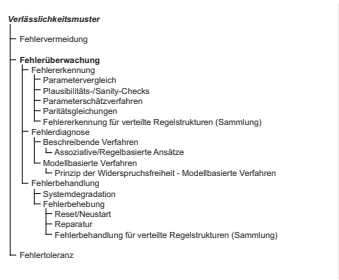
Weiterführende Informationen:

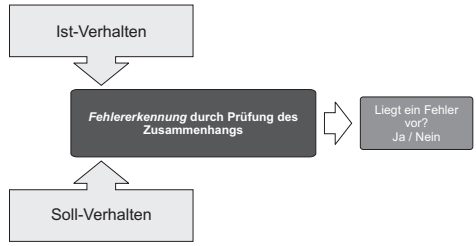
Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

Müller, Thomas; Wallaschek, Jörg: Musterdatenbank zur Konzipierung verlässlicher mechatronischer Systeme. In: VDI-Berichte 1984: TTZ2007 - Tagung Technische Zuverlässigkeit. Düsseldorf: VDI Verlag, 2007

Fehlererkennung

Verässlichkeitsmuster der *Fehlererkennung* beschreiben die Möglichkeit, Fehler durch Abweichungen von Soll-Werten zu identifizieren, ohne dabei Wissen über das Fehlerverhalten zu besitzen oder zu benutzen.





Prinzip der Fehlererkennung

Das Resultat der Fehlererkennung ist die Beantwortung der Frage, "Liegt ein Fehler vor?", nicht aber die Beantwortung der Frage "Was für ein Fehler liegt vor?". Notwendig ist dafür folglich neben dem Ist-Verhalten lediglich das Wissen über das korrekte Soll-Verhalten, sodass durch Vergleich von diesen (mindestens) zwei Werten, vorgegebene Zusammenhänge geprüft werden können. Abweichende oder unzulässige Zusammenhänge gelten als Fehler.
Gute Übersichten verschiedener Fehlererkennungsverfahren sind u. a. in [Münchhof2006], [Isermann2006], [Gertler1998] und [Lee1990] beschrieben. Insbesondere die Möglichkeiten der modellbasierten Fehlererkennung, die großes Innovationspotenzial besitzen, werden dort erläutert. Beispiele für Verlässlichkeitsmuster der Fehlererkennung sind Parametervergleich, Parameterschätzverfahren, Paritätsgleichungen und Plausibilitäts-Checks.

Weiterführende Informationen:

Münchhof, Marco: Model-Based Fault Detection for a Hydraulic Servo Axis. Technische Universität Darmstadt, Diss., 2006 [Münchhof2006]

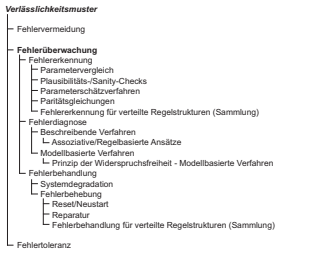
Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

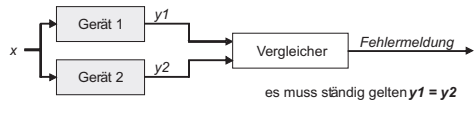
Gertler, Janos J.: Fault Detection and Diagnosis in Engineering Systems. New York: Marcel Dekker Inc., 1998 [Gertler1998]

Lee, P. A.; Anderson, T.: Fault Tolerance. Wien: Springer-Verlag, 1990 [Lee1990]

Parametervergleich

Beim Parametervergleich wird ein gemessener Parameter, der Ist-Wert, wird mit dem bekannten Parameter bei korrekter Funktion, dem Soll-Wert, verglichen. Bei einer größeren Abweichung wird von einem Fehler ausgegangen.





Prinzip des Parametervergleichs

Das Verlässlichkeitsmuster *Parametervergleich* stellt die einfachste Form einer Fehlererkennung dar, in dem ein gemessener Ist-Wert mit einem bekannten Soll-Wert bei korrekter Funktion verglichen wird. Es wird daher teilweise auch von Fremdüberprüfung bei diesem Muster gesprochen. Weichen diese Werte voneinander ab, Toleranzen können selbstverständlich berücksichtigt werden, so liegt ein Fehler vor. Stimmen sie überein, so funktioniert das System korrekt. Dieses Verlässlichkeitsmuster wird auch als *1v2 Voting* bezeichnet in dem Falle, dass der Soll-Wert durch einen zweiten redundanten Sensor ermittelt wird.

Weiterführende Informationen:

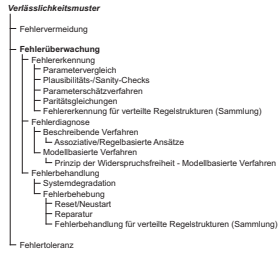
Mahmoud, Rachad: Sicherheits- und Verfügbarkeitsanalyse komplexer Kfz-Systeme. Universität-Gesamthochschule Siegen, Diss., 2000

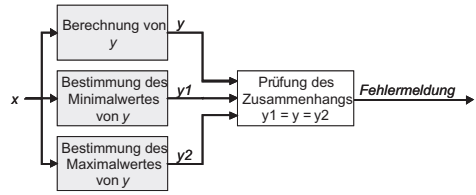
Münchhof, Marco: Model-Based Fault Detection for a Hydraulic Servo Axis. Technische Universität Darmstadt, Diss., 2006

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006

Plausibilitäts-Check

Das Verlässlichkeitsmuster *Plausibilitäts-Check*, auch Sanity-Check genannt, vergleicht den gemessenen Wert nicht mit einem anderen fremden Wert, sondern mittels *Eigenüberprüfung*.





Prinzip des Plausibilitäts-Checks

Beim Plausibilitäts-Check kann im Sinne der Fehlererkennung z. B. überprüft werden, ob sich der gemessene Wert innerhalb *plausibler* Grenzen befindet oder er im Vergleich zu anderen ermittelten Parametern, selbst *plausibel* ist. Die Ausprägung bzw. das Vorgehen für Plausibilitäts-Checks kann sich selbstverständlich in der Praxis wesentlich komplexer darstellen. Ein Beispiel für den Einsatz von Plausibilitäts-Checks ist das Sicherheitskonzept der elektrohydraulischen Bremse für ein Kraftfahrzeug nach [Binfett-Kull2001].

Weiterführende Informationen:

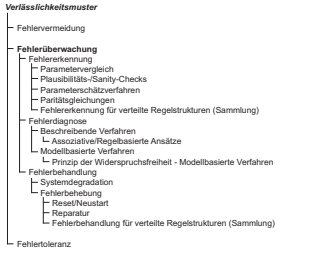
Binfett-Kull, Maria: Entwicklung einer Steer-by-Wire-Architektur nach zuverlässigkeits- und sicherheitstechnischen Vorgaben. Bergische Universität - Gesamthochschule Wuppertal, Diss., 2001 [Binfett-Kull2001]

Münchhof, Marco: Model-Based Fault Detection for a Hydraulic Servo Axis. Technische Universität Darmstadt, Diss., 2006

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006

Parameterschätzverfahren

Das Parameterschätzverfahren nutzt die Nachbildung eines parametrischen mathematischen Systemmodells, um Fehler zu erkennen.



keine Abbildung vorhanden

Das *Parameterschätzverfahren* erweitert das Verlässlichkeitsmuster des Parametervergleichs [Fritz2004] [Isermann2006]. Hier kann der bzw. können die zu vergleichende(n) Parameter nicht direkt bestimmt oder gemessen werden. Daher werden z. B. die Ein- und Ausgangsgrößen des Systems oder Teilsystems bestimmt und deren Zusammenhang in einem parametrischen mathematischen Systemmodell nachgebildet. Diese *geschätzten Parameter* des Modells werden mit den Nominalwerten verglichen. Bei Abweichung wird ein Fehler unterstellt. Die Abweichungen können für eine potenziell anschließende Fehlerdiagnose als Symptome eines Fehlers betrachtet werden. Verfahren der Parameterschätzung sind die Methode der kleinsten Quadrate, die Methode der Hilfsvariablen und das Maximum-Likelihood-Verfahren (Verfahren der größten Wahrscheinlichkeit). Ausführliche Beschreibungen verschiedener Parameterschätzverfahren sind in [Isermann2006] erläutert. Ein Anwendungsbeispiel für die Überwachung einer linearen hydraulischen Servo-Achse ist in [Münchhof2006] beschrieben.

Weiterführende Informationen:

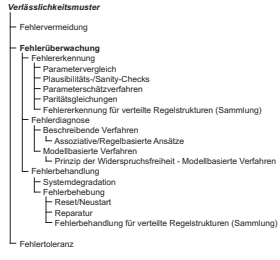
Fritz, M.; Albers, A.: Fehlererkennung an einem elektromechanischen Radbremsaktor mittels modellbasierter Methoden. In: AUTOREG, 2004 [Fritz2004]

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

Münchhof, Marco: Model-Based Fault Detection for a Hydraulic Servo Axis. Technische Universität Darmstadt, Diss., 2006 [Münchhof2006]

Paritätsgleichungen

Paritätsgleichungen verwenden zur Fehlererkennung ein statisches oder dynamisches mathematisches Modell.



keine Abbildung vorhanden

Das Verlässlichkeitsmuster *Paritätsgleichungen* verwendet für die Fehlererkennung als Grundlage ein mathematisches Systemmodell mit bereits bekannten Parametern. Durch Einsetzen der gemessenen Ein- und Ausgangsgrößen kann ein Residuum zwischen gemessenen Parametern und den resultierenden Nominalwerten des Modells gebildet werden, das im Fehlerfall signifikant von 0 abweicht. Insbesondere für additive Fehler ist dieses Verfahren gut anwendbar [Isermann2006]. Weitere Ausprägungen dieses Verlässlichkeitsmuster sind ebenfalls in [Isermann2006] dargestellt. Ein Anwendungsbeispiel anhand eines elektromechanischen Radbremsaktors wird in [Fritz2004] erläutert, das die modellbasierte Fehlererkennung durch ein zweistufiges Konzept, bestehend aus Paritätsgleichungen und rekursivem Parameterschätzverfahren, realisiert.

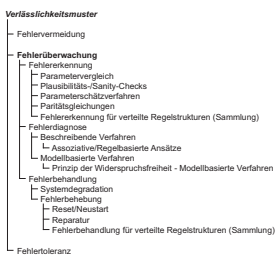
Weiterführende Informationen:

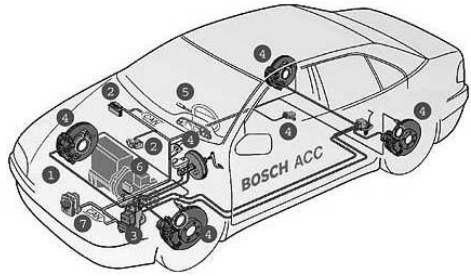
Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

Fritz, M.; Albers, A.: Fehlererkennung an einem elektromechanischen Radbremsaktor mittels modellbasierter Methoden. In: AUTOREG 2004 [Fritz2004]

Fehlererkennung für verteilte Regelstrukturen - CARTRONIC

Sammlung von exemplarischen Verlässlichkeitsmustern zur Fehlererkennung, die Fehler bei der Kommunikation und Vernetzung von Steuergeräten im Kraftfahrzeug erkennen sollen.





Verteilte Regelaufgaben im Automobil [www.offis.de]

Zur Konkretisierung der Verlässlichkeitsmuster zur *Fehlererkennung* sind nachfolgend ausgewählte Verfahren aufgezählt, die der Fehlererkennung bei der Kommunikation und Vernetzung von Steuergeräten im Kraftfahrzeug dienen [Bertram1999]:

- Empfangsbestätigung bei der Kommunikation
- Vergleich durch redundante Architekturen
- Referenz-Checks, realisiert durch das Stellen einer Frage mit vorher bekannter Antwort
- Paritäts-Checks, realisiert durch Prüfung auf Geradzahligkeit
- Überwachung physikalischer Eigenschaften der Steuergeräte, wie z. B. der Temperatur
- Logische oder zeitliche Überwachung der Programmausführung
- Dynamische Kommunikation – ein eigentlich gleich bleibender Output wird in verschiedenen Arten zu verschiedenen Zeiten ausgegeben; z. B. wird jeder zweite Wert mit einem negativen Vorzeichen ausgegeben, obwohl der Wert gleich geblieben sein kann.

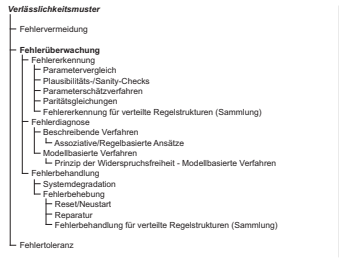
Weiterführende Informationen:

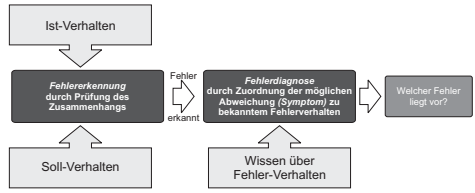
Bertram, Torsten; Dominke, Peter; Müller, Bernd: The Safety-Related Aspect of CARTRONIC. In: SAE International Congress & Exposition, Detroit(USA), 1999 [Bertram1999]

Hedenetz, B.: Entwurf von verteilten fehlertoleranten Elektronikarchitekturen in Kraftfahrzeugen. Diss., Tübingen, 2001

Fehlerdiagnose

Verlässlichkeitsmuster der *Fehlerdiagnose* beschreiben die Möglichkeit, die zur Fehlererkennung führenden Abweichungen als Symptome zu verstehen und darauf aufbauend den vorliegenden Fehler zu diagnostizieren.





Prinzip der Fehlerdiagnose

Muster der Fehlerdiagnose diagnostizieren identifizierte Abweichungen. Dazu ist Wissen über das Fehlerverhalten im Gegensatz zu den Mustern der Fehlererkennung zusätzlich notwendig, um die Frage "Was für ein Fehler liegt vor?" beantworten zu können. Die Abbildung zeigt das grundsätzliche Prinzip der Fehlerdiagnose, das Wissen über Ist-, Soll- und Fehlerverhalten benötigt. Der Vergleich von Ist- und Soll-Wert führt zur Fehlererkennung, während die Zuordnung einer potenziellen Abweichung, des so genannten Symptoms oder auch Residuums, zur Fehlerzuordnung und somit zur Fehlerdiagnose führt.
Die Fehlerdiagnose bzw. Fehlerzuordnung kann durch Interpretations- und Klassifikationsverfahren erfolgen, um den Fehler z. B. zu lokalisieren, zu bewerten oder sogar exakt zu identifizieren. Unterschieden wird bei wissensbasierter Diagnose z. B. zwischen beschreibenden und modellbasierten Verfahren gemäß [Heinzelmann1999]. Weitere Übersichten verschiedener Fehlerdiagnoseverfahren, teilweise inklusive Anwendungsbeispielen, sind in [Münchhof2006], [Isermann2006] und [Gertler1998] beschrieben.

Weiterführende Informationen:

Heinzelmann, Andreas: Produktintegrierte Diagnose komplexer mobiler Systeme. Universität Paderborn, Diss., 1999 [Heinzelmann1999]

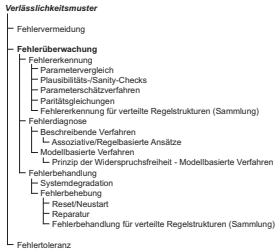
Münchhof, Marco: Model-Based Fault Detection for a Hydraulic Servo Axis. Technische Universität Darmstadt, Diss., 2006 [Münchhof2006]

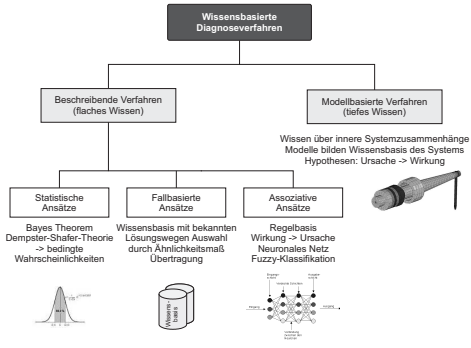
Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

Gertler, Janos J.: Fault Detection and Diagnosis in Engineering Systems. New York: Marcel Dekker Inc., 1998 [Gertler1998]

Beschreibende Fehlerdiagnose

Muster der beschreibenden Fehlerdiagnose basieren auf heuristischem Wissen, das mittels Ursache-Wirkungsbeziehungen Fehler analysieren und zuordnen kann.





Strukturierung und Beispiele für Diagnoseverfahren [Heinzelmann1999]

Beschreibende Verfahren der Fehlerdiagnose [Heinzelmann1999] versuchen Fehler zu analysieren, in dem sie Ursache-Wirkungsbeziehungen der beobachteten Größen eines Bauteils oder Systems nutzen. In der Literatur wird das verwendete Wissen auch als heuristische Diagnoseinformation oder deklarative Wissensinformation bezeichnet. Es gibt verschiedene Ansätze zur Erlangung des erforderlichen Wissens und zur Strukturierungen der Wissensspeicherung. Beispiele für beschreibende Verfahren der Fehlerdiagnose sind neben den in der Abbildung dargestellten Kategorien Entscheidungsbäume, Entscheidungstabellen und kausale Netze.

Weiterführende Informationen:

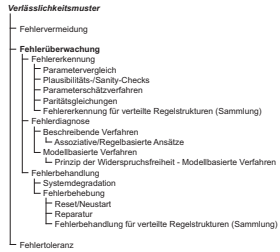
Heinzelmann, Andreas: Produktintegrierte Diagnose komplexer mobiler Systeme. Universität Paderborn, Diss., 1999 [Heinzelmann1999]

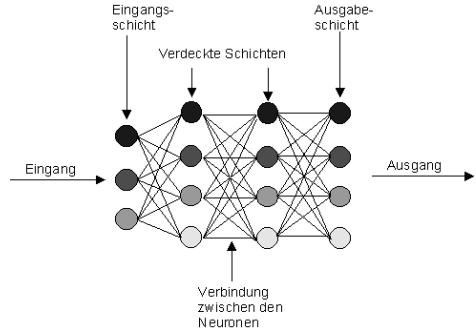
Hedenetz, B.: Entwurf von verteilten fehlertoleranten Elektronikarchitekturen in Kraftfahrzeugen. Diss., Tübingen, 2001

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006

Regelbasierte Fehlerdiagnose

Regelbasierte Diagnoseverfahren versuchen durch Anwendung geeigneter assoziativer Regeln im detektierten Fehlerfall, eine Fehlerdiagnose zu erstellen.





Regelbasierte Fehlerdiagnose kann z. B. durch Neuro-Fuzzy-Logik realisiert werden

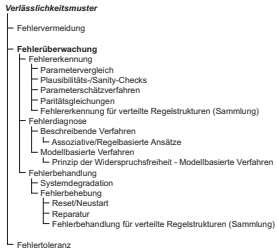
Regelbasierte Diagnoseverfahren [Heinzelmann1999] gehören zur Kategorie der beschreibenden Methoden. Sie versuchen durch Anwendung geeigneter Regeln im detektierten Fehlerfall, eine Fehlerdiagnose zu erstellen. Dafür soll Wissen eines menschlichen Diagnoseexperten nachgebildet werden. Es werden Regeln angegeben, die theoretisches Wissen aber auch Erfahrungen und Daumenregeln widerspiegeln. Durch Anwendung dieser Regeln versucht nun das regelbasierte Diagnosesystem das beobachtete Systemverhalten zu erklären. Bei einer Vorwärts-Verkettung werden die Regeln auf die Anfangssymptome angewendet, um eine so genannte Verdachtsdiagnose zu erstellen; bei der Rückwärts-Verkettung werden sie auf mögliche Ursachen angewendet, um Symptome zu erklären.

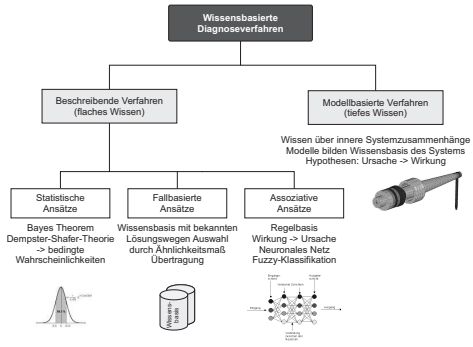
Weiterführende Informationen:

Heinzelmann, Andreas: Produktintegrierte Diagnose komplexer mobiler Systeme. Universität Paderborn, Diss., 1999 [Heinzelmann1999]

Modellbasierte Fehlerdiagnose

Modellbasierte Diagnoseverfahren vergleichen den tatsächlichen Zustand eines Systems mit dem Soll-Zustand eines Modells. Das Modell beinhaltet so genanntes *tiefes Wissen*.





Strukturierung und Beispiele für Diagnoseverfahren [Heinzelmann1999]

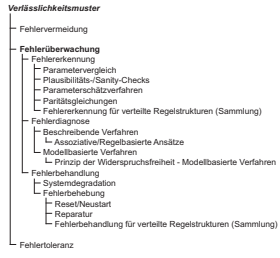
Modellbasierte Verfahren versuchen mit Hilfe von Verhaltens- und Strukturmodellen eine Fehlerdiagnose zu erstellen. Dabei wird der aktuelle Zustand eines Systems mit dem Soll-Zustand eines Systems verglichen. Treten Abweichungen auf, liegt ein Fehler vor. Zur Erklärung des Fehlers wird das Modell so angepasst, dass sich beide Zustände wieder gleichen. Durch Analyse der Anpassung des Modells, kann dann auf die Fehlerursache geschlossen werden. Hierbei kommen zwei grundsätzliche Prinzipien zum tragen. Das Prinzip der Widerspruchsfreiheit und das Prinzip der Erklärung von Beobachtungen.

Weiterführende Informationen:

Heinzelmann, Andreas: Produktintegrierte Diagnose komplexer mobiler Systeme. Universität Paderborn, Diss., 1999 [Heinzelmann1999]

Prinzip der Widerspruchsfreiheit - Modellbasierte Fehlerdiagnose

Modellbasierte Diagnoseverfahren mit dem Prinzip der Widerspruchsfreiheit überprüfen identifizierte Widersprüche zwischen technischem System und einem Verhaltens- oder Strukturmodell.



keine Abbildung vorhanden

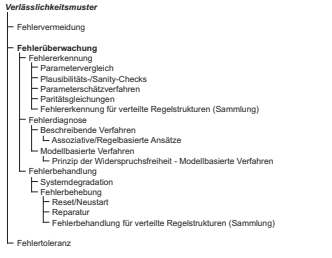
Das Prinzip der Widerspruchsfreiheit [Heinzelmann1999] überprüft Widersprüche zwischen Modell und technischem System. Die modellbasierte Diagnose allgemein betrachtet, vergleicht den tatsächlichen Zustand eines Systems mit dem Sollzustand eines Verhaltens- oder Strukturmodells. Treten Widersprüche auf, so beinhaltet diese Erkenntnis bereits das Wissen, dass ein Fehler vorliegt. Für die Fehlerdiagnose kann dann auf das Prinzip der Widerspruchsfreiheit zurück gegriffen werden, indem versucht wird, das Modell so anzupassen, dass beide Zustände wieder gleich sind; durch die Kenntnis bzgl. der Anpassung des Modells kann dann auf die Fehlerursache geschlossen werden. Das Prinzip der Widerspruchsfreiheit versucht somit, eine Fehlerdiagnose zu erstellen, in dem es durch Anpassung des Modells Widersprüche auflöst und damit erklären kann.

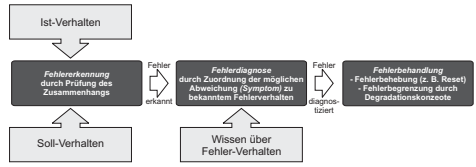
Weiterführende Informationen:

Heinzelmann, Andreas: Produktintegrierte Diagnose komplexer mobiler Systeme. Universität Paderborn, Diss., 1999 [Heinzelmann1999]

Resultierende Maßnahmen zur Fehlerbehandlung

Nachdem Fehler erkannt oder sogar diagnostiziert worden sind, können Muster zur Fehlerbehebung oder -eingrenzung eingesetzt werden.





Resultierende Maßnahmen zur Fehlerbehandlung erfolgen nach der Fehlerdiagnose oder direkt nach der Fehlererkennung

Nachdem Fehler erkannt und evtl. auch diagnostiziert werden konnten, dienen Verlässlichkeitsmuster für *Resultierende Maßnahmen* dazu, Fehler zu beheben oder zumindest einzugrenzen und damit beherrschbarer zu machen; z. B. durch Systemdegradation, Neustart, Reparatur oder den Austausch von Komponenten. Theoretisch könnten auch die Muster der Fehlertoleranz unter diesem Aspekt subsumiert werden, da sie teilweise Muster darstellen, die automatisch die resultierenden Maßnahmen einleiten und somit fehlertolerantes Verhalten gewährleisten. Die Begründung, dass die meisten Muster der Fehlerbehebung an dieser Stelle bereits aufgeführt werden, liegt darin, dass der Funktionsausfall zumindest zeit- oder teilweise durchaus eintritt. Diese Ausfallzeiten resultieren sowohl aus Instandhaltungs-, Neustart- und Reparaturdauern als auch aus Zeiten, in denen der funktionale Systemumfang bewusst reduziert wird und somit nicht vollständig zur Verfügung steht.

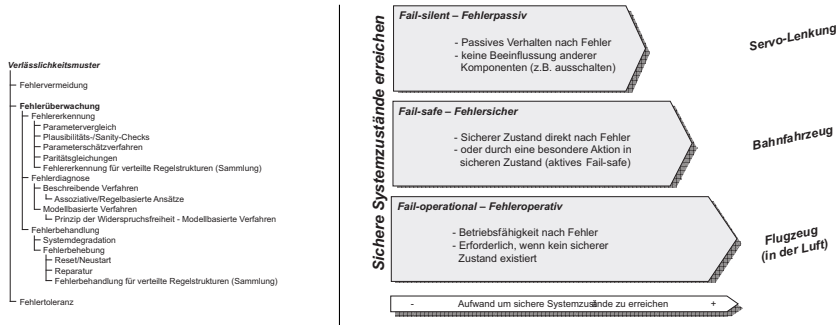
Weiterführende Informationen:

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006

Müller, Thomas; Wallaschek, Jörg: General Concepts of Dependability in the Design of Mechatronic Systems. In: Research and Education in Mechatronics. Stockholm, 2006

Systemdegradation

Das Verlässlichkeitsmuster *Systemdegradation* beschreibt das Einschränken der Funktionalität des Systems oder einzelner Komponenten. Je nach Umfang der Degradation kann zwischen den Konzepten *Fehlerpassiv*, *Fehlersicher* und *Fehleroperativ* unterschieden werden.



Systemdegradation mittels Fehlerpassiv-, Fehlersicher- oder Fehleroperativ-Konzept

Nach der Fehlererkennung können Muster zum Einschränken der Funktionalität des Systems angewendet werden. Abhängig vom Aufwand, um sichere Systemzustände zu erreichen, wird zwischen den nachfolgenden drei Degradationsstufen unterschieden [Isermann2006]:

- *Fehlerpassiv* (Fail-silent) bedeutet, dass ein Teilsystem oder eine Komponente nach einer Fehlererkennung in einen passiven Zustand versetzt wird. Dieses passiv geschaltete Teilsystem reduziert zwar die Funktion des Gesamtsystems, beeinflusst in diesem Zustand aber keine anderen Komponenten negativ, sodass die Gesamtsystemsicherheit gewährleistet bleibt.
- *Fehlersicher*(Fail-safe) bedeutet, dass direkt nach der Erkennung eines Fehlers ein sicherer Zustand für das Gesamtsystem erreicht werden muss. Kann dieses direkte Erreichen eines sicheren Zustands nur durch eine besondere Aktion realisiert werden, eine Aktion die über ein normales Abschalten der Energie hinaus geht, so ist diese Maßnahme zwar noch Inhalt dieses Konzepts, wird aber durch den erweiterten Begriff *Aktives Fail-safe* kenntlich gemacht. Bekannte Beispiele für Fail-safe-Systeme im Kraftfahrzeug sind u. a. das Anti-Blockier-System und das Elektronische Stabilitätssystem.
- *Fehleroperativ* (Fail-operational) bedeutet, dass die Betriebsfähigkeit des Systems nach einer Fehlererkennung gewährleistet wird. Dies ist dann erforderlich, wenn kein sicherer Zustand existiert, der direkt erreicht werden könnte, wie z. B. bei einem sich in der Luft befindenden Flugzeug. Diese Degradationsstufe kann auch als Verlässlichkeitsmuster für Fehlertoleranz angesehen werden.

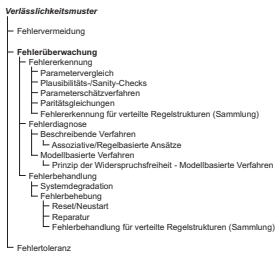
Weiterführende Informationen:

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

Müller, Thomas; Wallaschek, Jörg: General Concepts of Dependability in the Design of Mechatronic Systems. In: Research and Education in Mechatronics. Stockholm, 2006

Reset/Neustart

Ein Reset bezeichnet einen Vorgang, durch den ein System von einem fehlerhaften oder undefinierten Zustand in einen definierten Zustand überführt wird.



[www.stern.de] [www.AmazingPaul.com]

Reset durch die Tastenkombination Srtg+Alt+Entf

In der Regel nimmt ein System durch einen Reset den Zustand ein, den es nach dem Einschalten hat. Daher wird ein Reset im Deutschen oft auch als Neustart bezeichnet. Es werden grob vier verschiedene Arten des Resets unterschieden [wikipedia2007b]:

- *Neustart:* Hierunter versteht man das erneute Hochfahren des Computers, wenn dieser bereits eingeschaltet ist. Ein Neustart wird auch Warmstart genannt, da er durch einen Softwarebefehl ausgelöst wird. Er wird eingesetzt, wenn die grundsätzlichen Einstellungen des Systems beibehalten werden sollen oder müssen.
- *Hardwarereset:* Dieser Typ erfolgt mittels der Resettaste am Gehäuse. Die Resettaste löst ein direktes Signal auf der Hardware aus, diese schaltet sich kurzzeitig ab, ohne dass sie von der Stromversorgung getrennt wird. Danach geht das System in einen definierten Einschaltzustand über. Ist das Drücken der Resettaste mit der Software gekoppelt, kann diese entsprechend vor dem Ausschalten der Hardware reagieren (z. B. Daten sichern).
- *Kaltstart:* Bei einem Kaltstart wird die Stromversorgung unterbrochen und das System somit ausgeschaltet. Nach dem Einschalten geht das System in einen definierten Einschaltzustand über. Im Gegensatz zum Hardwarereset kann die Software keine vorherigen Befehle mehr ausführen.
- *Power On Reset:* Hiermit bezeichnet man einen Reset, der in dafür ausgelegten Digitalschaltungen nach dem Anlegen der Versorgungsspannung für einen definierten Start der Schaltung sorgt, sobald die Versorgungsspannung des Systems eine bestimmte Schwelle überschritten hat.

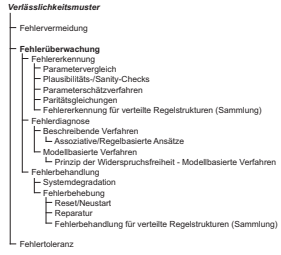
Weiterführende Informationen:

Wikimedia Foundation Inc.: Reset. Website - http://www.wikipedia.de - zuletzt besucht am 23.10.2007 [wikipedia2007b]

Müller, Thomas; Wallaschek, Jörg: General Concepts of Dependability in the Design of Mechatronic Systems. In: Research and Education in Mechatronics. Stockholm, 2006

Reparatur

Unter Reparatur wird der Vorgang verstanden, bei dem eine defekte Komponente in den ursprünglichen, funktionsfähigen Zustand zurückversetzt wird.



Reparatur kann z. B. einen Werkstattaufenthalt bedeuten

Der Begriff der Reparatur umfasst jede an einem fehlerhaften Bauteil/System auszuführende Maßnahme, die sicherstellen soll, dass dieses die Anforderungen der beabsichtigten Funktion erfüllen wird, obwohl es zunächst möglicherweise die ursprünglich festgelegten Forderungen nicht erfüllt. Eine Reparatur kann durch den Austausch defekter Teile, durch das Hinzufügen von Teilen oder durch eine Neuordnung von Teilen (z. B. Kleben oder Schweißen) erfolgen. Bei modernen technischen Geräten und Maschinen sowie in Autowerkstätten wird außerdem in zunehmendem Maße die Elektronik oder die elektrische Steuerung durch Programme zum Gegenstand von Reparaturen. Somit kann eine Reparatur Teile eines Produktes beeinflussen oder auch verändern [wikipedia2007c].

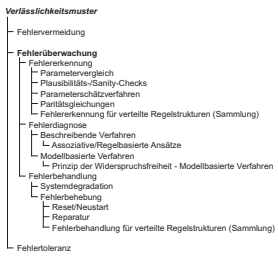
Weiterführende Informationen:

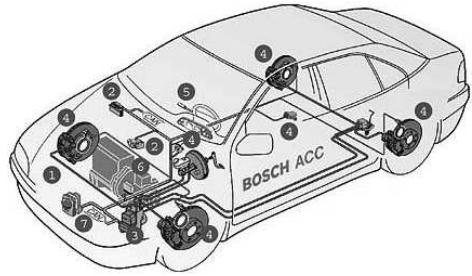
Wikimedia Foundation Inc.: Reparatur. Website - http://www.wikipedia.de - zuletzt besucht am 23.10.2007 [wikipedia2007c]

Müller, Thomas; Wallaschek, Jörg: General Concepts of Dependability in the Design of Mechatronic Systems. In: Research and Education in Mechatronics. Stockholm, 2006

Fehlerbehandlung für verteilte Regelstrukturen - CARTRONIC

Sammlung von exemplarischen Verlässlichkeitsmustern zur Fehlerbehandlung, die bei Störungen der Kommunikation und Vernetzung von Steuergeräten im Kraftfahrzeug eingesetzt werden.





Verteilte Regelaufgaben im Automobil [www.offis.de]

Zur weiteren Verdeutlichung von Verlässlichkeitsmustern für *Resultierende Maßnahmen* folgt eine Aufzählung von Fehlerbehandlungsverfahren, die bei der Kommunikation und Vernetzung von Steuergeräten im Kraftfahrzeug verwendet werden [Bertram1999]:

- Redundanz (siehe Fehlertoleranzmuster)
- Herunterfahren von Systembestandteilen
- Herunterfahren des gesamten Elektroniksystems
- Sicheren Park-Status erreichen
- Im Fehlerstatus bleiben (kein Konzept, sondern es dient der Vollständigkeit der Aufzählung)
- Fehlerbehebung durch Reset
- Fehlerbehebung durch Reparatur oder Wartung, z. B. durch das Abschleifen von Kontakten um den elektrischen Widerstand zu reduzieren
- Strategieänderung

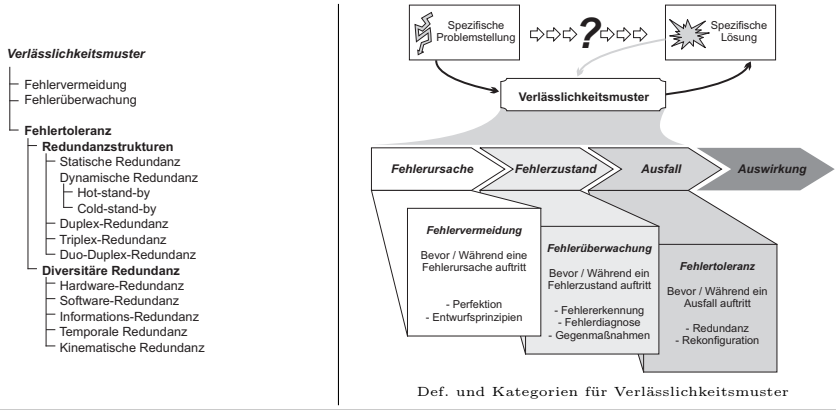
Weiterführende Informationen:

Bertram, Torsten; Dominke, Peter; Müller, Bernd: The Safety-Related Aspect of CARTRONIC. In: SAE International Congress & Exposition, Detroit(USA), 1999 [Bertram1999]

Hedenetz, B.: Entwurf von verteilten fehlertoleranten Elektronikarchitekturen in Kraftfahrzeugen. Diss., Tübingen, 2001

Fehlertoleranz

Fehlertoleranz beschreibt Verlässlichkeitsmuster, die trotz Ausfall von Teilsystemen die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten.



Def. und Kategorien für Verlässlichkeitsmuster

Verlässlichkeitsmuster der *Fehlertoleranz* beschreiben Konzepte, die trotz eines Fehlers die Betriebsfähigkeit und vollständige Funktionsfähigkeit des Gesamtsystems gewährleisten und damit Ausfälle vermeiden [VDI1988]. Die Aussage, dass alle Methoden der Fehlertoleranz auf Redundanz basieren, gemäß [Storey1996], beschreibt das Verständnis von Redundanz so, dass das System durch Redundanz komplexer wird, als es zur einfachsten Funktionsausübung erforderlich wäre, mit dem Ziel Fehler zu tolerieren. Die Art, in der das System komplexer entwickelt wird, beschreibt den Redundanztyp, der in verschiedensten Formen realisiert werden kann.

Eine Strukturierung der Redundanztypen basiert auf der Unterscheidung von zwei Sichtweisen: Zum einen lassen sich die Konzepte anhand der Struktur der redundanten Einheiten oder Mechanismen unterscheiden und zum anderen anhand des Typs der verwendeten Diversität. Während erstgenannte Sichtweise Muster wie Duplex-, Triplex- und Duo-Duplex-Strukturen betrachtet, unterscheidet die Diversität Muster durch die Unterschiedlichkeit der zu vergleichenden oder redundant auftretenden Komponente o. Ä.; z. B. durch Hardware-, Software-, Informations- oder Temporale Redundanz. Weitere Möglichkeiten zur Strukturierung von Fehlertoleranzmustern werden in [Auerswald2002] erläutert.

Weiterführende Informationen:

VDI 2244: Konstruieren sicherheitsgerechter Erzeugnisse. Berlin: Beuth Verlag, 1988 [VDI1988]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996 [Storey1996]

Auerswald, Marko; Herrmann, Martin; Kowalewski, Stefan; Schulte-Coerne, Vincent: Entwurfsmuster für fehlertolerante softwareintensive Systeme. In: at-Automatisierungstechnik, 8(2002) [Auerswald2002]

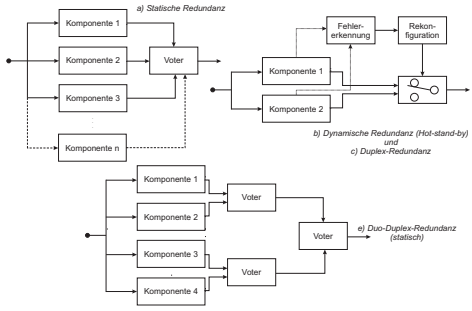
Müller, Thomas; Wallaschek, Jörg: Musterdatenbank zur Konzipierung verlässlicher mechatronischer Systeme. In: VDI-Berichte 1984: TTZ2007 - Tagung Technische Zuverlässigkeit. Düsseldorf: VDI Verlag, 2007

Strukturelle Redundanz

Verlässlichkeitsmuster durch *Strukturelle Redundanz* gewährleisten fehlertolerantes Verhalten dadurch, dass Einheiten mehrfach vorhanden sind und dadurch Fehler oder Ausfälle tolerieren können.

Verlässlichkeitsmuster

- Fehlervermeidung
- Fehlerüberwachung
- **Fehlertoleranz**
  - **Redundanzstrukturen**
    - Statische Redundanz
    - Dynamische Redundanz
      - Hot-stand-by
      - Cold-stand-by
    - Duplex-Redundanz
    - Triplex-Redundanz
    - Duo-Duplex-Redundanz
  - **Diversitäre Redundanz**
    - Hardware-Redundanz
    - Software-Redundanz
    - Informations-Redundanz
    - Temporale Redundanz
    - Kinematische Redundanz



Architekturkonzepte verschiedener struktureller Redundanzen [Isermann2006]

Strukturelle Redundanz gewährleistet fehlertolerantes Verhalten dadurch, dass mehrfach vorhandene Einheiten sich gegenseitig kontrollieren können und sich das System im Fehlerfall durch Mehrheitsvotum oder Rekonfiguration weiterhin korrekt verhält. Beispiele für strukturelle Redundanzen sind statische und dynamische Redundanz, Duplex-, Triplex- und Quadruplex-Redundanz oder auch Duo-Duplex-Redundanz. Beispiele für die Umsetzung unterschiedlicher Konzepte sind in [Binfett-Kull2001] dargestellt: Das *Anti-Blockier-System* als statische bzw. funktionsbeteiligte Redundanz, die *Elektro-Hydraulische Bremse* als dynamische bzw. nicht funktionsbeteiligten Redundanz in der Cold-stand-by-Ausprägung und das *Elektro-Mechanische Bremssystem* als fehlertolerante Duo-Duplex-Architektur. Ein Umsetzungsbeispiel eines redundanten diversitären Lenkwinkelgebers der Robert Bosch GmbH wird in [Dilger2003] beschrieben. Dieses verdeutlicht die Anwendung der Redundanzstrukturen ebenso wie das Zusammenwirken mit den Diversitätskonzepten.

Weiterführende Informationen:

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

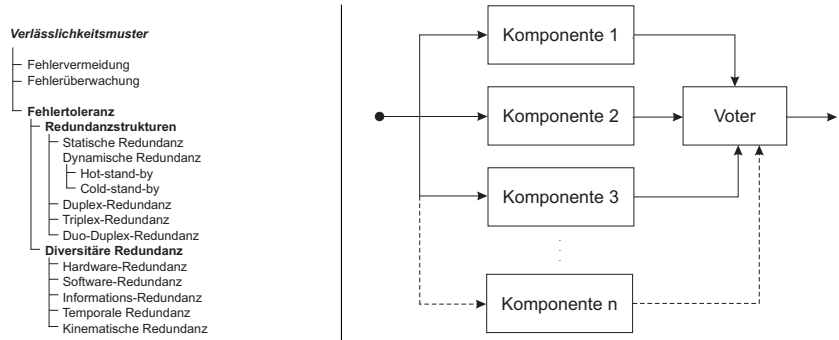
Binfett-Kull, Maria: Entwicklung einer Steer-by-Wire-Architektur nach zuverlässigkeits- und sicherheitstechnischen Vorgaben. Bergische Universität - Gesamthochschule Wuppertal, Diss., 2001 [Binfett-Kull2001]

Dilger, E.; Gulbins, M.; Ohnesorge, T.; Straube, B.: Redundanter diversitärer Lenkwinkelgeber. In: 15. GI/ITG/GMM Workshop "Testmethoden und Zuverlässigkeit von Schaltungen und Systemen", 2003 [Dilger2003]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996

Statische Redundanz

Verlässlichkeitsmuster der *Statischen Redundanz* gewährleisten fehlertolerantes Verhalten durch dauernd mitlaufende aktive Reserveeinheiten.



Prinzip der statischen Redundanz [Isermann2006]

Statische Redundanz bedeutet, dass die redundante Einheit dauernd als aktive Reserveeinheit mitläuft. Eine identifizierte fehlerhafte Einheit kann entweder nicht, oder nur am Ein- oder Ausgang, abgeschaltet werden. Häufig wird durch *Mehrheitsvotum* die fehlerhafte Einheit nicht berücksichtigt [Isermann2006]. Dieses Konzept wird auch als *Funktionsbeteiligte Redundanz* bezeichnet, bei der alle Mittel an der Erfüllung der geforderten Funktion beteiligt sind [VDI/VDE2000]. Ein Beispiel für die Umsetzung der statischen Redundanz ist das *Anti-Blockier-System*, das z. B. in [Binfett-Kull2001] kurz erläutert ist.

Weiterführende Informationen:

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

VDI/VDE: VDI/VDE Richtlinie 3542 - Blatt 1: Sicherheitstechnische Begriffe für Automatisierungssysteme. Qualitative Begriffe. VDI Verlag, Düsseldorf: 2000 [VDI/VDE2000]

Binfett-Kull, Maria: Entwicklung einer Steer-by-Wire-Architektur nach zuverlässigkeits- und sicherheitstechnischen Vorgaben. Bergische Universität - Gesamthochschule Wuppertal, Diss., 2001 [Binfett-Kull2001]

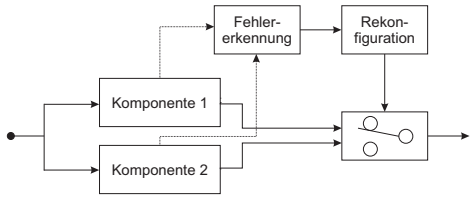
Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996

Dynamische Redundanz

Bei der *Dynamischen Redundanz* hat die redundante Einheit im fehlerfreien Fall keine Aufgabe. Im Fehlerfall wird auf sie umgeschaltet.

Verlässlichkeitsmuster

- Fehlervermeidung
- Fehlerüberwachung
- **Fehlertoleranz**
  - **Redundanzstrukturen**
    - Statische Redundanz
    - Dynamische Redundanz
      - Hot-stand-by
      - Cold-stand-by
    - Duplex-Redundanz
    - Triplex-Redundanz
    - Duo-Duplex-Redundanz
  - **Diversitäre Redundanz**
    - Hardware-Redundanz
    - Software-Redundanz
    - Informations-Redundanz
    - Temporale Redundanz
    - Kinematische Redundanz



Prinzip der dynamischen Redundanz [Isermann2006]

Dynamische Redundanz bedeutet, dass die redundante Einheit im fehlerfreien Fall keine Aufgabe hat; sie ist also eine passive Reserveeinheit. Erst im Fehlerfall erfolgt eine Umschaltung auf die fehlerfreie Einheit. Dabei wird dieses Muster weiter unterteilt in *Hot-stand-by*, d. h. dass die passive Reseerveeinheit für sich selbst aktiv ist, und in *Cold-stand-by*, d. h. dass die passive Reserveeinheit im fehlerfreien Fall nicht selbst aktiv ist. Zur Verdeutlichung: Bei einer Hot-stand-by-Struktur ist die Reserveeinheit selbst zwar aktiv, jedoch im fehlerfreien Systemzustand nicht an der Systemfunktionalität beteiligt; bei einer Cold-stand-by-Struktur ist die Reserveeinheit selbst nicht aktiv und ebenfalls nicht an der Systemfunktionalität beteiligt [Isermann2006]. Das Konzept der dynamischen Redundanz wird auch als *Nicht funktionsbeteiligte Redundanz* bezeichnet, bei der die zusätzlichen Mittel erst bei Störung bzw. Ausfall die geforderte Funktion übernehmen [VDI/VDE2000]. Ein Beispiel für die Umsetzung der dynamischen Redundanz ist die *Elektro-Hydraulische Bremse*, die z. B. in [Binfett-Kull2001] kurz erläutert wird: Im Fehlerfall wird eine direkte hydraulische Verbindung zwischen Bremspedal und den Bremsaktoren aktiviert; diese entspricht der dynamischen bzw. nicht funktionsbeteiligten Redundanz in der Cold-stand-by-Ausprägung.

Weiterführende Informationen:

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

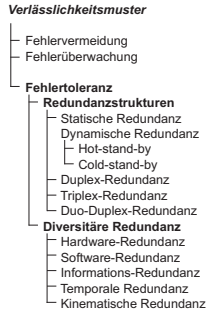
VDI/VDE: VDI/VDE Richtlinie 3542 - Blatt 1: Sicherheitstechnische Begriffe für Automatisierungssysteme. Qualitative Begriffe. VDI Verlag, Düsseldorf: 2000 [VDI/VDE2000]

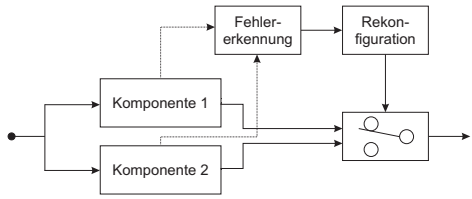
Binfett-Kull, Maria: Entwicklung einer Steer-by-Wire-Architektur nach zuverlässigkeits- und sicherheitstechnischen Vorgaben. Bergische Universität - Gesamthochschule Wuppertal, Diss., 2001 [Binfett-Kull2001]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996

Duplex-Redundanz

Die *Duplex-Redundanz* verwendet doppelte Einheiten und die Fehlererkennung durch Parametervergleich.





Prinzip der Duplex-Redundanz [Isermann2006]

Die *Duplex-Redundanzstruktur* entspricht dem Parametervergleich zweier Komponenten zur Fehlererkennung (siehe Muster *Parametervergleich*). Sie hat allerdings den Zusatz, dass *harte Fehler*, z. B. ein Kurzschluss, bereits durch den Vergleich lokalisiert werden können. Dadurch kann die Duplex-Struktur fehlertolerantes Verhalten erreichen, wenn sie gemäß der dynamischen Redundanz entworfen wird [Stölzl2000] [Isermann2006].

Weiterführende Informationen:

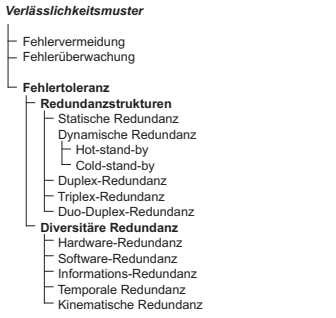
Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

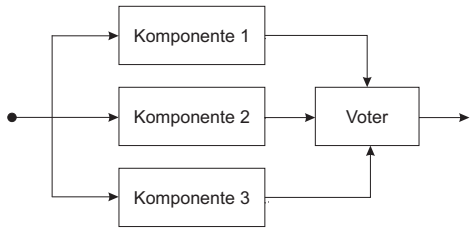
Stölzl, Stefan: Fehlertolerante Pedaleinheit für ein elektromechanisches Bremssystem. VDI Verlag, Düsseldorf, Technische Universität Darmstadt, Diss., 2000 [Stölzl2000]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996

Triplex-Redundanz

Die *Triplex-Redundanz* verwendet dreifache Einheiten zur Gewährleistung der Fehlertoleranz.





Prinzip der Triplex-Redundanz [Isermann2006]

Die Redundanzstruktur *Triplex*, die auch als *3v2 Voting* und international als *Triple Modular Redundancy (TRM)* bekannt ist, bezeichnet eine dreikanalige Struktur redundanter Komponenten, deren Outputs von einem Voter nach dem Mehrheitsprinzip verglichen werden. Im Fehlerfall einer Komponente kann der Fehler erkannt, lokalisiert und die fehlerhafte Komponente aus der Struktur durch Rekonfiguration ausgeschlossen werden. Durch den Ausschluss bleibt eine zweikanalige Struktur bestehen, die die Funktionsfähigkeit des Systems gewährleisten kann und Fehler weiterhin erkennt. Lediglich die fehlertolerante Eigenschaft ist dann nicht mehr, bzw. nur noch im Sinne der Duplex-Struktur vorhanden. Je nach implementierter Rekonfigurations-Strategie kann die Triplex-Redundanz statisch oder dynamisch realisiert werden [Stölzl2000] [Mahmoud2000] [Lee1990].

Weiterführende Informationen:

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

Stölzl, Stefan: Fehlertolerante Pedaleinheit für ein elektromechanisches Bremssystem. VDI Verlag, Düsseldorf, Technische Universität Darmstadt, Diss., 2000 [Stölzl2000]

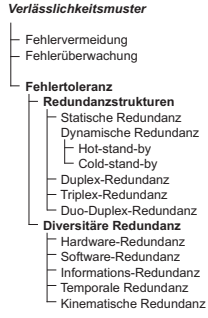
Mahmoud, Rachad: Sicherheits- und Verfügbarkeitsanalyse komplexer Kfz-Systeme, Universität-Gesamthochschule Siegen, Diss., 2000 [Mahmoud2000]

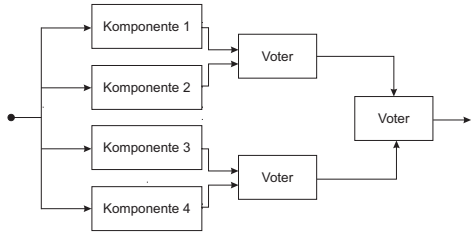
Lee, P. A.; Anderson, T.: Fault Tolerance. Wien: Springer-Verlag, 1990 [Lee1990]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996

Duo-Duplex-Redundanz

Zwei Duplex-Systeme bilden die Struktur einer *Duo-Duplex-Redundanz* zur Gewährleistung der Fehlertoleranz.





Prinzip der Duo-Duplex-Redundanz [Isermann2006]

Die *Duo-Duplex-Redundanz* beinhaltet vier redundante Komponenten, die jeweils zwei Duplex-Systeme bilden. Im Falle der Abweichung innerhalb einer Duplex-Einheit, wird diese als fehlerhaft betrachtet. Das fehlertolerante Verhalten entspricht der Triplex-Struktur [Stölzl2000]. Gemäß [Isermann2006] sind die Wahrscheinlichkeiten eines Totalausfalls von Triplex- und Duo-Duplex-Systemen annähernd gleich.

Weiterführende Informationen:

Isermann, Rolf: Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance. Berlin, Heidelberg: Springer-Verlag, 2006 [Isermann2006]

Stölzl, Stefan: Fehlertolerante Pedaleinheit für ein elektromechanisches Bremssystem. VDI Verlag, Düsseldorf, Technische Universität Darmstadt, Diss., 2000 [Stölzl2000]

Lee, P. A.; Anderson, T.: Fault Tolerance. Wien: Springer-Verlag, 1990

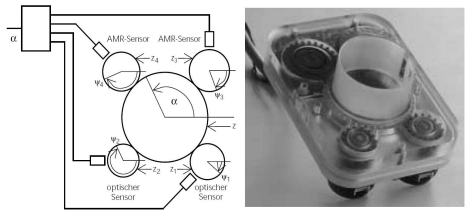
Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996

Diversitäre Redundanz

Die *Diversitäre Redundanz* gewährleistet fehlertolerantes Verhalten durch die Ungleichartigkeit der verwendeten Mittel.

Verlässlichkeitsmuster

- Fehlervermeidung
- Fehlerüberwachung
- **Fehlertoleranz**
  - **Redundanzstrukturen**
    - Statische Redundanz
    - Dynamische Redundanz
      - Hot-stand-by
      - Cold-stand-by
    - Duplex-Redundanz
    - Triplex-Redundanz
    - Duo-Duplex-Redundanz
  - **Diversitäre Redundanz**
    - Hardware-Redundanz
    - Software-Redundanz
    - Informations-Redundanz
    - Temporale Redundanz
    - Kinematische Redundanz



Redundanter diversitärer Lenkwinkelgeber der Robert Bosch GmbH [Dilger2003]

Die *Diversitäre Redundanz* beschreibt die Redundanz nicht durch strukturelle Darstellungen, sondern mittels der Ungleichartigkeit der verwendeten Mittel. Diese Mittel müssen nicht unbedingt Komponenten darstellen, sondern können z. B. andere physikalische Prinzipien, andere Lösungswege der gleichen Aufgabe oder andere Aufbauweisen sein [VDI/VDE2000]. Anhand der Ausprägung der Diversität bestimmt sich die Art der diversitären Redundanz. Exemplarisch für diese Kategorie der Verlässlichkeitsmuster sind die Hardware-, Software-, Informations-, Temporale und Kinematische Redundanz [Storey 1996]. Die Funktionsweise der diversitären Redundanz basiert auf der Erwartung, dass sich potenzielle Gefährdungen in ungleichartigen Systemteilen unterschiedlich auf das Verhalten auswirken. Ein Umsetzungsbeispiel eines redundanten diversitären Lenkwinkelgebers der Robert Bosch GmbH wird in [Dilger2003] beschrieben. Dieses verdeutlicht noch einmal die Anwendung der Diversitätskonzepte ebenso wie das Zusammenwirken mit den Redundanzstrukturen.

Weiterführende Informationen:

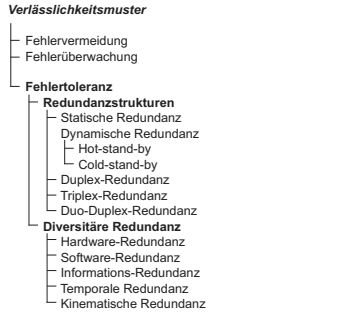
Dilger, E.; Gulbins, M.; Ohnesorge, T.; Straube, B.: Redundanter diversitärer Lenkwinkelgeber. In: 15. GI/ITG/GMM Workshop "Testmethoden und Zuverlässigkeit von Schaltungen und Systemen", 2003 [Dilger2003]

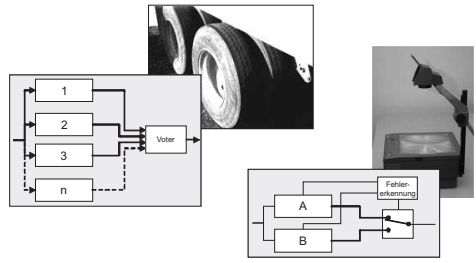
VDI/VDE: VDI/VDE Richtlinie 3542 - Blatt 1: Sicherheitstechnische Begriffe für Automatisierungssysteme. Qualitative Begriffe. VDI Verlag, Düsseldorf: 2000 [VDI/VDE2000]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996 [Storey1996]

Hardware-Redundanz

Hardware-Redundanz nutzt zusätzliche diversitäre Hardware, um ein fehlertolerantes Verhalten zu erreichen.





Beispiele für Hardware-Redundanz: LKW-Zwillingsreifen und Tageslichtprojektor

Die *Hardware-Redundanz* beschreibt den Typus Redundanz, der wahrscheinlich dem verbreitetsten Verständnis von Redundanz entspricht. Zusätzliche diversitäre Hardware, häufig in Komponentenform, wird eingesetzt, um im Fehlerfall die Funktionalität weiterhin gewährleisten zu können [Storey1996]. Beispiele für Hardware-Redundanz sind

- zusätzliche Sensoren mit anderem Funktionsprinzip [Dilger2003],
- Zwillingsreifen bei Lastkraftwagen, auf die unterschiedliche Belastungen wirken oder
- das zweite vorhandene Leuchtmittel in Tageslichtprojektoren, das die Hardware-Diversität durch Einsatz- und Herstellungsunterschiede vorweisen kann.

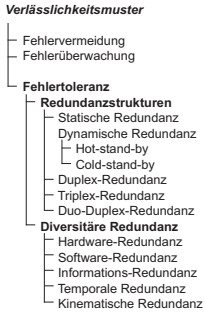
Weiterführende Informationen:

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996 [Storey1996]

Dilger, E.; Gulbins, M.; Ohnesorge, T.; Straube, B.: Redundanter diversitärer Lenkwinkelgeber. In: 15. GI/ITG/GMM Workshop "Testmethoden und Zuverlässigkeit von Schaltungen und Systemen", 2003 [Dilger2003]

Software-Redundanz

Software-Redundanz nutzt zusätzliche diversitäre Software, um ein fehlertolerantes Verhalten zu erreichen.



keine Abbildung vorhanden

Bei der *Software-Redundanz* gewährleistet zusätzliche Software die Fehlertoleranz. Dies kann einerseits dadurch realisiert werden, dass *Softwarebausteine* für Fehlererkennung, -diagnose und -behebung hinzugefügt werden; andererseits dadurch, dass Softwarekomponenten der eigentlich gleichen Funktionalität eingesetzt werden, die allerdings *unterschiedlich*, d.h. auch möglichst unabhängig, entworfen wurden. Dieses unterschiedliche Entwerfen wird auch *N-Version-Programmieren* genannt und kann verschiedene Ausprägungen dadurch annehmen, dass z. B. unterschiedliche Entwicklungswerkzeuge, Spezifikationssprachen, Entwicklungsteams etc. eingesetzt werden [Lee1990] [Storey1996].

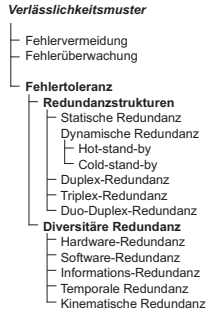
Weiterführende Informationen:

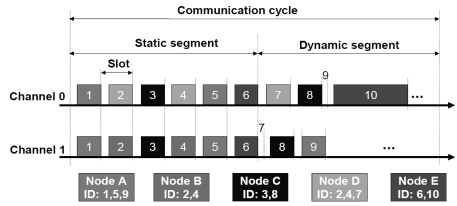
Lee, P. A.; Anderson, T.: Fault Tolerance. Wien: Springer-Verlag, 1990 [Lee1990]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996 [Storey1996]

Informationsredundanz

Informationsredundanz nutzt zusätzliche diversitäre Informationen, um ein fehlertolerantes Verhalten zu erreichen.





Ein Beispiel für Informationsredundanz ist die Time-Triggered-Technologie, die Fehlertoleranz für den Datenbus gewährleistet [www.tzm.de]

Die *Informationsredundanz* erfolgt durch Informationen, die zusätzlich zu den eigentlichen Nutzinformationen realisiert werden. Diese erlauben, neben den für den Betrieb erforderlich Nutzinformationen, zusätzlich Fehler bei der Abspeicherung oder Übertragung zu erkennen und gegebenenfalls auch zu behandeln. Vertreter dieser Redundanzform sind zum Beispiel die Checksummen, Korrektur-Codes oder Paritätsbits. Diese Redundanz beschränkt sich aber nicht nur auf Codierungstechniken, sondern auf alle redundanten Zusatzinformationen. Häufigen Einsatz findet dieses Muster auch bei der Kommunikationstechnik im Bereich der Time-Triggered-Technologien [Storey1996] [Lee1990].

Weiterführende Informationen:

Lee, P. A.; Anderson, T.: Fault Tolerance. Wien: Springer-Verlag, 1990 [Lee1990]

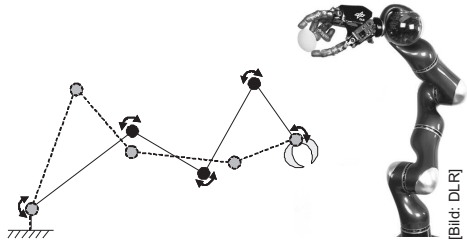
Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996 [Storey1996]

Kinematische Redundanz

Kinematische Redundanz nutzt zusätzliche Bewegungsmöglichkeiten, um ein fehlertolerantes Verhalten zu erreichen.

Verlässlichkeitsmuster

- Fehlervermeidung
- Fehlerüberwachung
- **Fehlertoleranz**
  - **Redundanzstrukturen**
    - Statische Redundanz
    - Dynamische Redundanz
      - Hot-stand-by
      - Cold-stand-by
    - Duplex-Redundanz
    - Triplex-Redundanz
    - Duo-Duplex-Redundanz
  - **Diversitäre Redundanz**
    - Hardware-Redundanz
    - Software-Redundanz
    - Informations-Redundanz
    - Temporale Redundanz
    - Kinematische Redundanz



Kinematische Redundanz am Beispiel eines Greiferarms

Die *Kinematische Redundanz* ermöglicht fehlertolerantes Verhalten dadurch, dass z. B. eine Ziel-Position von einem mehrgelenkigen Greifer durch unterschiedliche Gelenkstellungen erreichbar ist. Fällt ein Gelenk aus, d. h. wird eine kinematische Bewegung fixiert, so kann die Funktion trotzdem noch größtenteils erfüllt werden [Kochs2001].

Weiterführende Informationen:

Kochs, Hans-Dieter: Verlässlichkeitsanalyse mechatronischer Systeme. Forschungsbericht der Fachgruppe "Fehlertolerierende Rechensysteme" der Gesellschaft für Informatik, 2001 [Kochs2001]

Storey, Neil: Safety-Critical Computer Systems. Essex: Prentice Hall, 1996

Anhang C

Datenmaterial zum Anwendungsbeispiel

Hauptkomponenten	Subkomponenten	Merkmal	Funktionen
Fahrwerkrahmen			Tragen von Fahrzeug und Modulkomponenten (Verbindung Räder, Aufbau)
		Tragstruktur	Tragen und Befestigung der Komponenten (inkl. Kraftaufnahme)
			Tragen des Aufbaus
		Druckluftspeicher	Zusatzvolumen für Luftfedern bereitstellen
Verbindungsgelenke			Tragen von Fahrzeug und Modulkomponenten (Verbindung Räder, Aufbau)
	Kugelgelenk (8x)		Kräfte übertragen; translatorische Bewegungen unterbinden
			Momente nicht übertragen; rotatorische Bewegungen ermöglichen
	Querfeder		Drehbewegung der Achse zulassen
	Verbindungsmutter inkl. Schraubensicherungslack		Kräfte übertragen
Achsmodul			Tragen von Fahrzeug und Modulkomponenten (Verbindung Räder, Aufbau)
			Führen entlang der Strecke (Verbindung Räder, Schiene)
	Tragstruktur Achse		Tragen und Befestigung der Komponenten (inkl. Kraftaufnahme)
		Neigungswinkel 1:40	Selbstzentrierung
	Räder	zylindr. Lauffläche	Tragen des Aufbaus
			Führen entlang der Strecke (Verbindung Räder, Schiene); Ermöglichen der translatorischen Bewegung (Fahrtrichtung)
		Spurkranz	Begrenzung der Querbewegung des Fahrzeugs (oder Räder) gegenüber den Schienen
	Lager		Axiales Fixieren der Räder
			Rotation der Räder ermöglichen
	Inkrementalgeber		Drehbewegung der Räder detektieren
	Lenkaktor (Hydraulikzyl.)		drohende Spurkranzanläufe; daraus folgt: Relativ-Bewegung reduzieren
			drohenden Rucks gegensteuern
			Fahrzeug in Weichenkanal lenken
			Lenkwinkel anpassen (Lenkkraft einleiten; zwischen Rahmen und Achse)
		Zylindersensor	IST-Lenkwinkel messen
	hydraulische und elektr. Leitungen		Kommunikation, Energie

Tabelle C.1: Resultat der Komponentenbeschreibung des Spurführungsmoduls (Teil 1/2)

Hauptkomponenten	Subkomponenten	Merkmal	Funktionen
Spurführungssensoren			Positionsbestimmung
	Wirbelstromsensor (4x)		Position der Achse gegenüber Schiene aufnehmen
		elektr. Leitungen	Kommunikation, Hydraulikdruck
	Drehratensensor		Drehrate messen
	Querbeschleunigungssensor		Querbeschleunigung messen
Informationsverarbeitung (IV)			Erkennen eines drohenden zu großen Rucks
			Erkennen drohender Spurkranzanläufe
			Richtungsentscheidung aufnehmen (Weichenkanal bestimmen)
			"Fahrzeug fährt in Schiene" -Szenario erkennen
			"Schiene fährt in Fahrzeug" -Szenario lernen
			notwendigen Soll-Lenkwinkel bestimmen
			Ansteuerung Lenkaktor
	IV Shuttle	OCM	
		Sensorik (Strecke)	
		Aktorik (Strecke)	
	IV Bahnsteuer.(Lenkung)	OCM	
		Sensorik (Strecke)	
		Aktorik (Strecke)	
	IV Spurführung	OCM	
		Sensorik (Strecke)	
		Aktorik (Strecke)	
	IV Lenkzylinder vorne	OCM	
		Sensorik (Strecke)	
		Aktorik (Strecke)	
	IV Lenkzylinder hinten	OCM	
		Sensorik (Strecke)	
		Aktorik (Strecke)	

Tabelle C.2: Resultat der Komponentenbeschreibung des Spurführungsmoduls (Teil 2/2)

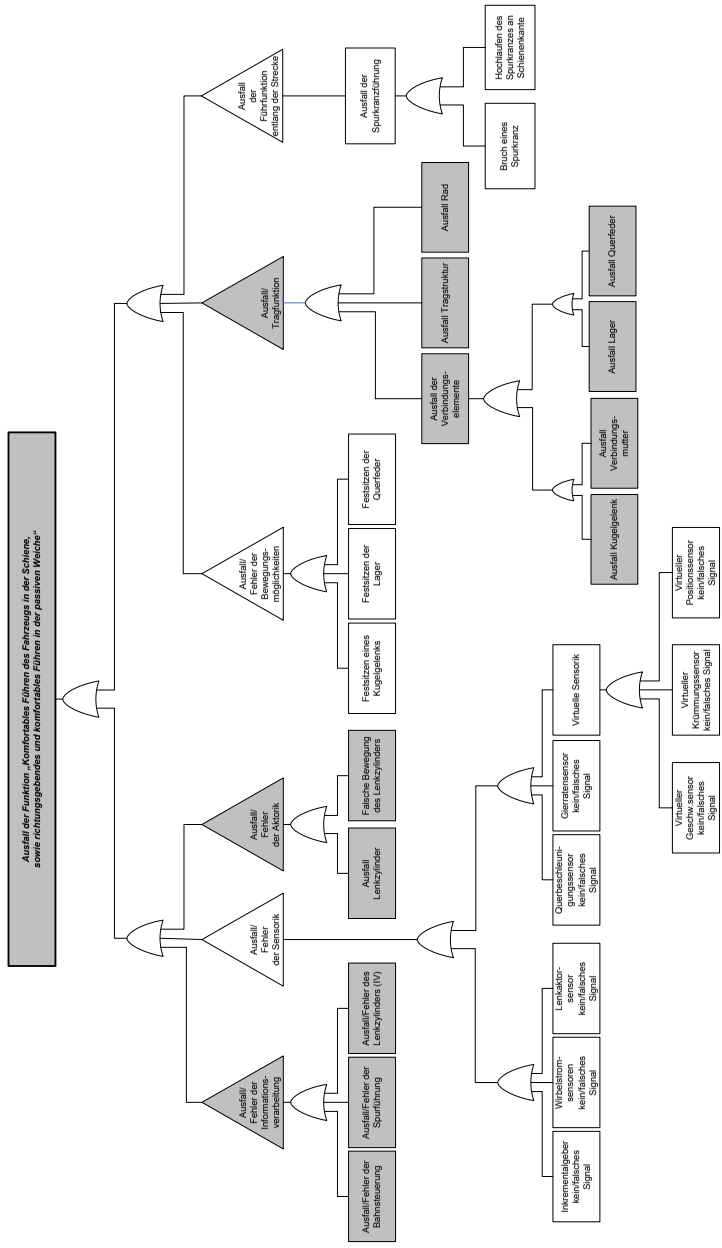


Abbildung C.1: Fehlerbäume des Spurführungsmoduls: Gesamtübersicht

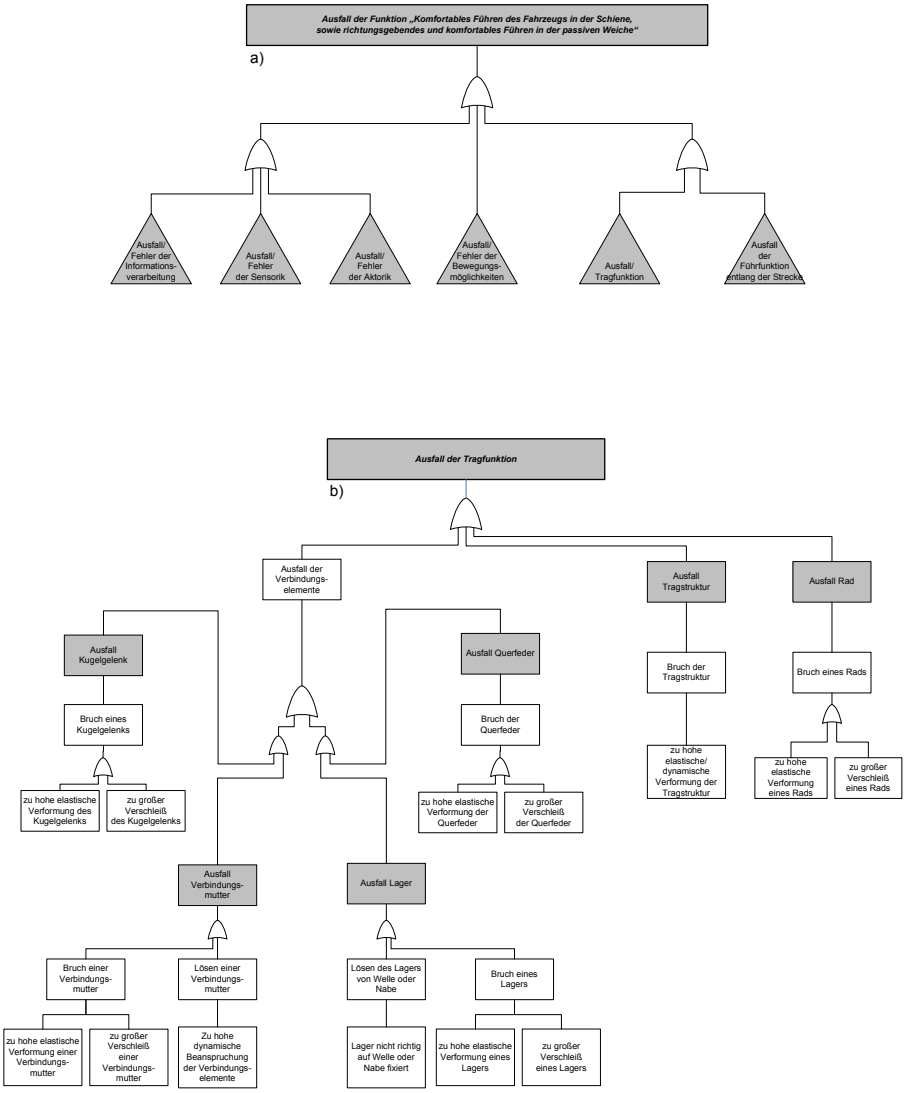


Abbildung C.2: Fehlerbäume des Spurführungsmoduls: a) Aufteilung der Einzelbäume; b) Tragfunktion

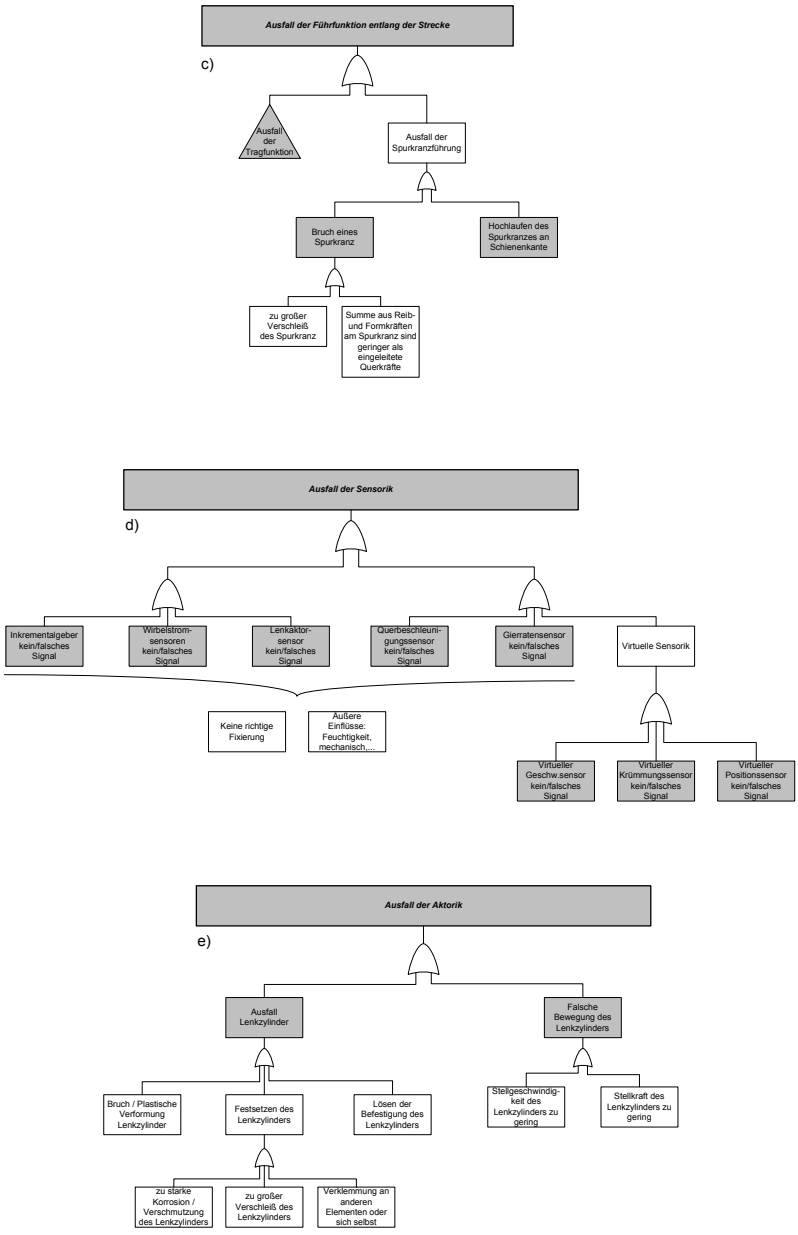


Abbildung C.3: Fehlerbäume des Spurführungsmoduls: c) Führfunktion; d) Sensorik; e) Aktorik

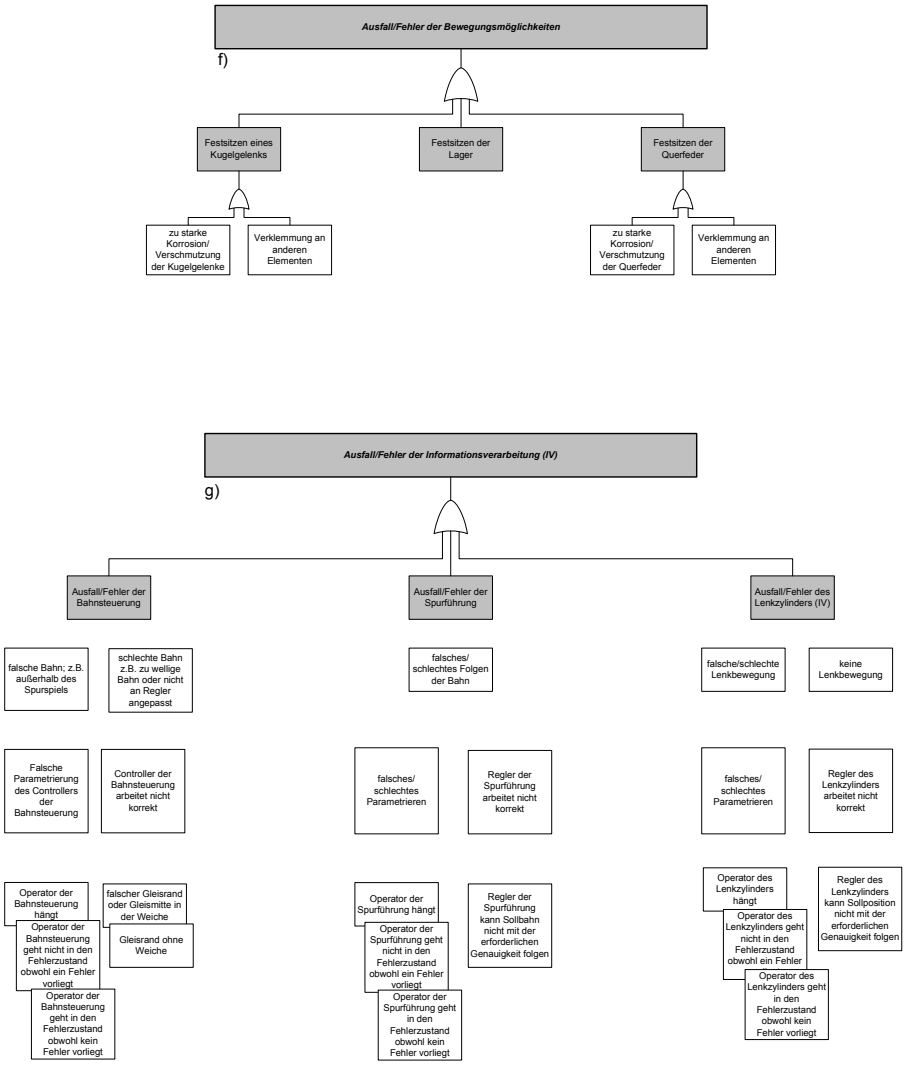


Abbildung C.4: Fehlerbäume des Spurführungsmoduls: f) Informationsverarbeitung; g) Bewegungsmöglichkeiten

Fehlerausfall/Fehlerzustand	Fehlerursache
Ausfall der Tragfunktion	Materialfehler, Auslegungsfehler, Missbrauch, Fertigungsfehler
Ausfall Tragstruktur	Materialfehler, Auslegungsfehler, Fertigungsfehler Überbelastung im Fahrwerksrahmen oder anderer Missbrauch
Ausfall Rad (tragende Funktion)	Materialfehler, Auslegungsfehler, Fertigungsfehler zu hohe Normalkraft auf Räder oder anderer Missbrauch
Ausfall Kugelgelenk	Verschleiß zu hohe Kraft im Kugelgelenk (Missbrauch) translatorische Bewegungen im Kugelgelenk (Missbrauch)
Ausfall Querfeder	Missbrauch, Materialfehler und -ermüdung
Ausfall Verbindungsmutter	mechanischer Missbrauch, Materialfehler,...
Ausfall Lager	Verschleiss, Schmutz, Missbrauch
Ausfall der Führfunktion (mechanisch)	
Bruch eines Spurkranz	Materialfehler, Auslegungsfehler, Missbrauch, Fertigungsfehler
Hochlaufen des Spurkranzes an der Schienenkante	Kontaktgeometrie-Problem
zu niedriger Reibbeiwert Rad-Schiene-Kontakt	siehe Umwelt*fehler*, Kontaktgeometrie-Problem
zu ungleichmäßiger Reibbeiwert Rad-Schiene-Kontakt	siehe Umwelt*fehler*, Kontaktgeometrie-Problem
Ausfall/Fehler der Sensorik	
Ausfall/Fehler Inkrementalgeber	Ausfälle in der Signalverarbeitungskette,... Falsches Signal Kein Signal Zu schlechtes Signal
Ausfall/Fehler Lenkaktorsensor	Ausfälle in der Signalverarbeitungskette,... Falsches Signal Kein Signal Zu schlechtes Signal
Ausfall/Fehler Wirbelstromsensor	Ausfälle in der Signalverarbeitungskette,... Falsches Signal Kein Signal Zu schlechtes Signal
Ausfall/Fehler Querbeschleunigungssensor	Ausfälle in der Signalverarbeitungskette,...
Ausfall/Fehler Gierratensensor	Ausfälle in der Signalverarbeitungskette,...
Ausfall/Fehler virtueller Geschwindigkeitssensor	Inputsignale fehlen/falsch, Softwarefehler keine Geschwindigkeit (virtueller Sensor) falsche Geschwindigkeit (virtueller Sensor)
Ausfall/Fehler virtueller Streckenkrümmungssensor	Inputsignale fehlen/falsch, Softwarefehler Kein Signal Krümmung Falsches Signal Krümmung
Ausfall/Fehler virtueller Längspositionssensor	Inputsignale fehlen/falsch, Softwarefehler kein Signal Längsposition falsches Signal Längsposition
Ausfall/Fehler der Aktorik	
Ausfall des Lenkzylinders	keine Kraft/kein Weg des Aktors
Falsche Bewegung des Lenkzylinders	z. B. falscher, zu hoher, zu niedriger, schwankender, stoßweiser Öldruck

Tabelle C.3: Gesamte Fehlerliste des Spurführungsmoduls als Resultat verschiedener zusammengeführter Fehleranalysen (Teil 1/2)

Fehlerausfall/Fehlerzustand	Fehlerursache
Ausfall/Fehler der Informationsverarbeitung (IV)	
Ausfall/Fehler der Fehlerüberwachung	Programmier-, Kommunikations-, oder Rechenfehler auf CPU keine Fehlerinformationen zu späte Fehlerinformationen falsche Fehlerinformationen
Ausfall/Fehler der Bahnsteuerung	Programmier-, Kommunikations-, oder Rechenfehler auf CPU kein Abbiegewunsch (j/n) ungewollter Abbiegewunsch (j/n) zu später Abbiegewunsch (j/n)
Ausfall/Fehler der Spurführung	Programmier-, Kommunikations-, oder Rechenfehler auf CPU
Ausfall/Fehler des Lenkzyklinders (IV)	Programmier-, Kommunikations-, oder Rechenfehler auf CPU kein Sollzustand (Lenkwinkel) falscher Sollzustand (Lenkwinkel) kein Istzustand (Lenkwinkel) Falscher Istzustand (zu großer Lenkwinkel)
Ausfall/Fehler der Bewegungsmöglichkeiten	
Festsitzen eines Kugelgelenks	Verschleiß, Missbrauch
Festsitzen eines Lagers	Verschleiss, Schmutz, Missbrauch
Festsitzen der Querfeder	Missbrauch, Materialfehler und -ermüdung
Einzelfehler/ Fehler des gesamten Shuttles mit Auswirkung	
Undichtigkeit des Druckluftspeichers	Materialermüdung, Löcher,...
zu hoher Luftdruck in Luftfeder	Fehler im Druckluftsystem
zu geringer Luftdruck in Luftfeder	Fehler im Druckluftsystem
zu hohe Geschwindigkeit des Fahrzeugs	
falsche Position des Fahrzeugs (Querposition)	
falsche Position des Fahrzeugs (Längsposition)	
Umwelt oder Betriebs*fehler*	
Beladungsfehler	zu viel, falsch verteiltes Gewicht
Wind*fehler* o.Ä.	zu viel, zu wechselhafter Seitenwind
Strecke zu extrem	zu steil, zu ungleichmäßige Steigung zu kleiner Radius, zu schnellen Radienwechsel zu starke Gleisüberhöhungen zu geringe Reibung durch z.B. Eis, Öl
Umweltbedingungen zu extrem	zu hohe Temperatur zu niedrige Temperatur zu viel Verschmutzungen

Tabelle C.4: Gesamte Fehlerliste des Spurführungsmoduls als Resultat verschiedener zusammengeführter Fehleranalysen (Teil 2/2)

Fehler/Fehlerursache	Gefahr	Häufigkeit	Auswirkung	Risiko
Ausfall der Tragfunktion (Tragstruktur u. Verbindungselemente)				II
Ausfall Tragstruktur				III
- Materialfehler, Auslegungsfehler, Fertigungsfehler	Entgleisung, Umkippen des Fahrzeugs	unwahrsch.	katastrophal	III
- zu hohe Kraft im Fahrwerksrahmen oder anderer Missbrauch	Entgleisung, Umkippen des Fahrzeugs	unwahrsch.	katastrophal	III
Ausfall Rad (tragende Funktion)				II
- Materialfehler, Auslegungsfehler, Fertigungsfehler	Entgleisung, Umkippen des Fahrzeugs	gering	katastrophal	II
- zu hohe Normalkraft auf Räder oder anderer Missbrauch	Entgleisung, Umkippen des Fahrzeugs	gering	katastrophal	II
Ausfall Kugelgelenk				III
- Verschleiß	Schlingern, bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung	gering	begrenzt	III
- zu hohe Kraft im Kugelgelenk (Missbrauch)	bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung	unwahrsch.	katastrophal	III
- translatorische Bewegungen im Kugelgelenk (Missbrauch)	bei Nicht-Erkennen und weiterer Ausfälle: Entgleisung	gering	begrenzt	III
Ausfall Querfeder				IV
- Missbrauch, Materialfehler und -ermüdung	leichtes Schlingern	gering	geringfügig	IV
Ausfall Verbindungsmutter				IV
- mechanischer Missbrauch, Materialfehler,...	ungleichmäßige Krafteinleitung, Schlingern	unwahrsch.	begrenzt	IV
Ausfall Lager				III
- Verschleiß, Schmutz, Missbrauch	Blockieren des Rads	gelegentlich	begrenzt	III
Ausfall der Führfunktion entlang der Strecke (mechanisch)		unwahrsch.	katastrophal	III
Bruch eines Spurkranz				III
- Materialfehler, Auslegungsfehler, Missbrauch, Fertigungsfehler	Entgleisung, Umkippen des Fahrzeugs	unwahrsch.	katastrophal	III
Hochlaufen des Spurkranzes an der Schienenkante				III
- Kontaktgeometrie-Problem	Entgleisung, Umkippen des Fahrzeugs	unwahrsch.	katastrophal	III
zu niedriger Reibbeiwert Rad-Schiene Kontakt				III
- Kontaktgeometrie-Problem	Entgleisung, Umkippen des Fahrzeugs	unwahrsch.	katastrophal	III
zu ungleichmäßiger Reibbeiwert Rad-Schiene Kontakt				III
- Kontaktgeometrie-Problem	ungleichmäßige Krafteinleitung, Schlingern	unwahrsch.	begrenzt	IV

Tabelle C.5: Resultat des Prozesschrittes *Fehler-, Gefahren- und Risikenanalysen* des Spurführungsmoduls (Teil 1/4)

Tabelle C.6: Resultat des Prozessschrittes *Fehler-, Gefahren- und Risikoanalysen* des Spurführungsmoduls (Teil 2/4)

Fehler/Fehlerursache	Gefahr	Häufigkeit	Auswirkung	Risiko
Ausfall/Fehler der Sensorik				II
Ausfall/Fehler Inkrementalgeber				II
- Ausfälle in der Signalverarbeitungskette,...	Position verlieren, Geschwindigkeit	gering	katastrophal	II
- Falsches Signal	Falsche Entscheidungen -> Entgleisung	gering	katastrophal	II
- Kein Signal		gering	begrenzt	III
- Zu schlechtes Signal		gering	geringfügig	IV
Ausfall/Fehler Lenkaktorsensor				III
- Ausfälle in der Signalverarbeitungskette,...	Lenken und komfortables Führen wird unmöglich	gering	begrenzt	III
- Falsches Signal	Falsches Lenken und unkomfortables Führen	gering	begrenzt	III
- Kein Signal	Lenken und komfortables Führen wird unmöglich	gering	begrenzt	III
- Zu schlechtes Signal	Lenken und komfortables Führen eingeschränkt	gering	geringfügig	IV
Ausfall/Fehler Wirbelstromsensor				III
- Ausfälle in der Signalverarbeitungskette,...	Nur Steuern möglich; Komfortverlust	gelegentlich	geringfügig	III
- Falsches Signal	Falsches Lenken und unkomfortables Führen	gering	begrenzt	III
- Kein Signal	Lenken und komfortables Führen wird unmöglich	gelegentlich	begrenzt	III
- Zu schlechtes Signal	Lenken und komfortables Führen wird unmöglich	gering	geringfügig	IV
Ausfall/Fehler Querbeschleunigungssensor				IV
- Ausfälle in der Signalverarbeitungskette,...	keine direkte Gefahr, da keine direkte Verwendung	unwahrsch.	geringfügig	IV
Ausfall/Fehler Gierratensensor				IV
- Ausfälle in der Signalverarbeitungskette,...	keine direkte Gefahr, da keine direkte Verwendung	unwahrsch.	geringfügig	IV
Ausfall/Fehler virtueller Geschwindigkeitssensor				IV
- Inputsignale fehlen/falsch, Softwarefehler	Falsche Position, Entgleisung,...	gering	kritisch	III
- keine SIgnal bzgl. Geschwindigkeit (virtueller Sensor)		gering	begrenzt	III
- falsche Geschwindigkeit (virtueller Sensor)		gering	kritisch	III
Ausfall/Fehler virtueller Streckenkrümmungssensor				II
- Inputsignale fehlen/falsch, Softwarefehler	Komfortverlust, bis zu Entgleisung	gelegentlich	kritisch	II
- Kein Signal bzgl. Streckenkrümmung		gelegentlich	begrenzt	III
- Falsches Signal bzgl. Krümmung		gelegentlich	kritisch	II
Ausfall/Fehler virtueller Längspositionssensor				III
- Inputsignale fehlen/falsch, Softwarefehler		gering	kritisch	III
- kein Signal Längsposition		gering	begrenzt	III
- falsches Signal Längsposition		gering	kritisch	III

Fehler/Fehlerursache	Gefahr	Häufigkeit	Auswirkung	Risiko
Ausfall/Fehler der Aktorik				III
Ausfall des Lenkzylinders				III
- keine Kraft/kein Weg des Aktors	keine Lenkung und komfortabel Spurführung möglich	gering	begrenzt	III
Falsche Bewegung des Lenkzylinders				III
- z.B. falscher, zu hoher, zu niedriger, schwankender, stoßweiser Öldruck	falsche Lenkung, Komforteinbußen	gering	kritisch	III
Ausfall/Fehler der Informationsverarbeitung (IV)				II
Ausfall/Fehler der Fehlerüberwachung				III
- Programmier-, Kommunikations-, oder Rechenfehler auf CPU	Falsche Entscheidungen	unwahrsch.	kritisch	III
- keine Fehlerinformationen	Falsche Entscheidungen	unwahrsch.	kritisch	III
- zu späte Fehlerinformationen	Falsche Entscheidungen	unwahrsch.	kritisch	III
- falsche Fehlerinformationen	Falsche Entscheidungen	unwahrsch.	kritisch	III
Ausfall/Fehler der Bahnsteuerung				II
- Programmier-, Kommunikations-, oder Rechenfehler auf CPU	Unkomfortables Fahren, Entgleisung bei hohen Geschwindigk.	unwahrsch.	katastrophal	III
- kein Abbiegewunsch (j/n)	Entgleisung bei hohen Geschwindigk.	gering	katastrophal	II
- ungewollter Abbiegewunsch (j/n)	Umweg; Strecke nicht frei	unwahrsch.	begrenzt	IV
- zu später Abbiegewunsch (j/n)	Entgleisung bei hohen Geschwindigk.	gering	katastrophal	II
Ausfall/Fehler der Spurführung				IV
- Programmier-, Kommunikations-, oder Rechenfehler auf CPU	Unkomfortables Fahren, Entgleisung bei hohen Geschwindigk.	unwahrsch.	begrenzt	IV
Ausfall/Fehler des Lenkzyklinders (IV)				II
- Programmier-, Kommunikations-, oder Rechenfehler auf CPU	Unkomfortables Fahren, Entgleisung bei hohen Geschwindigk.	unwahrsch.	begrenzt	IV
- kein Sollzustand (Lenkwinkel)	Unkomfortables Fahren, Entgleisung bei hohen Geschwindigk.	gering	katastrophal	II
- falscher Sollzustand (Lenkwinkel)	Unkomfortables Fahren, Entgleisung bei hohen Geschwindigk.	gering	katastrophal	II
- kein Istzustand (Lenkwinkel)	Unkomfortables Fahren, Entgleisung bei hohen Geschwindigk.	gering	katastrophal	II
- Falscher Istzustand (zu großer Lenkwinkel)	Unkomfortables Fahren, Entgleisung bei hohen Geschwindigk.	gering	katastrophal	II
Ausfall/Fehler der Bewegungsmöglichkeiten				III
Festsitzen eines Kugelgelenks				III
- Verschleiß, Missbrauch	ungleichmäßige Krafteinleitung, Schlingern	gering	begrenzt	III
Festsitzen eines Lagers				III
- Verschleiß, Schmutz, Missbrauch	Blockieren des Rads	gelegentlich	begrenzt	III
Festsitzen der Querfeder				IV
- Missbrauch, Materialfehler und -ermüdung	leichtes Schlingern	gering	geringfügig	IV

Tabelle C.7: Resultat des Prozesschrittes *Fehler-, Gefahren- und Risikenanalysen* des Spurführungsmoduls (Teil 3/4)

Tabelle C.8: Resultat des Prozessschrittes *Fehler-, Gefahren- und Risikenanalysen* des Spurführungsmoduls (Teil 4/4)

Fehler/Fehlerursache	Gefahr	Häufigkeit	Auswirkung	Risiko
Einzelfehler / Fehler des gesamten Shuttles mit Auswirkung				III
Undichtigkeit des Druckluftspeichers				IV
- Materialermüdung, Löcher,...	Fahrkomfort sinkt	unwahrsch.	geringfügig	IV
- zu hoher Luftdruck in Luftfeder				IV
- Fehler im Druckluftsystem	Platzen der Luftfeder, Komfort sinkt	unwahrsch.	geringfügig	IV
zu geringer Luftdruck in Luftfeder				IV
- Fehler im Druckluftsystem	Komfort sinkt	unwahrsch.	geringfügig	IV
zu hohe Geschwindigkeit des Fahrzeugs	Komfort sinkt, Entgleisen	unwahrsch.	katastrophal	III
falsche Position des Fahrzeugs (Querposition)	Komfort sinkt, Entgleisen	unwahrsch.	katastrophal	III
falsche Position des Fahrzeugs (Längsposition)	Komfort sinkt, Entgleisen	unwahrsch.	katastrophal	III
Umwelt oder Betriebs*fehler*				II
Beladungsfehler				III
- zu viel, falsch verteiltes Gewicht	Ausfall Tragstruktur	unwahrsch.	katastrophal	III
Wind*fehler* o.Ä.				II
- zu viel, zu wechselhafter Seitenwind	Entgleisung	gering	katastrophal	II
Strecke zu extrem				II
- zu steil, zu ungleichmäßige Steigung	Shuttle schafft die Steigung nicht	unwahrsch.	geringfügig	IV
- zu kleiner Radius, zu schnellen Radienwechsel	Entgleisung bei zu hoher Geschwindigkeit	gering	katastrophal	II
- zu starke Gleisüberhöhungen	Entgleisung	unwahrsch.	katastrophal	III
- zu geringe Reibung durch z.B. Eis, Öl	Fahrkomfort sinkt, Entgleisung, ...	gelegentlich	kritisch	II
Umweltbedingungen zu extrem				III
- zu hohe Temperatur	Ausfall Aktorik, Senorik, IV	gering	kritisch	III
- zu niedrige Temperatur	Ausfall Aktorik, Senorik, IV, Bewegungsmöglichkeiten	gering	kritisch	III
- zu viel Verschmutzungen	Ausfall Aktorik, Senorik, IV, Bewegungsmöglichkeiten	gering	begrenzt	III

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 zusammenzuführen, 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: Auf dem Weg zu den technischen Systemen von morgen“. In der Lehre engagiert sich das Heinz Nixdorf Institut in vielen Studiengängen der Universität. Hier ist das übergeordnete Ziel, den Studierenden die Kompetenzen zu vermitteln, auf die es in der Wirtschaft morgen ankommt.

Heute wirken am Heinz Nixdorf Institut sieben 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: Enroute 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 seven 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.

Stand: April 2006

Bände der HNI-Verlagsschriftenreihe

Bd. 1 FAHRWINKEL, U.: Methoden zur Modellierung und Analyse von Geschäftsprozessen zur Unterstützung des Business Process Reengineering. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 1, 1995 – ISBN 3-931466-00-0

Bd. 2 HORNBOSTEL, D.: Methode zur Modellierung der Informationsverarbeitung in Industrieunternehmen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 2, 1995 – ISBN 3-931466-01-9

Bd. 3 STEMANN, V.: Contention Resolution in Hashing Based Shared Memory Simulations. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 3, 1995 – ISBN 3-931466-02-7

Bd. 4 KETTERER, N.: Beschreibung von Datenaustausch eines verteilten Fertigungssteuerungssystems. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 4, 1995 – ISBN 3-931466-03-5

Bd. 5 HARTMANN, T.: Spezifikation und Klassifikation von Methoden zur Definition hierarchischer Abläufe. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 5, 1995 – ISBN 3-931466-04-3

Bd. 6 WACHSMANN, A.: Eine Bibliothek von Basisdiensten für Parallelrechner: Routing, Synchronisation, gemeinsamer Speicher. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 6, 1995 – ISBN 3-931466-05-1

Bd. 7 GAUSEMEIER, J. (Hrsg.): Die Szenario-Technik – Werkzeug für den Umgang mit einer multiplen Zukunft. 1. Paderborner Szenario-Workshop, 14. November 1995, HNI-Verlagsschriftenreihe, Paderborn, Band 7, 1995 – ISBN 3-931466-06-X

Bd. 8 CZUMAJ, A.: Parallel Algorithmic Techniques: PRAM Algorithms and PRAM Simulations. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 8, 1995 – ISBN 3- 931466-07-8

Bd. 9 HUMPERT, A.: Methodische Anforderungsverarbeitung auf Basis eines objektorientierten Anforderungsmodells. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 9, 1995 – ISBN 3-931466-08-6

Bd. 10 AMEUR, F.: Space-Bounded Learning Algorithms. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 10, 1995 –ISBN 3-931466-09-4

Bd. 11 PAUL, M.: Szenariobasiertes Konzipieren neuer Produkte des Maschinenbaus auf Grundlage möglicher zukünftiger Technologieentwicklungen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 11, 1996 – ISBN 3-931466-10-8

Bd. 12 HOLL, F.: Ordnungsmäßigkeit von Informations- und Kommunikationssystemen. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 12, 1996 – ISBN 3-931466-11-6

Bd. 13 GAUSEMEIER, J. (Hrsg.): First European Workshop on Global Engineering Networking - organized by GLENnet e.V., HNI-Verlagsschriftenreihe, Paderborn, Band 13, 1996 – ISBN 3-931466-12-4

Bd. 14 PETRI, K.: Vergleichende Untersuchung von Berechnungsmodellen zur Simulation der Dynamik von Fahrleitung-Stromabnehmer-Systemen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 14, 1996 – ISBN 3-931466-13-2

Bd. 15 LESCHKA, S.: Fallbasiertes Störungsmanagement in flexiblen Fertigungssystemen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 15, 1996 – ISBN 3-931466-14-0

Bd. 16 SCHNEIDER, U.: Ein formales Modell und eine Klassifikation für die Fertigungssteuerung - Ein Beitrag zur Systematisierung der Fertigungssteuerung. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 16, 1996 – ISBN 3-931466-15-9

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 17 FELSER, W.: Eine Methode zur Erstellung von Fertigungssteuerungsverfahren aus Bausteinen. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 17, 1996 – ISBN 3-931466-16-7

Bd. 18 GAUSEMEIER, J.; ALEXANDER FINK, A.: Neue Wege zur Produktentwicklung – Erfolgspotentiale der Zukunft. HNI-Verlagsschriftenreihe, Paderborn, Band 18, 1996– ISBN 3-931466-17-5

Bd. 19 DANGELMAIER, W.; GAUSEMEIER, J.: Fortgeschrittene Informationstechnologie in der Produktentwicklung und Fertigung. 2. Internationales Heinz Nixdorf Symposium, HNI-Verlagsschriftenreihe, Paderborn, Band 19, 1996 – ISBN 3-931466-18-3

Bd. 20 HÜLLERMEIER, E.: Reasoning about Systems based on Incomplete and Uncertain Models. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 20, 1997 – ISBN 3-931466- 19-1

Bd. 21 GAUSEMEIER, J.: International Symposium on Global Engineering Network - Antwerb, Belgium, HNI-Verlagsschriftenreihe, Paderborn, Band 21, 1997 – ISBN 3- 931466-20-5

Bd. 22 BURGER, A.: Methode zum Nachweis der Wirtschaftlichkeit von Investitionen in die Rechnerintegrierte Produktion. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 22, 1997 – ISBN 3-931466-21-3

Bd. 23 GAUSEMEIER, J.: Entwicklung und Transfer von Entwicklungssystemen der Mechatronik - Paderborner Workshop TransMechatronik. HNI-Verlagsschriftenreihe, Paderborn, Band 23, 1997 – ISBN 3- 931466-22-1

Bd. 24 GERDES, K.-H.: Architekturkonzeption für Fertigungsleitsysteme der flexiblen automatischen Fertigung. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 24, 1997 – ISBN 3-931466-23-X

Bd. 25 EBBESMEYER, P.: Dynamische Texturwände - Ein Verfahren zur echtzeitorientierten Bildgenerierung für Virtuelle Umgebungen technischer Objekte. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 25, 1997 – ISBN 3-931466-24-8

Bd. 26 FRANK, G.: Ein digitales Hardwaresystem zur echtzeitfähigen Simulation biologienaher neuronaler Netze. Dissertation, Fachbereich für Elektrotechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 26, 1997 – ISBN 3-931466-25-6

Bd. 27 DITTRICH, W.: Communication and I/O Efficient Parallel Data Structures. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 27, 1997 – ISBN 3-931466-26-4

Bd. 28 BÄUMKER, A.: Communication Efficient Parallel Searching. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 28 1997 – ISBN 3- 931466-27-2

Bd. 29 PINTASKE, C.: System- und Schaltungstechnik neuronaler Assoziativspeicher. Dissertation, Fachbereich für Elektrotechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 29, 1997 – ISBN 3-931466-28-0

Bd. 30 HENKEL, S.: Ein System von Software-Entwurfsmustern für die Propagation von Ereignissen in Werkzeugen zur kooperativen Fabrikmodellierung. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 30, 1997 – ISBN 3-931466-29-9

Bd. 31 DANGELMAIER, W.: Vision Logistik – Logistik wandelbarer Produktionsnetze. HNI-Verlagsschriftenreihe, Paderborn, Band 31, 1997 – ISBN 3-931466-30-2

Bd. 32 BREXEL, D.: Methodische Strukturmodellierung komplexer und variantenreicher Produkte des integrativen Maschinenbaus. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 32, 1997 – ISBN 3-931466-31-0

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 33 HAHN, A.: Integrationsumgebung für verteilte objektorientierte Ingenieursysteme. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 33, 1997 – ISBN 3-931466-32-9

Bd. 34 SABIN, A.: Semantisches Modell zum Aufbau von Hilfsorientierungsdiensten in einem globalen Engineering Netzwerk. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 34, 1997 – ISBN 3-931466-33-7

Bd. 35 STROTHMANN, W.-B.: Bounded Degree Spanning Trees. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 35, 1997 – ISBN 3-931466-34-5

Bd. 36 MÜLLER, W.; RAMMIG, F.-J.: Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen. HNI-Verlagsschriftenreihe, Paderborn, Band 36, 1998 – ISBN 3-931466- 35-3

Bd. 37 SCHNEIDER, W.: Anwenderorientierte Integration von CAE-Systemen. Ein Verfahren zur Realisierung eines durchgehenden Informationsflusses entlang des Produktentwicklungsprozesses. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 37, 1998 – ISBN 3-931466-36-1

Bd. 38 DEMEL, W.; SCHMITZ, G. (Hrsg.): Entwicklung und Transfer von Entwicklungssystemen der Mechatronik. Aachener Workshop TransMechatronik, 26. Juni 1998, Technologiezentrum am Europaplatz Aachen, HNI-Verlagsschriftenreihe, Paderborn, Band 38, 1998 – ISBN 3-931466-37-X

Bd. 39 GROBBEL, R.; LANGEMANN, T.: Leitfaden PPS-Systeme: Auswahl und Einführung in der Möbelindustrie. HNI-Verlagsschriftenreihe, Paderborn, Band 39, 1998 – ISBN 3-931466-38-8

Bd. 40 REHBEIN, P.: Tribologische Untersuchung von hochfrequent schwingenden Gleitkontakten für den Einsatz in Reibkraftschlüssigen Antrieben. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 40, 1998 – ISBN 3-931466-39-6

Bd. 41 DANGELMAIER, W.: KOMNET – Kommunikationsplattform für KMU-Netzwerke. HNI-Verlagsschriftenreihe, Paderborn, Band 41, 1998 – ISBN 3-931466-40-X

Bd. 42 KALLMEYER, F.: Eine Methode zur Modellierung prinzipieller Lösungen mechatronischer Systeme. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 42, 1998 – ISBN 3-931466-41-8

Bd. 43 TRAPP, R.: Stereoskopische Korrespondenzbestimmung mit impliziter Detektion von Okklusionen. Dissertation, Fachbereich für Elektrotechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 43, 1998 – ISBN 3-931466-42-6

Bd. 44 GAUSEMEIER, J.; FINK, A; SCHLAKE, O.: Grenzen überwinden - Zukünfte gestalten. 2. Paderborner Konferenz für Szenario-Management, HNI-Verlagsschriftenreihe, Paderborn, Band 44, 1998 – ISBN 3-931466-43-4

Bd. 45 wird noch vergeben!

Bd. 46 VÖCKING, B.: Static and Dynamic Data Management in Networks. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 46, 1998 – ISBN 3-931466-45-0

Bd. 47 SCHEKELMANN, A.: Materialflußsteuerung auf der Basis des Wissens mehrerer Experten. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 47, 1999 – ISBN 3-931466-46-9

Bd. 48 GECK-MÜGGE, K.: Herleitung und Spezifikation generischer Bausteine zur einheitlichen Modellierung von Fertigungsinformationen für die Fertigungssteuerung. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 48, 1999 – ISBN 3-931466-47-7

Bd. 49 WALLASCHEK, J.; LÜCKEL, J.; LITTMANN, W.: Heinz Nixdorf Symposium on Mechatronics and Advanced Motion Control. 3. Internationales Heinz Nixdorf Symposium, HNI-Verlagsschriftenreihe, Paderborn, Band 49, 1999 – ISBN 3-931466-48-5

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 50 FINK, A.: Szenariogestützte Führung industrieller Produktionsunternehmen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 50, 1999 – ISBN 3-931466-49-3

Bd. 51 HOLTKAMP, R.: Ein objektorientiertes Rahmenwerk zur Erstellung individueller, verteilter Fertigungslenkungssysteme. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 51, 1999 – ISBN 3-931466-50-7

Bd. 52 KUHN, A.: Referenzmodelle für Produktionsprozesse zur Untersuchung und Gestaltung von PPS-Aufgaben. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 52, 1999 – ISBN 3-931466-51-5

Bd. 53 SIEBE, A.: Systematik der Umsetzung von IT-orientierten Veränderungsprojekten in dynamischen Umfeldern. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 53, 1999 – ISBN 3-931466-52-3

Bd. 54 KLAHOLD, R. F.: Dimensionierung komplexer Produktionsnetzwerke. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 54, 1999 – ISBN 3-931466-53-1

Bd. 55 SCHÜRHOLZ, A.: Synthese eines Modells zur simulationsgestützten Potentialanalyse der Distribution. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 55, 1999 – ISBN 3-931466-54-X

Bd. 56 GEHNEN, G.: Integriertes Netzwerk zur Fertigungssteuerung und –automatisierung. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 56, 1999 – ISBN 3-931466-55-8

Bd. 57 KRESS, S.: Architektur eines workflowbasierten Planungsinstruments für die technische Auftragsbearbeitung unter besonderer Berücksichtigung des Einsatzes der Telearbeit. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 57, 1999 – ISBN 3-931466-56-6

Bd. 58 THIELEMANN, F.: Integrierte Methodik zur Gestaltung von Leistungserstellungsprozessen mittels Workflowmanagement. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 58, 1999 – ISBN 3-931466-57-4

Bd. 59 KROME, J.: Modelle zur Untersuchung des Schwingungsverhaltens von Statoren für piezoelektrische Ultraschall-Wanderwellen-Motoren. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 59, 1999 – ISBN 3-931466-58-2

Bd. 60 DEMEL, W.; SCHMITZ , G. (Hrsg.): Entwicklung und Transfer von Entwicklungssystemen der Mechatronik. Krefelder Workshop TransMechatronik, 24. August 1999 Fachhochschule Niederrhein, HNI-Verlagsschriftenreihe, Paderborn, Band 60, 1999 – ISBN 3-931466-59-0

Bd. 61 LANGEMANN, T.: Modellierung als Kernfunktion einer systemorientierten Analyse und Bewertung der diskreten Produktion. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 61, 1999 – ISBN 3-931466-60-4

Bd. 62 KÜMMEL, M.: Integration von Methoden und Werkzeugen zur Entwicklung von mechatronischen Systemen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 62, 1999 – ISBN 3-931466-61-2

Bd. 63 LUKOVSZKI, T.: New Results on Geometric Spanners and Their Applications. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 63, 1999 – ISBN 3-931466-62-0

Bd. 64 LÖFFLER, A.; MONDADA, F.; RÜCKERT, U. (Hrsg.): Experiments with the Mini-Robot Khepera, Proceedings of the 1st International Khepera Workshop. HNI-Verlagsschriftenreihe, Paderborn, Band 64, 1999 – ISBN 3-931466-63-9

Bd. 65 SCHÄFERMEIER, U.; BISCHOFF, C.: KMUnet - Ein Konzept zur ablauforganisatorischen Gestaltung der Lieferanteneinbindung. HNI-Verlagsschriftenreihe, Paderborn, Band 65, 2000 – ISBN 3-931466-64-7

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 66 HOLTHÖFER, N.: Regeln in einer Mengenplanung unter Ausbringungsgrenzen. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 66, 2000 – ISBN 3-931466-69-8

Bd. 67 SCHLAKE, O.: Verfahren zur kooperativen Szenario-Erstellung in Industrieunternehmen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 67, 2000 – ISBN 3-931466-66- 3

Bd. 68 LEWANDOWSKI, A.: Methode zur Gestaltung von Leistungserstellungsprozessen in Industrieunternehmen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 68, 2000 – ISBN 3-931466-67-1

Bd. 69 SCHMIDTMANN, A.: Eine Spezifikationssprache für die Fertigungslenkung. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 69, 2000 – ISBN 3-931466-68-X

Bd. 70 GROBBEL, R.: Eine Referenzarchitektur für Kooperationsbörsen. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 70, 2000 – ISBN 3-931466-69-8

Bd. 71 WESSEL, R.: Modelocked Waveguide Lasers in Lithium Niobate. Dissertation, Fachbereich für Physik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 71, 2000 – ISBN 3-931466-70-1

Bd. 72 LÖFFLER, A.: Energetische Modellierung neuronaler Signalverarbeitung. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 72, 2000 – ISBN 3-931433-71-X

Bd. 73 LUDWIG, L. A.: Computational Intelligence in der Produktionswirtschaft. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 73, 2000 – ISBN 3-931466-72-8

Bd. 74 WENSKI, R.: Eine objektorientierte Systemkomponente zur Workflow-Modellierung und -Ausführung unter besonderer Berücksichtigung der Telekooperation. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 74, 2000 – ISBN 3-931466-73-6

Bd. 75 GRASMANN, M.: Produktkonfiguration auf Basis von Engineering Data Management-Systemen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 75, 2000 – ISBN 3-931466-74-4

Bd. 76 DITZE, C.: Towards Operating System Synthesis. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 76, 2000 – ISBN 3-931466-75-2

Bd. 77 KÖRNER, T.: Analog VLSI Implementation of a Local Cluster Neural Network. Dissertation, Fachbereich für Elektrotechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 77, 2000 – ISBN 3-931466-76-0

Bd. 78 SCHEIDELER, C.: Probabilistic Methods for Coordination Problems. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 78, 2000 – ISBN 3-931466-77-9

Bd. 79 GAUSEMEIER, J.; LINDEMANN, U.; REINHART, G.; WIENDAHL, H.-P.: Kooperatives Produktengineering - Ein neues Selbstverständnis des ingenieurmäßigen Wirkens. HNI-Verlagsschriftenreihe, Paderborn, Band 79, 2000 – ISBN 3-931466-78-7

Bd. 80 GAUSEMEIER, J.; LÜCKEL, J.: Entwicklungsumgebungen Mechatronik - Methoden und Werkzeuge zur Entwicklung mechatronischer Systeme. HNI-Verlagsschriftenreihe, Paderborn, Band 80, 2000 – ISBN 3-931466-79-5

Bd. 81 RIEPING, I.: Communication in Parallel Systems-Models, Algorithms and Implementations. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 81, 2000 – ISBN 3-931466-80-9

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 82 GAUSEMEIER, J; LÜCKEL, J.: Auf dem Weg zu den Produkten für die Märkte von morgen. 4. Internationales Heinz Nixdorf Symposium, HNI-Verlagsschriftenreihe, Paderborn, Band 82, 2000 – ISBN 3-931466-81-7

Bd. 83 DEL CASTILLO, G.: The ASM Workbench - A Tool Environment for Computer-Aided Analysis and Validation of Abstract State Machine Models. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 83, 2000 – ISBN 3-931466-82-5

Bd. 84 SCHÄFERMEIER, U.: Eine Methode zur systemorientierten organisatorischen Gestaltung der Zweckaufgabenverrichtung in kooperativen Verbünden; Klassifikation, Aufgabenzuordnung. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 84, 2000 – ISBN 3-931466-83-3

Bd. 85 KRÜGER, J.: Ganzheitliche Beherrschung von Abläufen in und zwischen soziotechnischen Systemen: Ein Beitrag zur Modellbildung und zum paradigmatischen Verständnis von Industrieunternehmen zur Integration von Mensch und Maschine; Prozess und Struktur. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 85, 2000 – ISBN 3-931466-84-1

Bd. 86 BARTSCHER, T.: Methoden des Integrierten Workflowmanagements (IWFM). Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 86, 2000 – ISBN 3-931466-85-X

Bd. 87 QUINTANILLA, J.: Ein Verifikationsansatz für eine netzbasierte Modellierungsmethode für Fertigungssteuerungssysteme. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 87, 2000 – ISBN 3-931466-86-8

Bd. 88 PREIS, R.: Analyses and Design of Efficient Graph Partitioning Methods. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 88, 2001 – ISBN 3-931466-87-6

Bd. 89 wird noch vergeben!

Bd. 90 WESTERMANN, M.: Caching in Networks: Non-Uniform Algorithms and Memory Capacity Constraints. Dissertation, Fachbereich für Informatik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 90, 2001 – ISBN 3-931466-89-2

Bd. 91 LEMKE, J.: Nutzenorientierte Planung des Einsatzes von CAD- / CAE-Systemen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 91, 2001 – ISBN 3-935433-00-X

Bd. 92 VON BOHUSZEWICZ, O.: Eine Methode zur Visualisierung von Geschäftsprozessen in einer virtuellen Umgebung. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 92, 2001 – ISBN 3-935433-01-8

Bd. 93 BÖRNCHEN, T.: Zur Entwicklung dynamischer Komponenten für variables Kraftfahrzeug-Scheinwerferlicht. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 93, 2001 – ISBN 3-935433-02-6

Bd. 94 WINDELER, I.: Auswahl von Restrukturierungsprojekten in Forschungs- und Entwicklungsorganisationen der Automobilindustrie. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 94, 2001 – ISBN 3-935433-03-4

Bd. 95 WOLFF, C.: Parallele Simulation großer pulscodierter neuronaler Netze. Dissertation, Fachbereich für Elektrotechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 95, 2001 – ISBN 3-935433-04-2

Bd. 96 HENKE, A.: Modellierung, Simulation und Optimierung piezoelektrischer Stellsysteme. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 96, 2001 – ISBN 3-935433-05-0

Bd. 97 RÜCKERT, U.; SITTE, J.; WITKOWSKI, U. (Hrsg.): Autonomous Minirobots for Research and Edutainment AMiRE2001. 5. Internationales Heinz Nixdorf Symposium, HNI-Verlagsschriftenreihe, Paderborn, Band 97, 2001 – ISBN 3-935433-06-9

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 98 LI, P.: Datenkonversion für den Datenaustausch in verteilten Fertigungs-Lenkungssystemen. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 98, 2001 – ISBN 9-935433-07-7

Bd. 99 BRANDT, C.: Eine modellbasierte Methode zum strukturierten Entwurf virtueller Umgebungen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 99, 2001 – ISBN 9-935433-08-5

Bd. 100 WLEKLINSKI, C.: Methode zur Effektivitäts- und Effizienzbewertung der Entwicklung maschinenbaulicher Anlagen. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 100, 2001 – ISBN-3-935433-09-3

Bd. 101 HEMSEL, T.: Untersuchung und Weiterentwicklung linearer piezoelektrischer Schwingungsantriebe. Dissertation, Fachbereich für Maschinentechnik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 101, 2001 – ISBN 3-935433-10-7

Bd. 102 MAUERMANN, H.: Leitfaden zur Erhöhung der Logistikqualität durch Analyse und Neugestaltung der Versorgungsketten. Dissertation, Fachbereich für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 102, 2001 – ISBN 3-935433-11-5

Bd. 103 WAGENBLAßT, D.: Eine Analysemethode zur Beurteilung der Funktionssicherheit von gemischt analog-digitalen Schaltungen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 103, 2002 – ISBN 3-935433-12-3

Bd. 104 PORRMANN, M.: Leistungsbewertung eingebetteter Neurocomputersysteme. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 104, 2002 – ISBN 3-935433-13-1

Bd. 105 SEIFERT, L.: Methodik zum Aufbau von Informationsmodellen für Electronic Business in der Produktentwicklung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 105, 2002 – ISBN 3-935433-14-X

Bd. 106 SOETEBEER, M.: Methode zur Modellierung, Kontrolle und Steuerung von Produktstrategien. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 106, 2002 – ISBN 3-935433-15-8

Bd. 107 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 1. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 107, 2002 – ISBN 3-935433-16-6

Bd. 108 FLATH, M.: Methode zur Konzipierung mechatronischer Produkte. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 108, 2002 – ISBN 3-935433-17-4

Bd. 109 AVENARIUS, J.: Methoden zur Suche und Informationsbereitstellung von Lösungselementen für die Entwicklung mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 109, 2002 – ISBN 3-935433-18-2

Bd. 110 HELMKE, S.: Eine simulationsgegestützte Methode für Budgetentscheidungen im Kundenbindungsmanagement. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 110, 2002 – ISBN 3-935433-19-0

Bd. 111 CZUBAYKO, R.: Rechnerinterne Repräsentation von informationsverarbeitenden Lösungselementen für die verteilte kooperative Produktentwicklung in der Mechatronik. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 111, 2002 – ISBN 3-935433-20-4

Bd. 112 GOLDSCHMIDT, S.: Anwendung mengenorientierter numerischer Methoden zur Analyse nichtlinearer dynamischer Systeme am Beispiel der Spurführungsdynamik von Schienenfahrzeugen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 112, 2002 – ISBN 3-935433-21-2

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 113 LEHMANN, T.: Towards Device Driver Synthesis. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 113, 2002 – ISBN 3-935433-22-0

Bd. 114 HÄRTEL, W.: Issueorientierte Frühaufklärung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 114, 2002 – ISBN 3-935433-23-9

Bd. 115 ZIEGLER, M.: Zur Berechenbarkeit reeller geometrischer Probleme. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 115, 2002 – ISBN 3-935433-24-7

Bd. 116 SCHMIDT, M.: Neuronale Assoziativspeicher im Information Retrieval. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 116, 2003 – ISBN 3-935433-25-5

Bd. 117 EL-KEBBE, D. A.: Towards the MaSHReC Manufacturing System under Real-Time Constraints. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 117, 2003 – ISBN 3-935433-26-3

Bd. 118 PUSCH, R.: Personalplanung und -entwicklung in einem integrierten Vorgehensmodell zur Einführung von PDM-Systemen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 118, 2003 – ISBN 3-935433-27-1

Bd. 119 SOHLER, C.: Property Testing and Geometry. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 119, 2003 – ISBN 3-935433-28-X

Bd. 120 KESPOHL, H.: Dynamisches Matching – Ein agentenbasiertes Verfahren zur Unterstützung des Kooperativen Produktengineering durch Wissens- und Technologietransfer. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 120, 2003 – ISBN 3-935433-29-8

Bd. 121 MOLT, T.: Eine domänenübergreifende Softwarespezifikationstechnik für automatisierte Fertigungsanlagen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 121, 2003 – ISBN 3-935433-30-1

Bd. 122 GAUSEMEIER, J.; LÜCKEL, J.; WALLASCHEK, J. (Hrsg.): 1. Paderborner Workshop Intelligente mechatronische Systeme. HNI-Verlagsschriftenreihe, Paderborn, Band 122, 2003 – ISBN 3-935433-31-X

Bd. 123 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 2. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 123, 2003 – ISBN 3-935433-32-8

Bd. 124 LITTMANN, W.: Piezoelektrische resonant betriebene Ultraschall-Leistungswandler mit nichtlinearen mechanischen Randbedingungen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 124, 2003 – ISBN 3-935433-33-6

Bd. 125 WICKORD, W.: Zur Anwendung probabilistischer Methoden in den frühen Phasen des Systementwurfs. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 125, 2003 – ISBN 3-935433-34-4

Bd. 126 HEITTMANN, A.: Ressourceneffiziente Architekturen neuronaler Assoziativspeicher. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 126, 2003 – ISBN 3-935433-35-2

Bd. 127 WITKOWSKI, U.: Einbettung selbstorganisierender Karten in autonome Miniroboter. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 127, 2003 – ISBN 3-935433-36-0

Bd. 128 BOBDA, C.: Synthesis of Dataflow Graphs for Reconfigurable Systems using Temporal Partitioning and Temporal Placement. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 128, 2003 – ISBN 3-935433-37-9

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 129 HELLER, F.: Wissensbasiertes Online-Störungsmanagement flexibler, hoch automatisierter Montagesysteme. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 129, 2003 – ISBN 3-935433-38-7

Bd. 130 KÜHN, A.: Systematik des Ideenmanagements im Produktentstehungsprozess. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 130, 2003 – ISBN 3-935433-39-5

Bd. 131 KEIL-SLAWIK, R.; BRENNECKE, A.; HOHENHAUS, M.: ISIS -Installationshandbuch für lernförderliche Infrastrukturen. HNI-Verlagsschriftenreihe, Paderborn, Band 131, 2003 – ISBN 3-935433-40-9

Bd. 132 OULD HAMADY, M.: Ein Ansatz zur Gestaltung des operativen Fertigungsmanagements innerhalb der Lieferkette. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 132, 2003 – ISBN 3-935433-41-7

Bd. 133 HOLTZ, C.: Theoretical Analysis of Unsupervised On-line Learning through Soft Competition. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 133, 2003 – ISBN 3-935433-42-5

Bd. 134 UEBEL, M.: Ein Modell zur Steuerung der Kundenbearbeitung im Rahmen des Vertriebsmanagements. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 134, 2003 – ISBN 3-935433-43-3

Bd. 135 BRINKMANN, A.: Verteilte Algorithmen zur Datenplazierung und zum Routing in gegnerischen Netzwerken. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 135, 2003 – ISBN 3-935433-44-1

Bd. 136 FRÜND, E.: Aktive Kompensation von periodischen Schwingungen an rotierenden Walzen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 136, 2003 – ISBN 3-935433-45-X

Bd. 137 KEIL-SLAWIK, R. (Hrsg.): Digitale Medien in der Hochschule: Infrastrukturen im Wandel. HNI-Verlagsschriftenreihe, Paderborn, Band 137, 2004 – ISBN 3-935433-46-8

Bd. 138 STORCK, H.: Optimierung der Kontaktvorgänge bei Wanderwellenmotoren. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 138, 2004 – ISBN 3-935433-47-6

Bd. 139 KALTE, H.: Einbettung dynamisch rekonfigurierbarer Hardwarearchitekturen in eine Universalprozessorumgebung. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 139, 2004 – ISBN 3-935433-48-4

Bd. 140 ISKE, B.: Modellierung und effiziente Nutzung aktiver Infrarotsensorik in autonomen Systemen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 140, 2004 – ISBN 3-935433-49-2

Bd. 141 BÄTZEL, D.: Methode zur Ermittlung und Bewertung von Strategiealternativen im Kontext Fertigungstechnik. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 141, 2004 – ISBN 3-935433-50-6

Bd. 142 BÖKE, C.: Automatic Configuration of Real-Time Operating Systems and Real-Time Communication Systems for Distributed Embedded Applications. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 142, 2004 – ISBN 3-935433-51-4

Bd. 143 KÖCKERLING, M.: Methodische Entwicklung und Optimierung der Wirkstruktur mechatronischer Produkte. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 143, 2004 – ISBN 3-935433-52-2

Bd. 144 HENZLER, S: Methodik zur Konzeption der Struktur und der Regelung leistungsverzweigter Getriebe mit Toroidvariator. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 144, 2004 – ISBN 3-935433-53-0

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 145 GAUSEMEIER, J.; LÜCKEL, J.; WALLASCHEK, J. (Hrsg.): 2. Paderborner Workshop Intelligente mechatronische Systeme. HNI-Verlagsschriftenreihe, Paderborn, Band 145, 2004 – ISBN 3-935433-54-9

Bd. 146 LESSING, H.: Prozess zur multivariaten Prognose von Produktionsprogrammen für eine effiziente Kapazitätsplanung bei typisierten Dienstleistungen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 146, 2004 – ISBN 3-935433-55-7

Bd. 147 HAMOUDIA, H.: Planerische Ablaufgestaltung bei prozessorientierten Dienstleistungen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 147, 2004 – ISBN 3-935433-56-5

Bd. 148 BUSCH, A.: Kollaborative Änderungsplanung in Unternehmensnetzwerken der Serienfertigung – ein verhandlungsbasierter Ansatz zur interorganisationalen Koordination bei Störungen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 148, 2004 – ISBN 3-935433-57-3

Bd. 149 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 3. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 149, 2004 – ISBN 3-935433-58-1

Bd.150 MEYER, B.: Value-Adding Logistics for a World Assembly Line. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 150, 2004 – ISBN 3-935433-59-X

Bd. 151 GRIENITZ, V.: Methodik zur Erstellung von Technologieszenarien für die strategische Technologieplanung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 151, 2004 – ISBN 3-9354 33-60-3

Bd. 152 FRANKE, H.: Eine Methode zur unternehmensübergreifenden Transportdisposition durch synchron und asynchron kommunizierende Agenten. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 152, 2004 – ISBN 3-935433-61-1

Bd. 153 SALZWEDEL, K. A.: Data Distribution Algorithms for Storage Networks. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 153, 2004 – ISBN 3-935433-62-X

Bd. 154 RÄCKE, H.: Data Management and Routing in General Networks. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 154, 2004 – ISBN 3-935433-63-8

Bd. 155 FRANK, U.; GIESE, H.; KLEIN, F.; OBERSCHELP, O.; SCHMIDT, A.; SCHULZ, B.; VÖCKING, H.; WITTING, K.; GAUSEMEIER, J. (Hrsg.): Selbstoptimierende Systeme des Maschinenbaus – Definitionen und Konzepte. HNI-Verlagsschriftenreihe, Paderborn, Band 155, 2004 – ISBN 3-935433-64-6

Bd. 156 MÖHRINGER, S.: Entwicklungsmethodik für mechatronische Systeme. Habilitation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 156, 2004 – ISBN 3-935433-65-4

Bd. 157 FAHRENTHOLZ, M.: Konzeption eines Betriebskonzepts für ein bedarfsgesteuertes schienengebundenes Shuttle-System. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 157, 2004 – ISBN 3-935433-66-2

Bd. 158 GAJEWSKI, T.: Referenzmodell zur Beschreibung der Geschäftsprozesse von After-Sales-Dienstleistungen unter besonderer Berücksichtigung des Mobile Business. Dissertation Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 158, 2004 – ISBN 3-935433-67-0

Bd. 159 RÜTHER, M.: Ein Beitrag zur klassifizierenden Modularisierung von Verfahren für die Produktionsplanung. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 159, 2004 – ISBN 3-935433-68-9

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 160 MUECK, B.: Eine Methode zur benutzerstimulierten detaillierungsvarianten Berechnung von diskreten Simulationen von Materialflüssen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 160, 2004 – ISBN 3-935433-69-7

Bd. 161 LANGEN, D.: Abschätzung des Ressourcenbedarfs von hochintegrierten mikroelektronischen Systemen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 161, 2005 – ISBN 3-935433-70-0

Bd. 162 ORLIK, L.: Wissensbasierte Entscheidungshilfe für die strategische Produktplanung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 162, 2005 – ISBN 3-935433-71-9

Bd. 163 GAUSEMEIER, J.; RAMMIG, F.; SCHÄFER, W.; WALLASCHEK, J. (Hrsg.): 3. Paderborner Workshop Intelligente mechatronische Systeme. HNI-Verlagsschriftenreihe, Paderborn, Band 163, 2005 – ISBN 3-935433-72-7

Bd. 164 FISCHER, M.: Design, Analysis, and Evaluation of a Data Structure for Distributed Virtual Environments. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 164, 2005 – ISBN 3-935433-73-5

Bd. 165 MATYSCZOK, C.: Dynamische Kantenextraktion - Ein Verfahren zur Generierung von Tracking-Informationen für Augmented Reality-Anwendungen auf Basis von 3D-Referenzmodellen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 165, 2005 – ISBN 3-935433-74-3

Bd. 166 JANIA, T.: Änderungsmanagement auf Basis eines integrierten Prozess- und Produktdatenmodells mit dem Ziel einer durchgängigen Komplexitätsbewertung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 166, 2005 – ISBN 3-935433-75-1

Bd. 167 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 4. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 167, 2005 – ISBN 3-935433-76-X

Bd. 168 VOLBERT, K.: Geometric Spanners for Topology Control in Wireless Networks. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 168, 2005 – ISBN 3-935433-77-8

Bd. 169 ROSLAK, J.: Entwicklung eines aktiven Scheinwerfersystems zur blendungsfreien Ausleuchtung des Verkehrsraumes. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 167, 2005 – ISBN 3-935433-78-6

Bd. 170 EMMRICH, A.: Ein Beitrag zur systematischen Entwicklung produktorientierter Dienstleistungen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 170, 2005 – ISBN 3-935433-79-4

Bd. 171 NOWACZYK, O.: Explorationen: Ein Ansatz zur Entwicklung hochgradig interaktiver Lernbausteine. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 171, 2005 – ISBN 3-935433-80-8

Bd. 172 MAHMOUD, K.: Theoretical and experimental investigations on a new adaptive duo servo drum brake with high and constant brake shoe factor. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 172, 2005 – ISBN 3-935433-81-6

Bd. 173 KLIEWER, G.: Optimierung in der Flugplanung: Netzwerkentwurf und Flottenzuweisung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 173, 2005 – ISBN 3-935433-82-4

Bd. 174 BALÁŽOVÁ, M.: Methode zur Leistungsbewertung und Leistungssteigerung der Mechatronikentwicklung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 174, 2005 – ISBN 3-935433-83-2

Bd. 175 FRANK, U.: Spezifikationstechnik zur Beschreibung der Prinziplösung selbstoptimierender Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 175, 2005 – ISBN 3-935433-84-0

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 176 BERGER, T.: Methode zur Entwicklung und Bewertung innovativer Technologiestrategien. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 176, 2005 – ISBN 3-935433-85-9

Bd. 177 BERSSENBRÜGGE, J.: Virtual Nightdrive - Ein Verfahren zur Darstellung der komplexen Lichtverteilungen moderner Scheinwerfersysteme im Rahmen einer virtuellen Nachtfahrt. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 177, 2005 – ISBN 3-935433-86-7

Bd. 178 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 1. Symposium für Vorausschau und Technologieplanung Heinz Nixdorf Institut, 3. und 4. November 2005, Schloß Neuhardenberg, HNI-Verlagsschriftenreihe, Paderborn, Band 178, 2005 – ISBN 3-935433-87-5

Bd. 179 FU, B.: Piezoelectric actuator design via multiobjective optimization methods. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 179, 2005 – ISBN 3-935433-88-3

Bd. 180 WALLASCHEK, J.; HEMSEL, T.; MRACEK, M.: Proceedings of the 2nd International Workshop on Piezoelectric Materials and Applications in Actuators. HNI-Verlagsschriftenreihe, Paderborn, Band 180, 2005 – ISBN 3-935433-89-1

Bd. 181 MEYER AUF DER HEIDE, F.; MONIEN, B. (Hrsg.): New Trends in Parallel & Distributed Computing. 6. Internationales Heinz Nixdorf Symposium, 17. und 18. Januar 2006, HNI-Verlagsschriftenreihe, Paderborn, Band 181, 2006 – ISBN 3-939350-00-1

Bd. 182 HEIDENREICH, J.: Adaptierbare Änderungsplanung der Mengen und Kapazitäten in Produktionsnetzwerken der Serienfertigung. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 182, 2006 – ISBN 3-939350-01-X

Bd. 183 PAPE, U.: Umsetzung eines SCM-Konzeptes zum Liefermanagement in Liefernetzwerken der Serienfertigung. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 183, 2006 – ISBN 3-939350-02-8

Bd. 184 BINGER, V.: Konzeption eines wissensbasierten Instruments für die strategische Vorausschau im Kontext der Szenariotechnik. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 184, 2006 – ISBN 3-939350-03-6

Bd. 185 KRIESEL, C.: Szenarioorientierte Unternehmensstrukturoptimierung – Strategische Standort- und Produktionsplanung. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 185, 2006 – ISBN 3-939350-04-4

Bd. 186 KLEIN, J.: Efficient collision detection for point and polygon based models. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 186, 2006 – ISBN 3-939350-05-2

Bd. 187 WORTMANN, R.: Methodische Entwicklung von Echtzeit 3D-Anwendungen für Schulung und Präsentation. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 187, 2006 – ISBN 3-939350-06-0

Bd. 188 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 5. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 188, 2006 – ISBN 3-939350-07-9

Bd. 189 GAUSEMEIER, J.; RAMMIG, F.; SCHÄFER, W.; TRÄCHTLER, A.; WALLASCHEK, J. (Hrsg.): 4. Paderborner Workshop Entwurf mechatronischer Systeme. HNI-Verlagsschriftenreihe, Paderborn, Band 189, 2006 – ISBN 3-939350-08-7

Bd. 190 DAMEROW, V.: Average and Smoothed Complexity of Geometric Structures. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 190, 2006 – ISBN 3-939350-09-5

Bd. 191 GIESE, H.; NIGGEMANN, O. (Hrsg.): Postworkshop Proceedings of the 3rd Workshop on Object-oriented Modeling of Embedded Real-Time Systems (OMER 3), HNI-Verlagsschriftenreihe, Paderborn, Band 191, 2006 – ISBN 3-939350-10-9

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 192 RADKOWSKI, R.: Anwendung evolutionärer Algorithmen zur Unterstützung des Entwurfs selbstoptimierender Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 192, 2006 – ISBN 3-939350-11-7

Bd. 193 SHEN, Q.: A Method for Composing Virtual Prototypes of Mechatronic Systems in Virtual Environments. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 193, 2006 – ISBN 3-939350-12-5

Bd. 194 REDENIUS, A.: Verfahren zur Planung von Entwicklungsprozessen für fortgeschrittene mechatronische Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 194, 2006 – ISBN 3-939350-13-3

Bd. 195 KUHL, P.: Anpassung der Lichtverteilung des Abblendlichtes an den vertikalen Straßenverlauf. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 195, 2006 – ISBN 3-939350-14-1

Bd. 196 MICHELS, J. S.: Integrative Spezifikation von Produkt- und Produktionssystemkonzeptionen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 196, 2006 – ISBN 3-939350-15-X

Bd. 197 RIPS, S.: Adaptive Steuerung der Lastverteilung datenparalleler Anwendungen in Grid-Umgebungen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 197, 2006 – ISBN 3-939350-16-8

Bd. 198 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 2. Symposium für Vorausschau und Technologieplanung Heinz Nixdorf Institut, 9. und 10. November 2006, Schloß Neuhardenberg, HNI-Verlagsschriftenreihe, Paderborn, Band 198, 2006 – ISBN 3-939350-17-6

Bd. 199 FRANKE, W.: Wiederverwendungsorientierte Herleitung von Inter-Fachkomponentenkonzepten für Lagerverwaltungssoftwaresysteme. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 199, 2006 – ISBN 978-3-939350-18-7

Bd. 200 SCHEIDELER, P.: Ein Beitrag zur erfahrungsbasierten Selbstoptimierung einer Menge technisch homogener fahrerloser Fahrzeuge. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 200, 2006 – ISBN 978-3-939350-19-4

Bd. 201 KÖSTERS, C.: Ein ontologiebasiertes Modell zur Beschreibung der Abläufe in einem Produktionssystem unter besonderer Berücksichtigung einer diskreten Produktion. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 201, 2006 – ISBN 978-3-939350-20-0

Bd. 202 HALFMEIER, S.: Modellierung und Regelung von Halbtoroidvariationen in leistungsverzweigten Getriebestrukturen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 202, 2006 – ISBN 978-3-939350-21-7

Bd. 203 RÜHRUP, S.: Position-based Routing Strategies. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 203, 2006 – ISBN 978-3-939350-22-4

Bd. 204 SCHMIDT, A.: Wirkmuster zur Selbstoptimierung – Konstrukte für den Entwurf selbstoptimierender Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 204, 2006 – ISBN 978-3-939350-23-1

Bd. 205 IHMOR, S.: Modeling and Automated Synthesis of Reconfigurable Interfaces. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 205, 2006 – ISBN 978-3-939350-24-8

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 206 ECKES, R.: Augmented Reality – basiertes Verfahren zur Unterstützung des Anlaufprozesses von automatisierten Fertigungssystemen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 206, 2007 – ISBN 978-3-939350-25-5

Bd. 207 STEFFEN, D.: Ein Verfahren zur Produktstrukturierung für fortgeschrittene mechatronische Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 207, 2007 – ISBN 978-3-939350-26-2

Bd. 208 LAROQUE, C.: Ein mehrbenutzerfähiges Werkzeug zur Modellierung und richtungsoffenen Simulation von wahlweise objekt- und funktionsorientiert gegliederten Fertigungssystemen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 208, 2007 – ISBN 978-3-939350-27-9

Bd. 209 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 6. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 209, 2007 – ISBN 978-3-939350-28-6

Bd. 210 GAUSEMEIER, J.; RAMMIG, F.; SCHÄFER, W.; TRÄCHTLER, A.; WALLASCHEK, J. (Hrsg.): 5. Paderborner Workshop Entwurf mechatronischer Systeme. HNI-Verlagsschriftenreihe, Paderborn, Band 210, 2007 – ISBN 978-3-939350-29-3

Bd. 211 KAUSCHKE, R.: Systematik zur lichttechnischen Gestaltung von aktiven Scheinwerfern. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 211, 2007 – ISBN 978-3-939350-30-9

Bd. 212 DU, J.: Zellen-basierte Dienst-Entdeckung für Roboternetzwerke. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 212, 2007 – ISBN 978-3-939350-31-6

Bd. 213 DANNE, K.: Real-Time Multitasking in Embedded Systems Based on Reconfigurable Hardware. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 213, 2007 – ISBN 978-3-939350-32-3

Bd. 214 EICKHOFF, R.: Fehlertolerante neuronale Netze zur Approximation von Funktionen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 214, 2007 – ISBN 978-3-939350-33-0

Bd. 215 KÖSTER, M.: Analyse und Entwurf von Methoden zur Ressourcenverwaltung partiell rekonfigurierbarer Architekturen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 215, 2007 – ISBN 978-3-939350-34-7

Bd. 216 RÜCKERT, U.; SITTE, J.; WITKOWSKI, U.: Proceedings of the 4th International Symposium on Autonomous Minirobots for Research and Edutainment – AMiRE2007. Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 216, 2007 – ISBN 978-3-939350-35-4

Bd. 217 PHAM VAN, T.: Proactive Ad Hoc Devices for Relaying Real-Time Video Packets. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 217, 2007 – ISBN 978-3-939350-36-1

Bd. 218 VIENENKÖTTER, A.: Methodik zur Entwicklung von Innovations- und Technologie-Roadmaps. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 218, 2007 – ISBN 978-3-939350-37-8

Bd. 219 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 3. Symposium für Vorausschau und Technologieplanung Heinz Nixdorf Institut, 29. und 30. November 2007, Miele & Cie. KG Gütersloh, HNI-Verlagsschriftenreihe, Paderborn, Band 219, 2007 – ISBN 978-3-939350-38-5

Bd. 220 FRÜND, J.: Eine Architekurkonzeption für eine skalierbare mobile Augmented Reality Anwendung für die Produktpräsentation. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 220, 2007 – ISBN 978-3-939350-39-2

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 221 PEITZ, T.: Methodik zur Produktoptimierung mechanisch elektronischer Baugruppen durch die Technologie MID (Molded Interconnect Devices). Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 221, 2007 – ISBN 978-3-939350-40-8

Bd. 222 MEYER AUF DER HEIDE, F. (Hrsg.): The European Integrated Project "Dynamically Evolving, Large Scale Information Systems (DELIS)", Proceedings of the Final Workshop, Barcelona, February 27-28, 2008, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 222, 2008 – ISBN 978-3-939350-41-5

Bd. 223 GAUSEMEIER, J.; RAMMIG, F.; SCHÄFER, W. (Hrsg.): Self-optimizing Mechatronic Systems: Design the Future. 7. Internationales Heinz Nixdorf Symposium, 20. und 21. Februar 2008, HNI-Verlagsschriftenreihe, Paderborn, Band 223, 2008 – ISBN 978-3-939350-42-2

Bd. 224 RATH, M.: Methode zur Entwicklung hybrider Technologie- und Innovationsstrategien – am Beispiel des Automobils. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 224, 2008 – ISBN 978-3-939350-43-9

Bd. 225 GRÜNEWALD, M.: Protokollverarbeitung mit integrierten Multiprozessoren in drahtlosen Ad-hoc-Netzwerken. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 225, 2008 – ISBN 978-3-939350-44-6

Bd. 226 STRAUSS, S.: Theoretische und experimentelle Untersuchungen zum Einsatz gepulster Halbleiterlichtquellen in der Kraftfahrzeugbeleuchtung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 226, 2008 – ISBN 978-3-939350-45-3

Bd. 227 ZEIDLER, C.: Systematik der Materialflussplanung in der frühen Phase der Produktionssystementwicklung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 227, 2008 – ISBN 978-3-939350-46-0

Bd. 228 PARISI, S.: A Method for the intelligent Authoring of 3D Animations for Training and Maintenance. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 228, 2008 – ISBN 978-3-939350-47-7

Bd. 229 DITTMANN, F.: Methods to Exploit Reconfigurable Fabrics. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 229, 2008 – ISBN 978-3-939350-48-4

Bd. 230 TONIGOLD, C.: Programm-, Ressourcen- und Prozessoptimierung als Bestandteile der Anpassungsplanung von spanenden Fertigungssystemen in der Fließfertigung von Aggregaten. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 230, 2008– ISBN 978-3-939350-49-1

Bd. 231 BRANDT, T.: A Predictive Potential Field Concept for Shared Vehicle Guidance. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 231, 2008 – ISBN 978-3-939350-50-7

Bd. 232 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 7. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 232, 2008 – ISBN 978-3-939350-51-4

Bd. 233 CHANG, H.: A Methodology for the Identification of Technology Indicators. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 233, 2008 – ISBN 978-3-939350-52-1

Bd. 234 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.; TSCHEUSCHNER, T.; VÖCKING, H.; WITKOWSKI, U.; WITTING, K.; ZNAMENSHCHYKOV, O.: Selbstoptimierende Systeme des Maschinenbaus – Definitionen, Anwendungen, Konzepte. HNI-Verlagsschriftenreihe, Paderborn, Band 234, 2009 – ISBN 978-3-939350-53-8

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 235 DELL'AERE, A.; HIRSCH, M.; KLÖPPER, B.; KOESTER, M.; KRÜGER, M.; KRUPP, A.; MÜLLER, T.; OBERTHÜR, S.; POOK, S.; PRIESTERJAHN, C.; ROMAUS, C.; SCHMIDT, A.; SONDERMANN-WÖLKE, C.; TICHY, M.; VÖCKING, H.; ZIMMER, D.: Verlässlichkeit selbstoptimierender Systeme – Potenziale nutzen und Risiken vermeiden. HNI-Verlagsschriftenreihe, Paderborn, Band 235, 2009 – ISBN 978-3-939350-54-5

Bd. 236 GEHRKE, M.; GIESE, H.; STROOP J.: Proceedings of the 4th Workshop on Object-oriented Modeling of Embedded Real-Time Systems (OMER4), Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 236, 2008 – ISBN 978-3-939350-55-2

Bd. 237 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 4. Symposium für Vorausschau und Technologieplanung Heinz Nixdorf Institut, 30. und 31. Oktober 2008, Brandenburgische Akademie der Wissenschaften, Berlin, HNI-Verlagsschriftenreihe, Paderborn, Band 237, 2008 – ISBN 978-3-939350-56-9

Bd. 238 BRÖKELMANN, M.: Entwicklung einer Methodik zur Online-Qualitätsüberwachung des Ultraschall-Drahtbondprozesses mittels integrierter Mikrosensorik. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 238, 2008 – ISBN 978-3-939350-57-6

Bd. 239 KETTELHOIT, B.: Architektur und Entwurf dynamisch rekonfigurierbarer FPGA-Systeme. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 239, 2008 – ISBN 978-3-939350-58-3

Bd. 240 ZAMBALDI, M.: Concepts for the development of a generic Multi-Level Test Bench covering different areas of applications. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 240, 2008 – ISBN 978-3-939350-59-0

Bd. 241 OBERSCHELP, O.: Strukturierter Entwurf selbstoptimierender mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 241, 2009 – ISBN 978-3-939350-60-6

Bd. 242 STOLLT, G.: Verfahren zur strukturierten Vorausschau in globalen Umfeldern produzierender Unternehmen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 242, 2009 – ISBN 978-3-939350-61-3

Bd. 243 WENZELMANN, C.: Methode zur zukunftsorientierten Entwicklung und Umsetzung von Strategieoptionen unter Berücksichtigung des antizipierten Wettbewerbsverhaltens. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 243, 2009 – ISBN 978-3-939350-62-0

Bd. 244 BRÜSEKE, U.: Einsatz der Bibliometrie für das Technologiemanagement. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 244, 2009 – ISBN 978-3-939350-63-7

Bd. 245 TIMM, T.: Ein Verfahren zur hierarchischen Struktur-, Dimensions- und Materialbedarfsplanung von Fertigungssystemen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 245, 2009 – ISBN 978-3-939350-64-4

Bd. 246 GRIESE, B.: Adaptive Echtzeitkommunikationsnetze. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 246, 2009 – ISBN 978-3-939350-65-1

Bd. 247 NIEMANN, J.-C.: Ressourceneffiziente Schaltungstechnik eingebetteter Parallelrechner. Dissertation, Fakultät für Elek - trotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 247, 2009 – ISBN 978-3-939350-66-8

Bd. 248 KAISER, I.: Systematik zur Entwicklung mechatronischer Systeme in der Technologie MID. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 248, 2009 – ISBN 978-3-939350-67-5

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Bände der HNI-Verlagsschriftenreihe

Bd. 249 GANS, J. E.: Neu- und Anpassungsplanung der Struktur von getakteten Fließproduktionssystemen für variantenreiche Serienprodukte in der Montage. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 249, 2009 – ISBN 978-3-939350-68-2

Bd. 250 GAUSEMEIER, J.; RAMMIG, F.; SCHÄFER, W.; TRÄCHTLER, A. (Hrsg.): 6. Paderborner Workshop Entwurf mechatronischer Systeme. HNI-Verlagsschriftenreihe, Paderborn, Band 250, 2009 – ISBN 978-3-939350-69-9

Bd. 251 LESSMANN, J.: Protocols for Telephone Communications in Wireless Multi-Hop Ad Hoc Networks. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 251, 2009 – ISBN 978-3-939350-70-5

Bd. 252 GAUSEMEIER, J.; GRAFE, M. (Hrsg.): 8. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Paderborn, Band 252, 2009 – ISBN 978-3-939350-71-2

Bd. 253 KLÖPPER, B.: Ein Beitrag zur Verhaltensplanung für interagierende intelligente mechatronische Systeme in nicht-deterministischen Umgebungen. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 253, 2009 – ISBN 978-3-939350-72-9

Bd. 254 LOW, C. Y.: A Methodology to Manage the Transition from the Principle Solution towards the Controller Design of Advanced Mechatronic Systems. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 254, 2009 – ISBN 978-3-939350-73-6

Bd. 255 XU, F.: Resource-Efficient Multi-Antenna Designs for Mobile Ad Hoc Networks. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Paderborn, Band 255, 2009 – ISBN 978-3-939350-74-3

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn