Domänenübergreifende Zuverlässigkeitsbewertung in frühen Entwicklungsphasen unter Berücksichtigung von Wechselwirkungen

Dipl.-Ing. Michael Wedel, Prof. Dr.-Ing. Dr. h. c. Peter Göhner
Institut für Automatisierungs- und Softwaretechnik
Pfaffenwaldring 47, 70550 Stuttgart
Tel.: (0711) 685 - 67301
{michael.wedel, peter.goehner}@ias.uni-stuttgart.de

Dipl.-Ing. Jochen Gäng, Prof. Dr.-Ing. Bernd Bertsche
Institut für Maschinenelemente
Pfaffenwaldring 9, 70550 Stuttgart
Tel.: (0711) 685 - 66170
{jochen.gaeng, bernd.bertsche}@ima.uni-stuttgart.de

Dipl.-Ing. Talal Arnaout, Prof. Dr. rer. nat. Hans-Joachim Wunderlich
Institut für Technische Informatik
Pfaffenwaldring 47, 70550 Stuttgart
Tel.: (0711) 7816 - 362
{talal.arnaout, wu}@informatik.uni-stuttgart.de

Zusammenfassung

Aufgrund der unvollständigen Informationen über ein mechatronisches System stellt die frühe Zuverlässigkeitsbewertung eine große Herausforderung dar. Um die jeweiligen Vorteile zu nutzen, wurden klassische Ansätze in den einzelnen Domänen kombiniert und in eine ganzheitliche Methode zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen integriert. In Zusammenarbeit verschiedener Ingenieurdisziplinen wurde die ganzheitliche Methode um die rechnergestützte Ermittlung von Fehlerzusammenhängen im Rahmen einer Risikoabschätzung und verschiedene qualitative Modellierungs- und Analyseansätze erweitert. Für die systematische Analyse des wechselseitigen Einflusses der beteiligten Domänen und die Integration in die Zuverlässigkeitsbewertung wurden Wechselwirkungen zwischen den Domänen untersucht und klassifiziert.

Schlüsselwörter

Zuverlässigkeitsbewertung mechatronischer Systeme, frühe Entwicklungsphasen, domänenübergreifende Wechselwirkungen, quantitative und qualitative Methoden

1 Einleitung

Moderne mechatronische Systeme ermöglichen eine Vielzahl neuartiger Funktionen durch die Kombination mechanischer und elektronischer Bauelemente sowie von Softwaremodulen. Für den Kunden ist jedoch nicht nur die Funktionalität eines Produkts sondern auch dessen Zuverlässigkeit maßgebend für seine Kaufentscheidung. Je früher Probleme mit der Zuverlässigkeit eines Produkts entdeckt werden, umso einfacher können sie behoben werden. Aus diesem Grund wurden domänenspezifische Methoden für frühe Entwicklungsphasen entwickelt, in denen noch kein Produkt als Untersuchungsgegenstand vorliegt. Viele der bisherigen Methoden decken hauptsächlich nur jeweils eine der Domänen Mechanik, Elektronik oder Software ab und sind daher ungeeignet für eine ganzheitliche Bewertung mechatronischer Systeme. Entsprechend werden in Kapitel 2 zunächst Methoden zur Zuverlässigkeitsbewertung in den einzelnen Fachdisziplinen vorgestellt, welche sich auch in frühen Entwicklungsphasen einsetzen lassen. Eine ganzheitliche Zuverlässigkeitsbewertung auf Grundlage dieser Methoden wird in Kapitel 3 erläutert. Für die systematische Berücksichtigung von Wechselwirkungen zwischen Teilsystemen wird in Kapitel 4 ein Modell der Wechselwirkungen in mechatronischen Systemen aufgestellt und in die Zuverlässigkeitsbewertung integriert. Kapitel 5 gibt schließlich eine Zusammenfassung und einen Ausblick auf weitere Arbeiten.

2 Methoden der Zuverlässigkeitsbewertung

Jede Ingenieurdisziplin verfügt über spezielle Methoden der Zuverlässigkeitsbewertung, welche den unterschiedlichen Fehlermechanismen in den einzelnen Domänen Rechnung tragen. Im Folgenden wird vorgestellt, welche Methoden zur Zuverlässigkeitsbewertung bekannt sind und welche neuen Methoden aufgrund der Randbedingungen in frühen Entwicklungsphasen bereits entwickelt wurden. Da zu Beginn der Entwicklung noch kein zu analysierendes System und nur wenige Informationen vorliegen, stellt die Übertragbarkeit vorliegender empirischer Zuverlässigkeitsdaten über Vorgängersysteme eine wichtige Fragestellung dar.

2.1 Mechanik

Die Vorgehensweise der Zuverlässigkeitsbewertung bei mechanischen Systemen ist nach [VDA00b] in mehrere Schritte aufgeteilt. Voraussetzung für die Durchführung sind Informationen über das System, etwa in Form von Stücklisten, Lastenheften oder Zeichnungen. Durch eine Systemanalyse werden sämtliche Elemente des Systems und deren Systemfunktionen ermittelt. Im Funktionsblockdiagramm werden Verbindungsarten, wie z. B. Welle-Naben-Verbindung

und Wechselwirkungen zwischen den Elementen dargestellt. Bei der anschließenden qualitativen Analyse werden vor allem die Failure Mode and Effects Analysis (FMEA) und die Fault Tree Analysis (FTA) eingesetzt. Ziel ist es, Kenntnisse über die kritischen Systemelemente zu erhalten (Abbildung 1).

Für kritische Systemelemente wird zudem eine quantitative Analyse angeschlossen, sofern ausreichende Informationen vorliegen. Für die Berechnung der Zuverlässigkeit müssen jeweils Belastungen und Belastbarkeit bekannt sein [BL04]. Die Belastbarkeit eines mechanischen Systemelements lässt sich beispielsweise über Tests oder Feldrückläufer ermitteln. Eine weitere Möglichkeit ist die Kenntnis von Weibullfaktoren, wie z. B. die Ausfall-Steilheit *b*. Nach der Ermittlung der Zuverlässigkeit einzelner Systemelemente erfolgt die Berechnung der Systemzuverlässigkeit aus der Kombination der einzelnen Elemente etwa mithilfe der Booleschen Algebra.

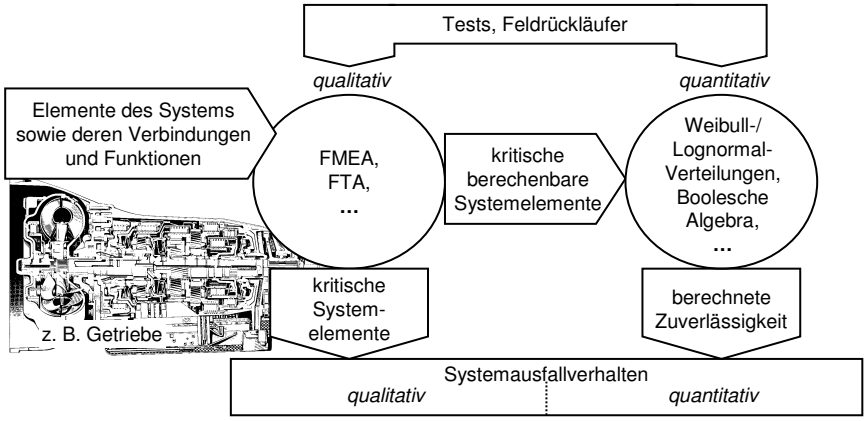

Abbildung 1: Zuverlässigkeitsbewertung mechanischer Systeme

In frühen Entwicklungsphasen ist die Belastbarkeit eines Systemelements oftmals nicht bestimmbar, da noch nicht alle Elemente im Detail bekannt sind oder beispielsweise deren Dimensionierung noch nicht erfolgt ist. Mittels Expertenwissen können jedoch Größen wie Dimensionierungen oder Fertigungsqualitäten unscharf bestimmt werden. Nach [GJB+06] ist es z. B. bei einem Getriebe möglich, aufgrund der vorhandenen Bauraumrestriktion, der auftretenden Belastung und eines entsprechenden Berechnungsmodells (z. B. DIN 3990) trotz Unsicherheiten bei den eingehenden Größen Zuverlässigkeitsaussagen zu machen. Die Informationen über ein einzelnes mögliches Lösungskonzept sind für die Ermittlung eines absoluten Zuverlässigkeitswerts zwar nicht ausreichend. Durch eine Gegenüberstellung unterschiedlicher Lösungskonzepte kann das voraussichtlich zuverlässigste aber aufgezeigt werden.

2.2 Elektronik

Die Zuverlässigkeit mikroelektronischer Systeme wird erst spät im Entwicklungsprozess ermittelt. Um die Fehlerrate zu evaluieren, wird der Fehlerprozess beschleunigt, indem produzierte Schaltungen extremen Bedingungen ausgesetzt werden. Beim „Burn In“ werden Schaltungen beispielsweise hohen Temperaturen und Spannungen ausgesetzt, um Schwachstellen zu entdecken [Cha05]. Beim „Stress Test“ werden Schaltungen mit hohen Signalraten und in rauen Umgebungen, z. B. in einem hochenergetischen Feld, betrieben [Cha04]. Durch die beschriebenen Mechanismen kann die Zuverlässigkeit einer Schaltung unter dem Einfluss physikalischer Fehler quantifiziert werden (Abbildung 2).

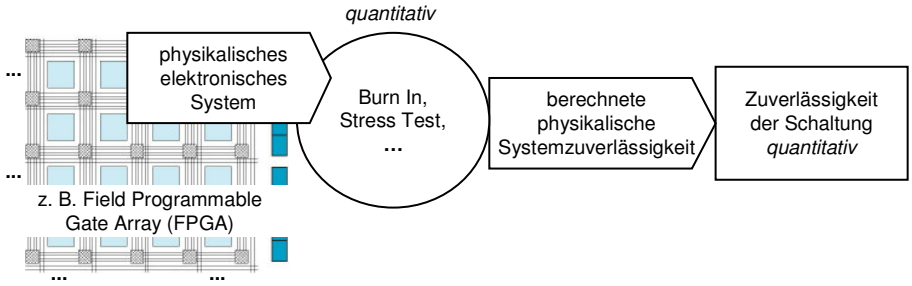

Abbildung 2: Zuverlässigkeitsbewertung einer produzierten Schaltung

Im Bereich eingebetteter Systeme und damit auch in der Mechatronik werden zunehmend Field Programmable Gate Arrays (FPGA), ein spezieller Typ mikroelektronischer Schaltungen, eingesetzt. Ein FPGA besteht aus einer Reihe konfigurierbarer Blöcke, welche unterschiedliche Module wie Prozessoren, Speicher und anwendungsspezifische Hardware auf einem einzigen Chip integrieren. Durch die einfache Möglichkeit der Konfiguration der Schaltungen werden eine schnelle Validierung sowie eine rasche Systemintegration ermöglicht.

Die Zuverlässigkeitsbewertung von FPGAs erfordert neben dem Faktor der physikalischen Zuverlässigkeit zusätzlich die Betrachtung des Designs der Schaltung. Die physikalische Zuverlässigkeit beruht auf der Zuverlässigkeit des verwendeten Materials und der physikalischen Verbindungen. Diese sind aufgrund des mehrfachen Einsatzes desselben FPGA für verschiedene Anwendungen bekannt oder können beim Hersteller erfragt werden. Das korrekte Design dagegen hängt von der fehlerfreien Konfiguration des FPGA ab, welche durch den Entwickler für die jeweilige Anwendung aufgrund der spezifischen funktionalen Anforderungen erfolgt. Eine Methode, die beide Faktoren bereits in frühen Entwicklungsphasen eines FPGA berücksichtigt, wurde in [HAW05] entwickelt.

2.3 Software

Im Gegensatz zu mechanischen und elektronischen Bauteilen unterliegen Softwaresysteme keinen physikalischen Fehlermechanismen. Enthaltene Fehler sind inhärenter, rein logischer Natur und wurden von Entwicklern, etwa beim Entwurf oder der Programmierung, begangen. Aus diesem Grund werden für Softwaresysteme keine Prüfstandsversuche durchgeführt, bei denen Systeme unter gleichartigen Betriebsbedingungen auf physikalische Ausfallursachen untersucht werden.

Um die Zuverlässigkeit eines Softwaresystems quantitativ zu beurteilen, werden Modelle verwendet, welche aus bereits gemessenen Daten die zukünftige Zuverlässigkeit beurteilen [Far96]. Zuverlässigkeitswachstumsmodelle [JM04] nehmen beispielsweise häufig an, dass die Fehler, die für das Versagen einer Software verantwortlich sind, nach dem Auftreten sofort korrigiert werden und dabei keine weiteren Fehler erfolgen (Abbildung 3). Ein bekanntes Modell, welches diese Annahme zugrunde legt, ist das Jelinski-Moranda-Modell.

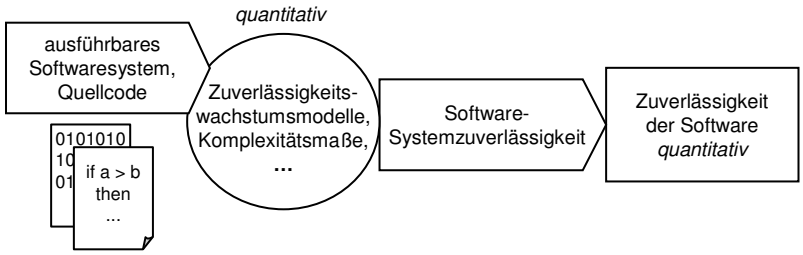

Abbildung 3: Zuverlässigkeitsbewertung einer implementierten Software

Ist ein ausführbares Softwaresystem in frühen Entwicklungsphasen noch nicht entworfen, so können keine empirischen Daten über dessen Versagen bestimmt werden. In diesem Fall wird häufig durch Beobachtung indirekter Größen wie der geschätzten Komplexität eines Programms (vgl. [MIO89]) versucht, die Zuverlässigkeit vorherzusagen. Aufgrund der geringen Aussagekraft wird diese Vorgehensweise jedoch kritisch betrachtet [FN99]. Als Alternative zur quantitativen Analyse kann die Zuverlässigkeit von Software ähnlich wie in der Mechanik auch qualitativ durchgeführt werden (siehe SW-FMEA [PA02] und SW-FTA [Lyu96]).

2.4 Forderung einer domänenübergreifenden Betrachtung

Bei den klassischen Methoden der Zuverlässigkeitsbewertung sind in allen Fachdisziplinen detaillierte Informationen über die Struktur und die Funktionen des Systems erforderlich. Speziell für die quantitative Analyse sind empirische Daten zur Zuverlässigkeit, wie das zeitabhängige Ausfallverhalten einzelner Bauteile, notwendig. Für jede der Domänen wurden daher spezifische Methoden erarbeitet

und vorgestellt, welche mit den unvollständigen Informationen in frühen Entwicklungsphasen umgehen können.

Obwohl die Fehlermechanismen in den Domänen verschieden sind, lässt sich eine vereinheitlichte Definition der Zuverlässigkeit über die geforderten Funktionen finden: nach [GZW+04] wird die Zuverlässigkeit hierbei als Überlebenswahrscheinlichkeit gegenüber Fehlfunktionen bzw. nach [ALR00] als die korrekte Erbringung der spezifizierten Dienste oder Funktionen bezeichnet. Trotz dieser einheitlichen Definition unterscheiden sich die Methoden und damit auch die Vorgehensweisen zur Zuverlässigkeitsbewertung wesentlich, was die ganzheitliche Bewertung eines mechatronischen Systems erschwert. Aus diesem Grund werden nachfolgend die Methoden für frühe Entwicklungsphasen zu einer ganzheitlichen Zuverlässigkeitsbewertung zusammengeführt.

3 Zuverlässigkeitsbewertung in frühen Entwicklungsphasen

Der Ablauf eines mechatronischen Entwicklungsprozess kann mittels des V-Modells für mechatronische Systeme nach [VDI04] beschrieben werden. Abbildung 4 zeigt die Aufgaben, die in frühen Entwicklungsphasen im Rahmen des Systementwurfs zu leisten sind.

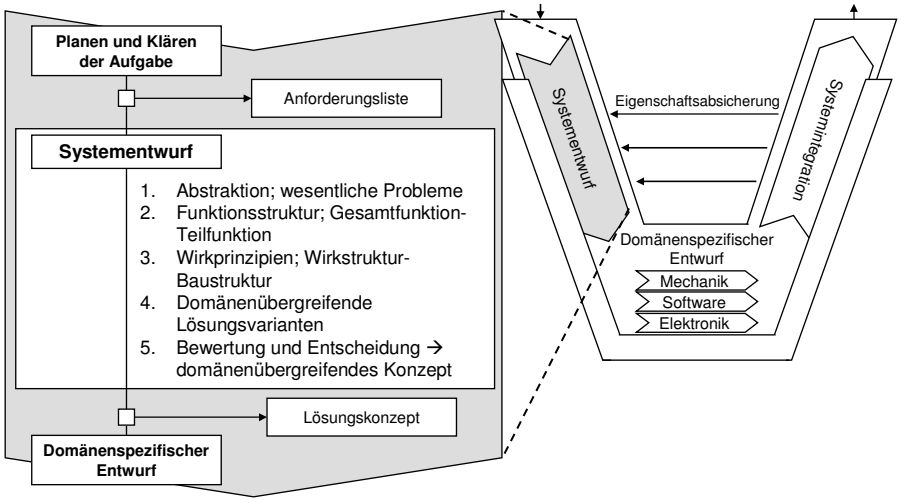

Abbildung 4: Aufgaben des Systementwurfs im V-Modell nach [VDI04]

Ein zu entwickelndes, zuverlässigkeitstechnisches Vorgehen in frühen Entwicklungsphasen muss sich an die in Abbildung 4 dargestellten Aufgaben angliedern lassen. Die in [JHB06] aufgezeigte Methode, welche die ganzheitliche quantitative Analyse in den Mittelpunkt stellt, wurde aufgegriffen und mit zusätzlichen Schritten versehen (Abbildung 5). Durch die Integration qualitativer Modellie-

rungs- und Analysemethoden ist je nach vorhandenen Informationen eine schrittweise Zuverlässigkeitsbewertung möglich. Die einzelnen Schritte werden im Folgenden kurz erklärt, auf Neuerungen wird im Speziellen eingegangen.

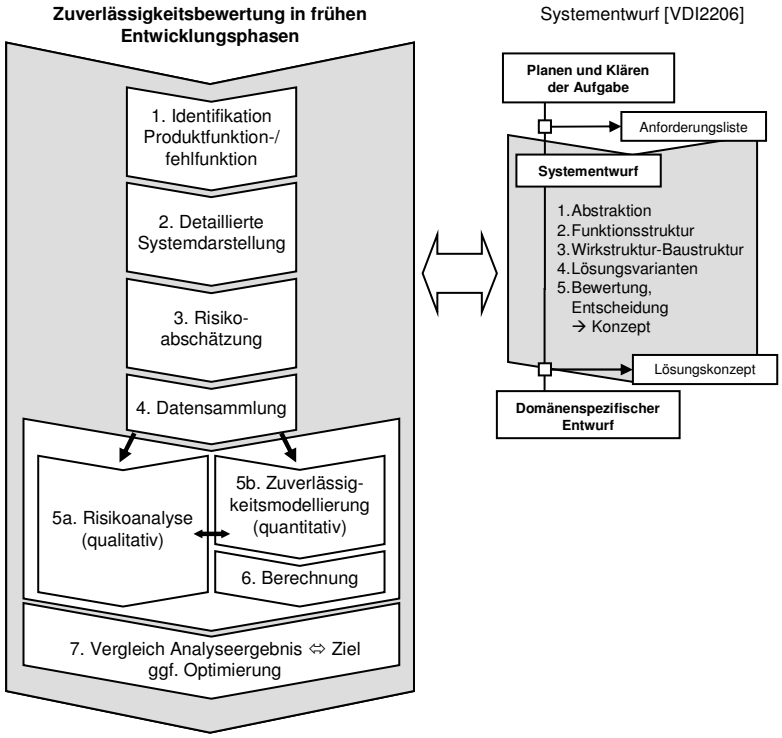

Abbildung 5: Angliederung der Zuverlässigkeitsbewertung an den Systementwurf

Zu Beginn der Zuverlässigkeitsbewertung werden die TOP-Funktionen und die TOP-Fehlfunktionen eines Produkts festgelegt. Neben einer Zuordnung von den einzelnen TOP-Fehlfunktionen zu Beanstandungsklassen nach [VDA00a] wird diesen Klassen jeweils ein Zuverlässigkeitszielwert zugewiesen, welcher sich zumeist aus gesetzlichen und marketingstrategischen Überlegungen ergibt (Schritt 1). Eine anschließende funktionale Betrachtung des Systems über Anwendungsfälle (Use Cases) ermöglicht es, an Informationen über Bauelemente für die Systemdarstellung zu gelangen (Schritt 2). Ein Prinzip der Modellerstellung, um zu einer Systemdarstellung des Gesamtsystems zu gelangen, ist die hierarchische Dekomposition über Bauelemente je nach vorhandenen Informationen bis hin zu einzelnen Bauteilen. Diese modulare Betrachtung eines Systems findet sich in allen Domänen wieder. Neben den Anwendungsfällen und der Beschreibung der möglichen modularen Strukturen wird in der erweiterten Vorgehensweise ein qualitatives, funktionales Modell der Software mit einbezogen. Die Situationsbasierte Qualitative Modellbildung und Analyse (SQMA) erlaubt eine ganzheitliche Beschreibung von mechatronischen Systemen durch eine komponentenorientierte Betrachtungsweise. Anhand des SQMA-Modells wird eine Risikoabschätzung an-

geschlossen (Schritt 3). Globale Fehlerauswirkungen im qualitativen Modell werden dabei ermittelt und in Kritikalitätsklassen eingeteilt. Durch eine Rückverfolgung in einzelne Systemkomponenten im Modell gelingt es, Schwachstellen im System zu ermitteln. Neben Schwachstellen und Fehlerzusammenhängen sind für die Zuverlässigkeitsbewertung entsprechende Daten erforderlich (Schritt 4). Daten können sowohl empirisch aus dem früheren Einsatz von Bauelementen ermittelt werden als auch in Form intuitiven, erfahrungsbasierten „Expertenwissens“ vorliegen. Je nach Datenlage kann daraufhin die qualitative (Schritt 5a) oder die quantitative (Schritte 5b und 6) Analyse des Systems vorgenommen werden. Bei einer hohen Ungenauigkeit der Daten wurde in [JHB06] die Möglichkeit aufgezeigt, eine Bewertung einzelner Systeme relativ zueinander vorzunehmen. Ergänzt wurden qualitative Analysemethoden (z. B. FMEA in Schritt 5a) sowie die Verwendung der Systemdarstellung, welche die geforderten Funktionen auf die Struktur abbildet, als gemeinsame Grundlage für die verschiedenen Analysen. Über einen Abgleich der quantitativen und qualitativen Ergebnisse können Schwachstellen im Gesamtsystem aufgezeigt werden. Aufgrund der Berechnung kann angegeben werden, welche der Varianten das zuverlässigere Produkt darstellt. Im letzten Schritt werden die vorliegenden Ergebnisse mit den gesetzten Zielen verglichen. Gegebenenfalls kann im Anschluss eine Optimierung durchgeführt werden. Eine Zuverlässigkeitsbewertung und -optimierung ist jedoch nur dann zielgerichtet möglich, wenn die gegenseitige Beeinflussung der Bauelemente bekannt ist. Um diese systematisch und unter ähnlichen Randbedingungen vergleichbar zu ermitteln, ist eine explizite Beschreibung der Wechselwirkungen erforderlich und muss in den vorgestellten Schritten berücksichtigt werden.

4 Integration der Wechselwirkungen zwischen Domänen

4.1 Schichtenmodell der Wechselwirkungen

Um Wechselwirkungen gezielt zu modellieren, wurde von den Autoren das Schichtenmodell aus [HG01] angepasst und in das Vorgehen der Zuverlässigkeitsbewertung integriert. Nach [VDI04] wurden dabei insgesamt drei abstrakte Arten von Wechselwirkungen berücksichtigt: Stofffluss, Leistungsfluss und Informationsfluss (Abbildung 6).

Art	Beispiele
Stoffffluss	Transport von Körpern, Gasen oder Flüssigkeiten z. B. in einer Wasserkühlung oder einer hydraulischen Bremse
Leistungsfluss	Druck, Biegung, Scherung, Wandlung elektrischer in mechanischer Leistung z. B. mittels eines Elektromotors
Informationsfluss	Methodenaufrufe, Datenaustausch zwischen Prozessen, Signale zwischen elektronischen Bauteilen

Abbildung 6: Arten von Wechselwirkungen mit Beispielen

Der Stoffffluss ergibt sich aus dem Aufbau der Mechanik zum Transport des jeweiligen Stoffes zwischen Bauteilen. Zusätzlich zu der Mechanik ergibt sich der Leistungsfluss aus dem Aufbau von Elektro-Mechanik und Elektronik. Er gehorcht physikalischen Naturgesetzen und ist damit zumindest theoretisch berechen- oder simulierbar, etwa durch den Einsatz numerischer Verfahren wie der Finiten-Elemente-Methode (FEM). Dagegen ergibt sich der Informationsfluss aus der Ansteuerung von elektro-mechanischen Bauteilen sowie dem Aufbau von Elektronik und Software. Im Gegensatz zu den anderen beiden Arten von Wechselwirkungen ist die Information selbst keine physikalische Größe, wird aber durch physikalische Größen, etwa elektrische Signale, repräsentiert und übertragen.

Untersucht man den Einfluss der Wechselwirkungen auf die Zuverlässigkeit eines Systems, so kann sich jede der drei Arten negativ auf die korrekte Funktionalität und damit auf die Zuverlässigkeit eines Systems auswirken. Gemäß der Spezifikation eines Systems muss zu einem gegebenen Zeitpunkt der jeweils geforderte Stoff-, Leistungs- und Informationsfluss vorliegen. Ein Fehlverhalten tritt auf, wenn eine dieser Anforderungen verletzt wird. Zwar ist die Zuverlässigkeit für bereits vorhandene Teilsysteme oder Systeme, wie in Kapitel 2 beschrieben, ermittelbar. Eine Übertragung von vorhandenen Systemen, bei denen der Informationsfluss einen großen Einfluss hat, auf neu zu entwickelnde Systeme in frühen Entwicklungsphasen ist jedoch schwierig. Für mechanische, elektro-mechanische und einfache elektronische Systemen lassen sich Klassen von vergleichbaren Systemen bilden, innerhalb derer sich empirisch ermittelte Aussagen zur Zuverlässigkeit übertragen lassen. Beispiel hierfür sind Lager, für die sich die Zuverlässigkeit aufgrund bestimmter Kenngrößen und früherer Experimente mit einer guten Aussagekraft frühzeitig bewerten lässt. Im Gegensatz dazu ist es für komplexe elektronische Schaltungen und Softwaresysteme schwierig, aus früheren Daten, etwa dem Auftreten der Versagensfälle bis zur Inbetriebnahme, auf die Zuverlässigkeit in einem neu zu entwickelnden System zu schließen. Ursachen hierfür sind die hohe Anzahl von Einflussgrößen sowie die hohe Veränderlichkeit, sodass bei einer Übertragung von System zu System Veränderungen beachtet und in die Bewertung mit einbezogen werden müssen. Ein Beispiel hierfür ist die hohe Anzahl möglicher Konfigurationen einer Schaltung in einem FPGA.

Das mechatronische Schichtenmodell wurde so konzipiert, dass sich ein System oder Teilsystem aus verschiedenen, miteinander benachbarten Schichten zusammensetzt. Abbildung 7 zeigt die Basisschichten, welche nach oben durch weitere Softwareschichten ergänzt werden können. Ein Teilsystem muss nicht notwendigerweise alle unteren Schichten enthalten, sondern kann sich beispielsweise auch nur aus Software zusammensetzen. Teilsysteme können über physikalische oder logische Verbindungen miteinander verbunden werden, etwa durch mechanische Kopplung, den Austausch elektrischer Signale oder die Verknüpfung mehrerer Softwaremodule.

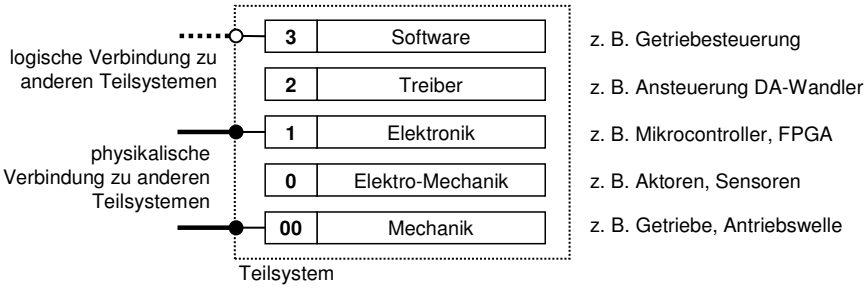

Abbildung 7: Schichtenmodell mechatronischer Teilsysteme oder Systeme

Verbindungen zwischen Teilsystemen können im vorgestellten Schichtenmodell - wie auch bei anderen Modellen etwa für Netzprotokolle - mit der nächsthöheren und der nächsttieferen Schicht sowie denselben Schichten in anderen Teilsystemen bestehen (Abbildung 8). Darüber hinaus gibt es auch Wechselwirkungen, die nicht über Verbindungen, sondern über den freien Raum wirken, beispielsweise in Form elektromagnetischer Strahlung. Diese können sowohl von einer Komponente innerhalb eines Systems ausgehen oder von außen auf alle Komponenten des Systems gleichermaßen einwirken.

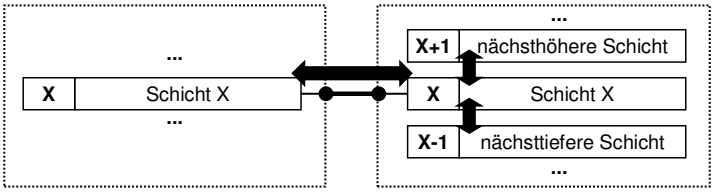

Abbildung 8: Mögliche Wechselwirkungen innerhalb des Schichtenmodells

Auf Grundlage des Modells der Wechselwirkungen sind nun mögliche Fehlerzusammenhänge in mechatronischen Systemen zu modellieren und zu analysieren.

4.2 Integration in die Zuverlässigkeitsbewertung

Ein Nachteil sowohl der beschriebenen quantitativen als auch der qualitativen Methoden besteht darin, dass die Fehlerzusammenhänge von Hand durch Experten ermittelt werden müssen. Eine frühe Beschreibung der Wechselwirkungen unterstützt die systematische Analyse, sodass komplexe Zusammenhänge nicht übersehen werden. Die eindeutig interpretierbare Beschreibung der Wechselwirkungen erlaubt zudem die Verarbeitung durch Rechnerwerkzeuge und so eine teilweise Automatisierung der Analyseschritte. Ein Schritt zur automatischen, werkzeuggestützten Analyse der beschriebenen Wechselwirkungen ist die Integration in die Modellierungssprache, welche zur Systemdarstellung verwendet wird. Die in Kapitel 3 beschriebene qualitative Modellierungssprache SQMA erlaubt die Definition von Schnittstellen zwischen Bauelementen eines Systems und die Zuordnung einer bestimmten Art von Wechselwirkung. Da Modelle in SQMA hierarchisch erstellt werden, lässt sich ein System, wie in [Bie03] gezeigt, in mehrere Teilsysteme mit verschiedenen Schichten unterteilen. Dementsprechend wurde das vorgestellte Schichtenmodell auf die Modellbildung und Analyse in SQMA abgebildet. Durch Injektion von Fehlern in einzelne Bauelemente werden im qualitativen Modell Fehlerzusammenhänge unter Beachtung der Wechselwirkungen schrittweise analysiert. Dadurch kann festgestellt werden, inwieweit Fehler in einzelnen Elementen zu einer Nichterfüllung einer Systemfunktion führen. Da die Zuverlässigkeit eingangs über die Erfüllung der Systemfunktionen definiert wurde, lässt sich aus den Fehlerzusammenhängen sowie vorhandenen Daten die Systemzuverlässigkeit quantitativ bewerten. Eine Übersicht über das Vorgehen gibt das folgende kurze Beispiel.

4.3 Beispiel für die Zuverlässigkeitsbewertung

Als Beispiel für die Zuverlässigkeitsbewertung dient ein Truckmodell im Maßstab 1:14. Zur Veranschaulichung wurde dieses Modell funktionsfähig aufgebaut, auf Laufrollen montiert und mit einer mikrocontrollerbasierten Softwaresteuerung versehen. Eine FPGA-basierte Steuerung wird derzeit entwickelt. Über das elektronische Cockpit stehen dem Fahrer Funktionen für Gas, Bremse und Schalten des 3-Gang-Getriebes (manuell, automatisch) zur Verfügung. Es wird davon ausgegangen, dass in frühen Entwicklungsphasen nur unvollständige Informationen über das spätere System vorliegen.

Nach der Formulierung der Anforderungen werden für die Zuverlässigkeitsbewertung im 1. Schritt die Produktfunktionen und Fehlfunktionen analysiert. Beispielsweise wird die Fehlfunktion „Drehmoment wird nicht gewandelt“ identifiziert und aufgrund der Beanstandungsklasse II mit einem Zuverlässigkeitszielwert $R_{II}(500h) = 0{,}99$ belegt. Im 2. Schritt wird das System modelliert. Abbildung 9 zeigt einen Ausschnitt des hierarchischen qualitativen SQMA-Modells, welches

die verschiedenen Schichten und ihre Wechselwirkungen beschreibt. Abhängig von der jeweiligen Schicht, werden an den Schnittstellen unterschiedliche Arten von Größen ausgetauscht.

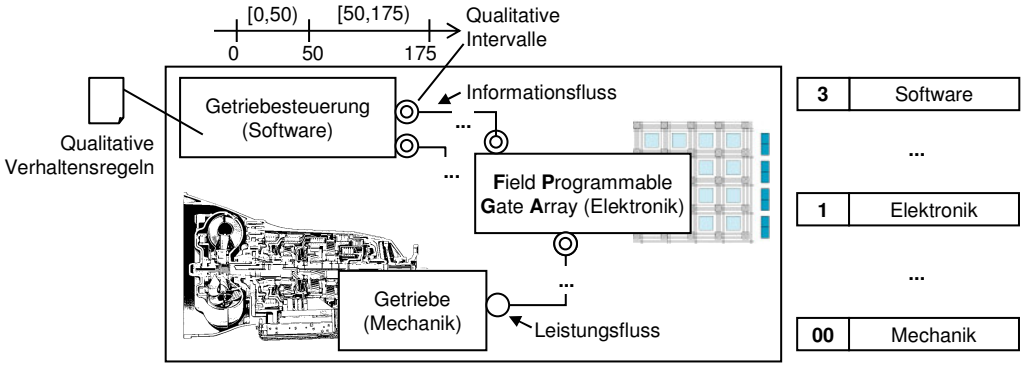

Abbildung 9: Ausschnitt aus einem qualitativen SQMA-Modell

Jede Komponente wird dabei mittels qualitativer Regeln über ihr Verhalten an den Schnittstellen beschrieben. In den unteren Schichten der Mechanik, Elektro-Mechanik und Elektronik können im ungesteuerten bzw. ungeregelten Fall Situationen eintreten, welche nicht den Anforderungen entsprechen und damit zu einem unzuverlässigen System führen können. Diese werden entsprechend markiert. Nach der Komposition mit den Schichten Treiber und Software wird im 3. Schritt durch Rechnerwerkzeuge geprüft, ob im Gesamtsystem diese markierten Situationen auftreten und sich global auswirken. Mittels Injektion von Fehlern wird weiter geprüft, welche Fehlerkombinationen zu einer globalen Auswirkung führen und ob es aufgrund der Wechselwirkungen zwischen den Schichten Schwachstellen im System gibt (Abbildung 10).

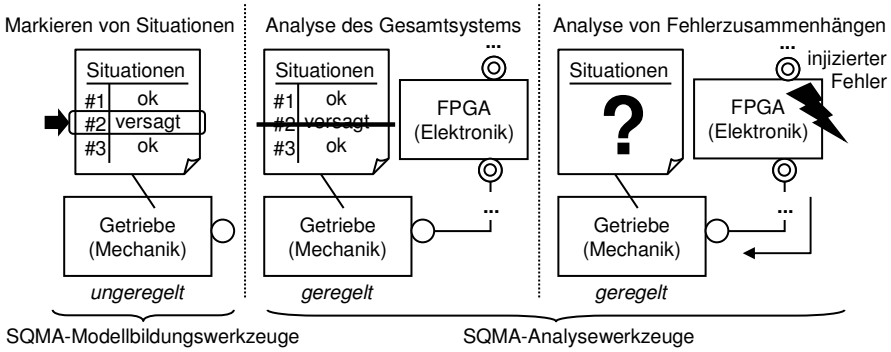

Abbildung 10: Analyse von Wechselwirkungen zwischen Komponenten

Im 4. Schritt ermittelte Daten dienen in den nachfolgenden Schritten 5 und 6 als Grundlage für detaillierte qualitative und quantitative Analysen. Ist die Zuverlässigkeit einzelner Komponenten aus dem mehrfachen Einsatz in anderen Systemen abschätzbar, so wird aufgrund des Zusammenwirkens die Zuverlässigkeit eines Teilsystems oder des neuen Gesamtsystems berechnet (z. B. Abbildung 11).

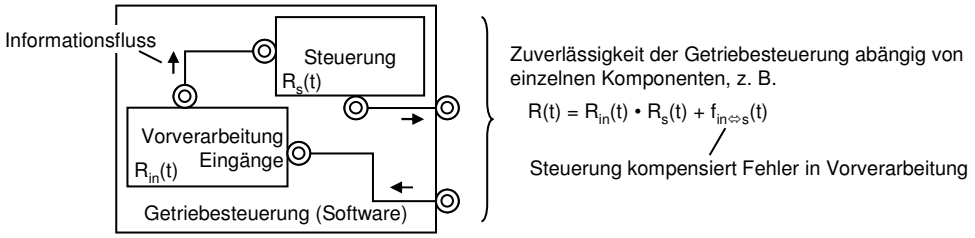

Abbildung 11: Auswertung des Informationsflusses der Softwarekomponenten

Wurde durch Vergleich mit dem Zuverlässigkeitszielwert ermittelt, dass die geforderte Zuverlässigkeit verfehlt wird, so sind im 7. Schritt schließlich aufgrund der modellierten Wechselwirkungen mögliche Optimierungen zu vergleichen und auszuwählen.

5 Zusammenfassung und Ausblick

Die vorgestellte Zuverlässigkeitsbetrachtung integriert die unterschiedlichen Methoden zur Zuverlässigkeitsbewertung in den verschiedenen Fachdisziplinen. Durch die Angliederung an das V-Modell kann sie entwicklungsbegleitend bereits frühzeitig durchgeführt werden. Die frühe Modellbildung und die Erweiterung um qualitative Methoden ermöglichen eine durchgängige Analyse. Die explizite Berücksichtigung von Wechselwirkungen erlaubt die systematische Untersuchung von Fehlerzusammenhängen in Modellbildung und Analyse sowie eine zielgerichtete Optimierung. Neben der Berücksichtigung der Wechselwirkungen in der Systemdarstellung wird an der mathematischen Beschreibung oder die Einbeziehung gemeinsamer Fehlerursachen in die Ermittlung der Systemzuverlässigkeit gearbeitet.

Der Beitrag entstand im Rahmen der Forschergruppe System-Zuverlässigkeit, welche durch die Deutsche Forschungsgemeinschaft gefördert wird.

Literatur

[ALR00] Avizienis, A., Laprie, J.-C., Randell, B.: Fundamental Concepts of Dependability. In: Proc. 3rd Inform. Survivability Workshop (ISW), Boston, 2000

[Bie03] Biegert, U.: Ganzheitliche modellbasierte Sicherheitsanalyse von Prozessautomatisierungssystemen. Dissertation, IAS-Forschunsgberichte, Shaker Verlag, Aachen, Bd. 2, 2003

[BL04] Bertsche, B., Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau. 3.Auflage, Springer, Berlin, 2004

[Cha04] Chan, H.A.: Accelerated Stress Testing for Both Hardware and Software. In: IEEE Reliability and Maintainability Symposium, 2004, pp. 346 - 351

[Cha05] Cha, J.H.: On Optimal Burn-In Procedures – A Generalized Model. In: IEEE Transactions on Reliability, Vol. 54, No. 2, 2005, pp. 198 - 206

[Ehr95] Ehrlenspiel, K.: Integrierte Produktentwicklung – Methoden für Prozeßorganisation, Produkterstellung und Konstruktion. Hanser Verlag, 1995

[Far96] Farr, W: Software reliability modeling survey. In: Software Reliability Engineering, Editor: M. R. Lyu, McGraw Hill and IEEE Computer Society Press, 1996, pp. 71-117

[FN99] Fenton N. E., Neil, M.: A Critique of Software Defect Prediction Models. In: IEEE Transactions on Software Engineering, Vol. 25, No. 5, 1999, pp. 675 - 689

[GF99] Gausemeier, J.; Fink, A. : Führung im Wandel – Ein ganzheitliches Modell zur zukunfts-orientierten Unternehmensgestaltung. Carl Hanser Verlag, München, 1999

[GFS96] Gausemeier, J.; Fink, A.; Schlake, O.: Szenario Management. Planen und Führen mit Szenarien, 2., bearbeitete Auflage, Carl Hanser Verlag, München, Wien, 1996

[GJB+06] Gandy, A., Jäger, P., Bertsche, B., Jensen, U.: Design support in early development phases – a case study from machine engineering, In: Reliability Engineering & System Safety (*in Druck*)

[GZW+04] Göhner, P., Zimmer, E., Arnaout, T., Wunderlich, H.-J.: Reliability Considerations for Mechatronic Systems on the Basis of a State Model. In: ARCS Workshop “Dependability and Fault Tolerance”, Augsburg, 2004

[HAW05] Heron, O., Arnaout, T., Wunderlich, H.-J.: On the Reliability Evaluation of SRAM-Based FPGA Designs. In: IEEE International Conference on Field Programmable Logic and Applications, 2005, pp. 403 - 408

[HG01] Hung, S. T., Gabel, M. J.: An Open System Interconnection Model for Mechatronics. In: Proc. IEEE/ASME International Conference on Advanced Intelligent Mechatronics, Vol.1, 2001, pp. 440 - 445

[JHB06] Jäger, P., Hitziger, T., Bertsche, B.: Zuverlässigkeitsbewertung mechatronischer Systeme in frühen Entwicklungsphasen. 4.Paderborner Workshop – Entwurf mechatronischer Systeme, Band 189, 2006, S. 25 - 44

[JM04] Jalote, P., Murphy, B.: Reliability growth in software products. In: Proc. Symposium on Software Reliability Engineering (ISSRE), 2004, pp. 47- 53

[MIO87] Musa, J. D., Iannino, A., Okumoto, K.: Software Reliability: Measurement, Prediction, Application .McGraw Hill, New York, 1987

[PA02] Pentti, H., Atte, H.: Failure Mode and Effects Analysis of Software-based Automation Systems. STUK-YTO-TR 190, Helsinki, 2002, http://www.stuk.fi/julkaisut/tr/stuk-yto-tr190.pdf

[VDA00a] VDA 3, Teil 1: Qualitätsmanagement in der Automobilindustrie - Zuverlässigkeitssicherung bei Automobilherstellern und Lieferanten, 3. Auflage, Frankfurt, 2000

[VDA00b] VDA 3, Teil 2: Qualitätsmanagement in der Automobilindustrie - Zuverlässigkeitssicherung bei Automobilherstellern und Lieferanten, 3. Auflage, Frankfurt, 2000

[VDI04] VDI 2206: Entwicklungsmethodik für mechatronische Systeme, Beuth-Verlag, Berlin, 2003