1 Einführung

1.1 Motivation und Problemstellung

Seit einigen Jahren nimmt der Anteil der Elektrik und Elektronik im Automobilbau stark zu [BFS+02, Dai02]. Es werden zunehmend komplexe Assistenz- und Sicherheitssysteme realisiert, die, wie zum Beispiel das Antiblockiersystem (ABS) oder das elektronische Stabilitätsprogramm (ESP), den Fahrer in kritischen Situationen unterstützen und damit die Sicherheit aller Teilnehmer im Straßenverkehr erhöhen. Schon bei der Entwicklung und Einführung dieser Generation von Fahrzeugsystemen hat sich gezeigt, dass die Frage nach der Systemsicherheit eine wichtige Rolle spielt [GBW01, RKR05, EPK+02]. Die Sicherheitsrelevanz dieser Systeme für das Gesamtprodukt Fahrzeug hat sich durch den Umstand des möglicherweise fehlerhaften, aktiven Eingriffs ins Fahrgeschehen signifikant erhöht. Das Sicherheitskonzept der meisten heutigen Assistenz- und Sicherheitssysteme beruht im Wesentlichen auf den drei Grundsäulen: Fehlererkennung, Funktionsdegradation und Vorhandensein einer mechanischen Rückfallebene. Damit ist garantiert, dass die Grundfunktionen eines Fahrzeugs, wie Lenken, Bremsen und Beschleunigen, gewährleistet sind.

Die Bandbreite möglicher zukünftiger Kraftfahrzeugsysteme geht jedoch weit über die bereits realisierten Produkte hinaus und reicht bis hin zu Systemen zum autonomen Fahren [ISS02]. Diese Konzepte erfordern jedoch noch weitreichendere Eingriffsmöglichkeiten der elektronischen Systeme in die Grundfunktionen des Fahrzeugs und sind damit in ihrer Sicherheitsrelevanz höher einzustufen. Zudem können diese erweiterten Funktionalitäten oft nur durch den Wegfall der mechanischen Kopplung und damit einer mechanischen Rückfallebene realisiert werden. Dies muss zwangsläufig zu noch höherer Sicherheitsrelevanz führen.

An sicherheitsrelevanten Kraftfahrzeugsystemen ohne mechanische Kopplung, den so genannten x-by-wire Systemen [XBWT98, ISS02], wird seit einigen Jahren geforscht und diverse Ansätze zur Beherrschung dieser Problematik wurden in den einzelnen Fachgebieten entwickelt. Redundante Systemkomponenten [Ech90], verteilte Systemarchitekturen [KKN95], zeitgesteuerte Kommunikations- und Betriebssysteme [Hed01], modellbasierte Fehlererkennungsmechanismen [Höf96], robuste Regelungskonzepte und Methoden der Softwaretechnik [Sie03] können dazu beitragen, die Komponenten eines Systems noch sicherer gegenüber Fehlern und Ausfällen zu machen. Letztendlich wird die Sicherheitsrelevanz sowohl der Einzelkomponenten als auch

des Gesamtsystems durch die Interaktion der Teilkomponenten, das Verhalten des Systemverbunds im Fehlerfall und die Verknüpfung mit der Systemumgebung, wie Fahrer, Fahrzeug oder anderer Verkehrsteilnehmer, bestimmt.

Mit Hilfe von Sicherheitsanalysen kann das vorhandene Risiko im Betrieb eines Systems untersucht werden. Klassische Analysemethoden - dazu zählen z.B. die Fehlermöglichkeits- und Einflussanalyse (FMEA) [MT00] oder die Fehlerbaumanalyse (FTA) [Sch99] - haben sich in vielfacher Hinsicht über Jahre hinweg bewährt. Gemein ist fast allen klassischen Analysemethoden die Durchführung in Form von Brainstorming-Prozessen durch Expertenteams. Dabei erörtern die Experten in Teamsitzungen die Fehlermöglichkeiten in den einzelnen Systemkomponenten und deren Fehlerauswirkungen auf das Gesamtsystem aus ihrer persönlichen Sicht. Es hat sich allerdings gezeigt, dass diese Vorgehensweise einige Nachteile mit sich bringt [Lev95]. Können die Experten die Fehlermöglichkeiten der Einzelkomponenten mit Hilfe von strukturierten Vorgehensweisen noch sehr detailliert und meist auch vollständig beschreiben, so sind hingegen die Fehlerauswirkungen im Zusammenspiel der Einzelkomponenten oft nicht eindeutig und vollständig zu identifizieren. Diese Problematik verschärft sich bei den sicherheitsrelevanten Systemen durch den Einsatz von Redundanz- und Verteiltheitskonzepten zudem erheblich. Eine größere Anzahl an Komponenten, die in einer deutlich komplexeren Art und Weise interagieren, zeigen die Grenzen der klassischen Analysen auf. Die bisher grundsätzlich rein statischen Analysen der Systeme lassen zudem eine zeitliche Betrachtung nicht zu. Fehlerausbreitungen, Folgefehler oder Fehlersequenzen können bisher nur unzureichend untersucht werden.

Das notwendige Systemwissen der Experten bildet sich meist erst im Laufe des Entwicklungsprozesses. Es ist damit einem ständigen Erweiterungs- und Veränderungsprozess unterworfen und lässt sich deshalb schwer dokumentieren. Damit sind die Einschätzungen der Experten bezüglich der Systemsicherheit diesem Veränderungsprozess unterworfen und von ihren aktuellen Erfahrungen und Herausforderungen während der Systementwicklung geprägt. Studien haben gezeigt, dass die Analyseergebnisse in starker Abhängigkeit weiterer Einflussgrößen stehen, die von der Teamzusammensetzung bis hin zur Tagesverfassung einzelner Experten reichen [Lev95, Bis90]. Die Reproduzierbarkeit der Analyseergebnisse ist nicht gegeben.

Der enorme Zeit- und Kostenaufwand für eine klassische Analyse verhindert deren iterative Durchführung während des Entwicklungsprozesses. Viele Fragestellungen, die die Relevanz von Komponenteneigenschaften für die Gesamtsystemsicherheit betreffen, können in einem frühen Stadium der Entwicklung mangels geeigneter Identifikations- und Bewertungsverfahren nicht beantwortet werden. Entscheidungen, wie z.B. die Festlegung der Systemarchitektur, müssen jedoch zu einem frühen Zeitpunkt der Systementwicklung getroffen werden, ohne deren Auswirkungen auf die Sicherheit des Gesamtsystems dynamisch und quantitativ bewerten zu können.

Eine parallele Entwicklung sowohl der funktionalen Charakteristika als auch der Sicherheitseigenschaften eines Systems erscheint mit heute bekannten Prozessen nur unzureichend realisierbar.

1.2 Zielsetzung der Methodik zur Systemanalyse

Gegenwärtig ist in der Automobilindustrie ein starkes Bestreben zur modellbasierten Systementwicklung festzustellen. Die in den letzten Jahren entwickelten Methoden eignen sich aber hauptsächlich für die Entwicklung funktionaler Systemeigenschaften, wie z.B. dem Entwurf eines Regelungsalgorithmus.

Ziel dieser Arbeit ist es, die Methoden der modellbasierten Systementwicklung auf Sicherheitsaspekte zu erweitern und mit den klassischen Verfahren zur Sicherheitsanalyse zu kombinieren. Dadurch sollen die eingangs dargelegten Schwachstellen heutiger Analysemethoden reduziert werden. Ergebnis dieser Arbeit sind neue Vorgehensweisen und Algorithmen, die vor allem im Hinblick auf folgende Eigenschaften Vorteile bieten:

dynamisch: Mathematische Modelle, die das zeitliche Verhalten eines Systems beschreiben, werden heute bereits bei der Funktionsentwicklung eines neuen Kraftfahrzeugsystems erzeugt. Diese Modelle sollen die Grundlage für eine dynamische Analyse des Systemverhaltens im Fehlerfall bilden. Die zeitliche Fehlerausbreitung und die Auswirkungen von Folgefehlern und Fehlersequenzen können damit untersucht und bewertet werden.

ganzheitlich: Durch die modulare Struktur solcher dynamischer Komponentenmodelle ist es möglich, sehr große Systemmodelle zu bilden, die das gesamte zu entwickelnde Kraftfahrzeugsystem und dessen Umgebung aus Fahrzeug, Fahrer und Straße beschreiben. Damit kann die Systemanalyse interdisziplinär und über das ganze System hinweg durchgeführt werden.

objektiv quantifizierbar: Mit Hilfe der modellbasierten Verhaltensbeschreibung für das System selbst als auch für dessen Umgebung können Auswirkungen von Fehlern berechnet werden. Die subjektiven Einschätzungen der Experten in den klassischen Sicherheitsanalysen werden ersetzt durch eine objektiv quantifizierbare Berechnungsvorschrift.

reproduzierbar: Diese Berechnungen sind jederzeit wiederholbar und zu einem späteren Zeitpunkt nachvollziehbar.

iterativ anwendbar: Mathematische Systembeschreibungen eröffnen die Möglichkeit zur rechnerunterstützten Durchführung der Analyse und versprechen eine schnellere und damit mehrmalige Anwendung während des Entwicklungsprozesses. Nach jeder Änderung am System im Laufe des Entwicklungsprozesses kann die Auswirkung dieser Änderung auf die Systemsicherheit überprüft und analysiert werden.

automatisierbar: Mit Hilfe komplexer Suchalgorithmen ist es möglich, die Sicherheitsanalyse zu automatisieren. Rechnergestützte Verfahren sind in der Lage, viele Fehlermöglichkeiten zu analysieren und selbständig nach den Fehlermöglichkeiten zu suchen, die besonders signifikante Fehlerauswirkungen im System hervorrufen.

strukturiert und gut dokumentiert: Viele der wichtigsten Informationen und Erfahrungen, die während einer Systementwicklung gewonnen werden, sind in den dynamischen Modellen gespeichert und dokumentiert.

1.3 Gliederung der Arbeit

Das zweite Kapitel fasst zunächst die Charakteristika mechatronischer, verteilter, sicherheitsrelevanter Kraftfahrzeugsysteme zusammen. Die folgende Gegenüberstellung von Beispielen für heutige und Konzeptionen für zukünftige mechatronische, verteilte, sicherheitsrelevante Kraftfahrzeugsysteme macht die Herausforderungen bei deren Entwicklung deutlich und bildet die Grundlage zur Erarbeitung der Anforderungen an eine modellbasierte, ganzheitliche System- und Sicherheitsanalyse im dritten Kapitel.

Die Untersuchung und Bewertung unterschiedlicher Verfahren zur Sicherheitsanalyse, heute bekannter Modellierungsarten und verschiedener Verfahren zur Automatisierung von Analysen hinsichtlich deren Anwendbarkeit unter den erstellten Anforderungen an eine modellbasierte, ganzheitliche Systemanalyse, ist Bestandteil des vierten Kapitels.

Im Kapitel 5 wird auf Basis der bisher erlangten Erkenntnisse das entwickelte Konzept zur ganzheitlichen, dynamischen Systemanalyse vorgestellt. Es ermöglicht neben der Analyse von Fahrzeugsystemen unter funktionalen Aspekten vor allem die Untersuchung des Verhaltens im Fehlerfall. Auf die Frage nach der Einbettung der Methodik in einen möglichen Entwicklungsprozess für sicherheitsrelevante Kraftfahrzeugsysteme wird anschließend eingegangen.

Neben der notwendigen hybriden Modellierung des Gesamtsystems, die in Kapitel 6 beschrieben wird, ist vor allem das Verfahren zur Identifikation signifikanter Fehlerauswirkungen ein elementarer Bestandteil der vorgestellten Analysemethode. Die entwickelten Algorithmen und deren

Verknüpfung mit dem Gesamtsystemmodell zur rechnergestützten und damit automatisierten Analyse sind Bestandteil von Kapitel 7.

Die praktische Anwendung der ganzheitlichen, dynamischen Analyse sicherheitsrelevanter, verteilter Fahrzeugsysteme erfolgt beispielhaft an einem Steer-by-wire System. Der Beschreibung der Systemarchitektur, der Systemfunktionalität und des Sicherheitskonzepts folgt eine Vorstellung der erstellten Simulationsmodelle. Anschließend wird der Einsatz der entwickelten Methodik erläutert. Die Identifikation sicherheitsrelevanter Fehlerszenarien, deren Bewertung und die daraus abgeleitete Ergreifung von Sicherheitsmaßnahmen bilden zusammen mit einer Aufstellung der gewonnenen Ergebnisse und Erkenntnisse der Analysemethodik das Kapitel 8.

Das neunte Kapitel beinhaltet eine zusammenfassende Beschreibung und Bewertung der Ergebnisse der Arbeit sowie einen Ausblick auf weiterführende Aspekte.

2 Charakteristika mechatronischer, verteilter, sicherheitsrelevanter Kraftfahrzeugsysteme

Schon bei der verbalen Beschreibung und Analyse von Systemen hinsichtlich ihrer Funktionsweise und insbesondere hinsichtlich ihrer Sicherheit stößt man auf das Problem eines nicht einheitlichen Verständnisses aufgrund unterschiedlicher Betrachtungsweisen und Hintergründe. Deshalb werden im ersten Teil dieses Kapitels die Charakteristika mechatronischer, verteilter, sicherheitsrelevanter Kraftfahrzeugsysteme und ihre Konzeptionen herausgearbeitet. Ziel ist eine kompakte, auf wesentliche Aspekte konzentrierte Analyse der Systemeigenschaften und eine Zusammenfassung der daraus resultierenden Herausforderungen. Der sich daran anschließende, zweite Teil dieses Kapitels befasst sich mit Beispielen für heutige, aber auch mit Konzeptionen für zukünftige mechatronische, verteilte, sicherheitsrelevante Kraftfahrzeugsysteme. Der Vergleich der verschiedenen Konzepte, der Systemarchitekturen und der zur Realisierung eingesetzten Technologien dient zur Verdeutlichung der besonderen Herausforderungen und Schwierigkeiten bei der Entwicklung von mechatronischen, verteilten, sicherheitsrelevanten Fahrzeugsystemen.

2.1 Eigenschaften mechatronischer Systeme

Das Kunstwort Mechatronik ist ursprünglich auf die Begriffe Mechanik und Elektronik zurückzuführen. Inzwischen umfasst der Begriff Mechatronik jedoch weit mehr und so kann heute festgestellt werden, dass ein mechatronisches System seine Funktionalität durch die enge Verknüpfung von mechanischen, elektronischen und datenverarbeitenden Komponenten erzielt. Der grundlegende Aufbau eines mechatronischen Systems ist in Abbildung 2.1 dargestellt.

Die Integration verschiedenster Teilsysteme und Technologien zu einem gemeinsamen Ganzen hat nicht nur Auswirkungen auf das mechatronische System selbst, sondern auch auf die Entwicklung solcher Systeme. Die Notwendigkeit zur interdiziplinären Kooperation der beteiligten Entwickler erfordert eine angepasste Entwicklungsweise und das Verständnis für die Herausforderungen der unterschiedlichen Ingenieurdisziplinen. Vor allem bei der Analyse der System-

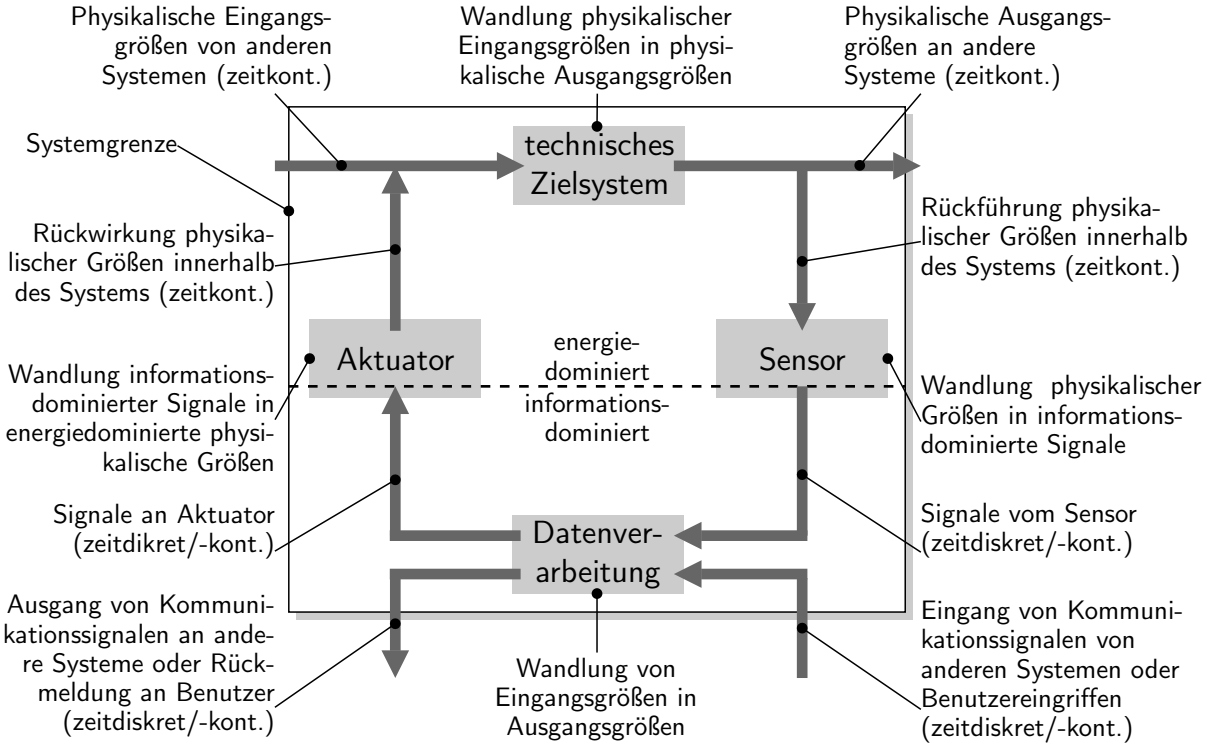

Bild 2.1: Typischer, prinzipieller Aufbau eines mechatronischen Systems

funktionalität hinsichtlich deren Einhaltung funktionsbezogener Anforderungen sind Methoden erforderlich, die sowohl das komplexe und interdisziplinäre Zusammenwirken wie auch die daraus resultierenden Herausforderungen berücksichtigen und beherrschen. Einen noch höheren Stellenwert kommt dieser Analyse zu, wenn es sich beim technischen System um einen Vorgang handelt, der potentiell Schaden an Menschen, Tieren oder Sachwerten verursachen kann.

2.2 Eigenschaften sicherheitsrelevanter Systeme

Die Sicherheit eines Systems kann beeinträchtigt werden, wenn Fehler auftreten. Als Fehler bezeichnet man die Abweichung des tatsächlichen Systemverhaltens von einem vorgegebenen oder erwarteten Sollverhalten. Fehler können ursächlich innerhalb einer Komponente entstehen und lassen sich entsprechend ihrer Fehlerursache nach [Ech90] klassifizieren:

Entwurfsfehler führen dazu, dass schon vor der Inbetriebnahme Fehler im System vorhanden sind. Die Klasse der Entwurfsfehler lässt sich weiter unterteilen in Spezifikationsfehler, Implementierungsfehler und Dokumentationsfehler.

Produktionsfehler können verhindern, dass aus einem korrekten Entwurf ein fehlerfreies Produkt entsteht. Zu hohe Fertigungstoleranzen aufgrund nicht eingehaltener Herstellungsprozesse können z.B. dafür verantwortlich sein, dass die Umsetzung des Entwurfs in ein fehlerfreies Produkt misslingt.

Betriebsfehler entstehen im Gegensatz zu den Entwurfs- und Herstellungsfehlern erst durch die Inbetriebnahme des Fahrzeugsystems. Sie lassen sich weiter detaillieren in störungsbedingte Fehler, Verschleißfehler, Bedienungsfehler und Wartungsfehler.

Im Bereich der Sicherheitstechnik werden Systeme entsprechend einem von ihnen ausgehenden Gefährdungspotential im Nominal- wie auch im Fehlerfall klassifiziert. Anhand dieser Klassen leiten sich die Anforderungen an die Systemarchitektur ab. Besondere Bedeutung für die Auslegung der verschiedenen Elektronikarchitekturen erlangt vor allem das notwendige Systemverhalten im Vorhandensein von Fehlern. Man unterscheidet dabei zwischen ausfallsicherem (fail-safe oder fail-silent) und ausfalloperationalem (fail-operational) Systemenverhalten:

ausfallsicher (fail-safe oder fail-silent) bezeichnet ein System, das nach dem Eintreten eines Fehlers unmittelbar in einen sicheren Zustand übergehen und auch nach weiteren Ausfällen in einem - eventuell auch anderen - sicheren Zustand verbleiben kann.

ausfalloperational (fail-operational) wird ein System genannt, wenn im Fehlerfall das System eine Grundfunktionalität solange erbringen kann, bis ein sicherer Systemzustand erreicht wird. Diese Eigenschaft wird von Systemen verlangt, die nicht unmittelbar einen sicheren Systemzustand erreichen können. Dazu gehört z.B. das Flugregelsystem moderner Passagierflugzeuge, das trotz eines Fehlers einen Weiterflug und eine sichere Landung ermöglichen muss.

Bei der Entwicklung von Systemarchitekturen, die das beschriebene ausfalloperationale Verhalten aufweisen müssen, wird oft auf den Mechanismus der Fehlertoleranz zurückgegriffen. Fehlertoleranz bezeichnet die Fähigkeit eines Systems auch mit einer begrenzten Anzahl an fehlerhaften Komponenten seine geforderte Funktion zu erbringen. Meist ist das jedoch nur durch redundante Strukturen zu erreichen, so dass eine Funktionalität von mehreren unabhängigen Komponenten angeboten wird. Die erhöhte Anzahl an Komponenten bedeutet jedoch eine deutliche Steigerung der Systemkomplexität und damit eine potentielle Reduktion der Systemsicherheit. Die augenscheinliche Herausforderung bei der Entwicklung sicherheitsrelevanter Systeme besteht also in der Beherrschung dieses Teufelskreises.