Sicherheits- und Verfügbarkeitsanalyse komplexer Kfz-Systeme

Vom Fachbereich Elektrotechnik und Informatik
der Universität-Gesamthochschule Siegen
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
(Dr.-Ing.)
genehmigte Dissertation

vorgelegt von
Diplom-Ingenieur Rachad Mahmoud

I. Gutachter: Prof. Dr.-Ing. O. Loffeld
II. Gutachter: Prof. Dr.-Ing. H. Wojtkowiak

Tag der mündlichen Prüfung: 10.01.2000

Vorwort

Diese Arbeit entstand während meiner Tätigkeit in der Abteilung „Systemsicherheit“ der Daimler-Benz Forschung in Stuttgart.

Mein besonderer Dank gilt zwei Herren.

Meinem Daimler-Benz-seitigen Betreuer, Prof. Dr. Thomas Vogel, Leiter der Abteilung Systemsicherheit. Neben dem regen Gedankenaustausch ermöglichte er mir die intensive Mitarbeit an Forschungs- und Entwicklungsprojekten. Erst durch diese Projekttätigkeiten konnte die vorliegende praxisbezogene Promotion entstehen.

In gleichem Maße danke ich meinem Doktorvater, Prof. Dr. Ing. Otmar Loffeld, Leiter des Projektbereichs 2 des Zentrums für Sensorsysteme der Universität-Gesamthochschule Siegen. Durch seine Förderung ermöglichte er mir die lehrstuhlferne Industrie-Promotion. Seine fachliche Begleitung bewahrte mich davor, meine gewonnenen Erkenntnisse in einem mit Tabellen und Charts überhäuften technischen Bericht münden zu lassen.

Herrn Prof. Dr. Wojtkowiak, Leiter des Institutes für technische Informatik der Universität-Gesamthochschule Siegen, möchte ich sehr herzlich Danken für die Übernahme des Koreferats, sein Interesse an dieser Arbeit sowie die inhaltlichen Anregungen zur Komplettierung dieser Arbeit.

Herrn Prof. Dr. Merzenich, Dekan des Fachbereichs Elektrotechnik und Informatik der Universität-Gesamthochschule Siegen, danke ich für die Leitung sowie Durchführung des Promotionsverfahrens.

Neben meinen Betreuern gilt mein besonderer Dank den Herren Dipl. Ing. Matthias Benzinger, Andreas Kurth, Marcus Steigerwald, Markus Stiegler und Dirk Wetter. Die von Ihnen unter meiner Betreuung durchgeführten Diplomarbeiten trugen maßgeblich zum Gelingen der vorliegenden Arbeit bei. Jedoch möchte ich ihnen nicht nur für ihre fachlichen Beiträge und die hervorragende Zusammenarbeit, sondern insbesondere für das freundschaftliche Verhältnis danken. Herrn Guido Justen danke ich für seine zahlreichen redaktionellen und inhaltlichen Anregungen.

Ebenso möchte ich ganz besonders den Herren Dipl. Ing. Friedrich Böttiger und Dipl. Ing. Avshalom Suissa danken. Sie standen mir als „geistige Väter“ des Systems Drive-by-Wire, auf welches die in der vorliegenden Arbeit entwickelte hierarchische Modellierung appliziert wurde, mit Rat und Tat zur Seite.

Mein innigster Dank gilt meiner Familie, die im Zuge der Promotion erheblich an Zuwachs erfuhr.

Meiner Frau Michaela möchte ich danken für ihre stete Auf- und Ermunterung bei der Durchführung dieser Arbeit. Ihre Geduld und Bedürfnisse wurden in den vergangenen fünf Jahren in vielerlei Hinsicht strapaziert bzw. vernachlässigt.

Ebenso danke ich meinen Eltern, die mich nunmehr schon seit etwas mehr als 30 Jahren durch jedes Hoch- und Tief begleitet, wie auch geführt haben.

Widmen möchte ich diese Arbeit unseren beiden jüngsten Familienmitgliedern, Michaelas und meinen Söhnen Fabian Manuel und Tim Oliver.
Ihr beiden habt die Phase des Zusammenschreibens der Arbeit durch Euer gleichzeitiges Heranreifen im Mutterleib, dem Ereignis Eurer Geburten und Eurem vergnügten Quietschen und Lachen zu einer besonders schönen und abwechslungsreichen Zeit werden lassen.

Abstract

Safety- and availability-analysis of complex automotive systems

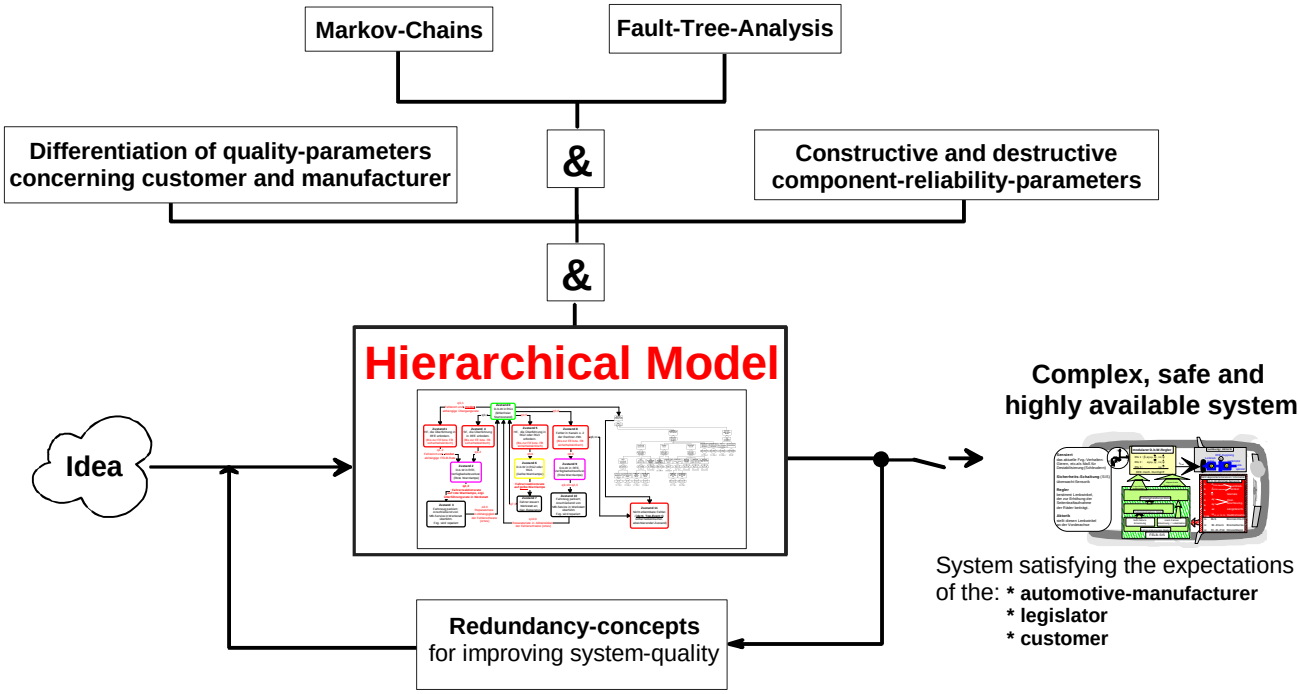
In the dissertation-thesis in hand a methodology is developed, which allows to determine the failure-probability, availability, safety and economy of complex safety-relevant automotive systems in a closed model. This methodology is based on the fusion of fault-trees and Markov-chains to a hierarchical model.

The hierarchical modelling generates a qualitative as well as quantitative prediction of the above mentioned system-quality-parameters. Modifications during the development-process of a complex system can be integrated in the analysis with small effort.

In order to demonstrate the potentials of the hierarchical modelling, it was applied to determine the failure-probability, availability, safety and economy of a driving-stability-control-system. This system, which is called Drive-by-Wire was in the early research-phase, when the first safety and availability-analysis had been performed. As it turned-out, failures of the wheel-speed-sensors are mainly responsible for the unsafety of this system.

Therefore redundancy concepts were developed which yield tolerance against above mentioned critical failures. Finally the influence of different redundancy concepts on the failure-probability, availability, safety and economy of Drive-by-Wire was determined by the hierarchical modelling.

The following picture shows the main elements which were fused to the hierarchical model. As the first phase of developement starts with a more or less precise idea of a new system, it is important to determine the deficits of this idea concerning the system-quality-parameters in the early states of development. After determining these deficits by hierarchical modelling, improvements need to be implanted into the system. The repeated determination of the system-quality-parameters and the further improvement of the system are performed in the described cyclic process until the system satisfies the expectations of the automotive manufacturer, the legislator, and most important - the customer.



Kurzfassung

In der vorliegenden Arbeit wird eine Methodik zur geschlossenen Bewertung der **F**ehlerhäufigkeit, **V**erfügbarkeit, **S**icherheit und **W**irtschaftlichkeit (F/V/S/W) komplexer sicherheitsrelevanter Kfz-Systeme entwickelt und anhand von Beispielen veranschaulicht. Diese Methodik fußt auf einer Fusion von Fehlerbäumen und Markov-Ketten zu hierarchischen Modellen.
Die hierarchische Modellierung erlaubt es, sowohl eine qualitative wie auch quantitative Systemaussage mit vertretbarem Analyseaufwand zu generieren. Modifikationen innerhalb des Entwicklungsstandes können mit geringem Aufwand in die Systembetrachtungen integriert werden.
Um die Leistungsfähigkeit der hierarchischen Modellierung zu verifizieren, wurde das noch im Forschungsstadium befindliche Fahrdynamikstabilisierungssystem **D**rive-**b**y-**W**ire (D-b-W) auf seine F/V/S/W hin untersucht. Wie sich zeigte, erwiesen sich Fehler der Raddrehzahlsensorik als kritischer Pfad hinsichtlich der Sicherheit des Systems.
Aus diesem Grund wurden Redundanzkonzepte entwickelt, die zur Toleranz gegen obige kritischen Fehler führen. Abschließend wurden die Auswirkungen der verschiedenen Redundanzkonzepte auf die Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit des Systems D-b-W mittels der hierarchischen Modellierung bewertet.

Kurzübersicht über die Arbeit

- Im Anschluß an die Einleitung/Motivation erfolgt in Kap. 2 eine Kurzeinführung in die Grundlagen der Zuverlässigkeits- und Sicherheitstheorie. In Kap. 3 werden die für die F/V/S/W-Bewertung sicherheitsrelevanter Kfz-Systeme geeigneten Methoden vorgestellt. Hierbei liegt der Schwerpunkt auf der Erläuterung der relevanten konstruktiven und destruktiven Zuverlässigkeitskenngrößen und -parameter.
- Kap. 4 dient dazu, das für die F/VS/W-Analyse des Applikationsbeispiels Drive-by-Wire erforderliche System-Know-how herauszuarbeiten. Hierbei gilt das Hauptaugenmerk den Fehlermoden der einzelnen Komponenten des Fahrdynamikregelungssystems.
- In Kap. 5 erfolgt die eigentliche F/VS/W-Analyse des D-b-W-Systems, wobei hierbei von einem Minimal-System ausgegangen wird. Begonnen wird mit der Untersuchung der Auswirkungen der in Kap. 4 erläuterten Fehlermoden auf das Systemverhalten. Exemplarisch wird hierfür eine Abwandlung der FMEA (**F**ehler**m**öglichkeiten- und **E**ffekt/Auswirkungs-**A**nalyse) vorgenommen und anschließend auf die aus Sicht des Autors für Mehrfachfehlerbetrachtungen geeigneten Fehlerbaumanalyse/Markov-Kettenmodellierungen und die im Rahmen dieser Arbeit entwickelten Mischformen (hierarchische Modelle) zurückgegriffen.
- Nachdem in Kap. 5 Zuverlässigkeits- und Sicherheitsdefizite des Minimalsystems aufgezeigt wurden, dient Kap. 6 dazu, Redundanzmechanismen zur gleichzeitigen Optimierung der Fehlerhäufigkeit, Verfügbarkeit und Sicherheit unter Berücksichtigung der Wirtschaftlichkeit vorzustellen. Die Auswirkungen der verschiedenen Redundanzkonzepte auf die Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit des Systems D-b-W werden anschließend mittels der hierarchischen Modellierung bewertet.
- Abschließend erfolgt in Kap. 7 die Zusammenfassung der Ergebnisse/Erkenntnisse und ein Ausblick auf mögliche weitere Aktivitäten.

Hinsichtlich der Vorgehensweise beim Studium der einzelnen Kapitel empfiehlt es sich aus Sicht des Autors, im Anschluß an die Einleitung und die Erläuterungen der Grundlagen der Zuverlässigkeits- und Sicherheitstheorie, die in Kap. 4 erfolgende Diskussion des Applikationsbeispiels D-b-W zu überfliegen. Diese Vorgehensweise fördert das Verständnis für die in Kap. 3 erläuterten systemspezifischen Zuverlässigkeitsparameter.

Inhaltsverzeichnis

1 Motivation / Einleitung

Unfallstatistiken zufolge wurden im Jahr 1995 in Deutschland ca. 450.000 Verkehrsunfälle registriert. Hiervon waren mehr als 70% auf menschliches Fehlverhalten bzw. Versagen zurückzuführen.
Fahrerassistenzsysteme tragen durch die Unterstützung des Fahrzeugführers hinsichtlich seiner Fahrzeugsteuerungsfunktionen zur Entlastung des Fahrers und damit Reduzierung der Unfallhäufigkeit bei.
Die Bandbreite derartiger Assistenzsysteme reicht von der Fahrdynamikstabilisierung durch aktiven Eingriff in das Fahrzeugverhalten bis hin zum autonomen Fahren.
Wesentliche Bestandteile dieser Assistenzsysteme sind aus der Luft- und Raumfahrt bekannte X-by-Wire-Systeme, die einen mechanischen Durchgriff des Fahrers auf den betreffenden Steller (Lenkung, Bremse etc.) unterbinden und somit als sicherheitsrelevant einzustufen sind.
Durch die mit zunehmender Funktionalität derartiger elektronischer Systeme stetig steigende Anzahl der Systemkomponenten kommt den Qualitätsmerkmalen Fehlerhäufigkeit, Verfügbarkeit und Sicherheit jedes einzelnen Bauteils und seiner Wechselwirkungen im System wie in Bezug auf das Gesamtfahrzeug eine immer größere Bedeutung zu.
Durch die Einführung komplexer elektronischer Systeme darf das Risiko nicht zunehmen. Vielmehr sollte ein der Sicherheitserhöhung dienendes Fahrerassistenzsystem trotz des Komplexitätszuwachses nicht zur Zunahme der Fehlerhäufigkeit oder Reduzierung der Verfügbarkeit des Automobils noch zur inakzeptablen Erhöhung der Anschaffungs- oder Haltungs- bzw. Wartungskosten führen.
Damit sind wichtige Voraussetzungen für die Zulassungsfähigkeit und Akzeptanz derartiger X-by-Wire-Systeme im Kfz ihre niedrige **F**ehlerhäufigkeit, hohe **V**erfügbarkeit, **S**icherheit und **W**irtschaftlichkeit (F/V/S/W) sowie deren Nachweis.

Aus obigem ergibt sich eines der beiden Anliegen der vorliegenden Arbeit:
Es soll eine Methodik vorstellt werden, mittels derer die F/V/S/W komplexer Kfz-Systeme in einem geschlossenen Ansatz modelliert, d.h. bereits während der Systementwicklung sowohl qualitativ wie auch quantitativ abgeschätzt werden können. Diese Methodik wird in Kap. 3 vorgestellt.

Bei Vorliegen einer quantitativen F/S/V/W-Abschätzung stellt sich unmittelbar die Frage, ob diese den Anforderungsspezifikationen an das System und somit an das Gesamtfahrzeug genügt. Auf die Problematik gesellschaftlich bzw. rechtlich akzeptierter F/V/S-Maßstäbe wird in Kap. 2 eingegangen.
Ein weiteres Anliegen dieser Arbeit ergibt sich aus der Annahme, daß die Anforderungsspezifikationen eines vorliegenden Systementwurfes hinsichtlich einer der obigen Systemparameter nicht erfüllt sind, weswegen eine Optimierung vorzunehmen ist. So liegt der Schluß nahe, sowohl die Fehlerhäufigkeit zu reduzieren, als auch die Verfügbarkeit und Sicherheit eines Systems zu erhöhen. Zwar werden in der Literatur perfektionistische Ansätze zur Vermeidung von Fehlern diskutiert, jedoch führen diese Konzepte zu immensen Anforderungen an die Systemkomponenten, was sich im Preis niederschlägt. Mit Blick auf die Wirtschaftlichkeit können Fehler während der Nutzungsdauer der Systeme innerhalb ihrer Komponenten nicht ausgeschlossen/vermieden werden.
Demzufolge muß man bemüht sein, einen fehlertoleranten Systementwurf vorzunehmen.
Die Voraussetzung zur Fehlertoleranz ist das Vermögen, Fehler zu erkennen, lokalisieren zu können und ihren Einfluß auf das System zu unterdrücken. Diese Voraussetzung wird im Begriff FELB/FDIR zusammengefaßt (**F**ehler**e**rkennung, **L**okalisation und **B**ehandlung/ **f**ault **d**etection, **i**solation and **r**ecovery). In diesem Sinne werden in den Kap. 2, 4 und 6 FELB-Konzepte vorgestellt. Abweichend von traditionellen Konzepten, die auf Drei- oder

Mehrkanaligkeit basieren, was den Systementwurf hinsichtlich Gewichtszuwachs, Platzbedarf und Wirtschaftlichkeit belastet, werden in dieser Arbeit funktionale bzw. analytische Redundanzkonzepte propagiert. Hierbei wird redundante Information auf der Basis mathematischer Modelle bzw. Schätzerstrukturen generiert, womit eine Reduzierung des Hardwareaufwandes für die FELB ermöglicht wird.
Aufgrund der Vorzüge gegenüber herkömmlicher Hardware-Redundanz werden diese Konzepte trotz eines erhöhten Softwareaufwandes oftmals als „intelligente“ FELB-Konzepte bezeichnet.
Da aber auch diese intelligenten FELB die Systementwicklungskosten und -zeit belasten, ist die wichtige Voraussetzung für die Einführung derartiger Konzepte in den Automobilsektor der Nachweis ihres Nutzens im Bereich Fehlerhäufigkeit, Verfügbarkeit, Wirtschaftlichkeit und vor allem Sicherheit.
Folglich werden die in Kap. 3 vorgestellten Methoden zur Bewertung der F/V/S/W der jeweiligen FELB-Konzepte verwandt. Blickrichtung ist hierbei das Erreichen der formulierten F/V/S/W-Maßstäbe. Diskrepanzen des Entwurfes zum jeweiligen Maßstab werden aufgezeigt und durch geeignete Mittel kompensiert. Ziel soll darüberhinaus sein zu untersuchen, welches Redundanzkonzept eine gleichzeitige Optimierung der Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit ermöglicht. Um obige Ausführungen transparent zu gestalten und den Praktikabilitätsnachweis der Methoden zur Bewertung der F/V/S/W zu erbringen, wurden die Methoden auf das Applikationsbeispiel eines zukünftigen Fahrdynamikregelungssystems **D**rive-**b**y-**W**ire (D-b-W) angewandt. Für dieses mit diversen Sensoren ausgestattete System wurden FELB-Konzepte entwickelt. Im Rahmen dieser Arbeit wird exemplarisch ein auf funktionaler Redundanz basierender FELB-Algorithmus hinsichtlich des erzielbaren F/V/S/W-Zuwachses bewertet. Es soll vorweggenommen werden, daß sich die Arbeit schwerpunktmäßig auf FELB zur Überwachung von Sensorfehlern konzentriert, da diese im Verbund mit den elektrischen Kontakten und Kabeln einen Anteil von 75% an der Gesamtfehlerhäufigkeit innerhalb elektronischer Kfz-Systeme aufweisen [Rat96].

Ein weiteres Anliegen der Arbeit ist die Motivierung des Lesers, die hier vorzustellenden Methoden der Zuverlässigkeits- bzw. Sicherheitstheorie für die Entwicklung seiner Systeme zu nutzen. Es werden Redundanzstrukturen präsentiert, mittels derer die Systemsicherheit erhöht werden kann, bei gleichzeitiger Aufrechterhaltung der Verfügbarkeit der Funktionalität und Minimierung der Fehlerhäufigkeit.
Wie sich in den Kap. 3 sowie 4 bis 6 zeigen wird, sind für die Bestimmung der quantitativen F/V/S-Aussage eines noch nicht im Feldeinsatz befindlichen Systems diverse Annahmen hinsichtlich der Zuverlässigkeits- bzw. Sicherheitsparameter zu treffen. Dies birgt zwangsläufig die Gefahr, über fehlerhafte oder unscharfe Annahmen, die Qualität der resultierenden Aussagen zu reduzieren. Durch die in den Kap. 5 und 6 durchzuführende „vergleichende“ Analyse verschiedener FELB-Konzepte bietet sich jedoch die Möglichkeit, die Auswirkungen der einzelnen Annahmen auf die F/V/S/W-Gesamtsystemaussage zu relativieren. Die einzelnen Annahmen verlieren bzgl. ihrer Unsicherheit an Einfluß.

Damit ist zusammenfassend folgender Nutzen der vorliegenden Arbeit zu nennen:
Im Rahmen dieser Arbeit wurde eine Analyse der Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit eines hochsicherheitsrelevanten Kfz-Systems vorgenommen.

- Zum Umfang der Arbeit gehört es, die für die Analyse des komplexen Kfz-Systems geeigneten Methoden vorzustellen. Hauptmerkmal ist hierbei die Möglichkeit der Generierung eines geschlossenen Modells zur gleichzeitigen Bewertung der F/V/S/W für Systeme, die sich noch nicht im Feldeinsatz befinden. Damit wird eine Abschätzung des zu erwartenden Feldverhaltens erzeugt. Sollte das Ergebnis der Analyse nicht akzeptabel erscheinen, kann der Systementwurf noch in der Entwicklungsphase optimiert werden.
- Wesentliche Voraussetzung und damit auch Anliegen der Arbeit ist das Greifbarmachen von F/V/S/W und somit die Möglichkeit zu schaffen, F/V/S/W-Maßstäbe zu formulieren, gegen die ein vorliegender Systementwurf geprüft werden kann.
- und Redundanzkonzepte vorzustellen, mittels derer sowohl die Optimierung der Fehlerhäufigkeit, wie auch Verfügbarkeit und Sicherheit eines Kfz-Systems bei gleichzeitiger Berücksichtigung der Kosten, des Platzes und Gewichtes gewährleistet werden können.
- sowie ihrer Auswirkungen hinsichtlich F/V/S/W neuerlich zu bewerten.

1.1 Stand der Technik

Da sich die Arbeit schwerpunktmäßig auf die F/V/S/W-Analyse elektronischer Kfz-Systeme, einschließlich der für sie entwickelten FELB-Konzepte beschränkt, werden die folgenden in Form von Unterabschnitten aufgeführten Werke als Stand der Technik verstanden.

1.1.1 Zustandsschätzerschemen zur Fehlererkennung, deren Zuverlässigkeit und Anwendung auf den spurgeführten Omnibus

Autor: Dirk van Schrick, Dissertationsschrift, Uni-GH-Duisburg [Van93]

Diese Dissertationsschrift diskutiert die Problematik der Sensorfehlererkennung basierend auf analytischen Redundanzkonzepten, die auf Kalman-Filter-Strukturen fußen. Den Kern der Arbeit stellt die Frage nach der Zuverlässigkeit derartiger Schätzer-Schemata, relativ zu Überwachungskonzepten basierend auf Hardware-Redundanz, dar. Diese Aussagen werden mittels Markov-Ketten-Modellierungen gewonnen.
Im Gegensatz zur vorliegenden Arbeit wurde in [Van93] jedoch nur die Frage der Fehlerhäufigkeit der zur Fehlererkennung erzeugten analytischen Redundanzkonzepte diskutiert. Hierbei bedient sich van Schrick diverser Näherungen, die im folgenden näher betrachtet werden:

- Wie bereits erwähnt, unterscheidet van Schrick nicht nach F/V/S, sondern beschränkt sich auf die Analyse der Fehlerhäufigkeit.
- Hinsichtlich der Fehlerhäufigkeit des FELB-Konzeptes wird der Algorithmus unabhängig von der Komplexität der analytischen Redundanz und der in sie einfließenden Sensorinformationen als „Task“ betrachtet. Diesem wird eine pauschale zeitinvariante Fehlerrate zugewiesen, die niedriger ist, als die der verwandten Sensoren, was unmittelbar die finale Aussage von v. Schrick erklärt, daß analytische Redundanzkonzepte „zuverlässiger“ sind, d.h. eine niedrigere Fehlerhäufigkeit aufweisen, als Hardware-Redundanz.
- Besonders kritisch erscheinen die beiden Annahmen, daß die Beobachtbarkeit der Fehlerphänomene innerhalb der analytischen Redundanzstrukturen permanent erfüllt ist bzw., daß sämtliche Eingangsgrößen des Kalman-Filter-basierten Schätzers fehlerfrei sind. Wie sich in Kap. 4 und 6 der vorliegenden Arbeit zeigt, liegen FELB-Schätzern mit geringen Modellierungsfehlern aufwendige Systemmodelle zugrunde, die ihrerseits auf

eine Vielzahl von Eingangsgrößen (Sensordaten) zurückgreifen. Ein Fehler innerhalb dieser Sensordaten kann jedoch zum Verlust der Beobachtbarkeit und somit zu Fehlinterpretation der FELB führen.

- Die Ausfallraten von Hardware-Komponenten entnimmt van Schrick [Kon77]. Für jede Komponente werden lediglich die beiden Zustände „fehlerfrei“ bzw. „ausgefallen“ angenommen. In der vorliegenden Arbeit wird nach Fehlerarten (Fehlermoden) der einzelnen Komponenten unterschieden. Erst diese Unterscheidung ermöglicht eine Differenzierung nach Fehlerhäufigkeit, Verfügbarkeit und Sicherheit des untersuchten Systems.
- V. Schrick modelliert die Markov-Ketten seiner analytischen Redundanzkonzepte in der Art, daß er von einer 100%igen Fehlererkennung ausgeht. Falschinterpretationen, wie sie in der vorliegenden Arbeit ausführlich diskutiert werden (siehe Fehler der FELB, Kap. 2 und Abschnitt 3.2) wurden in v. Schrick vernachlässigt, was nach Meinung des Autors für den Vergleich Hardware-/analytische-Redundanz eine nicht zulässige Vereinfachung darstellt.
- Da die FELB-Algorithmen nicht in der Detaillierung analysiert wurden, wie in Kap. 3, Bild 3.5 der vorliegenden Arbeit vorgeschlagen, werden die Ergebnisse aus van Schrick nicht vorbehaltlos geteilt.
- Sehr wichtig für den weiteren Verlauf der F/V/S/W-Beurteilung mittels Markov-Ketten ist die Aussage v. Schricks zur Gedächtnislosigkeit von Zustandsschätzerkonzepten. Gerade die für eine qualitativ hochwertige Fehlerlokalisation wichtigen Entscheiderschemata, wie der **G**eneralized **L**ikelihood-**R**atio-Test (GLR) [Pro88], greifen maßgeblich auf vergangene Sensorinformationen zurück. Diese „Historienauswertung“ widerspricht jedoch strenggenommen der Annahme konstanter Zustandsübergangsraten, wie sie für homogene Markov-Ketten zwingend sind. Van Schrick argumentiert jedoch aus Sicht des Autors zutreffend:

  „...daß das Gedächtnis von der zeitlichen Ausdehnung des Programms bzw. von den Zeitkonstanten des geregelten oder überwachten Systems abhängt. Im allgemeinen betragen diese Zeitkonstanten bis zu einigen Stunden, aber wegen der Tatsache, daß die für die F/V/S interessierenden Zeiträume im Bereich von Monaten oder Jahren liegen (siehe MTBF), kann das Ausfallverhalten von kontinuierlich laufenden Programmen und somit auch der FELB-Algorithmen annähernd gut durch eine Exponentialverteilung beschrieben werden.“
- Van Schrick geht davon aus, daß sämtliche Fehler stochastisch unabhängig voneinander sind. In diesem Sinne werden Störungen der Energieversorgung nicht betrachtet. Diese vereinfachende Annahme führt hinsichtlich der resultierenden Verfügbarkeits- bzw. Sicherheitsaussagen mitunter zu optimistischen Abschätzungen.
- On- und Offboard-Fehlerbehandlungen und die hierfür notwendigen Zeitspannen des Aufenthaltes in mitunter sicherheitskritischen Zuständen werden nicht betrachtet.

1.1.2 Weitere Werke

Mit Blick auf den Umstand, daß [Van93] aus Sicht des Autors den Stand der Technik auf dem die vorliegende Arbeit tangierenden Themengebiet am ehesten beschreibt, werden die folgenden Werke nur kurz diskutiert.

In [Sch73] wird die Sicherheit hardware-orientierter Vergleicherstrukturen (NvM-Systemen) bewertet. Hierfür werden die Aufenthaltswahrscheinlichkeiten in sicherheitsrelevanten Zuständen via Markov-Ketten bestimmt. Auf softwarebasierte FELB-Strukturen bzw. Onboard-Fehlerbehandlung und die Close-Loop-Betrachtung von FELB/Regelstrecke wird nicht eingegangen. Die in der vorliegenden Arbeit vorgenommene Unterscheidung nach Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit wird nicht berücksichtigt.
In [Kon77] wird zwar zwischen Zuverlässigkeit (Verfügbarkeit) und Sicherheit unterschieden, jedoch bezieht sich die dortige Betrachtung ausschließlich auf HW-Komponenten. Konakovsky vertritt die in der vorliegenden Arbeit widerlegte Ansicht, daß sämtliche Maßnahmen zur Steigerung der Zuverlässigkeit auch der Sicherheit zuträglich sind. Ähnlich wie in Kap. 3 der vorliegenden Arbeit für softwarebasierte FELB-Algorithmen, werden in [Kon77] für die betreffende Analyse hardwarebasierter Systeme geeignete Sicherheits- bzw. Zuverlässigkeitskenngrößen definiert.
In [Coz90] werden erstmalig die Methoden der Zuverlässigkeitstheorie, insbesondere der Wahrscheinlichkeitsrechnung auf ein Automobilsystem, hier ein Antiblockiersystem, angewandt. Wie bereits bei sämtlichen in diesem Abschnitt aufgeführten Werken beschränkt sich auch diese Arbeit auf die Analyse der HW-Komponenten. Im Gegensatz zu [Coz90] geht die vorliegende Arbeit ausführlich auf die Gewinnung bzw. den Ursprung der für die finale F/V/S/W-Aussage essentiellen Zuverlässigkeitskenngrößen ein.
Weitere Werke, so auch Veröffentlichungen des Autors bzw. im Zusammenhang mit dieser Arbeit erstellte Diplomarbeiten, sind Anhang A zu entnehmen.

1.2 Wissenschaftliche Erkenntnisse / Neuerungen hervorgehend aus der vorliegenden Arbeit

Im Rahmen der Einleitung wurde bereits der wesentliche Nutzen der vorliegenden Arbeit skizziert. An dieser Stelle sollen nochmals die gegenüber den in Abschnitt 1.1 aufgeführten Werken angestrebten Neuerungen erläutert werden.

- Über die in Abschnitt 1.1 aufgeführten Werke hinaus ist es, bedingt durch die Differenzierung nach verschiedenen Fehlerarten (Fehlermoden) der einzelnen Systemkomponenten möglich, Degraded Modes (Betriebszustände mit unterschiedlichen Leistungsmerkmalen, siehe Abschnitt 4.1) eines komplexen Kfz-Systems sowohl auf die Fehlerhäufigkeit, Verfügbarkeit wie auch Sicherheit hin zu untersuchen. Hilfreich ist hierbei das vorzustellende geschlossene Modell der F/V/S-Analyse, in das auch Wirtschaftlichkeitsaspekte integriert sind. Diese gleichzeitige, d.h. geschlossene Betrachtungsweise für F/V/S/W grenzt die vorliegende Arbeit ab.
- Neben der Betrachtung der Fehlerauswirkungen von Hardwarekomponenten können auch die Einflüsse der Fehlererkennungs-, Lokalisations- und Behandlungsalgorithmen in die Systemanalyse integriert werden.
- Bedingt durch den Umstand, daß in der vorliegenden Arbeit zwischen Soft- und Hard-Failures der einzelnen Systemkomponenten unterschieden wird, können Zeitspannen vom Auftreten des Fehlers bis zu seiner Erkennung, Lokalisation und Behandlung mitmodelliert werden. Hierdurch können Problemstellungen wie „Fehlalarm, Falschlokalisation“ etc. (siehe Kap. 3) modelliert werden. Dementsprechend lassen sich Aufenthaltswahrscheinlichkeiten in sicherheitsrelevanten oder anderen interessierenden Zuständen bestimmen.
- Grundvoraussetzung bzw. Motivator für die mitunter zeit- und kostenintensiven F/V/S-Analysen ist die Sicherheitsrelevanz des betrachteten Systems. Aufgrund dieser Sicherheitsrelevanz sollen resultierende F/V/S-Abschätzungen möglichst pessimistischer Natur sein. Aus diesem Grund werden im Gegensatz zu der in Abschnitt 1.1 aufgeführten Literatur in der vorliegenden Arbeit Common-Cause-Fehler mitbetrachtet. Im Sinne einer pessimistischen F/V/S/W-Abschätzung wird davon ausgegangen, daß Fehlfunktionen des Bordnetzes unmittelbar zum Ausfall des elektronischen Reglerbetriebs und damit zum Übergang in den mechanischen Notlauf führen (siehe Kap. 4 und 5). Weiterhin wird im Fehlerbaumtool die „Fast-Upper-Bound“-Näherung [Ste96] verwandt, die aufgrund der Vernachlässigung von Mintermen definierter Ordnung mitunter 10% höhere Fehlerwahrscheinlichkeiten liefert.
- Der Ausschluß von Fehlern innerhalb der Eingangsgrößen eines FELB-Schätzers bzw. das permanente Vorliegen der vollständigen Beobachtbarkeit des Fehlerphänomens, wie sie in v. Schrick angenommen werden, sind nach Meinung des Autors zu optimistisch bzw. nicht korrekt. Gerade mit Blick auf die Sicherheitsrelevanz zukünftiger X-by-Wire-Systeme wird in der vorliegenden Arbeit davon ausgegangen, daß der Fehler innerhalb einer beliebigen Eingangsgröße der FELB-Schätzer zum Versagen desselben führt. Untersuchungen über die Robustheit der Kalman-Filter der FELB und des D-b-W´s, wie auch der eigentlichen Reglerstrukturen, stehen noch aus.
- Wie bereits in [Van93] und [Sch73] erläutert, sind aufgrund der Zustandsraumexplosion nicht beliebig vielkomponentige bzw. komplexe Systeme mittels Markov-Ketten modellierbar. Um auch für diese Systeme eine F/V/S-Analyse durchführen zu können, werden in der vorliegenden Arbeit „hierarchische Modelle“ basierend auf einer Fusion von Markov-Ketten und Fehlerbäumen vorgestellt.
- Abweichend von den in Abschnitt 1.1 aufgeführten Werken, wird in der vorliegenden Arbeit ausführlich auf die Gewinnung bzw. den Ursprung der für die finale F/V/S/W-Aussage essentiellen Zuverlässigkeitskenngrößen eingegangen.

2 Grundlagen der Zuverlässigkeitstheorie

Im aktuellen Kapitel sollen die für den weiteren Verlauf der Arbeit erforderlichen Grundlagen der Zuverlässigkeitstheorie vermittelt werden.
Hierbei wird vorrangig Wert gelegt auf die klare Abgrenzung der Qualitätsmerkmale eines betrachteten Systems. Hierunter fallen Begriffe wie „Fehler, Ausfall, Beanstandung, Befundung, Fehlerhäufigkeit (-wahrscheinlichkeit), Zuverlässigkeit, Verfügbarkeit, Sicherheit, Risiko und Gefahr“, die im folgenden anhand eines überschaubaren Systembeispiels präzisiert werden.

2.1 Qualitätsmerkmale eines betrachteten Systems

Im vorliegenden Abschnitt sollen sämtliche für den weiteren Verlauf der Arbeit wichtigen Qualitätsmerkmale anhand eines Beispiels aus der Automobiltechnik vorgestellt und gegeneinander abgegrenzt werden. Aus Sicht des Autors wichtige Schlüsselworte sind in diesem Abschnitt kursiv und durch Unterstreichung hervorgehoben. Weitere Details, vor allem zu den mathematischen Grundlagen der Zuverlässigkeitstheorie und deren Abbildbarkeit auf den Automobilsektor, folgen in Kap. 3 und 4. In Anhang B finden sich Kurzdefinitionen der einzelnen Qualitätsmerkmale, die in [Din40041], [VDE08] und [Oco90] ausführlich diskutiert werden.

Systembeispiel:
Als Systembeispiel dient ein herkömmliches Bremssystem, das zusätzlich mit einem Anti-Blockier-System (ABS, [Bos95]) versehen ist. In Abschnitt 3.2.1.2. wird dieses Beispiel durch eine Zustandsraummodellierung mittels Markov-Ketten weiter veranschaulicht. Dort erfolgt auch die Diskussion der für die quantitative Bewertung der Zuverlässigkeit und Sicherheit wichtigen destruktiven und konstruktiven *Zuverlässigkeitskenngrößen*: Ausfallrate bzw. Fehlererkennungsrate, Reparaturrate.

***Zuverlässigkeit, Verfügbarkeit*:**

Gemäß [Din40041] ist die *Zuverlässigkeit* eines Systems definiert als die Beschaffenheit des Systems, bzgl. seiner Eignung, während einer vorgegebenen Zeitspanne bei vorgegebenen Anwendungsbedingungen die Zuverlässigkeitsforderung zu erfüllen.

Übertragen auf ein Bremssystem lautet die *Zuverlässigkeitsforderung*:

> Das Erreichen der vom System in Abhängigkeit des jeweiligen Kraftschlußpotentials maximal generierbaren Verzögerung. Als Zeitspanne wird im Automobil-Sektor die Zuverlässigkeit auf die mittlere Lebensdauer eines Pkw von 10 Jahren bezogen.

In Kap. 3 werden die wahrscheinlichkeitstheoretischen Konsequenzen der „Reparierbarkeit“ von Systemen detailliert. An dieser Stelle soll deshalb vorweggenommen werden, daß bei reparierbaren komplexen Systemen, wie Bremsanlagen, der Begriff der Zuverlässigkeit in den der *Verfügbarkeit* überführt wird. Aus diesem Grund soll im weiteren Verlauf der Arbeit vorrangig die Verfügbarkeit betrachtet werden.

***Fehler, Ausfall*:**

Fehler, d.h. nicht zulässige Abweichungen einer Systemkomponente von ihren geforderten Eigenschaften, die keinerlei Verstoß gegen obige System-Zuverlässigkeitsforderung bewirken, tragen somit auch nicht zur *Unzuverlässigkeit* des Bremssystems bei.

Hierunter fallen beispielsweise Fehler oder gar Ausfälle der Raddrehzahlsensoren. Derartige Defekte führen lediglich zur Abschaltung des Antiblockiersystems. Der Fahrer wird über eine Warnlampe über den Ausfall des in gewissen Bremssituationen hilfreichen Features „ABS“ informiert. Die *Auftrittshäufigkeit* eines derartigen Komponenten-Fehlers

kann mit einer gewissen bauteilespezifischen *Fehler- bzw. Ausfallwahrscheinlichkeit* oder -*rate* angegeben bzw. vorhergesagt werden.

Anmerkung: Gemäß Statistiken leitet der Fahrer innerhalb der Nutzungsdauer eines Fahrzeugs von 10 Jahren durchschnittlich 250.000 Bremsvorgänge ein, wovon nur 10.000 ABS-Bremsungen sind. In diesem Sinne sei die Möglichkeit eines gezielten Druckabbaus bzw. -wiederaufbaus an einem der Räder zur Vermeidung des Blockierens desselben als „Extra“ verstanden.

Bezogen auf das Gesamtsystem wird die Auftrittshäufigkeit eines beliebigen Fehlers durch die *Fehlerwahrscheinlichkeit* des Systems ausgedrückt.

Dahingegen tragen Fehler, die zu einem Verstoß gegen obige Zuverlässigkeitsforderung führen, zur Unzuverlässigkeit bzw. Unverfügbarkeit des Bremssystems bei. Hierunter fällt beispielsweise eine Leckage in einem der beiden Bremskreise, die zu einer Reduzierung der Bremsfähigkeit des Fahrzeugs führt. Dennoch kann ein derartiger Fehler nicht als *sicherheitsrelevant* bzw. *-kritisch* bezeichnet werden, da unabhängig vom Fehlerort (hinterer oder vorderer Bremskreis) weiterhin die gesetzlich geforderte Mindestverzögerung von 0,3g gewährleistet ist.

***Sicherheit*:**

Heutige Bremssysteme sind derart ausgelegt, daß ein einzelner Fehler (*Einfachfehler*) nicht zum Ausfall der Bremsanlage (Verlust der Mindestverzögerung) führen kann.

Diese Entwicklungsrichtlinie stellt gleichzeitig einen *Sicherheitsmaßstab* dar, an dem zukünftige Entwicklungen ungeachtet ihres Kundennutzens gemessen werden.

In Fortsetzung obigen Gedankens würde erst eine weitere Leckage im bisher funktionsfähigen Bremskreis sicherheitsrelevante Auswirkungen haben. In Abhängigkeit der Fehlerschwere würde nach einer gewissen Zeit im worst-case keine Verzögerung über das hydraulische Bremssystem erzeugbar sein. Bei dieser Leckage würde es sich jedoch um den zweiten Fehler innerhalb des Bremssystems handeln. Je nachdem, ob er zeitgleich mit dem ersten oder zeitlich versetzt auftritt, spricht man vom *Zweifach*- bzw. *Mehrfachfehler* oder *Folgefehler* innerhalb des Bremssystems.
Geht man davon aus, daß der zweite Fehler nicht durch den ersten ausgelöst wurde oder beide Fehler auf einen gemeinsamen Initiator zurückzuführen sind, spricht man von *stochastischer Unabhängigkeit* der Fehler. Die Auftretenswahrscheinlichkeit beider Fehler berechnet sich aus der Multiplikation der Auftretenswahrscheinlichkeiten der einzelnen Fehler, womit die Wahrscheinlichkeit für dieses Ereignis sehr klein gegenüber einem Einfachfehler ist. Vergleicht man die Aussagen zur „Zuverlässigkeit/Verfügbarkeit“ und „Sicherheit“, so ist festzustellen, daß der Zustand „sicherheitsrelevanter Fehler“, d.h. die Unsicherheit, eine Untermenge aller möglichen Fehler, wie auch der Unverfügbarkeit darstellt (siehe auch Bild 2.1).
Sind jedoch beide Leckagen auf eine gemeinsame Ursache zurückzuführen, spricht man von *Common-Cause-Fehlern (CCF)*. Es ist eines der vorrangigen Entwicklungsziele, CCF-Möglichkeiten konstruktiv auszuschließen.

Risiko/Gefahr:
Das oben beschriebene sicherheitsrelevante Szenario des Zweifachfehlers innerhalb der beiden Bremskreise darf jedoch nicht mit einer Verunfallung aufgrund obigen Fehlerszenarios bzw. der Auftretenswahrscheinlichkeit des Unfalls gleichgesetzt werden. Die in diesem Szenario inhärente *Gefahr* bzw. das *Risiko* der Verunfallung aufgrund des beschriebenen Zweifachfehlers hängt maßgeblich von dem zum Zeitpunkt des Auftretens bzw. des sich dem Fahrer Bemerkbarmachens des Fehlerszenarios ab. Will der Fahrer in diesem Moment aufgrund der Verkehrssituation eine massive Verzögerung herbeiführen, wird es vermutlich zu einem Auffahrunfall kommen, wenngleich auch hier die Möglichkeit

eines Ausweichmanövers besteht. Geringe Verzögerungen können jedoch bereits durch Ausnutzung des Motorschleppmoments bzw. durch Rollreibung der Reifen, Windwiderstand etc. aufgebracht werden.
Entdeckt der Fahrer den Fehler unmittelbar nach dem Startvorgang oder während des Parkiervorgangs, so ist die Wahrscheinlichkeit sehr hoch, daß der Fehler nicht zu einem Unfall mit schwerem Sach- oder gar Personenschaden führt. Grundsätzlich unterliegt die Zweifachfehlerbetrachtung der Annahme, daß der Fahrer auf den ersten Fehler des Bremsschlauchabrisses nicht mit dem *Aufsuchen der Werkstatt* reagiert bzw. reagieren kann. Es wird deutlich, daß auch *onboard*- und *offboard-Fehlerbehandlungsmechanismen*, unter dem Begriff *Reparaturmechanismen* zusammengefaßt, für die Sicherheit und Verfügbarkeit von großer Bedeutung sind.

***Kunden- und Werkstattbeanstandung , Befundung*:**
Sämtliche im vorliegenden Abschnitt bisher diskutierten Qualitätsmerkmale setzen das Vorliegen eines Fehlers bzw. Ausfalls einer Systemkomponente bzw. des Systems voraus.

Als *Kundenbeanstandungen* der Bremsanlage hingegen werden sämtliche durch den Endkunden in der Werkstatt artikulierten „Beschwerden“ bezeichnet, die dieser auf die Bremsanlage bezieht. Die Beanstandungshäufigkeit ist umgekehrt-proportional zur Kundenzufriedenheit, welche unmittelbar mit dem Marktanteil des Automobilisten zusammenhängt. Folglich ist das Werkstattpersonal angehalten, einen für die Kundenbeanstandung ursächlichen Fehler innerhalb des Bremssystems zu identifizieren und zu beheben. Aus Kostengründen, aber auch mit Blick auf die Bedeutung der Bremsanlage für die Fahrzeugsicherheit werden hierbei in aller Regel die potentiell fehlerhaften Bremssystem-Komponenten ausgetauscht und durch neue ersetzt. Aus Sicht des Automobilherstellers werden sämtliche getauschten Teile als *Werkstattbeanstandungen* bezeichnet.

Es sei angemerkt, daß Beanstandungen über die Begriffe der *Garantie*- und *Kulanzzeiträume* ebenfalls eine zeitliche Bindung haben. Erfolgt die Kundenbeanstandung innerhalb der Garantiezeit, werden dem Endkunden keinerlei Kosten in Rechnung gestellt.

Mit Blick auf die Sicherheitsrelevanz der Bremsanlage wird ein großer Anteil der getauschten Komponenten zur *Befundung* zum Zulieferer zurückgesandt. Ziel hierbei ist die Identifikation eines systematischen Fehlers bzw. einer Schwachstelle, die folglich ein unverzügliches Redesign der betreffenden Komponente zur Folge haben würde. Gleichzeitig dient die Identifikation des „Fehlerverursachers“ der Verteilung der angefallenen Werkstatt- und Materialkosten auf den Zulieferer und Automobilhersteller.

In der Regel werden hierzu die Befundungen in drei Klassen eingeordnet:

a) *Zuliefererverantwortung*: Es wurde ein Fehler festgestellt, der dem Zulieferer anzulasten ist. Meist weist somit die Komponente einen Herstellungsfehler auf.

b) *„Kunden“-Verantwortung*: Es wurde ein Fehler festgestellt, der dem Automobilhersteller oder dem Werkstattpersonal anzulasten ist. Hier sind vorrangig Montagefehler oder Zerstörungen beim Austausch in der Werkstatt ursächlich. Obige aus Sicht des Zulieferers entstandene Formulierung des „Kunden“ darf nicht verwechselt werden mit der des Endkunden (Fzg.-Halter). In aller Regel ist davon auszugehen, daß der Endkunde innerhalb der Garantie- und Kulanzzeit keinerlei Eingriffe an der Bremsanlage vornimmt. Erst mit zunehmendem Fahrzeugalter steigt die Häufigkeit von Werkstattbeanstandungen, die auf fehlerhafte Eingriffe des Endkunden, bis hin zum *Mißbrauch*, zurückzuführen sind.

c) *Kein Fehler feststellbar*: Diese Aussage ist nicht zwangsläufig gleichzusetzen mit der Feststellung, daß kein Fehler vorliegt. Vielmehr liefert die Befundung unter den gegebenen Umgebungsbedingungen und unter Verwendung der wirtschaftlich akzeptierten Prüfmittel keinen Befund.

Graphische Darstellung obiger Begrifflichkeiten

Die folgende Darstellung soll abschließend die Abhängigkeiten zwischen einigen der obigen Qualitätsmerkmale in einem graphischen Zusammenhang veranschaulichen.

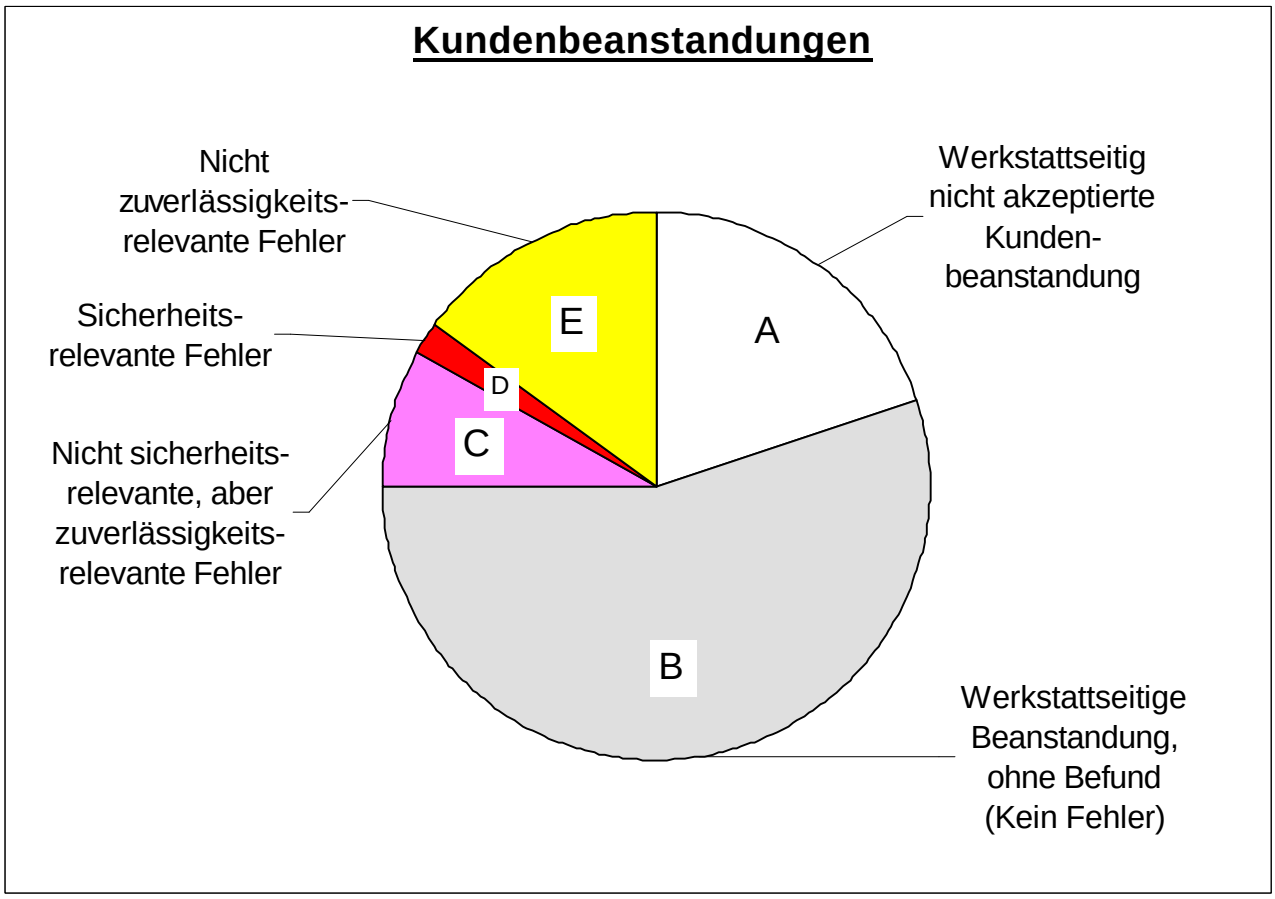


Bild 2.1: Qualitätsmerkmale als Anteile an den (End-) Kundenbeanstandungen

In Bild 2.1 umfassen die Tortenelemente A-E die Summe aller Kundenbeanstandungen. Tortenelemente B-E umfassen sämtliche werkstattseitig akzeptierten Beanstandungen, im folgenden als Werkstattbeanstandungen bezeichnet. Die Größe des Anteil A, der werkstattseitig nicht akzeptierten Kundenbeanstandungen, variiert von Automobilhersteller zu Automobilhersteller und hängt neben der Exklusivität des Fahrzeugs und der Qualitätsphilosophie des Hauses maßgeblich vom Fahrzeugalter bei Eintreffen in der Werkstatt ab.
Durch die Größe des Tortensegmentes B soll die Dominanz des Verhältnisses zwischen den werkstattseitigen Beanstandungen und den Befundungen verdeutlicht werden. Weit weniger als 50% der Werkstattbeanstandungen können heute auf eindeutig befundbare Fehler zurückgeführt werden.
Wenngleich die Summe der Anteile der Tortensegmente C-E auf einen Fehler zurückzuführen sind, sind jedoch nur die Anteile der Elemente C und D zuverlässigkeitsrelevant.
Ferner sind lediglich die im Tortensegment D zusammengefaßten Fehler sicherheitsrelevanter Natur. Durch die Größe dieses Segments soll nochmals verdeutlicht werden, daß der geringste Anteil der Kundenbeanstandungen, aber auch der befundeten Fehler, sicherheitsrelevanter Natur ist.
Darüberhinaus mündet nur ein Bruchteil dieser sicherheitsrelevanten Fehler in für den Kunden gefährliche Situationen oder birgt das Risiko der Verunfallung.

Abschließend soll auf das Potential einer verbesserten Fzg.-Onboard- und Offboard-Diagnose hingewiesen werden. Da jede in den Anteilen B-E zusammengefaßte Werkstattbeanstandung in einem Tausch mündet, fallen hierdurch in der Garantie- und Kulanzzeit beim Automobilhersteller und dem Zulieferer erhebliche Kosten an.
Durch die Verbesserung der Onboard- und Offboard-Diagnose ließ sich sowohl Anteil B minimieren, als auch der für die Kundenzufriedenheit maßgebliche Anteil A.

Weitere wichtige Begriffe der Zuverlässigkeitstheorie werden in den Abschnitten 2.2 bis 2.4 diskutiert und sind dort ebenfalls unterstrichen und kursiv hervorgehoben. Die mathematischen Hintergründe werden in Kap. 3 vorgestellt.

2.2 Zuverlässigkeits- / Sicherheitsmaßstab, Maßnahmen zur Steigerung dieser Qualitätsmerkmale

Im Rahmen der Einleitung wurde bereits erläutert, welches Potential in der Reduzierung der Fehler des Fahrers steckt. Es soll hier nicht weiter auf den Aspekt der Entmündigung des Fahrzeugführers (Kunden) eingegangen werden. In diesem Zusammenhang müßte hinterfragt werden, inwieweit es akzeptabel ist, durch Einführung von X-by-Wire-Systemen die Unfallhäufigkeit mit tödlichem Ausgang von jährlich 8.000 auf 1.000 zu senken, wenn die verbleibenden Unfalltoten auf ein Versagen des X-by-Wire-Systems zurückzuführen wären. Damit gerät man in den Bereich ethischer Fragestellungen, die in dieser Arbeit nicht beantwortet werden können. Dennoch soll die Frage des Zuverlässigkeits- und Sicherheitsziels bzw. –maßstabes diskutiert werden.

2.2.1 Zuverlässigkeits- / Sicherheitsmaßstab

Es sei vorweggenommen, daß es keine absolute Sicherheit geben kann. So ist sogar trotz der in der zivilen Luftfahrt eingesetzten Sicherheitskonzepte, wie eine 2v3-Geschwindigkeitserfassung, die im heutigen Automobilbau wirtschaftlich untragbar erscheint, in jüngster Vergangenheit gerade aufgrund eines Ausfalls dieses Sicherheitskonzeptes ein tragisches Unglück ausgelöst worden. Dennoch oder gerade in Anbetracht derartiger Unglücke stellt sich die Frage, welche Zuverlässigkeit bzw. Sicherheit ein System aufweisen muß.
Wie anhand des Beispiels aus Abschnitt 2.1 deutlich wurde, ist die Gefahr bzw. das Risiko der Verunfallung nicht durch Angabe einer Fehlerwahrscheinlichkeit bestimmbar. Vielmehr wird das Risiko im allgemeinen nicht quantitativ erfaßt. In [Din19250] wird das Risiko als Produkt aus der zu erwartenden Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und dem beim Ereigniseintritt zu erwartenden Schadensausmaß beschrieben.
Diese Vorgehensweise wird für die Entwicklung und Bewertung eines komplexen Kfz-Systems vom Autor nicht als zielführend betrachtet. So heißt es auch in der Literatur, daß technische Systeme meist auf ihre Sicherheit bzw. Unsicherheit, nicht jedoch auf ihre Gefahr hin untersucht werden. Letztere Vorgehensweise kann heute vom Automobilhersteller allein aus Sicht der *Produkthaftung* nicht verfolgt werden, da er somit ein Produkt vermarkten würde, wissend um die Verunfallungsgefahr, die von dem Produkt ausgeht.
Auch aus ethischer Sicht kann es dem Automobil-Hersteller nicht zugemutet werden, eine anzustrebende bzw. *akzeptierbare Verunfallungswahrscheinlichkeit* des Kunden aufgrund des Fehlers bzw. Versagens des Produktes zu benennen. Eine derartig kritische Aussage könnte allenfalls vom *Gesetzgeber* initiiert werden. Doch heißt es zum Thema Sicherheit des Fahrzeugs im *Paragraphen 30* der „Straßenverkehrszulassungsordnung (StVZO)“ lediglich, daß das Fahrzeug sicher sein muß. Was sich explizit hinter dieser Forderung verbergen soll, ist der Quelle nicht zu entnehmen.

Für sicherheitsrelevante Systeme wie Lenk- und Bremsanlagen müssen in Deutschland zur Erlangung der „Allgemeinen Betriebserlaubnis (ABE)“ die Vorschriften des §38 der (StVZO) erfüllt sein [Ste96]. So heißt es technisch vage formuliert: „ein leichtes und sicheres Lenken muß gewährleistet sein, bei Ausfall der Lenkhilfe (Servounterstützung) muß die Lenkbarkeit erhalten bleiben.“ Was hierbei „sicheres Lenken“ heißt, ist nicht detailliert. Weitere Ausführungen hierzu finden sich in [Ste96, Kap6.1, Seite 48-54]

Ein Sicherheits- und Zuverlässigkeitsmaßstab im Sinne einer zu erreichenden Wahrscheinlichkeit bzw. Häufigkeit wird im Automobilsektor, anders als in *der zivilen und militärischen Luftfahrt* nicht genannt.

Die Frage, warum der Gesetzgeber bisher eine derartige Angabe nicht tätigte, läßt sich durch die folgende Rechnung beantworten:

> In der zivilen Luftfahrt wird eine *Ausfallrate mit Folge des Verlustes „vieler Menschenleben“ von 10^{-9}/h akzeptiert, in der militärischen Luftfahrt sogar 10^{-7}/h*. Betrachtet man die äußerst geringe Zahl von weltweit nur etwa 12.000 kommerziellen, Personen befördernden Flugzeugen, so wird deutlich, daß obige geforderten bzw. akzeptierten Ausfallraten innerhalb der akkumulierten Lebensdauer sämtlicher Flugzeuge zu keinem akzeptierten „catastrophic event“ führen. Damit entsteht durch den geforderten bzw. akzeptierten „Zuverlässigkeits-Maßstab“ der Luftfahrt kein ethischer Konflikt. Leider wird jedoch aus den tragischen Flugzeugabstürzen bzw. Unglücken der Vergangenheit deutlich, daß obige Gesamtsystemfehlerrate eher akademischer Natur ist. Es muß jedoch auch angemerkt werden, daß aufgrund der geringen Anzahl von Flugzeugen die Verletzung bzw. Einhaltung des Zuverlässigkeits- bzw. Sicherheitsmaßstabes statistischer Natur mit wirtschaftlich vertretbaren Mitteln nicht nachweisbar ist.

Würde man obige Zuverlässigkeits- bzw. Sicherheitsanforderung auf den Automobilsektor übertragen, so ergäbe sich folgende Rechnung:

> Allein in Deutschland sind derzeit ca. 40 Mio. Pkw zugelassen. Geht man von der durchschnittlichen Nutzungsdauer von jährlich 300 Stunden bzw. einer mittleren Lebensdauer von 10 Jahren aus, so würde die geforderte Ausfallrate der zivilen Luftfahrt zu jährlich 12 akzeptierten Pkw-Unfällen mit tödlichem Ausgang führen.

Anhand dieser Rechnung ist leicht nachvollziehbar, daß eine derartige Forderung weder vom Gesetzgeber, der Gesellschaft, noch dem Automobilhersteller akzeptiert werden kann. Würde man, wie in der Luftfahrt eine Ausfallrate fordern, die innerhalb der Lebensdauer der Fahrzeuge zu keinem catastrophic-event führen würde, so resultieren hieraus Zuverlässigkeits- bzw. Sicherheitsmaßstäbe, die deutlich strenger wären, als die der Luftfahrt. Das Dilemma wird offenkundig, wenn man sich verdeutlicht, daß Sicherheits- und Zuverlässigkeitszuwächse heute meist nur mit erheblichem finanziellen Aufwand erzielbar sind, ein Pkw von den Entwicklungs- und Produktionskosten aber deutlich günstiger sein muß, als ein Flugzeug.

Mit Blick auf obige Ausführungen ist nachvollziehbar, warum bis heute weder Gesetzgeber noch Automobilhersteller in der Lage waren, einen quantitativen Zuverlässigkeits- bzw. Sicherheitsmaßstab zu benennen. Vielmehr orientiert sich die *Entwicklung zukünftiger Kfz-Systeme meist am Maßstab der Vorgängermodelle,* d.*h. es werden Relativ-Forderungen getätigt*. So wird man bestrebt sein, ein zukünftiges Bremssystem hinsichtlich seiner Funktionalität, Fehlerwahrscheinlichkeit, Zuverlässigkeit, Sicherheit und „Gefährdungswahrscheinlichkeit“ ***mindestens*** *genauso gut zu konzipieren, wie das Vorgängermodell*. Hier wird der Parameter Schadensschwere [DIN19250] in beiden Systemen gleich sein (die Wahrscheinlichkeit nach einer unübersichtlichen Kurve auf einen Stau zu treffen und aufgrund dessen das Fahrzeug verzögern zu wollen, ist unabhängig vom jeweiligen Bremssystem beim Vorgänger- wie auch Folgemodell als gleich anzusetzen).

In diesem Sinne liegt das Hauptaugenmerk der vorliegenden Arbeit auf der Präsentation bzw. Entwicklung von Methoden, die eine vergleichende Zuverlässigkeits- und Sicherheits-Analyse ähnlicher Systeme bzw. unterschiedlicher Systemkonzepte ermöglichen.

Mit Blick auf die Notwendigkeit, daß das zukünftige System den Maßstäben genügen muß, die durch Vorgänger gesetzt wurden, sind auch die folgende Forderungen zu erfüllen:

In [VDI88] heißt es zu den Schutzzielen in der Kfz-Elektronik:

- Gefährliche Einfachfehler müssen ausgeschlossen sein. Bleibt ein Einfachfehler unerkannt, so darf ein nachfolgend eintretender Fehler nicht zu einem gefährlichen Zustand führen.
- Jeder gefährliche Fehler muß erkannt werden und zu einer Schutzaktion führen, so daß zu keiner Zeit der Fehler eine gefährliche Auswirkung auf das Fahrzeug, Fahrzeug-Teilsysteme, Insassen oder andere Verkehrsteilnehmer hat.
- Die Funktionsbereitschaft des Fahrzeugsystems ist kontinuierlich und selbsttätig zu überwachen. Die Überwachungseinrichtungen selbst dürfen nicht durch Fehler unbemerkt ausfallen.
- Alle erkannten Fehler sind in einem Diagnosegerät abzulegen. Sofern sie eine Aktion des Fahrzeugführers (z.B. Aufsuchen der Werkstatt) erfordern, sind sie optisch und/oder akustisch anzuzeigen.

2.2.2 Maßnahmen zur Steigerung der Verfügbarkeit und Sicherheit

Dem Beispiel aus Abschnitt 2.1 ist zu entnehmen, daß die dem Oberbegriff der Qualität zuzuordnenden Begriffe Verfügbarkeit und Sicherheit voneinander abgrenzbar sind, jedoch nicht unkorreliert oder gar orthogonal zueinander sind. So wird man in Kap. 6 sehen, daß eine Reduzierung der Reparaturzeiten zu einer Erhöhung der Verfügbarkeit führt, die Fehlerwahrscheinlichkeit jedoch nicht nennenswert beeinflußt. Andererseits könnte eine „Vergoldung“ des Gesamtsystems sowohl die Sicherheit, Verfügbarkeit wie auch Fehlerwahrscheinlichkeit verbessern. Jedoch würde der resultierende Kaufpreis vom Kunden vermutlich nicht akzeptiert. Bemühungen, ein Fahrzeug auf die Lebensdauer des Benutzers oder gar noch länger hin auszulegen, sind bisher nicht in Massenproduktion überführt worden.
Auch das Bestreben, ein System mit so wenigen Komponenten wie möglich aufzubauen, ist nicht zwangsläufig zielführend. Zwar wird mit abnehmender Komponentenanzahl die Fehlerwahrscheinlichkeit abnehmen, jedoch steigt die Wahrscheinlichkeit, daß gefährliche Fehler nicht erkannt werden können (Abnahme der Sicherheit). Genau diese Problematik wird in Kap. 5 und 6 anhand des Vergleichs der Sicherheit des Minimal-Systems und des erweiterten Systementwurfs verdeutlicht.
Kehrt man zum Beispiel des Bremssystems zurück, so läßt sich, abgesehen von der Einführung von Verkehrsleitsystemen, aus Sicht des „eigenen“ Fahrzeugs die Gefährdungswahrscheinlichkeit nur über die Senkung der Auftretenswahrscheinlichkeit der sicherheitsrelevanten Fehler minimieren. **Aus diesem Grund beschränkt sich die vorliegende Arbeit im wesentlichen auf die Angabe der drei Qualitätsparameter Fehlerwahrscheinlichkeit, (Un-)Verfügbarkeit und (Un-)Sicherheit**. Weiterhin wichtig ist, insbesondere mit Blick auf die Realisierungschancen eines Nachfolgermodells, der Parameter ***Wirtschaftlichkeit***. Es ist transparent, daß Fehlerwahrscheinlichkeit, Verfügbarkeit und Sicherheit des Nachfolgemodells nicht beliebig optimiert werden können. So ist beispielsweise die Verwendung vergoldeter Kontakte zur Steigerung der Zuverlässigkeit mit einem Anstieg der Kosten verbunden. Der Einsatz derartiger Maßnahmen muß gezielt vorgenommen werden. Am effektivsten sind derartige Maßnahmen dort einzusetzen, wo sie sowohl der Reduzierung der Fehlerwahrscheinlichkeit, als auch der Erhöhung der Verfügbarkeit und Sicherheit des

Systems dienen. Diese als „*kritische Pfade*“ bezeichneten zentralen Stellen in einem möglichst frühen Entwicklungsstadium eines zukünftigen Systems zu finden, ist ein wesentliches Anliegen des „Zuverlässigkeitsingenieurs“.

Modell zur geschlossenen Analyse der F/V/S/W
Eine wesentliche Voraussetzung für das Finden des Optimums aus **F**ehlerwahrscheinlichkeit, **V**erfügbarkeit, **S**icherheit und **W**irtschaftlichkeit (F/V/S/W) bzw. der kritischen Pfade ist es, die oben anhand kleiner Beispiele aufgezeigten Wechselwirkungen zwischen den vier Parametern in einem geschlossenen Modell analysieren zu können. Genau hierbei helfen die in Kap. 3 dieser Arbeit vorzustellenden Methoden zur geschlossenen Modellierung und damit Bewertung der F/V/S/W eines komplexen Kfz-Systems.

Optimierung der F/V/S/W
In einem zweiten Schritt dienen die anschließend applizierbaren *FELB-Algorithmen* (siehe Abschnitt 2.3), basierend auf HW-einsparenden *funktionalen bzw. analytischen Redundanzkonzepten*, der Optimierung der F/V/S/W.

Sicherer Zustand, Rückfallebene, Notlauf
Eine weitere aus [VDI88] ableitbare Forderung lautet:

> Das Fahrzeug bzw. betrachtete System ist anschließend an die Erkennung des gefährlichen Einfachfehlers in den für Mensch, wie auch System *sicheren Zustand* zu überführen.

Im Falle des ABS-Raddrehzahlfühlers (Abschnitt 2.1) wird der Fehler zuverlässig erkannt und das System in den sicheren Zustand „rein hydromechanischer Bremsbetrieb bei voller Bremsfähigkeit ohne ABS-Feature“ überführt. Dieser sichere Zustand wird auch als mechanische *Rückfallebene (RFE)* bzw. etwas überspitzt als „*Notlauf*“ bezeichnet.

2.2.3 F/V/S-Maßstab des Applikationsbeispiels D-b-W

Aus obigen Unterabschnitten läßt sich ableiten, daß die Gefährdungswahrscheinlichkeit durch Verunfallung in einem zukünftigen System wie D-b-W mit einem akzeptierten System verglichen werden muß. Weiterhin sind die in Abschnitt 2.2.1 und 2.2.2 aufgeführten Forderungen aus [VDI88] zu erfüllen.

Garantie-Statistiken eines in Serie befindlichen Systems könnten einen Maßstab für das neu zu entwickelnde System darstellen. Mit Blick auf die Vertraulichkeit derartiger Daten soll in der vorliegenden Arbeit zur Veranschaulichung der Vorgehensweise eine andere Strategie gewählt werden. In Kap. 5 erfolgt die F/V/S/W-Analyse des in Kap. 4 vorzustellenden Minimal-Entwurfs des D-b-W-Systems. Diese Ergebnisse dienen als F/V/S-Maßstab für den in Kap. 6 vorzustellenden und zu bewertenden „erweiterten System-Entwurf“.
In obiger vergleichender Analyse verschiedener Systemkonzepte mit dem Ziel die optimale Konfiguration zu bestimmen, liegt ein weiterer Vorzug der in dieser Arbeit propagierten geschlossenen quantitativen Fehlerwahrscheinlichkeits-/Verfügbarkeits-/Sicherheits- und Wirtschaftlichkeits-Analyse.

2.3 Fehlererkennung, -Lokalisation und -Behandlung (FELB)

In Abschnitt 2.2 wurde deutlich, daß die Notwendigkeit besteht, sicherheitsrelevante Systeme mit der Fähigkeit auszustatten, gefährliche Einfachfehler zuverlässig erkennen zu können und deren schädlichen Einfluß auf das Systemverhalten zu unterbinden. Zwar bestünde auch die Möglichkeit, die Systemsicherheit zu gewährleisten, indem Fehler ausgeschlossen werden, jedoch kann diese in der Literatur als „perfektionistischer Ansatz" bezeichnete Vorgehensweise für das dem Kostendruck unterliegende Massenprodukt Automobil nur in den seltensten Fällen in die Praxis umgesetzt werden.
Obige unter dem Begriff FELB, d.h. ***F**ehler**e**rkennung, -**L**okalisation und -**B**ehandlung*, zusammengefaßten Strategien zur Erhöhung der Systemsicherheit und -verfügbarkeit fallen unter den Oberbegriff der Fehlertoleranz bzw. Fehlersicherheit eines Systems [Vog93].
In der Luft- und Raumfahrt bzw. der Kraftwerkstechnik, wo hohe Ansprüche an die Sicherheit bzw. Verfügbarkeit des Systems existieren, bei relativer Freiheit hinsichtlich der Kostensituation, führen die meist hardware-basierten FELB-Konzepte zu einer drastischen Erhöhung der Systemkomplexität und somit Erhöhung der Fehlerwahrscheinlichkeit. Um diesem Dilemma zu entgehen, werden in dieser Arbeit schwerpunktmäßig FELB-Konzepte basierend auf funktionaler bzw. analytischer Redundanz verwandt. Details hierzu folgen in den jeweiligen Unterabschnitten zur Fehlererkennung, -Lokalisation und -Behandlung. Auf die in der Literatur häufig anzutreffende Unterscheidung nach heißer, kalter und warmer Redundanz soll hier mit Verweis auf [Ric88] bewußt verzichtet werden.

Damit sind die weiteren Abschnitte dieses Kapitels wie auch die Kap. 4, 5 und 6 von den Fragen geleitet:

a) **Wie stellt man sicher, daß das Vorliegen eines Fehlers erkennbar, die Fehlerquelle lokalisierbar und im Sinne der Sicherheit und Verfügbarkeit behandelbar ist?**
b) **Welche Auswirkungen haben diese Maßnahmen auf die Gesamtsystem-F/V/S/W?**
c) **Welche zusätzlichen Fehlermöglichkeiten werden über die FELB in das System hineindesigned?**
d) **Wie wirken sich wiederum diese Fehler auf die Gesamtsystem F/V/S/W aus?**

Es ist zu betonen, daß die in der vorliegenden Arbeit vorzustellenden FELB-Konzepte für die im System D-b-W enthaltenen sicherheitskritischen Sensoren zur Erfassung der Fahrdynamik entwickelt wurden. Grund für die Beschränkung auf die Sensorik ist die Garantie- und Kulanzstatistiken zu entnehmende Dominanz von Sensorfehlern bzw. diesen zuordenbare Kabel- und Kontaktfehler.
Weitere FELB-Konzepte sind [Ben97, Sti95, Van93] zu entnehmen.

2.3.1 Fehlererkennung basierend auf Redundanzkonzepten und Eigenüberprüfung

Um Sensorfehler erkennen zu können, bietet sich das in der Literatur als Zweikanaligkeit bezeichnete Installieren zweier gleicher oder ähnlicher Sensoren zur Erfassung der gleichen Meßgröße an. Der als 1v2-Voting bezeichnete Vergleich beider Ergebnisse läßt Einfachfehler innerhalb der Anordnung im Sinne einer Diskrepanz beider Ergebnisse zuverlässig erkennen.
Im Sinne einer Fehlerbehandlung könnte das auf die Sensordaten zurückgreifende System abgeschaltet werden. Die der Systemsicherheit zuträgliche Möglichkeit, den Fehler zu erkennen und das System anschließend abzuschalten, wird auch als Fail-Safe-Eigenschaft bezeichnet.

Im weiteren Verlauf der Arbeit soll zwischen der Fehlererkennung durch Eigenüberprüfung und durch Fremdüberprüfung unterschieden werden:

a) Eigenüberprüfung: Das Verhalten einer Hardwarekomponente oder einer Funktion wird mit seinem Sollverhalten verglichen (Eigenüberprüfung), wobei das Sollverhalten zweifelsfrei bekannt sein muß. Aufgrund letzterer Einschränkung wird diese Methode meist nur zur Erkennung größerer Abweichungen (siehe Hardfailure-Erkennung, Kap. 4) vom Sollverhalten verwandt. Diese Form der Fehlererkennung führt gleichzeitig zur Lokalisation der Fehlerquelle. Eine Möglichkeit auch Softfailures durch Eigenüberprüfung zu identifizieren, bietet der Selbsttest durch Eigenanregung, wie er in Kap. 4 anhand des Gierratensensors erläutert wird.

b) Fremdüberprüfung: Eine Fehlfunktion bzw. der Ausfall einer Komponente wird durch den Vergleich mit einer Komponente gleichen Sollverhaltens erkannt. Hierbei ist wiederum zu unterscheiden nach dem Ursprung bzw. dem Zustandekommen der für den Vergleich benötigten Information.

   b1) Als zweikanalige *HW-Redundanz* wird das Vorhandensein zweier gleicher bzw. gleichartiger physikalischer Kanäle bezeichnet. Der simple Vergleich der beiden Ausgangssignale läßt einen Einfachfehler in einem der Kanäle erkennen.

   b2) Fußt die für die Fehlererkennung eines HW-Kanals benötigte „Vergleichsinformation“ auf einem mathematischen Modell, wie beispielsweise einfachen kinematischen Beziehungen, so spricht man von *funktionaler Redundanz*.

   b3) Reichen obige einfachen Modelle nicht mehr aus, besteht die Möglichkeit, die für den Vergleich nötige Information durch eine Schätzerstruktur zu prädizieren. Diese Schätzgröße wird als *analytische Redundanz* des zu überwachenden HW-Kanals bezeichnet.

In Anhang D findet sich eine Auflistung von Vorzügen und Defiziten der einzelnen Fehlererkennungsstrategien. Weitere Details zu HW- und anderen Redundanzkonzepten finden sich in [Van93, DeL90].

2.3.2 Fehlerlokalisation

Der reine Vergleich zweier Informationen zum Zwecke des Erkennens einer Abweichung und damit eines Fehlers impliziert meist noch nicht die eindeutige Lokalisation der fehlerhaften Komponente.
Innerhalb eines 2-kanaligen Sensorsystems, wie es in Abschnitt 2.3.1 beschrieben wurde, können nur Hardfailures (Verlassen des Meßbereichs, unplausibler Signalverlauf) dem fehlerhaften Sensor zugeordnet werden. Jedoch ist diese Fehlerlokalisation Voraussetzung dafür, durch Wegschalten des fehlerhaften Sensors, weiterhin auf die korrekte Sensorinformation zurückgreifen zu können. Diese Systemeigenschaft, auf einen Fehler in der Art zu reagieren, daß er keinen Einfluß auf das Systemverhalten hat und das System weiterhin aktiv bleiben kann, wird als Fehlertoleranz bezeichnet.

Damit ist die Fehlerlokalisation als wesentliche Voraussetzung für die Fehlertoleranz im Sinne der Aufrechterhaltung der Funktionalität des sicherheitsrelevanten Systems D-b-W zwingend erforderlich.
Eine in der Luft- und Raumfahrt verbreitete Strategie basiert auf der Dreikanaligkeit sicherheitsrelevanter Komponenten, wodurch unter Voraussetzung von Einfachfehlern durch ein Mehrheitsvoting die fehlerhafte Komponente lokalisiert werden kann und die

korrekten Sensoren als fehlersicheres Sensorsystem weiterverwendet werden können. Diese Vorgehensweise kann im Automobilsektor nur eingeschränkt akzeptiert werden, da sie mit einem nicht tolerierbaren Zuwachs an Kosten, Gewicht und Platzbedarf verbunden ist.
Aus diesem Grund gilt es, geeignete Strategien zu finden, Einfachfehler auch ohne aufwendige Dreikanalstrukturen zuverlässig lokalisieren zu können.

2.3.3 Fehlerbehandlung

Grundsätzlich sind die folgenden beiden Arten der Fehlerbehandlung zu unterscheiden:

A) Die Überführung in einen hinsichtlich der Funktionalität möglicherweise degradierten, in jedem Fall jedoch gegenüber dem ursprünglichen Systemzustand veränderten Zustand (error compensation). Der Schwerpunkt der vorliegen Arbeit liegt im Bereich dieser Fehlerbehandlungsstrategie. Ein typischer Vertreter dieser Klasse ist das in Abschnitt 2.3.2 bereits beschriebene traditionelle 2v3-Sensorsystem, welches im Rahmen der Fehlerbehandlung in ein 2v2-System überführt werden kann, womit es hinsichtlich Einfachfehlern von einem fehlertoleranten in ein fehlersicheres System überführt werden kann.

B) Dennoch soll auch die error recovery im weiteren Verlauf der Arbeit mitbetrachtet werden. Hierbei handelt es sich um die Rückführung in den ursprünglichen Systemzustand (error recovery). So wird das Fahrzeug bzw. das fehlerhafte System und seine Komponenten im Rahmen einer Reparatur in der Werkstatt (offboard-Fehlerbehandlung) näherungsweise in einen „Neuzustand“ überführt.

2.3.4 Grundsätzliche Überlegungen zur Erzeugung einer FELB

In [Mah94], [Sti95], [Ben97] und [Van93] finden sich diverse FELB-Schemata zur Überwachung von Sensorfehlern in Kfz-Applikationen. Bei der Entwicklung funktionaler bzw. analytischer Redundanzen ist kritisch anzumerken, daß die diesen zugrundeliegenden mathematischen Modelle stark applikationsabhängig sind. Für die spezielle Anwendung ist daher die Tauglichkeit bzw. das Vorhandensein entsprechender Modelle zu überprüfen.

Für die Entwicklung einer FELB sind folgende Aspekte zu berücksichtigen:

1. Bestimmung der Struktur des zu analysierenden Systems:
   Zu überwachende Meßgröße(n), deren Anzahl, Typ und erwünschter Redundanzgrad
2. Formulierung geeigneter Module (Vereinfachungen)
   Beispielsweise die Zusammenfassung von Meßwertaufnehmer, A/D-, D/A-Wandler, Kabel, Kontakten zum Modul „Sensor“. Derartige Modularisierungen reduzieren die Komplexität des F/V/S/W-Modelles (siehe Abschnitt 3.2, 3.3 und Kap. 4)
3. Festlegung eines geeigneten Modells (Struktur, Ordnung, Typ und Genauigkeit)
   3a: Zu überwachende System-Zustände etc.
   3b: Identifikation eines geeigneten Überwachungsschemas (funktionale Red. / Schätzer, d.h. Beobachter, Kalman-Filter, Filter-Bank etc.)
   - Struktur, Ordnung, Anzahl der Messungen, „Opferzustände“, Anzahl der Schätzer und Entwurfsmethode

   3c: Identifikation für die Fehlererkennung bzw. -lokalisation geeigneter Residuen, d.h. die Anzahl von Merkmalen, die innerhalb des jeweiligen Tests positiv ausfallen müssen, damit der Fehler erkannt werden soll bzw. bevor die Funktion als korrekt befunden werden soll:
   - Anzahl, Bildungsgesetz, Abhängigkeiten, Auswertungsmethode (GLR, etc.)

- Schwellwertbildung, d.h. Festlegung von zeitvarianten oder -invarianten Schwellwerten, deren Überschreitung als Fehler bzw. Fehlerfreiheit zu interpretieren ist. Die Schwellwerte beeinflussen die Fehlalarm- und Mißalarmraten. Zu hohe Schwellwerte verursachen eine höhere Rate an Mißalarm. Zu niedrige Schwellwerte verursachen häufige Fehlalarme. Beides beeinflußt also unmittelbar die Zuverlässigkeit des Gesamtsystems. Die Zuverlässigkeit des Gesamtsystems ist somit abhängig von der Wahl der Schwellwerte der Fehlererkennungs-, -lokalisations- und -behandlungslogik.

3d: Berücksichtigung des Rechenzeitaufwandes der FELB, der Frequenz mit der die unterschiedlichen Fehlererkennungs- bzw. -lokalisationstests durchzuführen sind, Zeitanforderung, Rechnersystem, Robustheit der FELB gegen Modellierungsfehler etc.

3e: Untersuchung der Robustheit der FELB gegenüber anderen als der zu überwachenden Fehlerphänomene. Im Falle nichtlinearer Modelle, wie sie beispielsweise in Extended-Kalman-Filtern [Mah94] und [Ben97] verwendet werden, ist gerade die Robustheit dieser FELB-Struktur, d.h. ihre Stabilität sehr schwierig nachzuweisen.

2.3.5 FELB-Fehler

Bezüglich des Entwurfs von FELB-Strategien ist es wichtig anzumerken, daß auch die FELB-Module ausfallen oder fehlerhaft sein können. Grundsätzlich stellt sich die Frage, welche Fehler in das System durch Hinzufügung der FELB injiziert werden. Gemäß Abschnitt 2.2. müssen Fehler bzw. das Versagen der FELB, deren Aufgabe in der Überwachung sicherheitsrelevanter Elemente besteht, zuverlässig erkannt werden.

Die Frage: „Wer überwacht den Wächter?“ führt schnell zu einem nicht mehr überschaubaren und finanzierbaren Teufelskreis. Aus diesem Grund muß es das Ziel sein, FELB-Konzepte so übersichtlich wie möglich zu konzipieren und nur auf sicherheitsrelevante Systemelemente zu beschränken.

Der Frage der Fehlermöglichkeiten der FELB und deren Auswirkungen auf das Closed-Loop-Verhalten des zu überwachenden Systems wird im weiteren Verlauf der Arbeit höchste Priorität zugeordnet, was in dieser Form bisher noch nicht praktiziert wurde. In Kap. 3 werden Methoden zur Beantwortung obiger Fragestellungen vorgestellt. Die Anwendung dieser Methoden auf die für D-b-W in [Mah94], [Sti95] und [Ben97] entwickelten FELB-Strukturen erfolgt in Abschnitt 3.2.1.2. und den Kap. 4-6.

2.3.6 Abschließende Anmerkungen zur FELB

FELB in heutigen Automobilen

In heutigen Serienfahrzeugen wird mit Blick auf die Robustheit von FELB-Mechanismen bzw. den Wunsch, Fehlalarme (siehe Abschnitt 3.2.1.2.) zu vermeiden, im Vergleich zu den technischen Möglichkeiten verhältnismäßig wenig Diagnoseaufwand getrieben.

Funktionale oder analytische Redundanzmechanismen wie sie in der Luft- und Raumfahrt, aber auch Kraftwerkstechnik häufig genutzt werden, haben sich im Automobilbau bisher nicht durchsetzen können. Plausibilitätskontrollen zur Detektion von Hardfailures hingegen sind bereits auch hier Stand der Technik.

Nur in sicherheitsrelevanten Systemen wird bereits heute im Automobilbau die teure Variante des Selbsttests bzw. der HW-Redundanz verwendet.

Bei nicht sicherheitsrelevanten Applikationen hingegen wird wegen der mit der zunehmenden Komplexität ansteigenden Fehlalarm-Wahrscheinlichkeit auf Überwachungsmechanismen weitestgehend verzichtet.

Gleiches gilt für die Fahrerinformation. So sind beispielsweise in den 80er Jahren eingeführte Strukturen zur Überwachung der Front- und Hecklichter in heutigen Fahrzeugen nur noch selten vorzufinden.

Potentiale der FELB in zukünftigen Automobilen

Die FELB ist ein wirksames Mittel zum Erzielen von Toleranz gegenüber...

- zufälligem Versagen der betrachteten Komponente im Betrieb (stochastische Fehler) und der
- Abnutzung und dem Verschleiß (Alterung) der betrachteten Komponente im Betrieb.

Grenzen der FELB in zukünftigen Automobilen

- Dahingegen ist die Wirksamkeit gegen konstruktive und systematische Fehler umstritten. Diese können nur durch den Einsatz diversitärer Strukturen, wie sie in Kap. 4 anhand der Lenkradwinkelsensorik veranschaulicht werden oder die in dieser Arbeit zu behandelnden funktionalen und analytischen Redundanzen erkannt werden.
- Auf die Problematik der Vermeidung systematischer Fehler durch Erstellung einer vollständigen Anforderungsspezifikation (Stichwort: V-Modell, Formale Methoden) soll in dieser Arbeit nicht eingegangen werden.

Die im weiteren Verlauf der Arbeit vorzustellenden FELB-Konzepte und die für ihre Bewertung geeigneten F/V/S/W-Methoden beschränken sich auf die Erkennung, Lokalisation und Behandlung nichtsystematischer Fehler.

2.4 Motivation für die Verfügbarkeits- und Sicherheitsanalyse eines zukünftigen Kfz-Systems, Zusammenfassung des Kap. 2

Bereits in der Konzeptphase neuer, sicherheitsrelevanter Systeme sollen qualitative und quantitative Verfügbarkeits- und Sicherheitsbetrachtungen vorgenommen werden. So können Schwachstellen des Systemkonzepts oder einzelner Komponenten bzgl. der Fehlerhäufigkeit, Verfügbarkeit und Sicherheit bereits frühzeitig erkannt und durch entsprechende konzeptionelle Maßnahmen kostengünstig beseitigt werden. Ferner bietet diese Systemanalyse die Möglichkeit, die Neuentwicklung gegenüber einem aktuellen Serienprodukt zu bewerten.
Jede Systemänderung in einer späteren Entwicklungs- oder Produktionsphase kann eine überproportionale Erhöhung der Entwicklungs- oder gar Garantie- und Kulanzkosten zur Folge haben.

Demzufolge liegt das Hauptanliegen dieser Arbeit darin, Methoden zur Verfügung zu stellen, mittels derer ein komplexes System mit vertretbarem Aufwand hinsichtlich obiger Qualitätsmerkmale bewertet werden kann. Im Anschluß an eine durchgeführte Systemanalyse gilt es zu hinterfragen, inwieweit die identifizierten Qualitätsmerkmale den Hersteller-Ansprüchen genügen bzw. gesellschaftlich und juristisch akzeptiert werden.

In Abschnitt 2.2 wurde der Aspekt der Hersteller-Ansprüche, sprich die Zuverlässigkeits- bzw. Sicherheitsmaßstäbe, diskutiert. Ferner wurden die folgenden Systemanforderungen zusammengetragen:

- Gefährliche Einfachfehler müssen zuverlässig erkannt werden.
- Das System ist nach Auftreten des Fehlers in einen geeigneten sicheren Zustand zu überführen.
- Verfügt der Systementwurf nicht über diese sicheren Zustände, so ist dieser in das Konzept hineinzudesignen.
- Der sichere Zustand muß solange beibehalten werden, bis der Fehler beseitigt ist bzw. seine sicherheitsrelevante Auswirkung auf das Systemverhalten ausgeschlossen werden kann.

Entsprechend den Ergebnissen der Systemanalyse ist gerade in Bezug auf obige Systemanforderungen der Systementwurf bzw. das -konzept gegebenenfalls zu optimieren.

Im Sinne der Optimierung der F/V/S/W wurde in Abschnitt 2.3 bzw. wird in den Kap. 5 und 6 gezeigt, daß eine FELB auch durch Reduzierung von HW-Redundanz bei gleichzeitiger Erhöhung bzw. Ausnutzung funktionaler bzw. analytischer Redundanz entwickelt werden kann. Diese Vorgehensweise stellt gleichzeitig einen Kompromiß aus fehlertolerantem und perfektionistischem Ansatz der HW-Reduzierung dar. Inwieweit diese Konzepte eine gleichzeitige Optimierung aller drei Qualitätsmerkmale erlauben, wird in Kap. 6 diskutiert. Wichtig ist hierbei allerdings, daß durch diese Reduzierung der Software-Aufwand steigt. Somit müssen die in dieser Arbeit propagierten Methoden zur Bewertung der F/V/S/W nicht nur auf HW, sondern auch auf FELB-Algorithmen anwendbar sein. Die Thematik der FELB-Fehler bzw. -Grenzen wird in Abschnitt 3.2.1.2. anhand eines Anwendungsbeispiels veranschaulicht und dort mittels einer Markov-Kette modelliert. Mit Blick auf die Fehlererkennungswahrscheinlichkeit und somit Sicherheit muß gewährleistet werden, daß die funktionalen bzw. analytischen Redundanzen nicht zu einer nicht tolerierbaren Zunahme von Überwachungslücken führen.

Es soll jedoch an dieser Stelle nochmals betont werden, daß sich die im weiteren Verlauf der Arbeit vorzustellenden FELB-Konzepte und die für ihre Bewertung geeigneten F/V/S/W-Methoden auf die Überwachung nichtsystematischer Fehler beschränken.

3 Methoden zur Bestimmung der Fehlerwahrscheinlichkeit, Verfügbarkeit und Sicherheit komplexer Systeme

In [Kur96 und Mey86] werden verschiedene Methoden zur qualitativen und vor allem quantitativen Bestimmung der System-Fehlerwahrscheinlichkeit, -Verfügbarkeit und -Sicherheit vorgestellt. Wie sich im weiteren Verlauf der Arbeit zeigen wird, erweisen sich die Fehlerbaumanalyse und Markov-Ketten-Modellierung für die Analyse der F/V/S/W von komplexen Kfz-Systemen als geeignet. Es soll jedoch bereits an dieser Stelle vorweggenommen werden, daß erst die als „Hierarchische Modellierung“ bezeichnete Fusion beider Methoden eine geschlossene Modellierung der F/V/S/W komplexer Kfz-Systeme erlaubt, in der sowohl zeitliche Betrachtungen von Folgefehlern, wie auch stochastische Abhängigkeiten mit vertretbarem Aufwand analysierbar sind.
Aus diesem Grund sollen im folgenden sowohl die Fehlerbaumanalyse wie auch die Markov-Ketten-Modellierung vorgestellt werden. Hierbei liegt der Schwerpunkt auf den für die Analyse eines Automobilsystems wichtigen Zuverlässigkeits- bzw. Sicherheitskenngrößen. Auf die für die Bestimmung dieser Kenngrößen wesentlichen mathematischen Grundlagen wird mit der aus Sicht des Autors hinreichenden Detaillierung eingegangen. Im Anschluß an die Vorstellung dieser beiden System-Analysemethoden wird auf ihre Fusion zu „hierarchischen Modellen“ eingegangen. Hierbei wird sich zeigen, daß es hilfreich ist, der hierarchischen Modellierung eine reduzierte Form der „FMEA“ vorauszuschicken. Hierbei werden die Fehlermöglichkeiten der Systemkomponenten und deren Einfluß auf das Systemverhalten hinterfragt, ohne auf die aus Sicht des Autors nicht zielführende Frage der Risikoprioritätszahlen einzugehen. Weitere Details der FMEA sind [Mey86, Oco90] zu entnehmen.

3.1 Fehlerbaumanalyse / Fault Tree Analysis (FTA)

Wie sich im weiteren Verlauf der Arbeit zeigen wird, beeinflussen die Zuverlässigkeitskenngrößen der einzelnen Systemkomponenten maßgeblich die F/V/S-Ergebnisse des zu bewertenden Systems. Da diese Kenngrößen aus Sicht des Autors in der Literatur jedoch nicht hinreichend für Automobil-Applikationen diskutiert wurden, soll der Schwerpunkt in diesem Abschnitt auf der Diskussion der für die Fehlerbaumanalyse (**F**ault-**T**ree-**A**nalysis, FTA) wesentlichen Zuverlässigkeits- bzw. Sicherheitskenngrößen liegen. Hierbei werden die für deren Bestimmung notwendigen mathematischen Grundlagen vermittelt. Jedoch soll auf die Vorstellung von Details zur Bool`schen Algebra, die die Grundlage der FTA darstellt, weitestgehend verzichtet werden. Hierfür sei auf [Ste96, NUR81, Sch92, Mey86, Sch89] verwiesen.
In Kap. 4 wird das für die F/V/S/W-Analyse des Applikationsbeispiels Drive-by-Wire (D-b-W) erforderliche System-Know-how vermittelt und die speziell für D-b-W relevanten Zuverlässigkeitsparameter identifiziert.
Da es sich beim D-b-W um ein zukünftiges Kfz-System handelt, über dessen Fehlerverhalten keine statistisch abgesicherten Felderkenntnisse vorliegen, gilt es bzgl. der Identifikation der Zuverlässigkeitskenngrößen eine Reihe von Annahmen zu treffen. In [Mah96_2] wurde anhand eines neuen Bremssystems die Qualität getroffener Annahmen verifiziert und somit die Zulässigkeit/Güte von Sicherheits- und Verfügbarkeitsabschätzung zukünftiger, noch nicht im Feldeinsatz befindlicher Kfz-Systeme mittels FTA bestätigt. Hierzu wurde eine FTA für ein herkömmliches Bremssystem durchgeführt und die über die Komponentenfehlerhäufigkeiten akkumulierte Fehlerhäufigkeit des Systems mit TÜV-, DEKRA-Auswertungen bzw. amtlichen Statistiken der Bundesanstalt für Straßenwesen verglichen. Die bei diesem Vergleich verzeichnete hohe Korrelation der Ergebnisse kann als Qualitätsmerkmal der FTA gewertet werden.

3.1.1 Kfz-spezifische Top-Events

Als Indikator für die mittels FTA zu bestimmende Systemfehlerwahrscheinlichkeit, -unzuverlässigkeit bzw. -unsicherheit dient die Auftrittswahrscheinlichkeit des als Top-Event bezeichneten „unerwünschten Ereignisses“. Ausgehend von diesem zu wählenden Top-Event (z. B. Ausfall eines Bremskreises), erfolgt im Rahmen der FTA eine Top-Down Analyse des zu untersuchenden Systems, bei der die Verknüpfung individueller Fehler, die zu obigem Top-Event führen können, innerhalb des Zuverlässigkeitsgraphen eine Baumstruktur ergibt. Die Enden der Verästelungen entsprechen schließlich den Fehlern bzw. Fehlerarten einzelner Komponenten des Gesamtsystems. Die auch als qualitative FTA bezeichnete Baumstruktur erlaubt eine Identifikation der „kritischen“ Ursachen bzw. Komponenten, deren Auftreten bzw. Fehlverhalten zum Eintritt des Top-Events führt.

Von ebenso großem Interesse ist die quantitative FTA. Sie resultiert aus der Verknüpfung der im Rahmen der qualitativen FTA bestimmten kritischen Komponentenfehlerarten mit entsprechenden Auftrittswahrscheinlichkeiten bzw. -raten dieser Fehlerarten. Als Ergebnis liefert sie die zu erwartende Auftrittswahrscheinlichkeit des Top-Events innerhalb bzw. nach einem definierten Zeitraum.

Hervorgehend aus der qualitativen und quantitativen FTA läßt sich unmittelbar ein Ranking hinsichtlich der die Unzuverlässigkeit bzw. Unverfügbarkeit oder Unsicherheit dominierenden Eingangsgrößen des Systems ableiten. Diese in Abschnitt 2.2.2 bereits als kritische Pfade bezeichneten Eingangsgrößen werden für D-b-W im Verlauf des Kapitels 5 mittels Pareto-Analyse bestimmt. Durch Optimierung der Qualitätsparameter der kritischen Pfade läßt sich die Gesamtsystemfehlerwahrscheinlichkeit, -verfügbarkeit bzw. -sicherheit oftmals mit verhältnismäßig geringem Aufwand gezielt und effizient optimieren.

Wichtig ist zu betonen, daß die Ergebnisse der FTA stark durch die Wahl des jeweiligen Top-Events bestimmt sind. Als einfaches Beispiel sollen hierzu die beiden Top-Events:

- „Beliebige Kunden-Beanstandung innerhalb der Bremse des Fahrzeugs“

und

- „Ausfall der **B**rems**k**raft**v**erstärkung (BKV)“

betrachtet werden.

Es ist transparent, daß bereits ohne Detailkenntnisse des zu analysierenden Bremssystems wesentlich mehr Fehlerursachen für das erstgenannte Top-Event zu finden sind, als es für das zweite möglich ist. Sollten sämtliche Fehlerursachen statistisch gleich häufig auftreten, wird folglich das erstgenannte Top-Event häufiger auftreten, als das zweite. In Bild 3.1 ist der Fehlerbaum für das Top-Event „AUSFALLBKV“ dargestellt. Die Fehlerursachen auf Komponentenebene entsprechen den Kreisen mit rechteckigem Kommentarfeld. Sämtliche Fehlerursachen fliessen in Oder-Gatter (z.B. „BKV-URSACH“) ein und führen somit bereits als Einfachfehler zum Eintritt des Top-Events. Damit spiegelt der Fehlerbaum ein n-von-n-System wider. Redundanzen, die als Und-Gatter zu modellieren wären, sind hier nicht vorhanden.

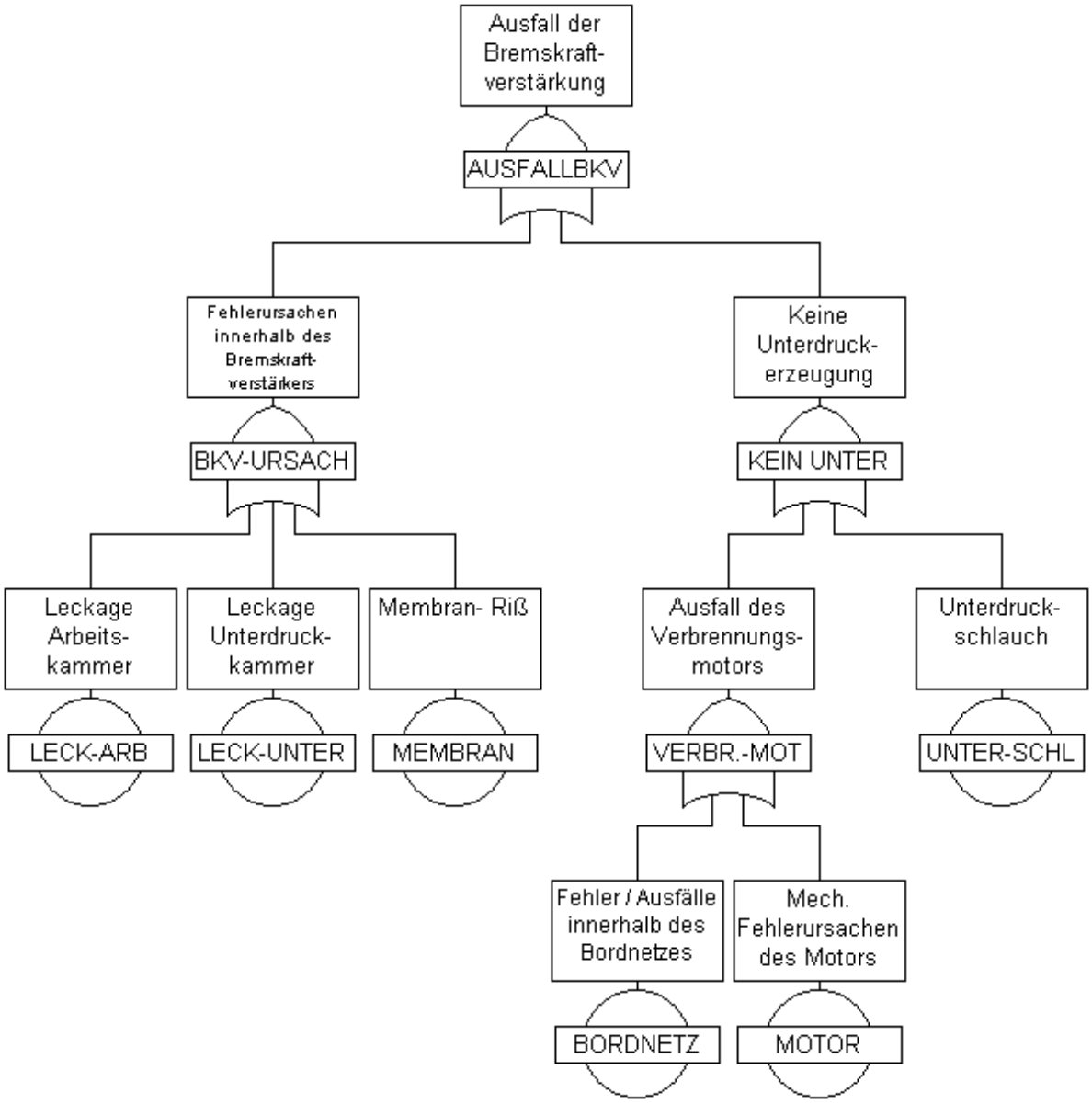


Bild 3.1: Fehlerbaum des Top-Events „Ausfall der Bremskraftverstärkung“

Somit wird deutlich, daß der Wahl der für die Systemanalyse relevanten Top-Events erhöhte Beachtung zukommen sollte. Mit Blick auf Kap. 2 soll es das Ziel sein, die FTA sowohl auf die Fehlerwahrscheinlichkeit, Verfügbarkeit wie auch Sicherheit des zu analysierenden Systems hin auszurichten. Wie sich jedoch in [Mah96_2] bzw. [Ste96] zeigte, sind für diese Systemparameter jeweils verschiedene Top-Events zu definieren, was zu unterschiedlichen Fehlerbäumen führt.

Damit wird bereits deutlich, daß die FTA allein keine geschlossene F/V/S/W-Analyse zuläßt.

In Anlehnung an [VDI88] wurden im Rahmen von [Mah96_2] bzw. [Ste96] für die Verfügbarkeits- und Sicherheitsanalyse komplexer X-by-Wire-Systeme geeignete Zuverlässigkeits- bzw. Sicherheitsklassen mit korrelierenden Top-Events definiert. Eine Übertragung dieser Klassifikation auf das System D-b-W führt ausgehend vom Systemzustand „voll funktionsfähiges D-b-W“ zu den im folgenden beschriebenen und in Tabelle 3.1 einer Sicherheitsklassifikation zugeordneten Top-Events.

Es sei angemerkt, daß bzgl. der Begrifflichkeiten teilweise bereits auf das in Kap. 4 vorzustellende System-Know-how vorgegriffen wird.
Weiteres Rüstzeug für die Fehlerbaumanalyse folgt in den anschließenden Unterabschnitten. Die eigentlichen Fehlerbäume des Applikationsbeispiels D-b-W und deren Diskussion werden in Kap. 5 und 6 vorgestellt.

3.1.1.1 Top-Event A: Degradation der Funktionalität (Regelgüte des D-b-W)

Unter Top-Event A sollen die Fehlerursachen gebündelt werden, die zu einer Degradation der Regelgüte von der höchsten Regelstufe RG1 auf die niedrigeren Stufen RG2 oder RG3 führen. Diese Degradation setzt die Erkennung und Lokalisation eines Fehlers voraus. Damit wird deutlich, daß Top-Event A nicht sämtliche für die Fehlerwahrscheinlichkeit des Gesamtsystems relevanten Komponenten-Fehler umfaßt, sondern lediglich die Fehler, die aus Sicht des Kunden zu einer geringen Funktionseinbusse führen.
An dieser Stelle soll nochmals die in Abschnitt 2.1 vorgestellte Definition der Zuverlässigkeit betrachtet werden. Demnach ist ein System zuverlässig, wenn es die an es gestellte(n) Zuverlässigkeitsforderung(en) erfüllt. Bei einem komplexen System wie D-b-W, welches über einen degradierbaren Fahrdynamikregler verfügt, kann es verschieden umfangreiche Zuverlässigkeitsforderungen geben. So könnte gefordert werden, daß jeder beliebige Komponentenfehler als Verstoß gegen die Zuverlässigkeit betrachtet wird. Dem Autor hingegen erscheint gerade mit Blick auf den kundenkommunizierbaren Nutzen des Systems D-b-W folgende Zuverlässigkeitsforderung als sinnvoll: Das System muß jederzeit in der Lage sein, eine elektronisch geregelte Fahrdynamikstabilisierung vorzunehmen. Kann diese nicht mehr gewährleistet werden, liegt ein Verstoß gegen die Zuverlässigkeitsforderung vor.
Da die Regelgüte in den Regelstufen RG2 und RG3 weiterhin eine elektronische Fahrdynamikstabilisierung ermöglicht, die in aller Regel die Fähigkeiten des Fahrers übersteigt, handelt es sich bei Top-Event A nicht um die Verletzung der Zuverlässigkeit bzw. Verfügbarkeit oder gar Sicherheit. Anhand obiger Diskussion wird die Bedeutung der Zuverlässigkeitsforderungen bzw. der Zuverlässigkeitsziele deutlich.
Es soll abschließend angemerkt werden, daß heutige Regelsysteme, wie ABS, ESP etc. in aller Regel nach Erkennung eines beliebigen Fehlers deaktiviert werden. Dort würde also jeder erkannte Fehler unmittelbar zur Unverfügbarkeit des Systems führen.
Damit drückt Top-Event A für D-b-W gegenüber heutigen Regelsystemen streng genommen einen Benefit aus, wenngleich hier das Fehlerverhalten von Systemkomponenten diskutiert wird.

3.1.1.2 Top-Event B: das verfügbarkeitskritische Top-Event

Das in Kap. 4 beschriebene Schließen der Kupplung ist gleichbedeutend mit dem Verlassen des elektronischen Regelbetrieb „D-b-W“. Gemäß den Ausführungen in Abschnitt 3.1.1.1 führen Fehler innerhalb des Systems, die das Schließen der Kupplung verursachen, zum Verlust der Verfügbarkeit des Systems D-b-W.
Entsprechend soll das **Top-Event** als **Degradation auf RG4, d.h. mechanische Rückfallebene** bezeichnet werden.
Jedoch ist auch dieses Top-Event nicht gleichbedeutend mit einem Sicherheitsverlust. Erst unter der Bedingung, daß die D-b-W-Regelung aufgrund des aktuellen Fahrmanövers aktiv sein müßte, aber abgeschaltet bleiben muß, kann man von einem Sicherheitsrisiko sprechen. Andererseits entspricht dieser Betriebszustand einem ohne Fahrdynamikregelsystem bestückten heute üblichen Fahrzeug. Da diese Grundkonfiguration dem heutigen Zulassungsstand entspricht, kann sie nicht als sicherheitsrelevant eingestuft werden.

3.1.1.3 Top-Event C: das sicherheitskritische Top-Event

Wie sich in Kap. 4 und 5 zeigen wird, existieren insbesondere in dem D-b-W-Minimal-System diverse Fehlermöglichkeiten, die nicht zuverlässig erkennbar, lokalisierbar bzw. behandelbar sind. Damit besteht die Möglichkeit, daß fehlerhafte Sensorsignale in die Fahrdynamikregelung einfließen, was zu einer hochsicherheitsrelevanten Reaktion des Reglers, bis hin zum Verunfallen des Fahrzeugs, führen kann. Streng genommen muß nicht jeder dieser Fehler sicherheitskritische Folgen haben. Um dies auszuschließen, bedarf es einer Untersuchung des D-b-W-Reglers auf Robustheit gegen fehlerhafte Eingangssignale. Da diese Untersuchung jedoch nicht Bestandteil der vorliegenden Arbeit ist, soll im Rahmen einer sicherheitskritischen und damit pessimistischen System-bewertung davon ausgegangen werden, daß jeder nicht erkannte, lokalisierte oder behandelte Fehler sicherheitskritische Auswirkungen hat.
Entsprechend soll das sicherheitskritische Top-Event C als „**von der FELB nicht zufriedenstellend kompensierbare Fehlfunktion innerhalb des D-b-W-Systems**“ bezeichnet werden.

DEFINITION DES TOP EVENTS					
	KLASSE 1	**KLASSE 2**	**KLASSE 3**	**KLASSE 4**	**KLASSE 5**
Klassifi-kation	**Sicherheits-relevanz** bzw. Gesetzes-verletzung	**Verfügbar-keitsverlust**	Schlafender Fehler	**Degradation der Funktionalität**	**Komfort-Beanstandung**
Fehler- / Schadens-schwere	**Systemtotal-ausfall oder Weiter-verarbeitung unentdeckt fehlerhafter Informationen im D-b-W-Betrieb** Auswirkungen können sicherheitskritisch sein.	**Verlust der D-b-W-Funktion** Übergang in Notlauf, d.h. Rückfallebene	Beispielsweise Ausfall der Schließfunktion der Lenk-Kupplung, d.h. Verlust der RFE-Funktion. **System befindet sich jedoch weiterhin im D-b-W-Betrieb.** Weitere Fehler können zu einem hochsicherheits-kritischen Systemzustand führen.	**Systemfehler verringert Regelgüte** Auftreten eines Fehlers bzw. Ausfalls, der zur Degradation von RG 1 auf RG 2 oder 3 führt. Jedoch weiterhin elektronischer Regelbetrieb möglich.	**Subjektive Verschlechterung der Funktionalität (J.D. Power-Studien)** Kunde empfindet bzw. beanstandet Defekt innerhalb D-b-W, der sich lediglich im Komfortbereich bemerkbar macht, jedoch nicht auf Bauteilefehler zurückzuführen ist (z.B. Geräusche, Schwergängigkeit, Lager-Spiel etc.).
Maß-nahme	**Verbesserung der Onboard-Diagnose** oder/und **Robustheit des D-b-W-Reglers gegen nicht erkennbare Fehler sicherstellen.**	**Rote Warnlampe Fahrzeug bald-möglichst parkieren und in Werkstatt überführen lassen.**	**Rote Warnlampe Fahrzeug baldmöglichst parkieren und in Werkstatt überführen lassen**	**Gelbe Warnlampe Kundenseitig bemerkbare System-veränderung Werkstatt möglichst bald anfahren.** Fahrdynamik nicht in Grenzbereich hineintreiben.	**Verbesserung der Diagnosefähigkeit**
Top-Event	**Top-Event C**	**Top-Event B**	Nicht modelliert (siehe [Ste96])	**Top -Event A**	Nicht modelliert (siehe [Mah_92_2])

Tabelle 3.1: Übertragung der in [Mah_96_2] bzw. [Ste96] für die Analyse komplexer X-by-Wire definierten Sicherheitsklassen auf eine Klassifikation für D-b-W

3.1.1.4 Top-Event D: Fehlerwahrscheinlichkeit des Gesamtsystems

Top-Event D soll die Fehlerwahrscheinlichkeit des Gesamtsystems wiedergeben. Da hierin sämtliche Komponentenfehler unabhängig von ihrer Erkennbarkeit bzw. Auswirkung auf das Gesamtsystemverhalten einfließen, stellen sie eine Obermenge der in Tabelle 3.1 aufgeführten Sicherheitsklassen dar.
Unter der Annahme, daß sämtliche Komponentenfehler dem Kunden kommuniziert werden bzw. dieser den Fehler früher oder später in irgendeinerweise erkennt, bietet Top-Event-D die Möglichkeit einer Abschätzung, wie häufig der Endkunde eine berechtigte Beanstandung tätigen wird. Unter obiger Voraussetzung stellt dieses Top-Event ein Maß für die Kundenzufriedenheit dar. Geht man weiterhin davon aus, daß werkstattseitig sämtliche defekten Teile identifiziert werden können und nur defekte Teile getauscht werden, so läßt Top-Event D auch Rückschlüsse auf die anfallenden Werkstatt- bzw. Garantie- und Kulanzkosten zu.

3.1.2 Voraussetzungen für die Zuverlässigkeits- und Sicherheitsanalyse mittels qualitativer und quantitativer FTA

Ausgehend von den in Abschnitt 3.1.1 definierten Top-Events stellt sich nunmehr die Frage, welche Fehlerursachen innerhalb des D-b-W-Systems zum Auftreten dieser Top-Events führen können. Diese Frage führt zu einer Top-Down-Analyse des Systems, wobei in letzter Instanz nach den Fehlern jeder Komponente (Fehlermoden) gefragt wird, die zum Auftreten des Top-Events beitragen können.
Für die Top-Down-Analyse des Systems bedarf es folgender Kenntnisse über das zu betrachtende System:

a) Systemaufbau sowie Fehlermöglichkeiten und -folgen jeder Betrachtungseinheit
b) Betrachtungszeitraum der Berechnung/Analyse
c) Verteilungsfunktion und -parameter aller Komponentenfehler

Auf die Unterpunkte b) und c) soll nunmehr detailliert eingegangen werden. Bzgl. des Unterpunkts a) sei auf Kapitel 4-6 verwiesen.

3.1.2.1 Verteilungsfunktion und -parameter aller Komponentenfehler

Bisher wurde lediglich angedeutet, daß die Auftrittswahrscheinlichkeit des Top-Events durch Fehlerursachen bestimmt sind, die auf Komponentenfehler zurückzuführen sind. Diese Aussage soll nunmehr präzisiert werden:
Die Auftrittswahrscheinlichkeit des Top-Events ist eine Funktion der Ausfall- bzw. Fehlerwahrscheinlichkeiten der Komponenten des zu analysierenden Systems [Oco90, Sch92]. Um also eine detaillierte Systemanalyse durchführen zu können, gilt es die Ausfall- bzw. Fehlerwahrscheinlichkeiten der einzelnen Komponenten des Systems möglichst genau zu bestimmen.
Wahrscheinlichkeitstheoretisch entspricht die Ausfallwahrscheinlichkeit der Verteilungsfunktion der Lebensdauer der Komponente F(t).
Allgemein gilt.

$$F(t) = \int_0^t f(t)dt \qquad \text{Gl. 3-1}$$

Die Verteilungsfunktion der Lebensdauer hängt von der Art der Komponente und deren Ausfallmechanismen ab. So ist die Exponentialverteilung sehr gut zur Beschreibung von Zufallsausfällen, wie sie elektronische und elektrische Bauteile dominieren, anwendbar.

Dabei besagt die Theorie der Zufallsausfälle, daß viele unabhängige Ausfallmechanismen vorliegen.
Die Exponentialverteilung beschreibt die Situation, in der die Ausfallrate λ (siehe Gl. 3.5) konstant ist. Entsprechend lautet die Verteilungsdichtefunktion hier:

$$f(t) = \lambda \cdot \exp(-\lambda \cdot t); t \geq 0 \qquad \text{Gl. 3-2}$$

Die Verteilungsdichtefunktion läßt sich durch folgendes Verhältnis veranschaulichen:

$$f(t) = \frac{\text{Anzahl defekter Einheiten in der betreffenden Zeiteinheit}}{\text{Gesamtzahl der (defekten) Einheiten bzw. Größe der Stichprobe}} \qquad \text{Gl. 3-3}$$

Mechanische Komponenten, wie sie in heutigen Lenkungen mehrheitlich enthalten sind, folgen hinsichtlich des Ausfallverhaltens oftmals einer Weibull-Verteilung. Diese in [NWH94 und Oco90] ausführlich diskutierte Verteilungsfunktion erlaubt es, Fehlerphänomene wie Alterung/Verschleiß, also die für mechanische Bauteile dominanten Fehlerursachen zu beschreiben.
Die exponentialverteilte Komponentenlebensdauer kann statistisch sehr unkompliziert zur letztendlich interessierenden Auftretenswahrscheinlichkeit des Top-Events weiterverarbeitet werden (siehe Abschnitt 3.1.2.2 und 3.1.2.5).
In Kap. 4 wird anhand eines Sensors exemplarisch gezeigt, wie die Verteilungsfunktion des Ausfallverhaltens bestimmt werden kann.

Weiterhin heißt es in [Len95]:

> „Systeme mit vielen verschiedenen Komponenten und unterschiedlichen Ausfallphänomenen können hinsichtlich ihres Ausfallverhaltens näherungsweise durch Zufallsausfälle beschrieben werden. Dies läßt den Schluß zu, daß zumindest für überschlägige Berechnungen der Systemausfallwahrscheinlichkeit für alle Bauteile eines Systems, auch für mechanische Komponenten, in erster Näherung eine Exponentialverteilung angenommen werden kann. Eine genauere Berechnung der Systemausfallwahrscheinlichkeit verlangt dagegen eine Beschreibung der mechanischen Bauteile mit einer Weibullverteilung, die speziell zeitabhängige Ausfallmechanismen und Lebensdauervorgänge berücksichtigt."

Mit Blick auf [Len95] und Kap. 4 soll im folgenden eine Exponentialverteilung des Ausfallverhaltens der elektronischen und elektrischen D-b-W-Komponenten angenommen werden.

Geht man von der exponentialverteilten Ausfallwahrscheinlichkeit aus, so ergibt sich aus Gl. 3-1 und 3-2 die Ausfallwahrscheinlichkeit als Verteilungsfunktion der Lebensdauer der Komponenten:

$$F(t) = 1 - e^{-\lambda \cdot t}; t \geq 0 \qquad \text{Gl. 3-4}$$

Damit ist die Ausfallwahrscheinlichkeit eine Funktion der Ausfallrate λ und der Missionsdauer t. Beide Parameter werden im Verlauf dieses Kapitels ausführlicher vorgestellt.

Vorab soll jedoch bereits auf eine hilfreiche Vereinfachung von Gl. 3-4 hingewiesen werden:

Approximiert man die Exponentialverteilung durch eine Taylor-Reihe, so ergibt sich:

$$F(t) \cong \lambda t \qquad \text{Gl. 3-5}$$

Sofern F(t) kleiner als 0,1 ist, liegt der Approximationsfehler aus Gl. 3-5 unterhalb von 5%. Mit Verweis auf [Bro84] wirkt sich die Approximation in einer überhöhten Angabe der Ausfallwahrscheinlichkeit aus, was im Sinne einer pessimistischen Analyse für sicherheitskritische Systembetrachtungen förderlich ist.

Anmerkungen:
In [Sch92] wird die Ausfallwahrscheinlichkeit durch eine dreiparametrige Exponentialverteilung beschrieben. In obigen Gleichungen wurde zwecks Vereinfachung bewußt auf den dritten Parameter μ, welcher der Reparaturrate der Komponente entspricht, verzichtet. Dieser auch für die Onboard-Fehlerbehandlung und damit die Systemverfügbarkeit und -sicherheit wichtige Parameter wird im Rahmen der Vorstellung der Markov-Ketten in Abschnitt 3.2 ausführlich diskutiert.

Weitere Details zur Zuverlässigkeitsmathematik finden sich in [Ber90, Rei88 und NWH94].

3.1.2.2 Die destruktive Zuverlässigkeitskenngröße „Ausfallrate“

Die Ausfallrate entspricht der Wahrscheinlichkeit eines Komponenten-Fehlers innerhalb des folgenden Zeitintervalls unter der Voraussetzung, daß die betrachtete Komponente bis zum Beginn dieses Zeitintervalls intakt ist, dividiert durch das Zeitintervall. So bedeutet eine Ausfallrate $\lambda = 10^{-6}$/h, daß ein mit dieser Ausfallrate behaftetes Bauteil bei zu Beginn des Betrachtungszeitraumes vorausgesetzter Fehlerfreiheit statistisch 1Mio. Stunden nach Beginn des Betrachtungszeitraumes ausgefallen ist. Verfügt man andererseits über einen Fuhrpark von 10^6 Pkw, wobei in jedem Pkw ein entsprechendes Bauteil enthalten ist, so fällt statistisch bereits nach einer Stunde in einem der Fahrzeuge das betreffende Bauteil aus. Damit entspricht die Ausfallrate auch dem Kehrwert der mittleren Brauchbarkeitsdauer der Komponente (siehe Gl. 3.8).

Ausfallrate:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{dF(t)}{dt} \cdot \frac{1}{(1-F(t))} \qquad \text{Gl. 3-6}$$

Mit R(t) als Zuverlässigkeitsfunktion = 1-F(t).

Die Ausfallrate läßt sich durch folgendes Verhältnis veranschaulichen:

$$\lambda(t) = \frac{\text{Anzahl defekter Einheiten in der betreffenden Zeiteinheit}}{\text{Anzahl der noch intakten Einheiten zum Beginn der Zeiteinheit}} \qquad \text{Gl. 3-7}$$

Wie Gl. 3-6 zu entnehmen ist, weisen mechanische aber auch elektrische und elektronische Bauteile streng genommen zeitvariante Ausfallraten auf. Mit Verweis auf die Badewannencharakteristik der Ausfallrate [Oco90] seien die Kfz-relevanten F/V/S-Betrachtung auf den Nutzungszeitraum (siehe Abschnitt 3.1.2.8) näherungsweise konstanter Ausfallraten der Systemkomponenten beschränkt.

Im weiteren Verlauf dieser Arbeit wird also von konstanten Ausfallraten ausgegangen.

Inwieweit diese Annahme für die D-b-W-Komponenten gilt, wird exemplarisch in Kap. 4 untersucht.

Anmerkung: Im Automobilsektor erfolgt häufig eine Darstellung der Ausfallrate über der Laufleistung in Kilometern/Meilen, anstelle der Zeit.

Eine unmittelbar mit der Ausfallrate zusammenhängende Zuverlässigkeitskenngröße ist die mittlere Lebensdauer, auch als mittlerer Ausfallabstand MTBF (**mean time between failure**) bezeichnet. Die mittlere Lebensdauer E(L) bestimmt als sich als Erwartungswert über das Integral über der Zuverlässigkeit R(t) und entspricht unter der Vorausetzung einer zeitinvarianten Ausfallrate (exponentialverteiltem Ausfallverhalten) deren Kehrwert.

$$E(L) = \int_0^t R(t)dt = \int_0^t (1 - F(t))dt = \int_0^t t \cdot f(t)dt = \frac{1}{\lambda} = MTBF \quad ; \text{für } \lambda \cong \text{konstant} \qquad \text{Gl. 3-8}$$

3.1.2.3 Quellen für die destruktive Zuverlässigkeitskenngröße Ausfallrate

Es stellt sich die Frage, woher die für die Verfügbarkeits- und Sicherheitsanalyse erforderlichen Informationen über Bauteile-Ausfallraten zu beziehen sind. Die im folgenden aufgeführten Quellen erheben keinen Anspruch auf Vollständigkeit.

Mögliche Quellen:

- Auswertung von Prüfstandserprobungen, Fahrzeug(dauer)erprobungen oder Feldversuchen
- Felddatenauswertungen (Gewährleistungsinformationen, Garantie- und Kulanz-Statistiken, Analyse von Austausch-Aggregaten, mittlerer Ersatzteilverbrauch).
- Literaturangaben (Datenbanken von Zuliefererfirmen, Prüfberichte von Prüfinstituten, NRRD, MIL-Handbook, Siemens-Norm SN29500 und Din 40039)

Da nach Einschätzung des Autors in der Literatur leider nur wenig über obige Quellen, ihre Vorteile, Übertragbarkeit auf Kfz-Belange und ihre Zugänglichkeit zu finden ist, sollen im folgenden einige Details zu den in dieser Arbeit genutzten Quellen erläutert werden.

3.1.2.3.1 NPRD: Nonelectric Parts Reliability Data

Hierbei handelt es sich um eine vom **D**epartment **o**f **D**efense (**DOD**) der Vereinigten Staaten aufgebaute Datenbank [NPR95], welche von Bauteileherstellern bzw. -zulieferern gespeist wird. In dieser Datenbank finden sich unabhängig davon, ob es sich um elektrische oder mechanische Bauteile handelt, nur Angaben zu Komponentenausfall-raten. Mit Verweis auf die Modellierung des Ausfallverhaltens mechanischer Bauteile durch die Weibullverteilung ist die Angabe einer Ausfallrate streng genommen nicht korrekt. Zu dieser ‘Näherung’ schreibt das DOD:

> „Leider sind die Hersteller in der Regel nicht in der Lage oder Willens, Angaben zu Weibull-Parametern beizusteuern. Die hier aufgeführten Ausfallraten müssen folglich als Näherung verwendet werden. Jedoch ist diese Näherung besser, als gar keine Angaben machen zu können.“

Durch die Annahme einer konstanten Ausfallrate wird also folgender Fehler bewußt in Kauf genommen:

> **Zu Beginn der Lebensdauer eines mechanischen Bauteils ist die Ausfallrate geringer als zum Ende hin (siehe Alterung/Verschleiß). Damit ist das Ausfall-verhalten mechanischer Bauteile in der Phase bis zum Einsetzen der Verschleißerscheinungen durch die Exponential-Verteilung pessimistisch modelliert. Zum Ende der Lebensdauer hingegen optimistisch.**

Wie sich im weiteren Verlauf des Kapitels zeigen wird, ist der für die F/V/S-Untersuchungen geeignete Zeitraum das erste Betriebsjahr mit D-b-W ausgestatteter

Fahrzeuge, was dem Beginn der Lebensdauer des Systems und seiner Komponenten gleichkommt. Damit dienen auch die [NPR95] zu entnehmenden Daten einer anzustrebenden pessimistischen Analyse des sicherheitskritischen Systems D-b-W.

Um jedoch die Qualität zukünftiger F/V/S-Analysen zu erhöhen, ließe sich an die Bauteilezulieferer sicherheitsrelevanter Kfz-Systeme die Forderung stellen, den Bauteilebeschreibungen aussagekräftiges Datenmaterial hinsichtlich ihrer Zuverlässigkeit bzw. des Ausfallverhaltens hinzuzufügen.

Neben dem Defizit, ausschließlich zeitinvariante Ausfallraten zur Verfügung zu stellen, weist das NPRD folgendes weitere Manko auf:

> Bekanntlich hängt das Ausfallverhalten eines Bauteils stark von seiner Einsatzumgebung ab. In [MIL82] wird dieser Umstand durch die Angabe einer Vielzahl von Parametern berücksichtigt. [NPR95] ist jedoch ausschließlich zu entnehmen, ob es sich um ein im Automobilbereich eingesetztes Bauteil handelt (Application: **G**round-**M**obile, GM) und welchen Qualitätsstandard es erfüllt. Als höchste Qualitätsstufe ist hier der „Military-Standard“ (MIL) aufgeführt. Gefolgt von „Commercial“ (COM) und „Unknown“ (UNK).
> **Es gilt also festzuhalten, daß die [NPR95] zu entnehmenden Ausfallraten nicht eindeutig einem im Pkw verwandten Bauteil zuzuordnen sind.**

Mit Blick auf die Unsicherheit hinsichtlich der Übertragbarkeit der NPRD-Daten auf Pkw-Belastungsverhältnisse und das Fehlen einer Verteilungsfunktion des Ausfallverhaltens der aufgeführten Bauteile wurden zur Erhöhung der Qualität der in dieser Arbeit durchzuführenden F/S/V/W-Analyse folgende Maßnahmen ergriffen:

- Soweit möglich wurden [NPR95] entnommene Ausfallraten durch weitere öffentlich zugängliche Feldangaben [Mey91, Rat96, Ste96, Len95, Coz90, Van93] verifiziert oder gar ersetzt.
- Der „Unschärfe“ der Zuverlässigkeitsparameter bzw. der zu berücksichtigenden Umgebungsbedingungen und der aus der Unschärfe erwachsenden Annahmen kann in gewissem Umfang durch die „vergleichende“ F/V/S-Analyse verschiedener Systemkonzepte begegnet werden. Dadurch, daß in den zu analysierenden Systemkonzepten eine Vielzahl gleicher oder ähnlicher Komponenten verbaut bzw. verplant sind, können Qualitätseinbußen bzgl. der F/V/S-Analyse aufgrund unkorrekter Annahmen durch die vergleichende F/V/S-Beurteilung reduziert werden.

Als ein wesentlicher Vorzug der Datenquelle [NPR95] soll jedoch noch ihre leichte Zugänglichkeit genannt werden. Komponentenhersteller sind in der Regel sehr zurückhaltend mit Informationen über Fehler ihrer Produkte. So hebt sich das [NPR95] hiervon deutlich ab, indem dieses Werk kommerziell über das Internet vertrieben wird.

Ferner soll angemerkt werden, daß trotz obiger Defizite die in [Mah_96_2] durchgeführte Bewertung zweier Bremssysteme, die maßgeblich auf NPRD-Daten fußte, in hohem Maße mit Hersteller-Feldangaben der Automobil-Branche korrelierte.

3.1.2.3.2 Mil-Handbook 217

Hierbei handelt es sich um ein vom DOD herausgegebenes Zuverlässigkeitshandbuch [MIL82], aus dem Fehlerraten elektrischer und elektronischer Bauteile ableitbar sind. Wie bereits im vorhergehenden Abschnitt erwähnt, werden hierfür vielparametrige Formeln verwendet, die eine Berücksichtigung von Einsatz- bzw. Herstellungsparametern ermöglichen. Angaben zu den Umgebungsbedingungen, denen Kfz-Systeme während des Fahrzeugeinsatzes ausgesetzt sind, finden sich in [Ste96, Seite 71] bzw. [Rat96].

Da die aus [MIL82] abgeleiteten Fehlerraten ursprünglich der Zertifizierung hochsensibler militärischer Systeme dienten, müssen sie im Vergleich zu Felddaten der Kfz-Beanstandungen als „zu pessimistisch“ eingestuft werden. Die Folge derartig strenger Qualitätsforderungen spiegelte bzw. spiegelt sich in den enormen Kosten militärischer Systeme wider.

Mit Blick auf den Umstand, daß die [MIL82]-Daten nicht als Stellvertreter von Kfz-Zuverlässigkeitskenngrößen geeignet sind, wurde nur im Fall des Drosselklappen-potentiometers (siehe Kap. 4), für das sich in [NPR95] kein passender Stellvertreter findet, auf eine [MIL82]-Angabe zurückgegriffen. Somit kann die Zuverlässigkeitskenngröße des Drosselklappenpotentiometers und seine Auswirkung auf das entsprechende Top-Event als pessimistische Angabe eingestuft werden.

3.1.2.3.3 Garantie- und Kulanzdaten der Automobil-Hersteller

Die beiden in Abschnitt 3.1.2.3.1 und 3.1.2.3.2 vorgestellten Quellen können dem Bereich „Literaturangaben“ zugeordnet werden. G/K-Daten der Automobilhersteller basieren auf Feldbeanstandungen die innerhalb des **G**arantie- bzw. **K**ulanzzeitraumes von den Vertragswerkstätten an den Hersteller gemeldet werden.

Der Vorteil dieser Daten besteht in der Gewißheit, Zuverlässigkeitsangaben zu erhalten, die für Pkw-Bauteile und -Systeme repräsentativ sind.

Bedingt durch den Umstand, daß es sich hierbei um Feldangaben der werkstattseitig bearbeiteten Garantie- und Kulanzfälle handelt, sind die aus der Datenbank ableitbaren Statistiken jedoch mit Vorsicht zu interpretieren. In den Statistiken ist eine nicht eindeutig identifizierbare Dunkelziffer an präventiv getauschten Bauteilen enthalten. Bemängelt ein Kunde beispielsweise einen ungewöhnlich langen Bremspedalweg, so wird aufgrund der Sicherheitsrelevanz der Bremse häufig rein präventiv der **H**aupt**b**rems**z**ylinder (HBZ) ausgetauscht. Der tatsächliche Defekt dieses Bauteils wird anschließend zwar hinterfragt, fließt aber nicht zwangsläufig in die Statistik zurück. Im Falle des HBZ geht man derzeit von einer Quote von 90-95% präventiver Austausche oder umgekehrt lediglich 5-10% aufgrund eines Mangels berechtigt getauschter HBZ aus.

Neben obigen Dunkelziffern weisen die Statistiken ein weiteres Defizit auf. Um eine qualitativ hochwertige F/V/S/W-Analyse durchführen zu können, ist es oftmals erforderlich, hinsichtlich des Detaillierungsgrades auf Bauteileebene die Fehlermoden (siehe Abschnitt 3.1.2.5) und ihre relativen Häufigkeit zu hinterfragen. Eine diesbezüglich repräsentative Angabe findet sich in den werkstattseitigen Angaben der Kundenbeanstandungen nur in Ausnahmefällen wieder. Auch in J.D. Power-Statistiken heißt es in aller Regel: Bremse quietscht, ruckelt o.ä. Hieraus unmittelbar das fehlerhafte bzw. ursächliche Bauteil abzuleiten, ist nicht immer möglich. In manchen Fällen handelt es sich auch um Komfort-Beanstandungen (Klasse 5, Tabelle 3.1) subjektiver Natur, hinter denen sich häufig kein fehlerhaftes Bauteil verbirgt.

Ein weiteres wichtiges Detail liegt in der Unterscheidung zwischen Garantie- und Kulanz-beanstandungen. Berechtigte Kunden-Beanstandungen, die innerhalb des Garantiezeit-

raumes des Pkw (in Deutschland meist das erste Jahr ab Zulassung) auftreten, werden werkstattseitig zu Lasten des Automobil-Herstellers behoben. Damit ist innerhalb des Garantiezeitraumes von einer lückenlosen Erfassung der für die Bestimmung der relativen Fehlerhäufigkeiten relevanten Beanstandungen auszugehen. Innerhalb des auf den Garantiezeitraum folgenden Kulanzzeitraum, der je nach Kfz-Subsystem und -Hersteller unterschiedlich lang ist, gilt diese vollständige Abbildbarkeit nicht mehr. **Deshalb sollten F/V/S/W-Analysen, die auf Hersteller- bzw. Zulieferer-Felddaten fußen, hinsichtlich des zeitlichen Bezugs der Häufigkeiten nicht über den Garantiezeitraum hinausgehen.**

Trotz obiger Defizite stellen die Garantie- und Kulanzdaten für den Automobilhersteller eine wertvolle Informationsquelle dar, die für seine Produkte aussagekräftig und leicht zugänglich ist.

3.1.2.3.4 Bauteilezulieferer der Automobil-Hersteller

Ein Vorteil der Bauteilezulieferer besteht in der Möglichkeit einer detaillierten Befundung der innerhalb des G/K-Zeitraumes beanstandeten Bauteile. Hier lassen sich die tatsächlichen Fehlerursachen oder auch die Fehlerfreiheit des beanstandeten Bauteils bestimmen.

Es ist jedoch zu betonen, daß mit finanziell vertretbarem Aufwand auch eine Detail-Befundung nicht mit letzter Gewißheit die korrekte Beurteilung liefert. So können beispielsweise leichte Haarrisse auf Platinen oder Wackelkontakte an Steckverbindungen durch Aufstecken eines Steuergerätes auf dem Prüfstand nicht immer lokalisiert werden.

Eine weitere Schwierigkeit besteht in der Bewertung der Zuverlässigkeit zukünftiger Systeme oder neuentwickelter Komponenten. Für diese liegen in der Regel keine oder für eine statistisch abgesicherte Aussage nur unzureichende Felddaten vor. In diesem Fall sind Tests bzw. Prüfstandauswertungen zu fahren (siehe auch Abschnitt 3.1.2.3.5, Stellvertreter-Methode).

Eine wesentliche Voraussetzung für die Bewertung zukünftiger sicherheitsrelevanter Kfz-Systeme ist der offene Austausch von Informationen zwischen Automobilhersteller und -Zulieferern. Weitere Vor- und Nachteile zuliefererseitig gewonnener Zuverlässigkeitskenngrößen sind Abschnitt 3.1.2.3.3 zu entnehmen.

3.1.2.3.5 „Stellvertretermethode“

Mit Blick auf die Zielsetzung der Forschungs- und Entwicklungsabteilungen, neue Systeme zu entwickeln, ist es nur bedingt möglich, diese mit „Serienbauteilen“ zu realisieren. Häufig kann die neue Funktionalität nur unter Einsatz einiger neuentwickelter Bauteile bzw. Subsysteme erreicht werden. Für diese Elemente besteht die Schwierigkeit, ohne auf Felddaten zurückgreifen zu können, abgesicherte Zuverlässigkeitskenngrößen zu generieren.
Um dennoch eine Aussage über die Bauteilezuverlässigkeit machen zu können, bieten sich folgende Möglichkeiten:

- Aufwendige Tests generieren kurzfristig hinreichend aussagekräftige Zuverlässigkeitsangaben. Meist handelt es sich hierbei jedoch um Prüfstandserprobungen. Die einsatzspezifischen Umgebungsbedingungen etc. sind nicht vollständig nachbildbar. Grundsätzlich handelt es sich hierbei um eine sehr kostenintensive Form der Beschaffung von Zuverlässigkeitsangaben, die auch nur dann möglich ist, wenn entsprechende Teile in ausreichender Serienreife vorhanden sind. In der Konzeptphase verwendete A-Muster-Teile weichen hinsichtlich Komplexität, Einbauort etc. häufig erheblich von den letztendlichen Serienteilen ab.

- Existieren die zu analysierenden Bauteile noch nicht, kann für die F/V/S/W-Analyse unter Umständen auf ein ähnliches Bauteil zurückgegriffen werden, für welches die relevanten Daten bereits aufgenommen wurden. Die Güte der resultierenden **Stellvertreter-Analyse** bzw. **-Methode** hängt von der Ähnlichkeit beider Bauteile ab. Häufig handelt es sich bei „neuen" Bauteilen um eine Weiterentwicklung eines Vorgängermodells, so daß die Stellvertreter-Methode gute Ergebnisse liefern wird. Wesentlicher Vorteil dieser Methode ist, daß auf aufwendige Tests verzichtet werden kann. Nachteilig ist jedoch, daß Einsatzbedingungen des zukünftigen Bauteils vom Stellvertreter abweichen können. Diesen Umstand zu berücksichtigen, gelingt in der Regel nur unvollständig. **Es gilt also festzuhalten, daß es sich bei der Zuverlässigkeitsaussage mittels Stellvertreter-Methode um eine Abschätzung handelt.**

Bei der Verwendung von Zahlenmaterial aus [NPR95, MIL82, etc.] wird das Prinzip der Stellvertretermethode bereits intensiv genutzt. Gleiches gilt bei der Verwendung von Kfz-Hersteller- bzw. Bauteilezulieferer-Daten zur Abschätzung der Zuverlässigkeits-kenngrößen neuentwickelter Bauteile.

Es ist also festzuhalten, daß in der vorliegenden Arbeit die Stellvertretermethode mehrheitlich im Sinne einer Abbildung von [NPR95]-Daten auf Pkw-Komponenten eingesetzt wird. Da diese Vorgehensweise in [Mah_96_2, Ste96] zu sehr guten Korrelationen zum Feldverhalten von Serienfahrzeugen führte, wird sie auch als geeignet zur F/V/S/W-Abschätzung zukünftiger Kfz-Systeme betrachtet. Gleichzeitig ermöglicht diese Vorgehensweise „realitätsnahe" Zuverlässigkeitskenngrößen für die D-b-W-Komponenten zu beschaffen, ohne öffentlich nicht zugängliche Daten verwenden zu müssen.

Unschärfen des Datenmaterials, welche sich in einem breiten Konfidenzintervall der resultierenden Zuverlässigkeitskenngrößen widerspiegeln [NWH94, Oco90], könnten unter der Voraussetzung einer Normalverteilung durch die Einführung einer Standard-abweichung in den durchzuführenden F/V/S/W-Analysen berücksichtigt werden. Da diese Angaben dem [NPR95] jedoch nicht zu entnehmen sind, würden sie eine nicht existente Fülle an Zuverlässigkeits- bzw. G/K-Daten vortäuschen, weswegen hier auf diese Möglichkeit verzichtet wird.

Bei Übertragung der in dieser Arbeit vorzustellenden Methoden auf andere Aufgaben-stellungen, in die entsprechende Felddaten einfließen können, ist die Berücksichtigung von Konfidenzintervallen jedoch unbedingt zu empfehlen [Uhl97].

3.1.2.4 Fehlerursachen

An dieser Stelle wird eine Unterscheidung zwischen systematischen, zufälligen und Handhabungsfehlern vorgenommen.

Systematische Fehler sind bereits mit Beginn der Lebensdauer einer HW-Komponente, wie beispielsweise einem Rechner bzw. eines Softwareproduktes, in diesem enthalten. Sie bleiben im Regelfall im Betrieb längere Zeit unerkannt und wirken sich bei bestimmten Zuständen oder in bestimmten Betriebssituationen aus und können damit zu einem Versagen führen. Diese Fehler gehen auf grundsätzlich bestimmbare und reproduzierbare Ursachen zurück. Es handelt sich meist um allgemeine Konstruktions-, Entwurfs-, Spezifikations- oder Fertigungsfehler. Ursache ist damit häufig menschliches Versagen [Dhi88]. Die Wahrscheinlichkeit des Auftretens systematischer Fehler ist nicht durch eine Exponentialverteilung beschreibbar. Mit Blick auf Abschnitt 3.1.2.2 bzw. 3.2.1 ist jedoch diese Verteilungsfunktion Voraussetzung für die Möglichkeit, das transiente Gesamtverhalten des zu untersuchenden Systems hinsichtlich F/V/S in geschlossener Form zu analysieren.

Das Unvermögen, systematische Fehler mittels der hier vorzustellenden Methoden mitmodellieren zu können, stellt jedoch aus Sicht des Autors kein gravierendes Defizit dar. Grund für diese Ansicht ist die Möglichkeit, systematische Fehler durch geeignete Entwurfsmethoden (siehe V-Modell, [VDE080]) aus dem System weitestgehend zu eliminieren. Hier bietet also sorgfältige methodische Systementwicklung einen guten Hebel zur Vermeidung systematischer Fehler. Dahingegen werden auch bei einem mit Auslieferung bzw. Inbetriebnahme fehlerfreien Produkt Alterungserscheinungen mit zunehmender Betriebsdauer unweigerlich zum Versagen von Bauelementen und damit möglicherweise zum Verlust der Systemfunktionalität oder gar Systemsicherheit führen.

Hinsichtlich Softwarefehlern soll hier ergänzend angemerkt werden, daß diese weder physikalischem Verschleiß noch zufällig auftretenden Defekten unterliegen. Softwarefehler treten beim Durchlaufen des fehlerhaften SW-Moduls mit kritischen Eingangsparametern auf und sind ebenfalls systematischer Natur. In der Literatur werden zwar gewisse Häufigkeitsbetrachtungen für die Entstehung von Softwarefehlern angeführt [Kur96, Sin95, Neu96, VDE080 (Anhang B2.1.8), Oco90, Abschnitt 8.12 Statistik der Softwarezuverlässigkeit], jedoch ist es bisher nicht gelungen, eine nachweislich gültige Verteilungsfunktion des Ausfallverhaltens von Softwarefehlern zu formulieren. Vielmehr sind die Auswirkungen von Softwarefehlern im Betrieb des Rechners keine statistisch unabhängigen Ereignisse. Darüberhinaus werden in der Literatur genannte Ausfallraten meist so klein gewählt, daß der Verlauf der resultierenden exponentialverteilten Fehlerhäufigkeit so „flach“ ist, daß innerhalb der betrachteten Missionsdauer praktisch kein SW-Fehler auftreten kann. Diese mathematisch nicht korrekte Vorgehensweise schafft die Möglichkeit, Softwarefehler in die geschlossene Systemmodellierung aufzunehmen, ohne die Verteilungsfunktion des Ausfallverhaltens modellieren zu müssen/können. Andere Ansätze gehen von einer Fehlerrate von 6 Fehlern pro 1.000 Zeilen programmierten Source-Codes aus. Diese Fehlerrate führt über der Zeit gemäß obiger Literatur zu sehr hohen Fehlerwahrscheinlichkeiten, infolge derer Software grundsätzlich als nicht funktionsfähig betrachtet werden müßte, was nicht mit den praktischen Erfahrungen von Computer-Benutzern korrelieren dürfte.

Da somit beide Strategien der Modellierung des Ausfallverhaltens von Software mathematisch fragwürdig sind und lediglich zu einem Anstieg der Komplexität der Zustandsraummodellierung bzw. des Fehlerbaumes führen, wird auf sie im weiteren Verlauf der Arbeit verzichtet. Fehler der FELB-Software werden also nur in der Form mitmodelliert, wie sie durch Informationsverlust, hervorgerufen durch einen Sensorfehler o.ä., ausgelöst werden können.

Zufälliger (stochastischer) Fehler:

Wie bereits im Bereich „systematische Fehler“ erläutert, sind diese durch eine methodische Systementwicklung weitestgehend vermeidbar, zufällige Fehler jedoch nicht. Als zufällige (stochastische) Fehler sind alle Defekte bzw. Ausfälle einer Einheit zu betrachten, deren Auftrittszeitpunkte nicht vorhersagbar sind, jedoch über der Betriebszeit durch eine Verteilungsfunktion beschreibbar sind.

Für elektronische Bauelemente gilt hierbei im wesentlichen die Exponentialverteilung des Ausfallverhaltens mit konstanter Ausfallrate. In Kap. 4 wird exemplarisch die Gültigkeit dieser für die weitere F/V/S/W-Analyse mittels FTA bzw. Markov-Modellen wichtigen Voraussetzung nachgewiesen. Wesentliches Merkmal der Zufallsfehler ist, daß einzelne Fehlerursachen, d.h. „Einzelfehler“, statistisch unabhängig von anderen sind. Umgekehrt heißt dies, daß eine Fehlerursache und alle daraus resultierenden Fehlerwirkungen oder Folgefehler als Einzelfehler anzusehen sind.

Handhabungsfehler:

Unter Handhabungsfehlern werden alle Fehler verstanden, die beim Umgang mit der Einheit nach Auslieferung im Anwendungsfall verursacht werden. Hierunter fallen im wesentlichen Fehler beim Laden bzw. Installieren von Software, bei Bedienung und während des Dialogs mit der Einheit, beim Testen vor Ort und bei Systemänderungen in Hardware und Software.

Im weiteren Verlauf der Arbeit sollen systematische Fehler und Handhabungsfehler, die die Qualität heutiger Systeme zwar noch maßgeblich bestimmen, mit Blick auf ihre Vermeidbarkeit durch den Einsatz eines strukturierten methodischen Entwicklungsprozesses, für die F/V/S/W-Analyse zukünftiger Systeme nicht mitbetrachtet werden. Vielmehr beschränkt sich die F/V/S/W-Analyse auf Ausfall- bzw. Fehlerverhalten stochastischer Natur, deren Auftretenswahrscheinlichkeit durch eine Exponentialverteilung modelliert werden kann.

3.1.2.5 Stochastische Fehlermoden

Wie sich im Verlauf der Kapitel 4-6 zeigen wird, hängt die Qualität der F/V/S-Analyse maßgeblich vom Detaillierungsgrad der Fehlerursachenrecherche ab. In diesem Sinne stellt sich die Frage, in welcher Weise ein Bauteil fehlerhaft sein kann und wie sich diese als Fehlermoden bezeichneten Fehlermöglichkeiten des Bauteils auf das Gesamtsystemverhalten auswirken.

An Bedeutung gewinnt die in Kap. 4 folgende Differenzierung nach Sensorik-Fehlermoden insbesondere wegen der FELB-Algorithmen. Mit Blick auf den Umstand, daß bereits in heutigen Kfz-Systemen und dem in Kap. 4 beschriebenen Minimal-System Hardfailures erkannt werden können, soll eine Aufspaltung in Hard- und Softfailures erfolgen (siehe Abschnitt 4.2.1.1.1). Da die Fehlererkennung wesentliche Voraussetzung für die Fehlerbehandlung ist, wirkt sich obige Differenzierung der Fehlermoden bereits unmittelbar auf die Unterscheidung nach F/V/S aus.
Die Frage nach den Fehlermoden ist auch bei der FMEA [Mey86, Kur96] von Bedeutung. Quantitative Analysemethoden wie die FTA und Markov-Ketten-Analyse bedürfen neben der qualitativen Angabe möglicher Fehlermoden auch eine Aussage zu ihrer quantitativen Verteilung.
Ausgehend von obiger Unterscheidung nach Hardfailure (HF) und Softfailure (SF) soll nunmehr die Komponenten-Fehlerwahrscheinlichkeit als Funktion der Fehlermoden-Wahrscheinlichkeiten hergeleitet werden.
Allgemein gilt:

$$F_{Komp}(t) = F(HF \cup SF) = F_{HF}(t) + F_{SF}(t) - F(HF \cap SF) \qquad \text{Gl. 3-9}$$

In der Literatur wird häufig von der Disjunktheit verschiedener Fehlermoden einer Komponente ausgegangen. Entsprechend „verschwindet“ die Verbundwahrscheinlichkeit aus Gleichung 3-9.
Stochastisch unabhängige Ereignisse sind in Fehlerbaumanalyse und hierarchischen Modellen sehr komfortabel modularisierbar und erlauben somit eine erhebliche Reduzierung des Modellierungs- und Rechenaufwands. Deshalb gilt es zu hinterfragen, inwieweit in der vorliegenden Arbeit von stochastisch unabhängigen Fehlermoden einer Komponente ausgegangen werden darf.

Abschnitt 3.1.2.8 vorgreifend beträgt die durchschnittliche Missionsdauer eines Automobils über der gesamten Lebensdauer 3000 Stunden.
Fehlerraten automotiv-tauglicher Komponenten liegen in der Regel deutlich unterhalb $0{,}3 \cdot 10^{-4}$ 1/h. Setzt man obige Randbedingungen unter der vereinfachenden Annahme $\lambda_{HF} = \lambda_{SF} = \lambda_{Mode} = 0{,}15 \cdot 10^{-4}\ \frac{1}{h}$ in Gleichung 3-9 ein, so ergibt sich für stochastisch unabhängige Fehlermoden:

$$\begin{aligned} F_{Komp}(t) &= F_{HF}(t) + F_{SF}(t) - F_{HF}(t) \cdot F_{SF}(t) \\ &= 2 \cdot \left(1 - e^{-\lambda_{Mode} \cdot t}\right) - \left(1 - 2e^{-\lambda_{Mode} \cdot t} + e^{-2 \cdot \lambda_{Mode} \cdot t}\right) \\ &= \left(1 - e^{-2 \cdot \lambda_{Mode} \cdot t}\right) = \left(1 - e^{-0{,}3 \cdot 10^{-4}\ \frac{1}{h} \cdot 3000h}\right) \\ &= 1 - e^{-0{,}09} = 0{,}086 \approx 0{,}09 = 2 \cdot \lambda_{Mode} \cdot t \end{aligned}$$

Gl. 3-10

Die in Gleichung 3-10 abschließend vorgenommene Taylor-Reihen-Approximation setzt auf den Angaben zu Gleichung 3-5 auf.

Analog ergibt sich für disjunkte Fehlermoden:

$$\begin{aligned} F_{Komp}(t) &= F_{HF}(t) + F_{SF}(t) = 2 \cdot \left(1 - e^{-\lambda_{Mode} \cdot t}\right) \\ &= 2 \cdot \left(1 - e^{-0{,}15 \cdot 10^{-4}\ \frac{1}{h} \cdot 3000h}\right) = 2 \cdot \left(1 - e^{-0{,}045}\right) \\ &= 0{,}088 \approx 0{,}09 = 2 \cdot \lambda_{Mode} \cdot t \end{aligned}$$

Gl. 3-11

Der Vergleich von Gl. 3-10 und 3-11 verdeutlicht, daß für die im Automobilbereich üblichen Zuverlässigkeitsparameter, die Annahme stochastisch unabhängiger Fehlermoden einer Komponente zulässig ist.
Entsprechend gilt für die Komponenten-Fehlerrate:

$$\lambda_{Komponente} = \sum_{m=1}^{n} \lambda_{Mode_m}$$

Gl. 3-12

und

$$\lambda_{Mode} = \alpha \cdot \lambda_{Komponente}$$

Gl. 3-13

Mit

λ_{Mode} entspricht der Moden-Ausfallrate

$\lambda_{Komponente}$ entspricht der Gesamtfehlerrate des Bauteils

α = Wahrscheinlichkeit, daß eine Komponente mit dem Fehlermode „Mode“ ausfällt

n = Anzahl verschiedener Fehlermoden der Komponente

Wird, wie in Abschnitt 3.1.2.1 bzw. 3.1.2.2 beschrieben, von einer exponentialverteilten Ausfallwahrscheinlichkeit und konstanter Ausfallrate der Komponente ausgegangen, so ergibt sich für die Ausfall- bzw. Fehlerwahrscheinlichkeit des Bauteils im Fehlermode „Mode“:

$$F_{Mode}(t) = 1 - e^{-\lambda_{Mode} \cdot t} = 1 - e^{-\alpha \cdot \lambda_{Komponente} \cdot t} \qquad \text{Gl. 3-14}$$

Geht man davon aus, daß die Komponente durch jeden der Fehlermoden im Sinne der Definition des Fehlers bzw. Ausfalls versagt, so stellt sich das Zuverlässigkeitsblockdiagramm wie folgt dar:

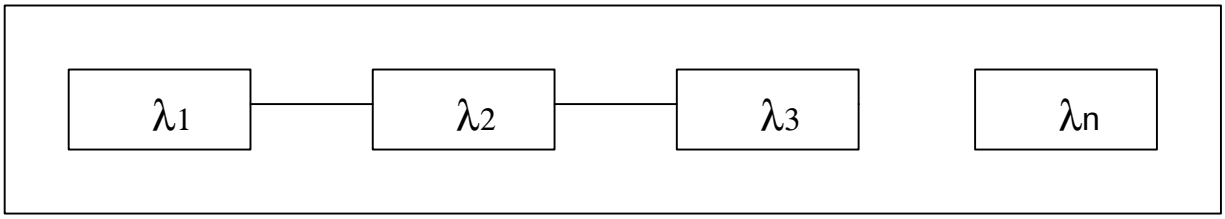


Bild 3.2: Zuverlässigkeitsblockdiagramm einer Komponente mit n Fehlermoden

Die Komponentenzuverlässigkeit ist gewährleistet, wenn keiner der Fehlermoden auftritt bzw. vorliegt. Somit gilt hier:

$$R_{Komponente}(t) = \prod_{m=1}^{n} R_{Mode_m}(t) \qquad \text{Gl. 3-15}$$

Unter Verwendung von Gl. 3-14, dem Komplement der Moden-Zuverlässigkeit, ergibt sich:

$$R_{Komponente}(t) = \prod_{m=1}^{n} \left(1 - F_{Mode_m}(t)\right) = \prod_{m=1}^{n} \left(1 - \left(1 - e^{-\lambda Mode_m \cdot t}\right)\right) = \prod_{m=1}^{n} e^{-\lambda Mode_m \cdot t} \qquad \text{Gl. 3-16}$$

Entsprechend lautet die Komponenten-Fehlerhäufigkeit:

$$F_{Komponente}(t) = \left(1 - R_{Komponente}(t)\right) = 1 - \prod_{m=1}^{n} e^{-\lambda Mode_m \cdot t} = 1 - e^{-\sum_{m=1}^{n} \left(\lambda Mode_m\right) t} \qquad \text{Gl. 3-17}$$

Obige Darstellung wird zuverlässigkeitstheoretisch als „n von n „ System bezeichnet, da das „System“ Komponente nur fehlerfrei funktioniert, wenn keiner der n Fehlermoden vorliegt. D.h., man kann die Ausfallraten der Fehlermoden insgesamt auch im Exponenten der resultierenden Verteilungsfunktion additiv überlagern.
Bereits in Abschnitt 3.1.2.3.3 wurde darauf hingewiesen, daß die werkstattseitig übermittelten Kundenbeanstandungen in den wenigsten Fällen eine Fehlermoden-Aufsplittung mit Blick auf die für die Top-Event-Differenzierung geeignete Schadensschweredetaillierung zuläßt. Aus diesem Grund wurde in dieser Arbeit für die F/V/S/W-Analyse auf eine weitere Datenbank des DOD zurückgegriffen. Im **F**ailure-**M**ode/Mechanism **D**istribution [FMD91] können für eine Vielzahl von Bauteilen detaillierte Angaben zu Fehlermoden und deren Verteilung entnommen werden. Hinsichtlich des Ursprungs dieser Daten und der Problematik der Repräsentativität für Pkw-Komponenten sei auf Abschnitt 3.1.2.3.5 verwiesen.

3.1.2.6 Mehrfachfehlerbetrachtungen

Im Gegensatz zur FMEA (**F**ehler**m**öglichkeiten und **E**influß-**A**nalyse, DIN 25 448), bei der aufgrund des explodierenden Aufwandes oftmals von einer Mehrfachfehlerbetrachtung abgesehen wird, ist dies bei der FTA mit vertretbarem Aufwand möglich. Jedoch sollte man im Blick behalten, daß Systeme oftmals bereits nach Einfachfehlern in kritische Zustände übergehen oder gar ausfallen. Diese einschränkende Anmerkung reduziert oftmals den für die FTA zu betreibenden Aufwand und läßt sich durch das Absorptionsgesetz veranschaulichen:
Man gehe davon aus, daß der Ausfall bzw. Fehler der Komponente A bereits zum Eintreten des Top-Events führt. Darüberhinaus tritt das Top-Event unter der Bedingung ein, daß die Komponente B und die Komponente A fehlerhaft bzw. ausgefallen sind.
Gemäß Absorptionsgesetz läßt sich dieser Zusammenhang wie folgt reduzieren:

$$A + A \cdot B = A \qquad \text{Gl. 3-18}$$

Entsprechend wurde für die im Kapitel 5 und 6 aufgeführten Fehlerbäume dann auf eine Mehrfachfehlerbetrachtung verzichtet, wenn bereits ein Einfachfehler zum Erreichen des Top-Events führte.

3.1.2.7 Die FTA, eine statische Zuverlässigkeitsanalyse

Bei der FTA handelt es sich im Gegensatz zu zustandsraumorientierten Analysemethoden wie den Markov-Ketten [Mah96_1, Mah97] um eine statische Analyse. Hierunter versteht man den Umstand, daß das System hinsichtlich der Zuverlässigkeit zu einem bestimmten „eingefrorenen“ Zeitpunkt betrachtet wird.
Ist beispielsweise die Auftrittswahrscheinlichkeit einer Fehlfunktion innerhalb der Lenkung während der Startphase des Fahrzeugs und während des normalen Fahrbetriebs zu bestimmen, müssen hierfür zwei individuelle Fehlerbäume erstellt werden.

Aufgrund dieser Eigenschaft der FTA eignet sie sich nur eingeschränkt für F/V/S-Analysen, in denen folgende Problematiken detailliert untersucht werden sollen:

- Geschlossene F/V/S-Analysen unter Berücksichtigung verschiedener Systemzustände bzw. Betriebsphasen.
  So kann ein Bruch innerhalb der Lenkspindel im Moment des Einparkens völlig unkritisch sein. Zwar führt er zum Verlust der Systemverfügbarkeit, jedoch ist die Sicherheit des Benutzers in diesem Moment meist nicht tangiert. Die oben angesprochenen Verfügbarkeits- und Sicherheitsaspekte können mittels Markov-Modellen analysiert werden.
- Zeitlich aufeinanderfolgende Mehrfachfehlerbetrachtungen
- Graceful-Degradation-Betrachtungen [Con90, Mah96_1, Mah97] unter Berücksichtigung entsprechender Diagnose- und Fehlerbehandlungsstrategien.

3.1.2.8 Missionsdauer der Bauteile / Betrachtungszeitraum der Fehlerbaumanalyse

Mit Blick auf Gl. 3-4 u. 3-5 soll nunmehr der Parameter Betriebsdauer bzw. Missionsdauer „t“ vorgestellt werden. In [Len95 u. NUR81] findet sich hierzu eine ausführliche Diskussion. Es wird unterschieden zwischen der Lebensdauer der Komponente bzw. des Fahrzeugs, was dem Alter in Jahren oder Stunden entspricht, und der Missionsdauer.
Unter Missionsdauer sei im folgenden die effektive Nutzungs- bzw. Einsatzdauer einer Komponente bzw. des Systems, ab ihrem ersten Einsatz, verstanden.
Da die FTA eine statistische Aussage generiert, gilt es eine durchschnittliche Missionsdauer der Komponenten bzw. des Systems zu definieren. So geht man hinsichtlich der Pkw-Missionsdauer von folgendem Gedanken aus:

> Die durchschnittliche Lebensdauer eines Pkw beträgt 10 Jahre, was der durchschnittlichen Laufleistung von 150.000km gleichkommt. Letzteres impliziert bei einer Durchschnittsgeschwindigkeit von 50km/h eine Pkw-Gesamtmissionsdauer von 3.000 Stunden. Damit beträgt die durchschnittliche Missionsdauer/Jahr „$t_{Durchschnitt}$“ eines Pkw:

$$t_{Durchschnitt} = \frac{\text{Missionsdauer}}{\text{Jahr}} = \frac{s_{Durchschnitt}}{v_{Durchschnit}} = \frac{15.000\text{km/Jahr}}{50\text{km/h}} = 300\frac{\text{Stunden}}{\text{Jahr}} \qquad \text{Gl. 3-19}$$

In Abschnitt 3.1.2.3.5 wurde darauf hingewiesen, daß die Mehrzahl der in Kapitel 4-6 verwendeten Komponentenausfallraten [NPR95] entnommen sind. In dieser Datenbank wurden die Ausfallraten unter Verwendung der effektiven Nutzungsdauer der jeweiligen Komponente aus der Ausfallwahrscheinlichkeit bestimmt. So wird beispielsweise die Gesamtmissionsdauer eines „Valve, Hydraulic, Check“ mit 31,25 Stunden angegeben.
Will man also für die in [NPR95] aufgeführten Bauteile die Ausfallwahrscheinlichkeit nach einem Jahr bestimmen, so müssen diese Raten gemäß Gl. 3-4 bzw. 3-5 mit den effektiven Missionsdauern multipliziert werden.
Entsprechend gilt es also, für jede in der F/V/S/W-Analyse des D-b-W berücksichtigte Komponente, die effektive Missionsdauer $t_{Durchschnitt}$ zu bestimmen. Es sei vorweggenommen, daß der Parameter „Missionsdauer“ in der vergleichenden FTA von großem Einfluß ist.

a) Komponenten mit der Missionsdauer des Pkw-Alters

Wie in [Len95] diskutiert, wäre die einfachste Lösung, für alle Komponenten das jeweilige Fahrzeugalter als Missionsdauer zu verwenden. In diesem Zusammenhang sei auch auf [NUR81] verwiesen, wo unterschiedliche Ausfallraten für den Standby-Betrieb (Standby-Failure-Rate) und die eigentliche Nutzung des Systems (Operation-Failure-Rate) definiert werden. Wie jedoch bereits erwähnt, sind die dem [NPR95] entnommenen Fehlerraten bereits auf die effektive Nutzungsdauer der Komponenten bezogen.
Da sämtliche in Kap. 4 betrachtete Systemkomponenten nur während des Fahrbetriebs aktiviert werden, soll das Fahrzeugalter nicht als Missionsdauer in der F/V/S-Analyse verwandt werden.

b) Komponenten mit der Missionsdauer der mittleren Pkw-Gesamtmissionsdauer

Mit Blick auf Abschnitt 3.1.2.3.3 (G/K-Daten der Automobil-Hersteller) werden die in dieser Arbeit vorzunehmenden F/V/S/W-Abschätzungen des D-b-W-Systems als Fehler- bzw. Ausfallwahrscheinlichkeiten bezogen auf das erste Betriebsjahr des Pkw quantifiziert. Aus diesem Grund soll also für die Komponenten, die während des gesamten Fahrbetriebs aktiviert sind, eine Missionsdauer von 300 Stunden (siehe auch Gl. 3-19) angenommen werden. Beispiele für derartige Komponenten sind sämtliche Sensoren, die Lichtmaschine, Steuergeräte etc.. Diese Komponenten sind mit Starten des Fahrzeugs bestromt bzw. belastet, womit sie als „in Aktion" betrachtet werden. Wie sich in Kap. 4 zeigen wird, sind sämtliche in der vorzunehmenden Analyse berücksichtigten Komponenten obiger Natur.

c) Komponenten mit der Missionsdauer „Operations-Dauer" / Zeitfaktoren

Für die in den Kap. 5-6 durchzuführenden FTAs bzw. Markov-Ketten-Analysen werden die Tools „Fault-Tree +" und „MKV" verwandt. Innerhalb dieser Tools kann lediglich eine gemeinsame Systemmissionsdauer verarbeitet werden. Um dennoch unterschiedliche Komponentenmissionsdauern berücksichtigen zu können, wurden in [Mah_96_2] gemäß dem Assoziativ-Gesetz der Multiplikation [Bro84] die Komponentenausfallraten des Bremssystems mit einem entsprechenden „Zeitfaktor" multipliziert. Diese Notwendigkeit ist bereits der Funktionsbeschreibung des ABS-Bremssystems aus Abschnitt 2.2 zu entnehmen. Hier wurde auf eine gegenüber herkömmlichen Bremsmanövern deutlich geringere Anzahl von ABS-Bremsungen hingewiesen. Da aber auch die Bremse mit Ausnahme der entsprechenden Sensorik-/Steuergeräteanordnung nicht permanent aktiviert wird, galt es in diesem Beispiel gleich drei unterschiedliche Missionsdauern zu unterscheiden.

Beispiel:

Um die Ausfallwahrscheinlichkeit einer Komponente nach einem Jahr zu bestimmen - Missionsdauer des Fahrzeugs = 300h, die Komponente ist jedoch effektiv nur 30 Stunden innerhalb dieses Jahres aktiv - wäre folgende Gleichung zu lösen:

$$F_{Komp}(t = 300h) = 1 - e^{-\lambda_{Komp} \cdot 30h} \qquad \text{Gl. 3-20}$$

Gemäß dem Assoziativ-Gesetz der Multiplikation ergibt sich für die Komponenten-ausfallrate der Zeitfaktor 1/10:

$$F_{Komp}(t = 300h) = 1 - e^{-(\lambda_{Komp} \cdot Zeitfaktor) \cdot 300h} = 1 - e^{-\left(\lambda_{Komp} \cdot \frac{1}{10}\right) 300h} \qquad \text{Gl. 3-21}$$

d) Innerhalb der F/V/S/W-Analyse des Applikationsbeispiels D-b-W verwandte Zeitfaktoren

Die in Unterabschnitt „c" beschriebene Strategie der Berücksichtigung unterschiedlicher Zeitfaktoren ist für das in Kap. 4 vorzustellende Fahrdynamikstabilisierungssystem D-b-W nicht notwendig. Der Vollständigkeit halber wird jedoch der Zeitfaktor $Z_1 = 1$ eingeführt, um somit auch dem Umstand vorzubauen, in einem späteren Schritt die durchgeführte F/V/S/W-Analyse in die Analyse des Gesamtfahrzeugs zu integrieren.

3.1.3 Fehlerbaumtool Fault Tree +

Bei dem von der Firma Isograph entwickelten Softwaretool „Fault Tree + for Windows Version 7.0“ handelt es sich um ein Programm zur rechnerunterstützten Fehler- und Ereignisbaum-Analyse. Neben der Bestimmung der Auftretenswahrscheinlichkeit des Top-Events bietet das Tool einen Graphik-Editor, mittels dessen der qualitative Fehlerbaum aus Und-/Oder-Gattern etc. zusammengesetzt werden kann. Details zu dem Tool und seiner Praxistauglichkeit sind [Ste96] bzw. der Dokumentation der Firma ITEM zu entnehmen.
Neben der Möglichkeit, Komponentenfehler über eine zeitinvariante Fehlerrate zu formulieren, können sie auch über eine konstante Fehlerwahrscheinlichkeit beschrieben werden. Damit bietet sich beispielsweise die Möglichkeit, ohne Kenntnis der Verteilungsfunktionen des Fehlerverhaltens der einzelnen Komponenten, die Fehlerwahrscheinlichkeit zum Ende des Garantiezeitraumes einzugeben und somit für diesen einen Zeitpunkt die resultierende Auftretenshäufigkeit des Top-Events zu bestimmen.

Hinsichtlich der im Anhang der vorliegenden Arbeit aufgeführten Fehlerbäume ist anzumerken, daß der für die Beschriftung der Gatter vorgesehene Platz von Seiten des Tools eingeschränkt ist und somit die in den Gattern aufgeführten Kommentare an manchen Stellen lückenhaft erscheinen. Die vollständigen textuellen Beschreibungen finden sich in dem entsprechenden Abschnitt der Kap. 5 und 6.

Ferner ist anzumerken, daß die Ausfallraten mit dem Buchstaben r und die Auftretenswahrscheinlichkeit des Top-Events mit dem Buchstaben Q abgekürzt werden.

3.1.4 Abschließende Anmerkungen zur FTA

Ziel des Abschnittes 3.1 war es, die Grundlagen der F/V/S-Analyse mittels FTA zu vermitteln. Auf die noch nicht diskutierten Aspekte der Wirtschaftlichkeitsanalyse wird im Rahmen des Abschnittes 3.2 eingegangen. Es sollte verdeutlicht werden, daß die Qualität der resultierenden F/V/S-Aussage stark von der Identifikation der Zuverlässigkeitskenngrößen der Systemkomponenten abhängt. Da es sich bei dem in dieser Arbeit zu analysierenden Fahrdynamikregelungssystem um eine im Forschungsstadium (A-Muster-Stand) befindende Neuentwicklung handelt, sind hinsichtlich der Zuverlässigkeitsparameter, wie auch der Systemstruktur, Annahmen zu treffen. Als Folge obiger Annahmen dürfen die in den Kap. 4-6 resultierenden Ergebnisse nur als F/V/S/W-Abschätzungen verstanden werden. Jedoch ist es wichtig, bereits in diesem frühen Entwicklungsstadium erste Vorhersagen der zu erwartenden F/V/S/W zu erhalten, damit entsprechende Maßnahmen zur Optimierung dieser Parameter frühstmöglich in die Systementwicklung einfließen können.

Es soll nochmals betont werden, daß die F/V/S/W-Analyse eines noch nicht im Feldeinsatz befindlichen Systems nur eine Vorhersage des zu erwartenden Verhaltens dieses Systems liefern kann. Dies gilt besonders, wenn gravierende Neuentwicklungen in dieses System einfließen. Ziel muß es also sein, die Größenordnung der zu erwartenden F/V/S korrekt abzuschätzen. Entgegen anderer Hoffnungen ist es schon allein mit Blick auf das Wort „Statistik“ nicht möglich, das Feldverhaltens eines Systems, welches erst in einigen Jahren Serieneinführung haben wird, bis auf wenige Prozent Genauigkeit vorherzusagen.

Da es sich bei dem zu analysierenden Fahrdynamikregelungssystem D-b-W um ein sicherheitsrelevantes System handelt, sollte auch in Anwesenheit gewisser Unschärfen eine möglichst kritische F/V/S/W-Untersuchung vorgenommen werden. In diesem Sinne sei das DOD zitiert:

> „Es ist besser mit einer konstanten Ausfallrate zu rechnen, anstatt überhaupt keine Untersuchung durchführen zu können."

Dennoch ist hervorzuheben, daß die Auswirkungen der Unschärfe obiger Annahmen auf die resultierende F/V/S/W-Analyse durch eine „vergleichende" Bewertung verschiedener Systemkonzepte in gewissem Umfang reduziert werden.

Bezüglich des NPRDs soll nochmals betont werden, daß die Ausfallraten aus Felddaten bestimmt wurden. Die ausgefallenen Systeme weisen zumeist ein hohes Alter auf, so daß für ihren Ausfall Verschleiß/Alterung dominant sein wird. Mit Verweis auf Abschnitt 3.1.2.3.1 liefert die mit diesen Zuverlässigkeitsparametern durchgeführte Analyse also eine pessimistische Upper-Bound-Abschätzung.

Abschließend soll noch die für die FTA erforderliche Einschränkung, der Monotonie-Eigenschaft des zu analysierenden Systems erläutert werden.

- Diese Monotonieeigenschaft besagt, daß durch Ausfall eines Elements das bereits ausgefallene System nicht wieder arbeitsfähig werden kann.
- Bei Arbeitsfähigkeit aller Elemente ist auch das System arbeitsfähig.
- Bei Ausfall aller Elemente ist auch das System ausgefallen.

3.1.4.1 Anmerkung zum Detaillierungsgrad der FTA

Soll über eine FTA eine mit der Realität möglichst stark korrelierende Qualitäts-Vorhersage für das zukünftige Fahrdynamikregelungs- und Lenksystem erzeugt werden, liegt die Vermutung nahe, daß die Güte der Zuverlässigkeitsaussage mit Erhöhung des Detaillierungsgrades der Systemanalyse anwächst.
Diese Annahme ist nur bedingt korrekt. Vielmehr gilt bzgl. des Detaillierungsgrades der Systemanalyse mittels FTA die Empfehlung, das System so grob wie möglich und nur so detailliert wie erforderlich zu modellieren. So empfiehlt es sich nicht, die FTA im Bereich der Rechner-HW bis auf jeden pn-Übergang innerhalb der Prozessoren herunter-zubrechen. Die Folge wäre ein sehr komplexer Fehlerbaum, der zur quantitativen Zuverlässigkeitsaussage mit Zuverlässigkeitskenngrößen (Ausfallraten etc.) gespeist werden müßte. Hinsichtlich der Ausfallraten wird der Automobil-Hersteller seitens des Bauteilezulieferers nur einen für diesen sinnvollen Detaillierungsgrad erhalten. So reicht der Detaillierungsgrad der Zuverlässigkeitskenngrößen im Bereich der Rechner-HW meist nur bis auf die Angabe einer Ausfallrate des Prozessors.

3.1.4.2 Kurzanleitung zur Aufstellung eines Fehlerbaumes

1) Für die Durchführung einer detaillierten FTA ist es zwingend erforderlich, ein hohes Maß an System-Know-how aufzubauen. Hierzu gehören Dokumentationen der Systemumfänge, Komponentenbeschreibungen und Detaillierungen der Wechselwirkungen der Komponenten und Submodule zu- und miteinander. Hilfreich sind hierbei alle Arten von System-Dokumentationen wie Datenblätter, Rahmen- oder Lastenhefte.
2) Ermittlung der Zuverlässigkeitskenngrößen der relevanten Systemkomponenten:
   Neben der Kenntnis des korrekten bzw. erwünschten Systemverhaltens ist es genauso wichtig, das Fehlerverhalten der einzelnen Komponenten, deren mögliche Ursachen und Auswirkungen auf das Systemverhalten zu hinterfragen. Hilfreich ist hierbei die Anfertigung bzw. Nutzung einer FMEA.
3) Definition des /der "Unerwünschten Ereignisse(s)".
4) Aufstellung des qualitativen Fehlerbaums durch Verknüpfung der unter „2)“ gewonnenen Fehlermöglichkeiten mittels Bool'scher-Algebra (Und-, Oder-Gatter etc.).
5) Einspeisung der quantitativen Zuverlässigkeitskenngrößen in den Fehlerbaum und Durchführung der quantitativen FTA.
6) Prüfung der FTA-Ergebnisse auf Plausibilität (wenn möglich Vergleich mit Seriensystemen (TÜV-/DEKRA-Statistiken o.ä.)).
7) Aufstellung von Pareto-Diagrammen zur Bestimmung der kritischen Pfade des Systementwurfs bzw. Ableitung von Verbesserungsvorschlägen.

3.1.4.3 Vor- und Nachteile der Fehlerbaumanalyse relativ zu anderen in der Literatur beschriebenen Zuverlässigkeits- und Sicherheitsanalyse-Methoden

Abschließend sollen nochmals die wesentlichen Vor- und Nachteile der Fehlerbaumanalyse relativ zu anderen in der Literatur beschriebenen Zuverlässigkeits- und Sicherheits-Analyse-Methoden bzw. der in Abschnitt 3.2 zu diskutierenden Markov-Ketten-Analyse aufgeführt werden :

Wesentliche Vorteile der FTA gegenüber anderen Z/S-Analyse-Methoden

- Die FTA erlaubt es, für Systeme mit vielen Komponenten, die untereinander jedoch nur schwach vernetzt sind, mit relativ geringem Modellierungsaufwand eine Systemanalyse durchzuführen.
- Hierbei generiert sie sowohl eine qualitative wie auch quantitative F/V/S-Aussage.
- Die flußdiagrammähnliche graphische Darstellung ermöglicht es, systemseitige Zusammenhänge detailliert darzustellen. Durch diese Visualisierung werden Rückschlüsse auf konzeptionelle Defizite bzw. Verbesserungspotentiale erleichtert.
- Zeitlich gleichzeitig auftretende bzw. vorliegende Mehrfachfehler können mit geringem Modellierungsaufwand betrachtet werden.

Wesentliche Nachteile der FTA

- Um eine detaillierte F/V/S-Aussage für ein System generieren zu können, bedarf es eines hohen Maßes an System-Know-how. Hierzu gehört neben der Frage der Wechselwirkungen einzelner Komponenten zu/miteinander auch die Frage, welche Fehlerarten die einzelnen Komponenten aufweisen können. Gerade die Zuverlässigkeitskenngrößen sind für neuentwickelte oder nur in geringen Stückzahlen verbaute Komponenten schwierig ermittelbar. Bedingt durch die Notwendigkeit vor Beginn der FTA, wie auch sämtlicher anderer F/V/S-Analysemethoden, einen „recht konkreten" Systementwurf vorliegen zu haben, können detaillierte F/V/S-Aussagen erst in einem späteren Stadium des Systementwicklungsprozesses generiert werden. Damit besteht die Gefahr, daß Defizite des Systementwurfs erst verspätet aufgedeckt werden, was sich negativ auf Entwicklungszeit und -kosten auswirkt.
- Ebenso teilt die FTA mit sämtlichen F/V/S-Analysemethoden das Manko, keinen Nachweis über die Vollständigkeit der durchgeführten Analyse liefern zu können. Wird beispielsweise ein sicherheitsrelevanter Fehlermode einer Komponente nicht bedacht, was gerade bei Neuentwicklungen möglich ist, so können seine Auswirkungen auf das jeweilige Top-Event nicht analysiert werden. Dies wirkt sich sowohl auf die qualitative, wie auch quantitative FTA aus.
- Da es sich bei der FTA um eine statische Analysemethode handelt, kann auf diese Weise das Systemverhalten nur zu einem Zeitpunkt, d.h. in einem „eingefrorenen" Zustand analysiert werden. Somit sind Graceful-Degradation- und FELB-Strategien, deren zeitliches Verhalten mittels Markov-Ketten modellierbar ist, nur in einem statischen Modell analysierbar. Aus selbigem Grund eignet sich die FTA nicht, um zeitliche Betrachtungen, wie beispielsweise zeitlich aufeinander folgende Fehler zu modellieren.
- Bedingt durch die der FTA zugrundeliegende Bool'sche Algebra, können unterschiedliche Grade der Systemfunktionsfähigkeit, beispielsweise verursacht durch verschiedene Komponentenfehlermoden, nicht innerhalb einer Top-Event-Analyse modelliert werden. Folglich müssen für eine Fehlerwahrscheinlichkeit-, Verfügbarkeits- und Sicherheitsanalyse jeweils unterschiedliche Top-Events und somit auch Fehlerbäume generiert werden (siehe hier insbesondere Kap. 5-6).
- Stochastische Abhängigkeiten, wie beispielsweise gemeinsame Reparatureinheiten für verschiedene Komponenten oder beschränkte Ersatzteilressourcen sind mittels FTA nicht modellierbar.
- Im bisherigen Verlauf der Arbeit wurde zwar erläutert, daß die durchzuführenden Analysen auch den Faktor Kosten beinhalten, jedoch ist die FTA für die Berücksichtigung der Wirtschaftlichkeit eines Systemkonzeptes nicht geeignet. Diese wird erst durch die in Abschnitt 3.2 vorzustellende Markov-Ketten-Analyse im Systemverbund modellierbar.

3.2 Markov-Ketten-Analyse

In Abschnitt 3.1 wurde die zur Gruppe der „nicht zustandsraumorientierten“ Analysewerkzeuge gehörende Fehlerbaumanalyse (FTA, **F**ault-**T**ree-**A**nalysis) vorgestellt. Mit Blick auf die in Abschnitt 3.1.4.3 dargestellten Defizite der FTA soll nunmehr die im Zustandsraum durchzuführende **M**arkov-**K**etten-**A**nalyse (MKA) diskutiert werden. Abweichend von der Vorgehensweise bei der Vorstellung der FTA soll hier auf die in der Literatur oftmals sehr aufwendig und damit schwer verständlichen mathematischen Grundlagen der MKA eingegangen werden. Hierbei beschränkt sich die Detaillierung jedoch auf die aus Sicht des Autors für die F/V/S/W-Analyse erforderlichen Grundlagen. Insbesondere um über die FTA hinausgehende Detaillierungen der Zuverlässigkeitskenngrößen vorzustellen, werden in diesem Abschnitt exemplarisch zwei Beispiele diskutiert. Weitere mathematische Grundlagen sind [Rei88, Sch92] zu entnehmen. Nach Meinung des Autors genügen für den Zuverlässigkeitsingenieur bereits die in [Mah96_1] und [Mah97] beschriebenen praxisbezogenen Informationen, aus denen auch die beiden Systembeispiele hervorgehen.

3.2.1 Voraussetzungen für die System-Analyse mittels Markov-Ketten

Wie der Begriff Markov-Ketten-Analyse besagt, ist die wesentliche Voraussetzung des zu betrachtenden stochastischen Prozesses, daß die weiterreichende Vorgeschichte eines Zustandes für sein Erreichen bzw. Zustandekommen irrelevant ist. Die Eigenschaft, daß die Zukunft des Prozesses von seiner Gegenwart, nicht von seiner Vergangenheit abhängt, wird mit Markov-Eigenschaft bezeichnet. Diese Unabhängigkeit von der Vorgeschichte wird auch als Gedächtnislosigkeit bezeichnet. Markov-Prozesse sind durch folgende Zustandsgleichung beschreibbar:

$$\pi_j(t') = \sum_{i=1}^{m} \pi_{ji}(t',t) \cdot \pi_i(t) \qquad \text{Gl. 3-22}$$

Gleichung 3-22 besagt, daß wenn zum Zeitpunkt t sämtliche Aufenthaltswahrscheinlichkeiten in sämtlichen m Zuständen eines Systems bekannt sind, so läßt sich für jeden folgenden Zeitpunkt t‘ die Aufenthaltswahrscheinlichkeit in jedem beliebigen Zustand j über die Summe der Produkte der Aufenthaltswahrscheinlichkeiten in den m Zuständen zum Zeitpunkt t und den Übergangswahrscheinlichkeiten aus sämtlichen Zuständen in den Zustand j bestimmen. Obiger Sachverhalt fußt auf dem Satz von Bayes [Lof90], demzufolge die Übergangswahrscheinlichkeiten bedingte Wahrscheinlichkeiten dafür sind, daß der Folgezustand der Zustand j ist, unter der Bedingung, daß der aktuelle Zustand der Zustand i ist.
Zur Veranschaulichung soll obiger Sachverhalt an einem Kleinstsystem bestehend aus den Zuständen 0 und 1 verdeutlicht werden.

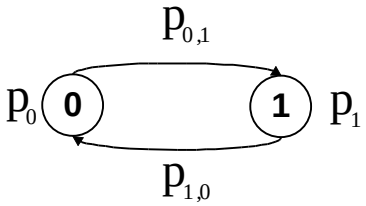


Bild 3.3: Zustandsübergangsdiagramm für ein Kleinstsystem

Gleichung 3-22 reduziert sich zu:

$$\pi_1(t') = \pi_{01}(t',t) \cdot \pi_0(t) - \pi_{10}(t',t) \cdot \pi_1(t) \qquad \text{Gl. 3-23}$$

Ergänzend zur Kommentierung der Gleichung 3-22 ist Gleichung 3-23 zu entnehmen, daß zur Bestimmung der Aufenthaltswahrscheinlichkeit im Folgezustand j der Produktterm der bedingten Wahrscheinlichkeit, daß sich das System zum Zeitpunkt t bereits im Zustand j befand und zum Zeitpunkt t‘ in einen anderen Zustand übergeht und der Aufenthaltswahrscheinlichkeit im Zustand j zum Zeitpunkt t, abzuziehen ist.
In [Rei88, Sch92, Mah96_1] findet sich die Herleitung der Umwandlung obiger bedingten Übergangswahrscheinlichkeiten in Zustandsübergangsraten. Dieser Umwandlung liegt die zeitliche Ableitung von Gleichung 3-22 zugrunde, die letztlich zur Chapman-Kolmogorov-Gleichung führt.

3.2.1.1 Chapman-Kolmogorov-Differentialgleichung

Über die Lösung der **C**hapman-**K**olmogorov-**Gl**eichung (C-K-Gl) erhält man die wichtigen Zuverlässigkeitskenngrößen „Fehler- u. Ausfallwahrscheinlichkeit, mittlere Lebensdauer des Systems, kritische Zustände“ des Systems, seiner Teilsysteme und Komponenten.

$$\frac{d\underline{\pi}(t)}{dt} = \underline{Q} \cdot \underline{\pi}(t) \qquad \text{Gl. 3-24}$$

Existiert der Grenzwert $\lim_{t\to\infty} \underline{\pi}(t)$, so ergibt sich aus Gleichung 3-24 folgendes lineares Gleichungssystem der Grenzwertwahrscheinlichkeiten:

$$\underline{Q} \cdot \underline{\pi} = 0 \qquad \text{Gl. 3-25}$$

und

$$\underline{e} \cdot \underline{\pi} = 1 \qquad \text{Gl. 3-26}$$

Mit $\underline{e}$ = (1,1,1,1,...,1)

In obiger Gleichung entspricht $\underline{\pi}$ dem Zustandsaufenthaltswahrscheinlichkeitsvektor. Mit Blick auf die F/V/S/W-Analyse geben die Komponenten des Zustandsvektors die Wahrscheinlichkeit an, daß sich das modellierte System zu einem bestimmten Zeitpunkt beispielsweise im Zustand „Teilsystem defekt“ befindet. Die Komponenten der Intensitätsmatrix „$\underline{Q}$“ sind die Zustandsübergangsraten „q_{ij}“. Um die Intensitätsmatrix von der Unverfügbarkeit „Q“ unterscheiden zu können, wird sie unterstrichen dargestellt. Zustandsübergangsraten sind beispielsweise die in Abschnitt 3.1.2.1 beschriebenen Ausfall- bzw. Reparaturraten. Weitere, insbesondere konstruktive Übergangsraten werden in Abschnitt 3.2.1.2 diskutiert. Um die C-K-Gl in geschlossener Form Lösen zu können müssen sämtliche Zustandsübergangsraten zeitinvariant sein.

Die in Gleichung 3-25 beschriebene stationäre Chapman-Kolmogorov-Gleichung ist für die Systemanalyse aus zweierlei Gründen von Interesse:

- Sie ist mathematisch sehr einfach lösbar.
- **Mit Blick auf die Systemsicherheit sollte es das Bestreben sein, ein System in der Art zu designen, daß es über einen stationären Zustandsvektor verfügt, der nicht sicherheitsrelevant ist. Darüberhinaus sollte das System diesen Zustand bereits frühzeitig (deutlich vor Erreichen der mittleren System-Lebensdauer) einnehmen.**

Weitere wichtige Eigenschaft der Chapman-Kolmogorov-Gleichung:

- Die Summe aller Elemente einer Spalte der Intensitätsmatrix $\underline{Q}$ muß gleich 0 sein, was zur Folge hat, daß die Hauptdiagonalelemente der negativen Summe der übrigen Elemente der betreffenden Hauptdiagonalelement-Spalte entsprechen. Bis auf die Hauptdiagonalelemente geben die Elemente $q_{i,j}$ einer Spalte die Übergänge (Übergangsraten) vom Zustand π_i in den Zustand π_j wieder (siehe Bild 3.3 bzw. 3.4 und Gl. 3-27).
- Gl. 3-26 besagt, daß die Summe der Aufenthaltswahrscheinlichkeiten in sämtlichen Systemzuständen/Zustandsvektorelementen zu jedem Zeitpunkt gleich 1 ist.

3.2.1.2 Mittels Markov-Ketten modellierbare Zuverlässigkeitskenngrößen

Wie bereits in Abschnitt 3.2.1.1 angedeutet, fließen die Zuverlässigkeitskenngrößen „Ausfall- bzw. Reparaturrate“ in die Intensitätsmatrix der Chapman-Kolmogorov-Gleichung ein. Die Missionsdauer des betrachteten Systems wird über den Parameter t berücksichtigt. Weitere für die automobilspezifische F/V/S/W-Analyse wichtige Zustandsübergänge werden im Verlauf dieses Abschnittes diskutiert.

3.2.1.2.1 Systembeispiel 1: F/V/S/W-Analyse in einem geschlossenen Modell

Systembeschreibung:
Als Anwendungsbeispiel dient hier das in Abschnitt 2.2 qualitativ diskutierte ABS-Bremssystem. Die F/V/S/W-Analyse beginnt mit der Erstellung der Markov-Kette.

Der Zustandsvektor umfaßt 7 Zustände, von denen an dieser Stelle die ersten beiden ausführlicher diskutiert werden. In Tabelle 3.2.1-4 finden sich Beschreibungen sämtlicher Zustände, Übergänge bzw. Übergangsraten des 1. Systembeispiels.

- Im Startzustand, d.h. dem fehlerfreien Systemzustand „0“ beginnt die Systemanalyse. Entsprechend ist die Startaufenthaltswahrscheinlichkeit π_0 in Zustand 0 gleich 1. In Bild 3.4 ist der Zustand aufgrund der Fehlerfreiheit des Systems farblich grün hervorgehoben.
- Zustand „1“ wird bei Auftritt der nicht verfügbarkeitskritischen Fehler bzw. Ausfällen der Raddrehzahlsensoren als Folgezustand von Startzustand 0 eingenommen. Entsprechend ist die Startaufenthaltswahrscheinlichkeit $\pi_1(t=0)$ in Zustand 1 gleich 0. Da Raddrehzahlfehler mit Aktivieren der ABS-Warnlampe quittiert werden, ist Zustand 1 in Bild 3.4 (siehe Seite 61) farblich gelb hervorgehoben.

Zum besseren Verständnis sei hier exemplarisch die Übergangsrate $q_{0,1}$ beschrieben.

- Wie bereits bei der Vorstellung von Zustand 1 beschrieben, erfolgt der Übergang von Startzustand 0 in den Folgezustand 1 bei Auftritt eines beliebigen Raddrehzahlsensorfehlers. Entsprechend setzt sich die Übergangsrate $q_{0,1}$ aus den Übergangsraten der 4 Raddrehzahlsensoren zusammen.

Zustand	Beschreibung des Zustands	Übergang (-srate)	Beschreibung des Übergangs
0	Fehlerfreier Startzustand • (Zustand in Bild 3.4 farblich grün hervorgehoben) • (Startaufenthaltswahrscheinlichkeit = 1)	$q_{0,1}$	Fehler- bzw. Ausfallrate der vier Raddrehzahlsensoren (siehe auch Kap. 4) $\lambda_{4\text{Rd}-\text{Sensoren}} \approx 35 \cdot 10^{-6} \frac{1}{\text{h}}$
		$q_{0,2}$	Fehler- bzw. Ausfallrate für den Abriß eines der vier Bremsschläuche (siehe [Mah96_2]) $\lambda_{4\text{Hyd.}-\text{Schlauch}} \approx 0{,}5 \cdot 10^{-6} \frac{1}{\text{h}}$
1	Zustand „ABS-Ausfall“ • Aktivierung der „gelben“ ABS-Warnlampe. (Zustand in Bild 3.4 farblich gelb hervorgehoben) • Abschalten der ABS-Funktion • Abspeichern von Fehlermeldung in Diagnosespeicher • (Startaufenthaltswahrscheinlichkeit = 0)	$q_{1,2}$	Auch nach einem Fehler in der Raddrehzahlsensorik besteht die Möglichkeit eines stochastisch unabhängigen Abrisses eines oder mehrerer Bremsschläuche. Die Ausfallrate ist identisch $q_{0,2}$
		$q_{1,6}$	Nach Aktivierung der gelben Warnlampe steuert der Fahrzeugführer durchschnittlich innerhalb der nächsten 3 Stunden die Werkstatt an. $u_{\text{Fahrer}} = \frac{1}{3} \frac{1}{\text{h}}$ Hinsichtlich obiger Übergangsrate sei auf Abschnitt 3.2.1.2.2 verwiesen.

Tabelle 3.2.1: Diskussion der für das Beispiel ABS-Bremssystem erforderlichen Systemzustände

Zustand	Beschreibung des Zustands	Übergang (-srate)	Beschreibung des Übergangs
2	Verfügbarkeitskritischer Zustand • Aktivierung der „roten“ Warnlampe. (Zustand in Bild 3.4 violett hervorgehoben) • Abspeichern von Fehlermeldung in Diagnosespeicher • (Startaufenthaltswahrscheinlichkeit = 0)	$q_{2,1}$	Auch nach einem Abriß eines Bremsschlauches kann einer der Raddrehzahlsensoren ausfallen. **Im Sinne eines stochastisch abhängigen Folgefehlers kann die über den abgerissenen Bremsschlauch austretende Bremsflüssigkeit zum Zusetzen des Polrads des Drehzahlgebers führen, was wiederum zur Fehlermeldung des Drehzahlgebers führt.** Diese in der Vergangenheit bei Nutzfahrzeugen gelegentlich aufgetretene Fehlerfolge ist zwar recht unwahrscheinlich, soll jedoch mit Blick auf die Veranschaulichung der Möglichkeit mittels Markov-Ketten auch stochastische Abhängigkeiten modellieren zu können, mitberücksichtigt werden. Als Übergangsrate sei eine gegenüber der herkömmlichen Fehlerrate der Drehzahlsensorik doppelt so hohe Rate angenommen. $\lambda_{4Rd-Hyd} \approx 2 \cdot \lambda_{4Rd-Sensoren}$ $\approx 70 \cdot 10^{-6} \frac{1}{h}$ Dennoch wird sich diese aus mathematischer Sicht interessante stochastische Abhängigkeit bedingt durch die geringe Übergangsrate $q_{0,2}$ nicht gravierend auf die Aufenthaltswahrscheinlichkeit im Zustand 1 auswirken.
		$q_{2,3}$	Fehler- bzw. Ausfallrate für den Abriß in einem der beiden Bremsschläuche des verbleibenden (bisher fehlerfreien) Bremskreises. Hierbei handelt es sich also um den Zweitfehler. Auch hier ist davon auszugehen, daß beide Abrisse stochastisch unabhängig sind. $\lambda_{Hyd.2,3} \approx \lambda_{2Hyd.Kr.1o2} \approx 0{,}26 \cdot 10^{-6} \frac{1}{h}$ Weitere Details hierzu finden sich in Abschnitt 3.3
		$q_{2,4}$	Es sei davon ausgegangen, daß der Fahrzeugführer auf das Aufleuchten der roten Warnlampe wie gefordert durch baldmöglichstes Parkieren des Fahrzeugs reagiert. Der anschließend zu informierende MB-Service erreicht das Fahrzeug innerhalb einer angenommenen Zeitspanne von durchschnittlich 1 Stunde. $u_{Wartezeit\,2,4} = 1\frac{1}{h}$ Hinsichtlich der Übergangsrate „Wartezeit“ sei auf Abschnitt 3.2.1.2.2 verwiesen.

Tabelle 3.2.2: Diskussion der für das Beispiel ABS-Bremssystem erforderlichen Systemzustände

Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
3	Sicherheitskritischer Zustand • Aktivierung der „roten“ Warnlampe. (Zustand in Bild 3.4 rot hervorgehoben) • Im worst-case keine Verzögerung des Fahrzeuges durch Bremssystem möglich • Abspeichern von Fehlermeldung in Diagnosespeicher • (Startaufenthaltswahrscheinlichkeit = 0)	$q_{3,4}$	In Analogie zur Übergangsrate $q_{2,4}$ sei davon ausgegangen, daß das Fahrzeug nach Aufleuchten der Warnlampe baldmöglichst parkiert wird. Mit Blick auf den Umstand, daß der Fahrer bereits vor dem Aufleuchten der Warnlampe den Bremsleistungsverlust wahrnehmen wird, sei hier eine gegenüber $q_{2,4}$ geringere Wartezeit von nur einer halben Stunde angenommen. $\upsilon_{\text{Wartezeit}3,4} = \frac{2}{1}\frac{1}{\text{h}}$
4	MB-Service • MB-Service holt Fahrzeug ab und überführt es in Werkstatt. • Abschleppkosten 500 DM (Zustand in Bild 3.4 schwarz hervorgehoben) • (Startaufenthaltswahrscheinlichkeit = 0)	$q_{4,5}$	Es sei davon ausgegangen, daß MB-Service mit dem zu überführenden Fahrzeug innerhalb einer halben Stunde die Werkstatt erreicht. $\upsilon_{\text{MB-Service}\,4,5} = \frac{2}{1}\frac{1}{\text{h}}$ Hinsichtlich der Übergangsrate sei auf Abschnitt 3.2.1.2.2 verwiesen.
5	Werkstattaufenthalt zwecks Bremsschlauch-Austausch • Hier wird der Schaden behoben • Reparaturkosten 100 DM (Zustand in Bild 3.4 schwarz hervorgehoben) • (Startaufenthaltswahrscheinlichkeit = 0)	$q_{5,0}$	Es sei davon ausgegangen, daß der Austausch des bzw. der Bremsschläuche inklusive Entlüftung 15 Minuten dauert, der Kunde idealerweise nach dieser Zeit wieder auf sein in den Zustand 0 zurückversetztes fehlerfreies Fahrzeug zurückgreifen kann. $\mu_{\text{Hyd.Schlauch}} = \frac{4}{1}\frac{1}{\text{h}}$ Hinsichtlich der Reparaturrate sei auf Abschnitt 3.2.1.2.2 verwiesen. Anmerkung: **Nur aufgrund der Gedächtnislosigkeit des Markov-Prozesses und des Wunsches, auch die Kosten der jeweiligen Reparatur korrekt berücksichtigen zu können, sind zwei Zustände „Werkstatt“ mit unterschiedlichen Aufenthaltsdauern und Kosten notwendig.** Strenggenommen müßte sogar unterschieden werden, ob ein oder zwei Bremsschläuche getauscht werden müssen, jedoch wurde hierauf mit Blick auf den resultierenden Aufwand verzichtet. Da aber die Entlüftung eines Bremskreises näherungsweise genauso lange dauert, und genausoviele Arbeitseinheiten beansprucht, wie die beider Bremskreise, ist obige Unschärfe tolerierbar.

Tabelle 3.2.3: Diskussion der für das Beispiel ABS-Bremssystem erforderlichen Systemzustände

Zustand π_i	Beschreibung des Zustands	Übergang (-srate)	Beschreibung des Übergangs
6	Werkstattaufenthalt zwecks Drehzahlfühler-Austausch • Hier wird der Schaden behoben • Reparaturkosten 300 DM (Zustand in Bild 3.4 schwarz hervorgehoben) • (Startaufenthaltswahrscheinlichkeit = 0)	$q_{6,0}$	Es sei davon ausgegangen, daß die eindeutige Identifikation eines Fehlers innerhalb eines Drehzahlfühlers sowie dessen Austausch 30 Minuten dauert, und der Kunde idealerweise nach dieser Zeit wieder auf sein in den Zustand 0 zurückversetztes fehlerfreies Fahrzeug zurückgreifen kann. $m_{\text{Rd-Sensor}} = \frac{2}{1}\frac{1}{h}$

Tabelle 3.2.4: Diskussion der für das Beispiel ABS-Bremssystem erforderlichen Systemzustände

Anhand Tabelle 3.2.1 bis 3.2.4 und Bild 3.4 wird bereits der für ein kleines Systembeispiel erforderliche Aufwand einer Markov-Ketten-Modellierung verdeutlicht.
Im worst-case bedarf es für die Modellierung eines n-Komponenten-Systems, in dem jede Komponente die beiden Zustände funktioniert/defekt annehmen kann, einer Markov-Kette bestehend aus 2^n Zuständen.

Durch Modularisierungen, wie sie in Abschnitt 3.3 sowie Kap. 5 und 6 vorgestellt werden, läßt sich das Manko des Modellierungsaufwand über eine Reduzierung der Komplexität des Zustandsraummodells in gewissem Umfang minimieren.

Andererseits wird bereits an dieser Stelle deutlich, daß die Markov-Ketten-Analyse gegenüber der FTA wesentlich vielfältigere, vor allem konstruktive Zuverlässigkeitskenngrößen verarbeitet. So wurde zwar im bisherigen Verlauf der Arbeit erläutert, daß die durchzuführenden Analysen auch den Faktor Kosten bzw. Wirtschaftlichkeit beinhalten, jedoch konnte dies nicht mittels der FTA realisiert werden.
Weiterhin sind in Tabelle 3.2.1-4 sowohl stochastisch unabhängige, wie auch abhängige Folgefehler enthalten, deren Modellierung mittels der FTA ebenfalls nicht möglich ist.

Markov-Kette (Zustandsraummodellierung):

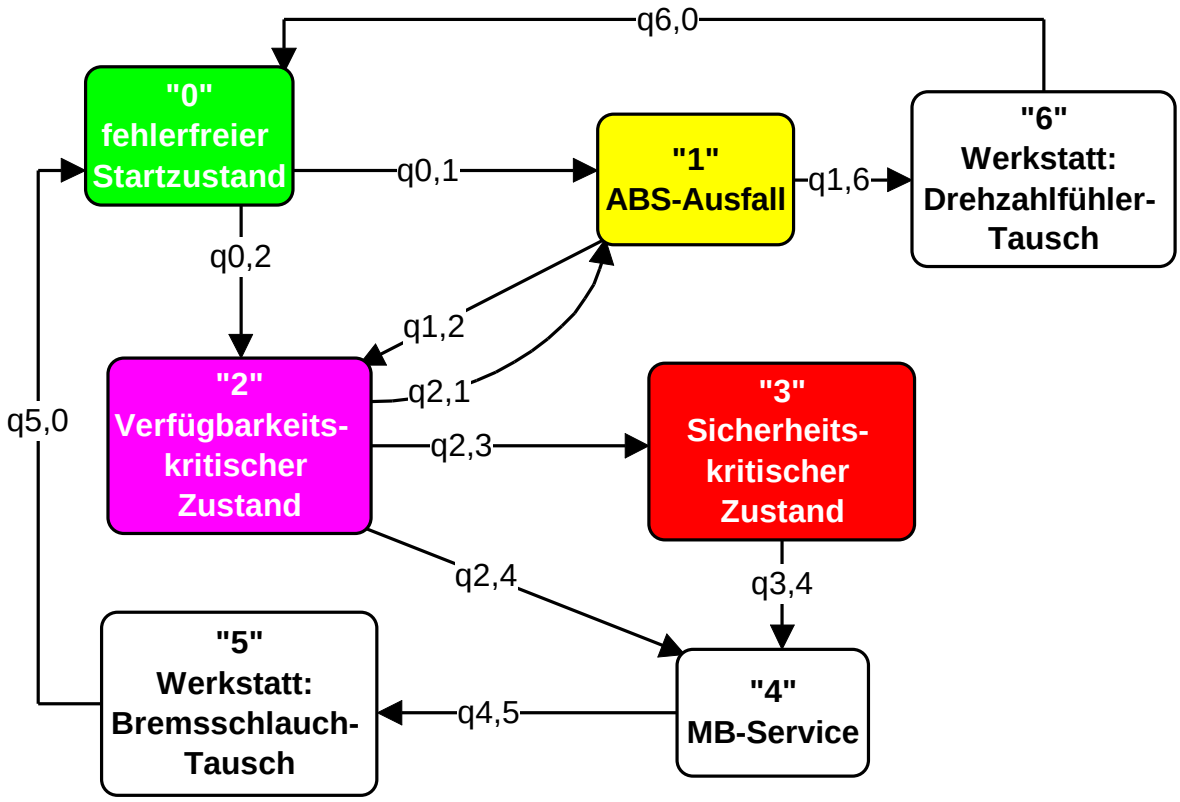


Bild 3.4: Markov-Kette des Systembeispiels ABS-Bremssystem

Kommentare zu den Zuständen in Tabelle 3.2.1 bis 3.2.4 und Bild 3.4:

Rekurrente Zustände sind solche, die innerhalb des unendlich langen Betrachtungszeitraumes vom System unendlich oft eingenommen werden. Durch den Austausch bzw. die Reparatur ausgefallener Komponenten sind die meisten Zustände eines reparierbaren Systems rekurrenter Natur. Für die Zuverlässigkeits- bzw. Sicherheitsbetrachtung sollten auch rekurrente Zustände daher möglichst sicherheits-unkritisch sein.
Im vorliegenden Systembeispiel sind sämtliche Zustände rekurrent.

Absorbierender Zustand: Ein Zustand, der sobald das System in ihn übergeht, nie wieder verlassen wird. Verfügt eine Markov-Kette bei endlich vielen Zuständen nur über einen absorbierenden Zustand, so wird dieser letztendlich irgendwann erreicht. Der Systementwurf sollte dahin wirken, daß der absorbierende Zustand nicht sicherheitsrelevant ist.
In dem vorliegenden Systembeispiel existiert kein absorbierender Zustand. Würde hingegen Zustand 3 immer mit einer Verunfallung enden, d.h. fatale Folgen haben, so würde er absorbierend sein. Eine Einschränkung stellen „**attraktive Zustände**“ dar. Nach [Kur96] handelt es sich hierbei im Gegensatz zu absorbierenden Zuständen um solche, aus denen das System zwar eventuell in einen Folgezustand übergehen kann, wobei die Übergangswahrscheinlichkeit hierfür jedoch sehr gering ist.

Gemäß [Rei88] verfügt eine Markov-Kette über **ergodische** Zustandsteilmengen, wenn sie über mindestens einen Einzelzustand oder einen Teilgraphen verfügt, der - einmal erreicht - im weiteren Prozeßablauf nicht mehr verlassen werden kann. Besteht eine ergodische Menge aus nur einem Zustand, so nennt man diesen absorbierend. Nach Erreichen einer ergodischen Zustandsmenge liegt im weiteren de facto ein Prozeß ohne transiente Zustände vor. Interessant sind daher vor allem die Aussagen bis zum Erreichen der ergodischen Zustandsmenge. Das vorliegende Systembeispiel ist nicht ergodisch.

In [Mah96_1] sind weitere Zustandsklassifikationen aufgeführt.

Chapman-Kolmogorov-Differentialgleichung:
Die Vorgehensweise bei der Aufstellung der Chapman-Kolmogorov-Gleichung ist in [Mah96_1] beschrieben. Für das vorliegende Systembeispiel ergibt sich folgende Gleichung:

$$\frac{d\underline{\pi}(t)}{dt} = \underline{Q} \cdot \underline{\pi} \quad \text{mit } \underline{Q} = \begin{bmatrix} -(q_{01,} + q_{0,2}) & 0 & 0 & 0 & 0 & q_{5,0} & q_{6,0} \\ q_{0,1} & -(q_{1,2} + q_{1,6}) & q_{2,1} & 0 & 0 & 0 & 0 \\ q_{0,2} & q_{1,2} & -(q_{2,1} + q_{2,3} + q_{2,4}) & 0 & 0 & 0 & 0 \\ 0 & 0 & q_{2,3} & -q_{3,4} & 0 & 0 & 0 \\ 0 & 0 & q_{2,4} & q_{3,4} & -q_{4,5} & 0 & 0 \\ 0 & 0 & 0 & 0 & q_{4,5} & -q_{5,0} & 0 \\ 0 & q_{1,6} & 0 & 0 & 0 & 0 & -q_{6,0} \end{bmatrix}$$

Gl. 3-27

$$\underline{Q} \approx \begin{bmatrix} -35{,}5 \cdot 10^{-6} & 0 & 0 & 0 & 0 & 4 & 2 \\ 35 \cdot 10^{-6} & -\frac{1}{3} & 70 \cdot 10^{-6} & 0 & 0 & 0 & 0 \\ 0{,}5 \cdot 10^{-6} & 0{,}5 \cdot 10^{-6} & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0{,}26 \cdot 10^{-6} & -2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -4 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & -2 \end{bmatrix} \cdot \frac{1}{h}$$

$$\underline{\pi} = \begin{pmatrix} \pi_0 \\ \pi_1 \\ \pi_2 \\ \pi_3 \\ \pi_4 \\ \pi_5 \\ \pi_6 \end{pmatrix}$$

Gl. 3-28

Die für die Lösung des Differentialgleichungssystems zusätzlich erforderliche - unabhängige Gleichung lautet:

$$\sum_{i=0}^{6} \pi_i = 1$$ Gl. 3-29

Dieses Gleichungssystem könnte nunmehr via Laplace-Transformation gelöst werden [Mah96_1]. In Abschnitt 3.2.2 wird das Tool MKV vorgestellt, welches eine numerische Lösung der relevanten Zuverlässigkeitskenngrößen liefert, die anschließend dargestellt wird.

Modellierung der Markov-Kette mittels des Tools MKV

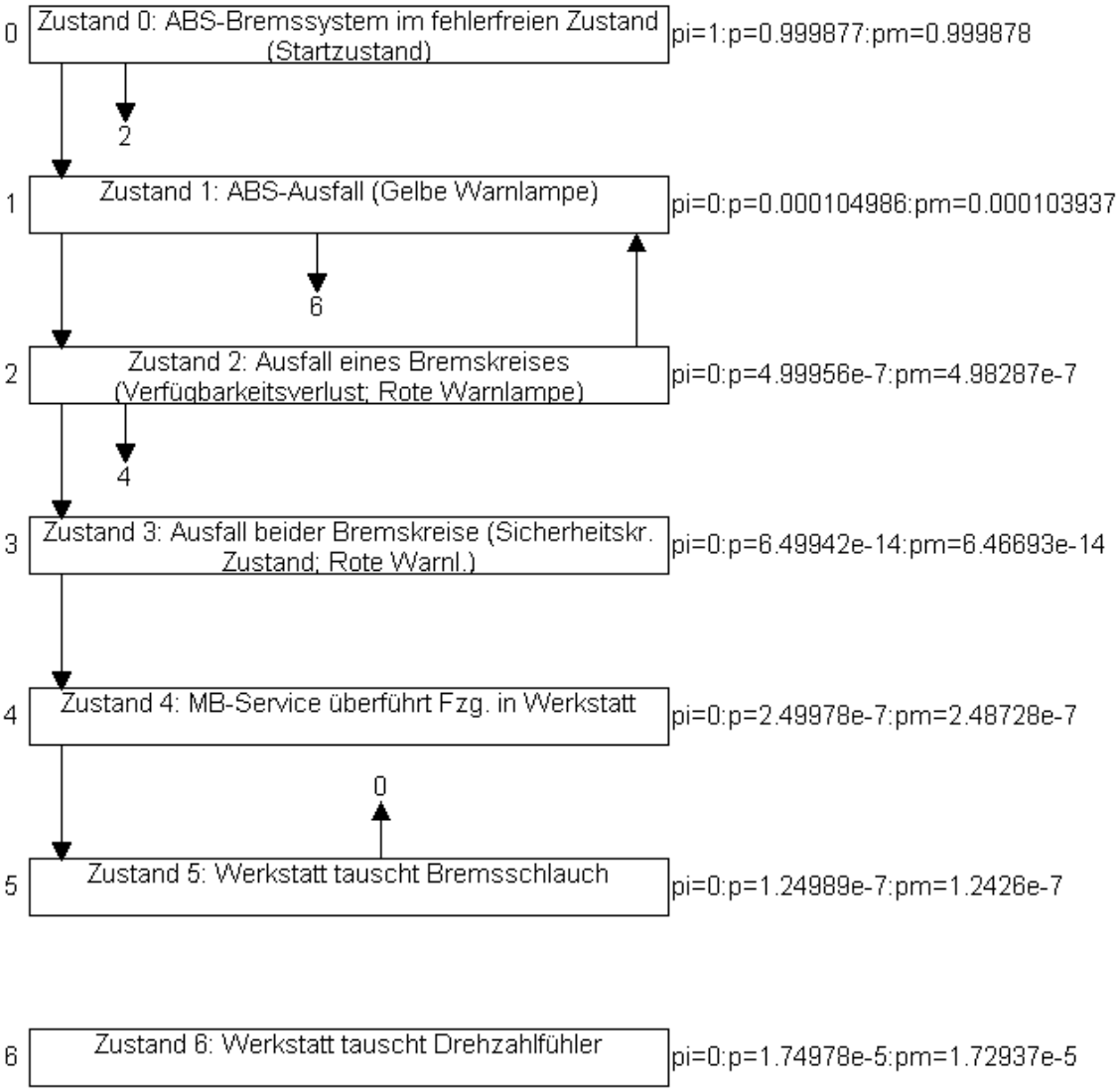


Bild 3.5: MKV-Plot der Markov-Kette des ABS-Bremssystembeispiels

In Bild 3.5 entsprechen

- aus den Zustands-„Rechtecken“ heraustretende Pfeile den Zustandsübergängen bzw. Übergangsraten. Eine an der Pfeilspitze befindliche Nummer weist auf den Zustand hin, in den der Zustandsübergang mündet.
- pi den Startwahrscheinlichkeiten im jeweiligen Zustand.

- p den zum Zeitpunkt t = 300 Stunden bestimmten Aufenthaltswahrscheinlichkeiten im jeweiligen Zustand.
- pm den mittleren Aufenthaltswahrscheinlichkeiten im jeweiligen Zustand.

Stationäre Lösung
Aufsetzend auf Gl. 3-25 ergibt sich für das Systembeispiel folgende stationäre Lösung der C-K-Gl.:

$$\begin{pmatrix}\pi_0\\ \pi_1\\ \pi_2\\ \pi_3\\ \pi_4\\ \pi_5\\ \pi_6\end{pmatrix} = \begin{pmatrix}0{,}999877\\ 0{,}000104987\\ 4{,}99956\cdot 10^{-7}\\ 6{,}4994\cdot 10^{-14}\\ 2{,}49978\cdot 10^{-7}\\ 1{,}24989\cdot 10^{-7}\\ 1{,}74978\cdot 10^{-5}\end{pmatrix} \qquad \text{Gl. 3-30}$$

Betrachtet man Gl. 3-30 mit den in Bild 3.5 bestimmten Aufenthaltswahrscheinlichkeiten, so wird deutlich, daß für das vorliegende Systembeispiel bereits nach 300 Stunden der eingeschwungene Zustand erreicht wurde.

Diskussion der F/V/S/W
Um die Systemparameter F/V/S/W anschaulich zu diskutieren, werden die in Bild 3.5 aufgeführten Zuverlässigkeitskenngrößen für den Zeitpunkt t = 300 Stunden (Nutzungsdauer innerhalb des ersten Betriebsjahres = Garantiezeitraum) auf die Anzahl von 1 Mio. produzierter Fahrzeuge abgebildet.
So führt beispielsweise die Wahrscheinlichkeit p ≥ (10^{-6}≡1ppm) zu einem Fehler in mindestens einem der produzierten Fahrzeuge.

Die Fehlerwahrscheinlichkeit F(t=300h) = 0,000123 entspricht der Wahrscheinlichkeit, daß der Zustand 0 zum Zeitpunkt t=300h verlassen wird. Als Komplement entspricht die Aufenthaltswahrscheinlichkeit im Zustand 0 (0,999877) der Fehlerfreiheit des Systems zum Zeitpunkt t=300h. Ausgehend von 1 Mio. ein Jahr alter, mit dem Antiblockiersystem ausgestatteten Pkw würden 123 dieser Fahrzeuge einen Fehler aufweisen, der zum Verlassen des Zustands 0 führt.

Die Unverfügbarkeit bezieht sich hier auf die Unverfügbarkeit der elektronischen Antiblockier-Funktionalität während des Fahrbetriebs. Hierbei befindet sich das Fahrzeug jedoch nicht in einem sicherheitsrelevanten Zustand. Entsprechend bestimmt sich die Unverfügbarkeit aus der Summe der Aufenthaltswahrscheinlichkeiten in den Zuständen (π_2(t=300h)+π_6(t=300h))=1,8E-5). Ausgehend von der Annahme, daß alle Fahrzeuge innerhalb des ersten Betriebsjahres eine Missionsdauer von 300 Stunden aufweisen, sind zu diesem Zeitpunkt 18 Fahrzeuge im Sinne obiger Definition nicht verfügbar.

Die Unsicherheit, als aus Sicht des Autors wichtigste Kenngröße, bestimmt sich aus der Aufenthaltswahrscheinlichkeit im Zustand 3. Wie Bild 3.5 zu entnehmen ist, befindet sich von 1 Mio. ein Jahr alter, mit dem Antiblockiersystem ausgestatteten Pkw keines im sicherheitskritischen Zustand. Interessant ist jedoch auch die Frage, wieviele Fahrzeuge innerhalb des ersten Betriebsjahres den Zustand 3 einnehmen. Diese quasi Akkumulation der Zustandsaufenthaltswahrscheinlichkeit kann mittels den in dieser Arbeit nicht betrachteten Markov-Reward-Modellen [Sah96] vorgenommen werden. Eine Näherung läßt sich jedoch finden, indem Zustand 3 in einen absorbierenden

Zustand umgewandelt wird. Hierzu wird die Übergangsrate $q_{3,4}$ aus der Markov-Kette entfernt. Die resultierende Aufenthaltswahrscheinlichkeit im Zustand 3 von $3{,}886 \cdot 10^{-11}$ würde bei der angenommen Anzahl von 1Mio. Fahrzeugen jedoch auch noch zu keinem betroffenen Fahrzeug führen. Hierbei ist jedoch zu bedenken, daß diese Näherung bedingt durch den Umstand, daß in den Zustand eingetretene Fahrzeuge nicht wieder repariert, also nicht ein weiteres Mal in den gleichen Zustand geraten können, eine optimistische Abschätzung liefert.

Im weiteren Verlauf der Arbeit sei als Merkmal der Wirtschaftlichkeit eines Systementwurfs vorrangig die Höhe der zu erwartenden Garantie- und Kulanz-Kosten verstanden. Um einen Konzeptvergleich herbeizuführen, wären wie in [Mah97] weiterhin Entwicklungskosten und -zeit sowie Material- und Produktionskosten mitzuberücksichtigen. Die G/K-Kosten lassen sich über das Produkt der in Tabelle 3.2.1-4 aufgeführten Reparatur- und Abschleppkosten mit der Anzahl der in den entsprechenden Zuständen eingetroffenen Fahrzeugen bestimmen. Auch die Garantie- und Kulanz-Kosten sollen nicht für das gesamte Betriebsjahr, sondern für den Zeitpunkt t = 300h ermittelt werden. Folglich bestimmen sie sich aus dem Produkt der Reparatur- und Abschleppkosten mit der Anzahl der in den entsprechenden Zuständen zum Zeitpunkt t =300 h befindlichen Fahrzeugen.

- G/K-Kosten Hydraulikschlauch-Tausch (inkl. Abschleppkosten) :
  Wie Bild 3.5 zu entnehmen ist, wird zum Zeitpunkt t=300h kein Fahrzeug aufgrund eines zu tauschenden Bremsschlauches in die Werkstatt abgeschleppt oder befindet sich bereits dort.
- G/K-Kosten Drehzahlfühler-Tausch :
  Gemäß Bild 3.5 ergeben sich hier folgende G/K-Kosten:
  Zustand 6 = π_6(t=300h)* 1E6 Fzg. * Kosten für Reparatur = 5.249 DM

Abschließende Bemerkungen zu Systembeispiel 1:
Es ist zu betonen, daß obige F/V/S/W-Ergebnisse maßgeblich durch die Wahl der verwendeten in Bild 3.4 bzw. Tabelle 3.2.1-4 skizzierten Zuverlässigkeitskenngrößen bestimmt wurden. Oftmals sind jedoch die Zuverlässigkeitskenngrößen mit einer derart großen Unsicherheit behaftet (siehe Abschnitt 3.1.2.3.5), daß die oben diskutierten Näherungsfehler zur Bestimmung der Unsicherheit und G/K-Kosten als vernachlässigbar anzusehen sind.
Anhand dieses Systembeispiels konnten bereits diverse Leistungsmerkmale der Markov-Ketten-Analyse, wie etwa die geschlossene Modellierung der F/V/S/W, veranschaulicht werden.
So erkennt man weiterhin, daß die hier angesprochenen verfügbarkeitsrelevanten und sicherheitskritischen Zustände eine Teilmenge des Ereignisraumes der fehlerhaften Zustände darstellen.
Damit wird deutlich, daß die Problematik der Sicherheit eine Teilmenge der Zuverlässigkeitstheorie darstellt.
Mittels der hier vorgestellten Markov-Ketten läßt sich beispielsweise unmittelbar ableiten, welche Auswirkungen eine redundante Drehzahlsensorik auf die F/V/S/W des Systems hätte. Wie in Kap. 6 beschrieben, läßt sich durch den in [Ben97] entwickelten analytischen FELB-Algorithmus der fehlerhafte Drehzahlfühler ermitteln. Durch Umschalten auf den fehlerfreien Sensor würde die Notwendigkeit der Fahrerwarnung ausbleiben. Dies trägt unmittelbar zur Steigerung der Kundenzufriedenheit bei. Der Fehler kann beim turnusmäßigen Werkstattaufenthalt aus dem Fehlerspeicher eindeutig dem Drehzahlfühler zugeordnet werden, was zu einer Reduzierung der Arbeitseinheiten und somit G/K-Kosten führt. Natürlich müßten bei einer vollständigen Konzeptbewertung die dem Redundanzgedanken zugrundeliegenden erhöhten Material- und Entwicklungskosten gegenüber

gestellt werden. Wie sich in Abschnitt 3.2.1.2.2 und Kap. 6 zeigen wird, führt ein Komplexitätszuwachs der FELB auch zwangsläufig zu weiteren Fehlermöglichkeiten.
In diesen Ausführungen werden erneut die Wechselwirkungen zwischen F/V/S/W deutlich, womit die durchaus als aufwendig zu bezeichnende geschlossene Systemmodellierung mittels Markov-Ketten an Attraktivität bzw. Berechtigung gewinnt.
Bevor in Abschnitt 3.2.3.1 die Vor- und Nachteile der MKA detailliert werden, sind in Systembeispiel 2 weitere mittels der MKA modellierbare konstruktive Zuverlässigkeitskenngrößen vorzustellen.

3.2.1.2.2 Systembeispiel 2: Detaillierung der FELB-Modellierung / konstruktive Zuverlässigkeitskenngrößen

Mit Blick auf die in Abschnitt 2.3.2 formulierte Sicherheitsanforderung, gefährliche Einfachfehler zuverlässig erkennen und ihren Einfluß auf das Systemverhalten unterdrücken zu können, stellt sich die Frage, welche Qualitätsmerkmale die hierfür erforderliche FELB aufweisen muß.
Nach Einschätzung des Autors finden sich in der Literatur noch keine die FELB-Qualitätsmerkmale hinreichend detailliert modellierenden Ansätze.
So wurde beispielsweise in [Van93] die FELB lediglich als ein geschlossenes Modul (Task) betrachtet und mit einer Fehlerrate behaftet. [Konakovsky] und [Coza] unterschieden bereits nach Fehlerentdeckungswahrscheinlichkeit, wobei hier der Fehlalarm, Falschbehandlung etc. ebenfalls nicht betrachtet wurden. Jedoch ist gerade das Systemverhalten in diesen sicherheitskritischen Zuständen von Interesse.
Anhand des vorliegenden Beispiels soll die aus Sicht des Autors geeignete Detaillierung für die FELB-Modellierung im Zustandsraum erfolgen. Aufsetzend auf der bereits in Abschnitt 3.1 beschriebenen Ausfallrate werden hierfür weitere Übergangsraten definiert.

Systembeschreibung:
In Bild 3.6 sind die einzelnen möglichen Folgezustände der FELB auf einen einfachen Komponentenfehler zu erkennen. Dieses Beispiel soll der Veranschaulichung der Thematik dienen, ohne den Betrachter durch unnötig komplexe Zustandsraumdarstellungen zu verwirren. An dieser Stelle soll daher auch mit Verweis auf Systembeispiel 1 und Kap. 5-6 auf die quantitative Bestimmung der Zustandsaufenthaltswahrscheinlichkeiten verzichtet werden.
Die softwaremäßige Realisierung der FELB sei unabhängig von der Schwere des Fehlers, den das betreffende Modul erkennt, lokalisiert oder behandelt als **Si**cherheits**s**oftware (SIS) bezeichnet.
Über die Ausfallrate und die werkstattseitige bzw. Offboard-Reparaturrate sind für die FELB sowohl „konstruktive“ wie auch „destruktive“, d.h. der FELB zuträgliche bzw. diese erschwerende Zuverlässigkeitskenngrößen von Bedeutung.

„Konstruktive“ Zuverlässigkeitskenngrößen
In Anlehnung an [Sch73] werden für die vorliegende Arbeit die mit erfolgreicher Fehlererkennung, -lokalisation und -behandlung verknüpften Onboard-FELB-Übergangsraten definiert:

- Fehlererkennungsrate ε = 1/MTTD (**m**ean **t**ime **t**o **d**etect).
- Fehlerlokalisationsrate χ = 1/MTTL (**m**ean **t**ime **t**o **l**ocate).
- Onboard Fehlerbehandlungsrate ζ = 1/MTTO (**m**ean **t**ime **t**o rec**o**ver) bzw. Kehrwert der Zeitspanne bis zur Aktivierung einer optischen Aufforderung an den Fahrer, die Werkstatt anzufahren.

Hinsichtlich ihres zeitlichen Verhaltens sei wie bei der MTBF (siehe Abschnitt 3.1.2.2) von einer Zeitinvarianz ausgegangen, was exponentialverteilte Übergangswahrscheinlichkeiten impliziert. Diese Annahme scheint insbesondere vor dem Hintergrund der zeitlich sehr viel größeren MTBFs akzeptierbar, was für die geschlossene Lösbarkeit der C-K-Gl eine wichtige Voraussetzung ist. Zeitvariante Übergangsraten würden lediglich eine numerische Lösung der C-K-Gl ermöglichen. Unter gewissen Umständen lassen sich jedoch durch Einführung zusätzlicher „Hilfszustände“ zeitvariante Übergangsraten in zeitinvariante überführen. Hierfür sei auf [Rei88] verwiesen.

Neben den oben skizzierten Onboard-Größen gibt es auch die mit dem Werkstatt-aufenthalt zusammenhängenden Offboard-F/V/S/W-Parameter, die ebenfalls als konstante Zustandsübergangsraten verstanden seien:

- Werkstatterreichensrate ν = 1/MTTS (**m**ean **t**ime **t**o reach **s**ervice)
  Hierunter sei der Kehrwert der mittleren Dauer bis zum Erreichen der Werkstatt verstanden.
- Offboard-Fehlerbehebungsrate bzw. -Reparaturrate (~Werkstattaufenthaltsdauer) μ = 1/MTTR (**m**ean **t**ime **t**o **r**eturn to customer bzw. **m**ean **t**ime **t**o **r**epair). Hierunter sei der Kehrwert der mittleren Dauer vom Erreichen der Werkstatt bis zur Rückgabe des Fahrzeugs an den Kunden verstanden.
  Der Umstand, daß werkstattseitig ein Bauteil ausgetauscht wird, welches nicht ursächlich für die Fehlermeldung war bzw. ein defektes Bauteil eingebaut wird, sollen an dieser Stelle nicht weiter betrachtet werden.

FELB-Fehler / „destruktive“ Zuverlässigkeitskenngrößen
Sämtliche im letzten Abschnitt diskutierten Zuverlässigkeitskenngrößen sind konstruktiver, d.h. dem Fehlersymptom „heilend“ entgegenwirkender Natur.
Wie jedoch bereits in Abschnitt 2.4 erwähnt bzw. sich in den Kap. 5 und 6 zeigen wird, darf die FELB nicht als fehlerfreier Wächter angesehen werden.
Fehler der FELB sind entsprechend der in Abschnitt 2.4 vorgenommenen Modularisierung auf die folgenden destruktiven Zuverlässigkeitskenngrößen reduzierbar:

- **Fehlalarm**
  Hierunter sei ein Fehler des Fehlererkennungsmoduls verstanden, der sich in der Art bemerkbar macht, daß das Modul beispielsweise einen Sensorfehler meldet/erkennt, obwohl keiner vorliegt. Somit wird unbegründeterweise ein Alarm abgegeben. Wird dem Kunden dieser Alarm mitgeteilt, trägt dies zu seiner Verunsicherung oder Unzufriedenheit gegenüber dem System bzw. der Automobilmarke bei. Da diese Fehler meist auf eine unzureichende Modellierung der zu detektierenden Sensorfehlerszenarien zurückzuführen sind, handelt es sich hierbei um Softwarefehler. **Wie bereits in Abschnitt 3.1.2.4 erläutert, sollen diese Fehler im Rahmen der vorliegenden Arbeit nicht hinsichtlich ihrer Auswirkungen auf die F/V/S/W untersucht werden.** Obwohl

derzeit das Fehlerverhalten von Software nicht befriedigend modellierbar ist, soll der Übergang in Bild 3.6 qualitativ berücksichtigt werden. Der Umstand, daß keine Fehlerrate angebbar ist, ist durch das Weglassen der Übergangsrate berücksichtigt.

- **Mißalarm**
  Hierunter sei ein Fehler des Fehlererkennungsmoduls verstanden, der sich in der Art ausdrückt, daß das Modul trotz Vorhandensein eines Sensorfehlers diesen nicht signalisiert. Entsprechend bleibt der berechtigte Alarm aus. Da dieses „Schweigen" in der in Bild 3.6 gewählten Modellierung nicht zum Verlassen des Zustands „Komponente fehlerhaft" führt, ist hier für den Mißalarm keine Zustandsübergangsrate anzugeben.
  Es ist jedoch wichtig zu betonen, daß der nicht erkannte Fehler je nach Art dieses Fehlers und seiner Auswirkungen auf das Gesamtsystemverhalten sicherheitsrelevant sein kann.
  In den in Kap. 5 und 6 folgenden Markov-Ketten-Modellierungen wird durch die Analyse der Auswirkungen verschiedener Fehlermoden der Sensorik die Frage des Mißalarms um die Facette des absorbierenden Zustands „Fehler nicht erkennbar, da nicht im Fehlererkennungsmodul modelliert" erweitert. Die Übergangsrate in diesen Zustand entspricht der Fehlerrate des betrachteten Fehlermodes.

- **Falschlokalisation**
  Hierunter sei der Umstand verstanden, daß bei Vorliegen eines bestimmten Sensorfehlers und erfolgter Fehlererkennungsmeldung ein anderer Sensor, als der ursächliche als fehlerhaft lokalisiert wird. Ein fehlerfreies Objekt wird also als ursächlich angezeigt, das fehlerhafte folglich als korrekt interpretiert. Wenn sich dieser Fehler bis auf die Fehlerbehandlung überträgt, kann dies sicherheitskritische Auswirkungen haben.
  Wie schon im Falle des Fehlalarms, ist die Falschlokalisation auf einen nicht stochastischen Softwarefehler zurückzuführen und ist daher in Kap. 5 und 6 nicht berücksichtigt.

- **Mißlokalisation**
  Hierunter sei eine „Unterlassung" des Fehlerlokalisationsmoduls verstanden, die sich in der Art ausdrückt, daß das Modul trotz Vorhandensein eines Sensorfehlers und des Vorliegens einer Fehlermeldung den fehlerhaften Sensor nicht identifiziert. Die berechtigte Fehlerlokalisation bleibt aus. Hierbei muß es sich nicht zwangsläufig um einen Fehler des Fehlerlokalisationsmoduls handeln. Eine mögliche Ursache ist eine auftretende zeitliche Verzögerung, da beispielsweise ein Softfailure innerhalb eines Sensors vor Überschreiten der Fehlerlokalisationsschwelle nicht eindeutig zugeordnet werden kann. Wie schon im Fall des Mißalarms, ist hier keine Zustandsübergangsrate anzugeben. Auch dieses Verbleiben im aktuellen Zustand kann je nach Art des vorliegenden Sensorfehlers sicherheitsrelevant sein.
  Durch die Fehlermodendetaillierung wird in Kap. 5 und 6 die Übergangsrate in den Zustand „Fehler nicht lokalisierbar" durch die Fehlerrate des betreffenden Fehlermodes des ursächlichen Sensors bestimmt.

- **Falschbehandlung**
  Hierunter sei der Umstand verstanden, daß trotz Vorliegen einer eindeutigen Fehlerlokalisation bzw. eines Hardfailure-Alarms ein nicht ursächliches Bauteil aus dem Funktionsumfang eliminiert wird, das defekte sein Signal jedoch weiter einbringen kann. Auch dieser Sachverhalt kann sicherheitsrelevant sein. Wie schon im Falle des Fehlalarms und der Falschlokalisation ist die Falschbehandlung auf einen nicht stochastischen Softwarefehler zurückzuführen.

- **Mißbehandlung**
  Hierunter sei eine „Unterlassung" des Fehlerbehandlungsmoduls verstanden, die sich in der Art ausdrückt, daß das Modul trotz Vorhandensein einer Fehlerlokalisationsmeldung bzw. einer Hardfailure-Meldung keine Fehlerbehandlung vornimmt. D.h. die berechtigte Fehlerbehandlung bleibt aus. Hierbei muß es sich nicht zwangsläufig um einen Fehler des Fehlerbehandlungsmoduls handeln. Eine mögliche Ursache ist eine zeitliche Verzögerung vom Zeitpunkt der Fehlerlokalisation bis zur möglicherweise HW-seitigen Eliminierung der fehlerhaften Sensorinformation aus dem Funktionsumfang bzw. der Warnung des Fahrers und der Ablegung der Fehlerbehandlungsmeldung im Fehlerspeicher. Wie schon im Fall von Mißalarm und -lokalisation ist hier keine Zustandsübergangsrate anzugeben, der Verbleib im Ausgangszustand eventuell sicherheitsrelevant.
  Durch die Fehlermodendetaillierung wird in Kap. 5 und 6 die Übergangsrate in den Zustand „Fehler nicht behandelbar" durch die Fehlerrate des betreffenden Fehlermodes des Sensors bestimmt.

Weitere Anmerkung zu den destruktiven Zuverlässigkeitskenngrößen der FELB

- In der hier gewählten Modellierung der FELB-Fehlermöglichkeiten lassen sich die destruktiven Zuverlässigkeitskenngrößen nicht quantifizieren.
- Wie sich jedoch in Kap. 5 und 6 zeigen wird, sind diese Zuverlässigkeitskenngrößen über die Fehlerraten der betreffenden Sensor-Fehlermoden bestimmt. Gerade diese Zustände bzw. Zustandsübergänge sind für die Bewertung der Verfügbarkeit aber vor allem der Sicherheit von größter Bedeutung.
- Ein „Falschalarm" der FELB kann ausgeschlossen werden, da ein Alarm nur die Anwesenheit eines Fehlers signalisiert, nicht aber auf seinen Ursprung hindeutet.
- Eine „Fehllokalisation" würde implizieren, daß zwar kein Alarm, also keine fehlerhafte Komponente vorläge, dennoch eine bestimmte Komponente als fehlerhaft identifiziert würde. Diese Fehllokalisation wird ausgeschlossen, da erst bei Vorliegen einer Fehlermeldung (Signal des Fehlererkennungsmoduls) das Fehlerlokalisationsmodul aktiviert, d.h. durchlaufen wird.
- Eine „Fehlbehandlung" würde implizieren, daß keine Fehlerlokalisation bzw. kein Fehlalarm vorläge, jedoch eine Fehlerbehandlung eingeleitet würde. Diese Art der Behandlung wird ausgeschlossen, da erst bei Vorliegen der Fehlerlokalisationsmeldung bzw. des Hardfailure-Alarms das Fehlerbehandlungsmodul aktiviert, d.h. durchlaufen wird.
- Weiterhin besteht ebenso die Möglichkeit, daß während des Werkstattaufenthaltes trotz korrektem Eintrag im Fehlerspeicher das falsche Bauteil getauscht wird. Diese Fehlaustäusche sollen jedoch im weiteren Verlauf der Arbeit vernachlässigt werden.

Markov-Kette (Zustandsraummodellierung)

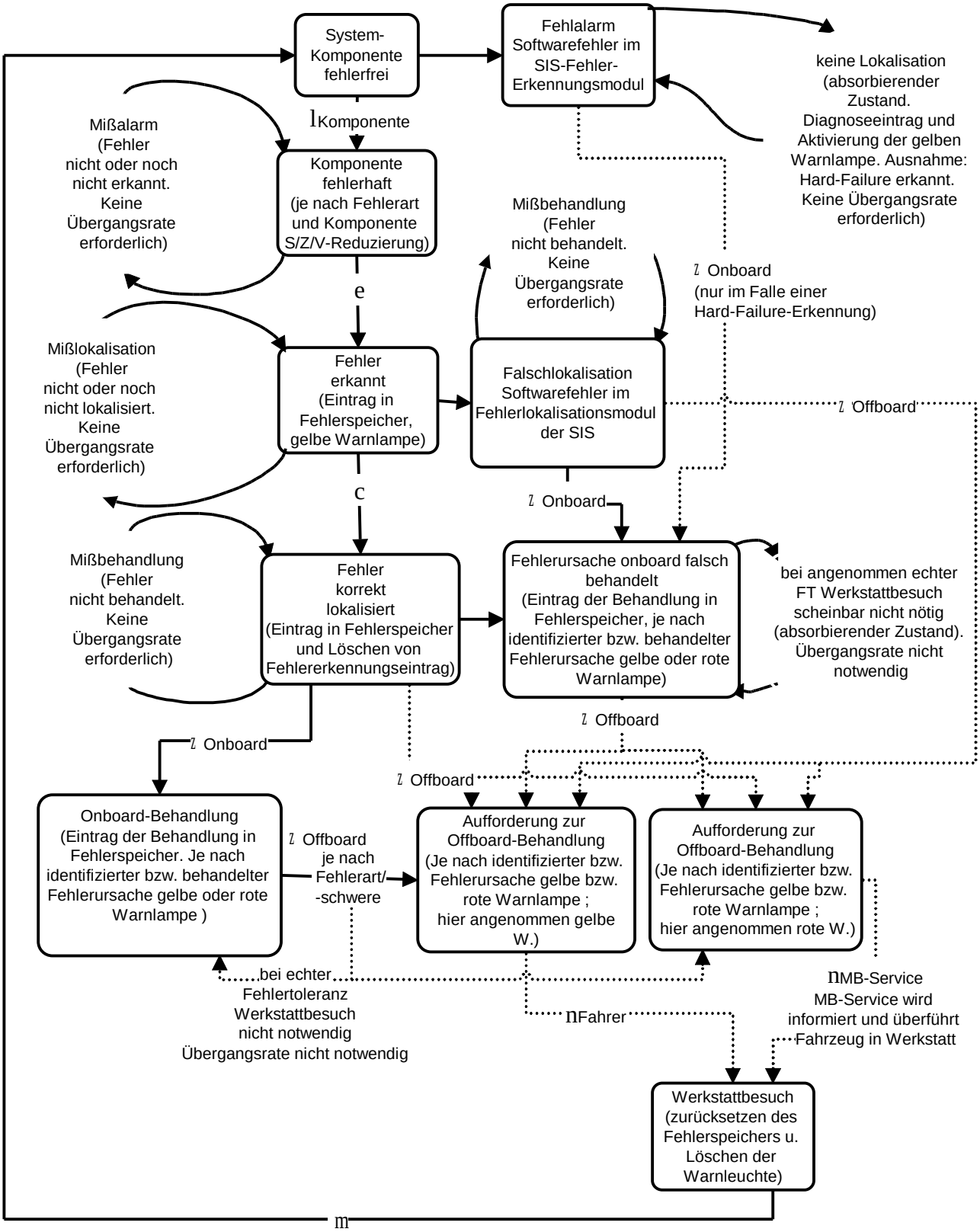


Bild 3.6: Darstellung der Markov-Kette einer SIS zur FELB einer Hardwarekomponente.

In obiger Darstellung wird davon ausgegangen, daß die Fehlerbehandlung onboard vorgenommen werden kann. Gestrichelt sind jedoch auch die Übergänge hin zu den Offboard-Fehlerbehandlungen bzw. zur werkstattseitigen Reparatur skizziert.

Da die Hardwarekomponente und ihr Fehlerverhalten nicht weiter spezifiziert wurde, kann in diesem Systembeispiel nicht nach sicherheits- und verfügbarkeitskritischen Zuständen differenziert werden. Entsprechend wurde hier abweichend von Bild 3.4 auf die farbliche Hervorhebung verzichtet.

Kommentare zu den Zuständen und Zustandsübergängen

$\nu_{MB\text{-}Service:}$ dient der Berücksichtigung des Umstandes, daß nach Aufleuchten der roten Warnlampe das Fahrzeug unverzüglich zu parkieren ist. Anschließend wird das Fahrzeug durch den MB-Service in die Werkstatt überführt und dort repariert.

ν_{Fahrer}: im Falle des Aufleuchtens der gelben Warnlampe wird dem Fahrer die Empfehlung zum baldigen Aufsuchen der Werkstatt signalisiert. Die Übergangsrate entspricht dem Kehrwert der zu veranschlagenden Zeitspanne von der Fahrerwarnung bis zum Eintreffen in der Werkstatt.

Anmerkung zu den Zustandsübergängen, wo Start- und Zielzustand identisch sind:

In diesen Übergängen, denen keine Übergangsraten zugeordnet sind, spiegeln sich auch systematische Fehler wieder. So ist eine mögliche Ursache für einen Mißalarm, daß das vorliegende Fehlerszenario nicht bedacht und Algorithmen zu seiner Erkennung nicht mitmodelliert wurden.

Anmerkung zur „Gedächtnislosigkeit“ der Markov-Ketten der FELB-SIS:

In [Wal86] wird darauf hingewiesen, daß herkömmliche Markov-Ketten, wie sie in dieser Arbeit verwendet werden, nicht zur Modellierung von Memory-Funktionen angewandt werden dürfen. Wie sich jedoch in Kap. 4-6 zeigen wird, sehen die meisten Algorithmen zur Erkennung und Lokalisation von verrauschten Sensorsignalen die Glättung durch Butterworth-Tiefpaßfilter und den Einsatz von Fehlerzählern vor. Insbesondere die Fehlerzähler basieren auf der Verarbeitung bzw. Speicherung eines limitierten zeitlichen Fehlerfensters. So werden in heutigen Seriensystemen wie ABS und ASR Fehlerzähler eingesetzt, was bedeutet, daß die ABS-Regelung, aber auch eine Fehlererkennung erst einsetzt, wenn zu mehreren aufeinanderfolgenden Zeitpunkten eine definierte Schlupfgrenze bzw. eine Fehlerschwelle überschritten wurde. Damit stellt sich die Frage, inwieweit die Berücksichtigung von der Vergangenheit entnommenen Sensorwerten eine Modellierung mittels Markov-Ketten erlaubt.

Wie sich in Kap. 4 zeigen wird, nutzt die D-b-W-Sicherheitssoftware einen Fehlerzähler basierend auf der Verarbeitung von 6 aufeinanderfolgenden Meßwerten. Das erforderliche Fehlerfenster beträgt bei einer Zykluszeit von 10ms lediglich 60ms. Diese Zeitspanne ist relativ zum interessierenden F/V/S/W-Verhalten des Systems innerhalb des ersten Betriebsjahres derart gering, daß [Van93] hier von einer tolerierbaren Verletzung der „Markov’schen“-Forderung spricht (siehe auch Abschnitt 1.1.1).

Da Bild 3.6 ansonsten selbsterklärend ist, soll hier auf weitere Ausführungen verzichtet werden. In Kap. 5 und 6 finden sich quantitative Auswertungen der für die D-b-W-SIS entwickelten Markov-Ketten. Hier kann auch, wie in Abschnitt 3.2.1.2.1 eine eindeutige Klassifikation der Zustände hinsichtlich ihrer Verfügbarkeits- und Sicherheitsrelevanz erfolgen.

Diskussion der F/V/S/W, Maßnahmen zur Optimierung dieser Qualitätsparameter

- Betrachtet man beispielsweise die Definition der Fehlererkennungsrate, so wird deutlich, daß sich eine Verkürzung der Zykluszeit, mit der die SIS durchlaufen wird, positiv auf die Fehlererkennungszeit und damit auf die Verfügbarkeit und Sicherheit des Systems auswirkt. Inwieweit sich der Einsatz leistungsfähigerer Rechner finanziell lohnt, ist durch Abwägung der Materialkosten gegenüber der G/K-Kosten, aber auch der Auswirkungen auf das Markenimage bzw. die Kundenzufriedenheit, zu bestimmen.
- Eine in [Wal86] beschriebene Möglichkeit zur Reduzierung der FELB-Zeiten und damit zur Steigerung der Verfügbarkeit und Sicherheit basiert auf der Optimierung der Fehlerzählerstrategien. So führt eine Reduzierung des zeitlichen Fensters oder eine Senkung der zu überschreitenden Fehlerschwelle zu einer Verkürzung der Fehlererkennungszeit. Gleichzeitig nimmt somit aber auch die Wahrscheinlichkeit eines Fehlalarms zu, da bereits tolerierbares Sensorrauschen als Fehler interpretiert werden könnte. Diese dem Gebiet der Entscheidungstheorie zuzuordnende Thematik soll jedoch in der vorliegenden Arbeit nicht vertieft werden.
- In [Sch77] wird eine Verkürzung der Missionsdauer als Strategie zur gleichzeitigen Optimierung der Verfügbarkeit wie auch Sicherheit dargestellt. Diese Verkürzung wird durch turnusmäßige Inspektionen bzw. Austäusche hochbeanspruchter Komponenten erwirkt. Da jedoch im Automobilsektor das Bestreben besteht, Wartungsintervalle zu verlängern bzw. wartungsfreie Systeme zu entwickeln, soll obige Strategie in der vorliegenden Arbeit nicht verfolgt werden.

Abschließende Bemerkungen zum Systembeispiel 2

- In Systembeispiel 2 wurden erstmalig für die detaillierte F/V/S/W-Analyse von FELB-Algorithmen geeignete Zuverlässigkeitskenngrößen definiert. Diese werden in Kap. 4-6 zur quantitativen Bestimmung der Zustandsaufenthaltswahrscheinlichkeiten der für die D-b-W-SIS zu formulierenden Markov-Ketten verwendet.
- In Bild 3.6 wurden bereits Fahrer-Warnphilosophien für zukünftige X-by-Wire-Systeme diskutiert. Im weiteren Verlauf der Arbeit sei davon ausgegangen, daß dem Fahrer sämtliche Fehler, die eine Funktionsdegradierung zur Folge haben, durch optische Signale kommuniziert werden müssen. Es wird weiterhin davon ausgegangen, daß der Fahrer das Fahrzeug infolge einer roten Warnlampe innerhalb kürzester Zeit parkiert und einen Abschleppvorgang einleitet. Auf eine gelbe Warnlampe reagiert der Fahrer mit einem der Fehlermeldung angepaßten Fahrverhalten und baldigem Aufsuchen einer Werkstatt, wobei hier davon ausgegangen wurde, daß er die Werkstatt binnen durchschnittlich 3 Stunden erreicht.
- Wie Bild 3.6 zu entnehmen ist, wird im weiteren Verlauf der Arbeit auch für Markov-Ketten von der Monotonie des Systemverhaltens ausgegangen. Dies schließt beispielsweise aus, daß die einer Falschlokalisation folgende Falschbehandlung das fehlerhafte Bauteil wegschaltet. Die Wahrscheinlichkeit für einen derartigen „heilenden“ Folgefehler sei mit Blick auf den Umstand, daß es sich hierbei um den dritten Fehler im System handeln würde als vernachlässigbar gering angenommen.
- Vielmehr beschränkt sich die Markov-Ketten-Analyse mit Blick auf die Zustandsraumexplosion auf Einfachfehler innerhalb des D-b-W-Umfanges bzw. Folgefehler innerhalb der FELB-SIS.

3.2.2 Markov-Ketten-Tool „MKV“

Das Tool MKV wurde detailliert in [Kur96] bzw. in der Dokumentation der Firma ITEM beschrieben. An dieser Stelle sollen daher lediglich für den weiteren Verlauf wichtige Eigenschaften beschrieben werden.

- Das Tool bietet die Möglichkeit, explizit „Unavailability-States“ anzuwählen. Die anschließend berechnete Systemunverfügbarkeit bestimmt sich aus der Summe der aktuellen Aufenthaltswahrscheinlichkeiten der angewählten Zustände. Die berechnete Unreliability entspricht der Summe der Eintretenswahrscheinlichkeiten in die Unavailability-States. Handelt es sich um absorbierende Zustände, so ist die berechnete Unverfügbarkeit und Unreliability identisch.
- Weiterhin bietet das Tool die Möglichkeit, turnusmäßige Inspektionen zu modellieren. Hiermit ließe sich der Umstand berücksichtigen, daß während des Fahrbetriebs nicht entdeckte Fehler in der Werkstatt erkannt und behoben werden können. Dieses Feature soll in der vorliegenden Arbeit jedoch aus folgenden Gründen nicht zum Einsatz kommen:
    - Es ist das Bestreben der Automobil-Hersteller wartungsfreie Fahrzeuge zu entwickeln. Mit Blick auf den gewählten Betrachtungszeitraum des ersten Betriebsjahres des Fahrzeugs sind Inspektionen bereits in naher Zukunft vermeidbar. Folglich ist kein fester Turnus anzugeben.
    - Da noch keine Robustheitsuntersuchungen für den sicherheitsrelevanten D-b-W-Regler vorgenommen wurden, ist im Sinne einer pessimistischen Sicherheitsanalyse davon auszugehen, daß sämtliche Fehler zu einer nicht tolerierbaren und damit über kurz oder lang vom Fahrer bemerkbaren Funktionsminderung führen.

3.2.3 Abschließende Anmerkungen zur Markov-Ketten-Analyse

Anliegen des Abschnittes 3.2 war es, eine Einführung in die Theorie der Markov-Ketten und ihr Anwendungspotential hinsichtlich der geschlossenen F/V/S/W-Analyse zukünftiger Kfz-Systeme zu vermitteln. Zu diesem Zweck wurden speziell für die Markov-Ketten-Analyse sicherheitsrelevanter Kfz-Systeme geeignete Zuverlässigkeitskenngrößen vorgestellt und anhand zweier Anwendungsbeispiele verdeutlicht. Abschließend sollen Vorzüge und Defizite der Markov-Ketten gegenüber der Fehlerbaumanalyse zusammengefaßt werden.

3.2.3.1 Vor- und Nachteile der Markov-Ketten-Analyse gegenüber nicht zustandsraumorientierten Zuverlässigkeitsanalysemethoden wie der FTA

Wesentliche Vorzüge der Markov-Ketten-Analyse

- **Geschlossene Modellierung der F/V/S**
  Mittels Markov-Ketten können die Systemparameter Fehlerhäufigkeit, Verfügbarkeit und Sicherheit im Zustandsraum in einer geschlossenen Darstellung qualitativ wie auch quantitativ bestimmt werden.
- **Berücksichtigung des Faktors Kosten/Wirtschaftlichkeit**
  In Abschnitt 3.2.1.2.1 wurde die Modellierung des Faktors Wirtschaftlichkeit mittels Markov-Ketten vorgestellt. Markov-Reward-Modelle [Sah96], die jedoch nicht Bestandteil der vorliegenden Arbeit sind, erlauben es darüberhinaus, zeitvariante Kostenfunktionen zu berücksichtigen.

- **Dynamische Systemanalyse / Graceful-Degradation / Diversitäre Strukturen.**
  Gegenüber der rein statischen Systembetrachtung „nicht-zustandsraumorientierter" Analysemethoden erlaubt es die Markov-Ketten-Analyse, das Systemverhalten über den Fehler bzw. die Umkonfiguration (Graceful-Degradation) hinaus zu betrachten. Somit sind mittels MKA zeitlich aufeinander folgende Mehrfachfehler wie auch Degradationsmechanismen und diversitäre Strukturen modellierbar. Siehe auch Abschnitt 3.2.1.2.2, Kap. 4 und [Mah97].
- **Stochastische Abhängigkeiten**
  Mittels Markov-Ketten lassen sich Abhängigkeiten der Systemkomponenten, wie beispielsweise kalte und warme Redundanzen im Standby-Betrieb, gemeinsame Reparatureinrichtungen bzw. -personal für mehrere Komponenten bzw. Subsysteme modellieren (siehe Abschnitt 3.2.1.2.1 und [Mah96_1]).
- **Semi-Markov Ketten**
  Bei homogenen Markov-Ketten mit konstanten Übergangsraten ist die Zustandsverweildauer exponentialverteilt. Semi-Markov Ketten erlauben es, darüberhinaus, andere Verteilungsfunktionen wie beispielsweise die Weibull-Verteilung zu approximieren, die das Ausfallverhalten mechanischer Bauteile wiedergibt.

Defizite der Markov-Ketten-Analyse

- **Zustandsraumexplosion**
  Wie den bisherigen Ausführungen des Abschnitt 3.2 zu entnehmen ist, steht den Vorzügen der Markov-Ketten-Modellierung ein relativ zur betrachteten Systemgröße enormer Modellierungsaufwand entgegen.
  Für die Modellierung des Ausfallverhaltens eines Systems von n Komponenten, die ihrerseits jeweils die beiden Zustände (OK/DEFEKT) einnehmen können, bedarf es eines Markov-Ketten-Modells, bestehend aus 2^n Zuständen. Dieser Modellierungsaufwand wird auch als Zustandsraumexplosion bezeichnet.
  Die Lösung der Chapman-Kolmogorov-Differentialgleichung (Gl. 3-24) praxisrelevanter Systeme ist ohne Zuhilfenahme geeigneter Software-Tools nicht denkbar. Die in Kap. 2.3 (Sicherheitsmaßstäbe) fixierten Forderungen an die zuverlässige Erkennung gefährlicher Einfachfehler bietet jedoch die Möglichkeit, die F/V/S/W-Betrachungen in dieser Arbeit auf Einfachfehler innerhalb der Sensorik (siehe Kap. 4 und 5) bzw. Reaktionen der FELB auf diese Fehler, sowie Fehler letzterer zu beschränken.
  Grundsätzlich gilt die Empfehlung, Markov-Ketten lediglich für die F/V/S-Modellierung der Subsysteme zu verwenden, deren Eigenschaften (siehe Vorteile der MKA) eine zustandsraumorientierte Analyse bedürfen. Alle anderen Teilsysteme werden in der vorliegenden Arbeit mittels der FTA analysiert. Eine damit einhergehende Fusion der resultierenden Ergebnisse beider Analysemethoden führt zu den in Abschnitt 3.3 vorzustellenden „Hierarchischen Modellen".
- **Modellierungsaufwand bei Systemmodifikationen**
  Veränderungen des Systementwurfs bedürfen Modifikationen der Zustandsraumdarstellung, die mitunter mit erheblichem Aufwand verbunden sind. Dies führt unmittelbar zum Anwachsen der Wahrscheinlichkeit von Modellierungsfehlern, die mögliche Fehlerquelle bei der F/V/S-Analyse komplexer Systeme darstellen.

- **„Steife“ Markov-Ketten**
  Bedingt durch die in Abschnitt 3.2.1.2. bzw. Kap. 4 beschriebenen enormen Größenordnungsunterschiede zwischen Ausfallraten und Reparatur- bzw. FELB-Raten, können sich numerische Probleme bei der Lösung der Chapman-Kolmogorov-Differentialgleichung via Runge-Kutta-Methode ergeben. Diese Problematik wird in der Literatur als „stiffness“ der Markov-Ketten bezeichnet. Das Tool MKV bietet die Möglichkeit, durch eine reduzierte Rechengenauigkeit diese Schwierigkeit zu umgehen. Jedoch stellt sich die Frage, ob die verbleibende Rechengenauigkeit akzeptiert werden kann. In [Kur96] ergaben sich hierbei mitunter negative und damit unplausible Zustandsaufenthaltswahrscheinlichkeiten.
  Eine aus Sicht des Autors akzeptable Möglichkeit die Thematik zu entschärfen, basiert auf der Reduzierung der Missionsdauer. So hilft es bereits, die Missionsdauer auf nur eine 1 Stunde zu verkürzen. Diese erscheint zwar in Relation zur Gesamtnutzungsdauer des Fahrzeugs sehr kurz, womit nur eine sehr geringe Fehlerwahrscheinlichkeit zu verzeichnen sein wird, jedoch bietet hier gerade die Möglichkeit der vergleichenden Analyse verschiedener Systemkonzepte Abhilfe. Indem nämlich verschiedene Systemkonzepte mit der gleichen Missionsdauer analysiert werden, kann die F/V/S/W-Aussage als Relativaussage erfolgen. Aus Kap. 4 wird hervorgehen, daß der Rechenzyklus des Systems D-b-W 10ms betragen soll. Damit werden innerhalb der Missionsdauer von 1 Stunde immerhin 360.000 Rechenzyklen absolviert. Eine Optimierung dieses Ansatzes erfolgt, wenn die zu analysierende Markov-Kette über eine stationäre Lösung (siehe Gl. 3-25) verfügt und die verwandte Missionsdauer in der Größenordnung der Zeitspanne bis zum Erreichen des stationären Zustandes liegt. Inwieweit die für D-b-W zu formulierenden Markov-Ketten bereits nach einer Missionsdauer von einer Stunde den stationären Zustand erreichen, ist in Kap. 5 und 6 zu untersuchen.

3.2.3.2 Kurzanleitung zur Aufstellung von Markov-Ketten

1. Wie bei der FTA, ist eine wesentliche Voraussetzung der F/V/S/W-Modellierung mittels Markov-Ketten, das zu analysierende System hinsichtlich Funktion, Wechselwirkungen der einzelnen Subsysteme und Komponenten, möglicher Fehler und deren Auswirkungen zu durchleuchten.
2. Sollte das System mehr als 20 in die Analyse einzubeziehende Komponenten enthalten, ist eine Modularisierung anzudenken, mit dem Ziel schwach vernetzte Module mittels FTA zu behandeln und nur für die komplexeren Module eine MKA durchzuführen. Diesbzgl. sei auch auf Abschnitt 3.3 verwiesen.
3. Identifikation der in Anlehnung an die zu bewertenden Systemparameter geeigneten Zustände.
4. Ermittlung der in Abschnitt 3.2.1.2 vorgestellten Zuverlässigkeitskenngrößen/ Zustandsübergangsraten. Hierzu gehört das Hinterfragen der Gültigkeit der Markov-Bedingung sowie die Bestimmung der Startwahrscheinlichkeiten sämtlicher Zustände.
5. Aufstellung der „qualitativen“ Markov-Kette(n), d.h. Erstellen des Zustandsgraphen.
6. Aufstellen und Lösen der Chapman-Kolmogorov-Differentialgleichung (Toolunterstützt).
7. Bestimmung des Systemverhaltens im stationären Zustand.
8. Bewertung der F/V/S/W des Systems sowie Auslotung des Verbesserungspotentials.

3.3 Hierarchische Modellierung

In den Abschnitten 3.1 und 3.2 wurden die Fehlerbaumanalyse bzw. Markov-Ketten-Analyse mit ihren Vor- und Nachteilen diskutiert. Die FTA eignet sich zur Analyse wenig vernetzter Systeme mit vielen Komponenten. Dahingegen erlaubt die MKA eine geschlossene Modellierung der F/V/S/W komplexer Systeme mit wenigen Komponenten. Nunmehr sollen die beiden Methoden zu optimierten „Hierarchischen Modellen“ fusioniert werden.

3.3.1 Einbindung von FTAs in Markov-Ketten

Fehlerbäume lassen sich, wenn auch mit Einschränkungen, zur Bestimmung der zeitinvarianten Zustandsübergangsraten von Markov-Ketten verwenden. So sind beispielsweise Komponenten zu Systemmodulen zusammenfaßbar, was den Modellierungsaufwand erheblich reduziert. Grundvoraussetzung für diese Modularisierung ist die Modellierbarkeit des relevanten Fehlerverhaltens der zusammenzufassenden Komponenten in einem nvn-System (siehe Abschnitt 3.1.2.5).
Betrachtet man das in Abschnitt 3.2.1.2.1 diskutierte Systembeispiel, so wurde hier bereits diese Form der hierarchischen Modellierung eingesetzt. Die Übergangsraten aus dem fehlerfreien Zustand 0 in den Zustand 1 basieren auf der Fehlermöglichkeit eines der vier Raddrehzahlsensoren. Folglich läßt sich via Fehlerbaum die Übergangsrate dieses 4v4-Systems bestimmen.

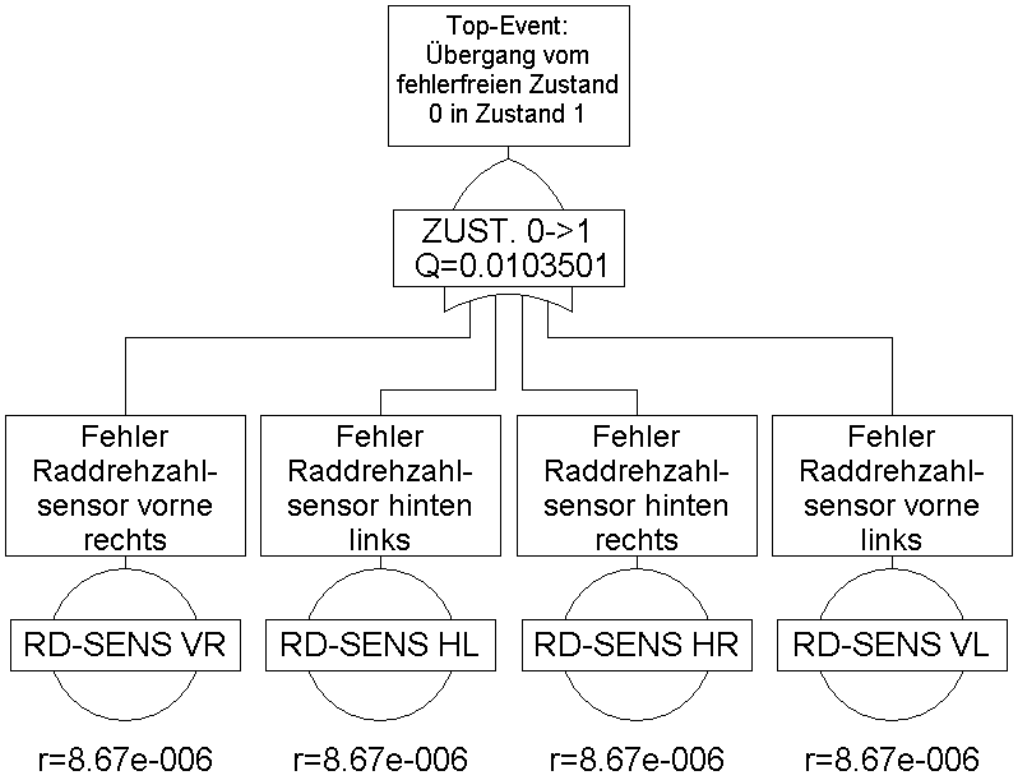


Bild 3.7: Fehlerbaum der Raddrehzahlsensorik

In Bild 3.7 entspricht „r“ der Fehler- bzw. Ausfallrate des jeweiligen Raddrehzahlsensors und „Q“ der Unverfügbarkeit bzw. der Auftretenswahrscheinlichkeit des Top-Events.
Wie Bild 3.7 zu entnehmen ist, bestimmt sich die Übergangsrate vom Zustand 0 in den Zustand 1 als zeitinvariante Fehlerrate des 4v4-Systems bestehend aus den 4 Raddrehzahlsensoren. D.h. jeder beliebige Fehler innerhalb eines der vier Raddrehzahlsensoren

führt zum Eintritt des Top-Events, was mittels „Veroderung“ der einzelnen Raddrehzahlfehler (-raten) modelliert wurde.
Damit bestimmt sich die Modul-Fehlerrate bzw. Übergangsrate als zeitinvariante Summe der einzelnen Fehlerraten der Raddrehzahlsensoren. Die resultierende Auftrittswahrscheinlichkeit des Top-Events entspricht F_{Modul} aus Gleichung 3-31.

$$F_{Modul} = 1 - e^{-\lambda_{Modul} \cdot t} = 1 - e^{-\lambda_{Rd-VL} \cdot t} \cdot e^{-\lambda_{Rd-VR} \cdot t} \cdot e^{-\lambda_{Rd-HL} \cdot t} \cdot e^{-\lambda_{Rd-HR} \cdot t} = 1 - e^{-\left(\sum_{i=1}^{4} \lambda_{Rd_i}\right) \cdot t} \qquad \text{Gl. 3-31}$$

Ohne die hier vorgenommene Zusammenfassung müßte jeder einzelne Raddrehzahlfehler in einem Zustand münden, was den in Bild 3.4 dargestellten Graphen um 3 weitere Zustände „aufblähen“ würde.

Grenzen dieser Modularisierungs-Strategie
Wie bereits angedeutet, beschränkt sich obige Strategie der Einbindung von Fehlerbäumen in homogene Markov-Ketten auf einfache nvn-Systeme. In den Tabellen 3.2.1-3.2.4 bzw. Bild 3.4 erfolgt keine Modellierung des direkten Übergangs vom fehlerfreien Zustand 0 in den sicherheitsrelevanten Zustand 3. Damit das fehlerfreie System in obigen sicherheitsrelevanten Zustand übergeht, muß sowohl im vorderen, wie auch hinteren Bremskreis ein Abriß eines Bremsschlauchen vorliegen.
Dieses Szenario läßt sich durch folgenden Fehlerbaum modellieren:

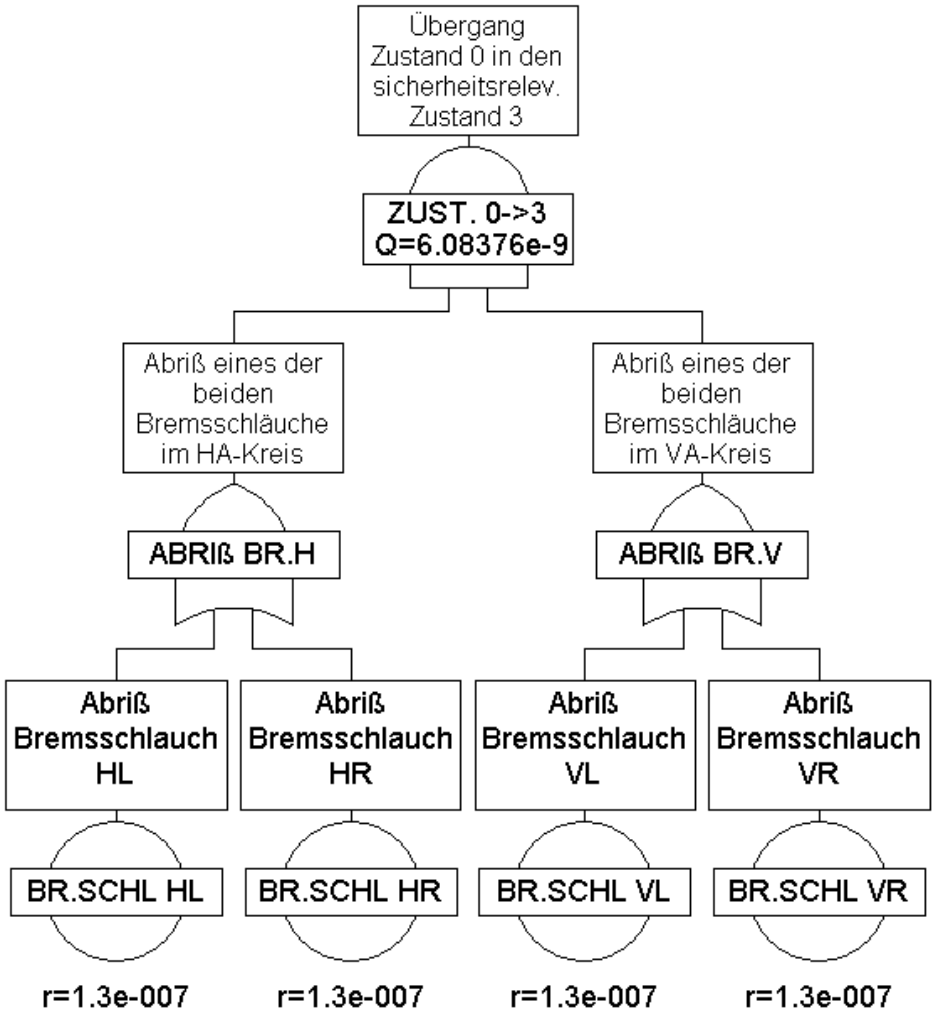


Bild 3.8: Fehlerbaum des Abrisses mindestens eines Bremsschlauches in beiden Bremskreisen

Entsprechend bestimmt sich die Übergangsrate vom Zustand 0 in den Zustand 3 über die Fehlerrate obigen Fehlerbaums bzw. der „Eintrittsrate“ des Top-Events.
Berücksichtigt man Gl. 3-4 und Abschnitt 3.2.1.2.1 bestimmt sich die Auftrittswahrscheinlichkeit mindestens eines Bremsschlauchabrisses im vorderen bzw. hinteren Bremskreis zu:

$$F_{Abriß_{Kreis-V}} = 1-\left(1-F_{Abriß_{RadVL}}\right)\cdot\left(1-F_{Abriß_{RadVR}}\right) = 1-e^{-(\lambda_{VL}(t)+\lambda_{VR}(t))\cdot t} \qquad \text{Gl. 3-32}$$

Die Auftretenswahrscheinlichkeit je mindestens eines Abrisses in beiden Bremskreisen, hier als „Modul“-Wahrscheinlichkeit bezeichnet, bestimmt sich bei gleichen Fehlerraten des Schlauchabrisses an allen vier Rädern folglich zu:

$$\begin{aligned} F_{Modul} &= F_{Abriß_{Kreis-V}}\cdot F_{Abriß_{Kreis-H}} = \left(1-e^{-(\lambda_{VL}(t)+\lambda_{VR}(t))\cdot t}\right)\cdot\left(1-e^{-(\lambda_{HL}(t)+\lambda_{HR}(t))\cdot t}\right) \\ &= 1-2e^{-2\cdot\lambda_{Schlauchabriß}\cdot t}+e^{-4\cdot\lambda_{Schlauchabriß}\cdot t} \end{aligned} \qquad \text{Gl. 3-33}$$

Um eine Separierung der Modul-Fehlerrate zu erreichen, muß folgendes Gleichungssystem gelöst werden:

$$\begin{aligned} &F_{Modul} = 1-e^{-\lambda_{Modul}(t)\cdot t} = 1-2e^{-2\cdot\lambda_{Schlauchabriß}\cdot t}+e^{-4\cdot\lambda_{Schlauchabriß}\cdot t} \\ &\Rightarrow \lambda_{Modul}(t) = -\frac{1}{t}\cdot \ln\left(2\cdot e^{-2\cdot\lambda_{Schlauchabriß}\cdot t}-e^{-4\cdot\lambda_{Schlauchabriß}\cdot t}\right) \end{aligned} \qquad \text{Gl. 3-34}$$

Durch Taylor-Reihenapproximation mit Abbruch nach dem dritten Glied und anschließender Lösung der quadratischen Gleichung ergibt sich:

$$\lambda_{Modul-Näherung}(t) = \frac{1}{t}-\sqrt{\frac{1}{t^2}-8\cdot\lambda^2_{Schlauchabriß}} \qquad \text{Gl. 3-35}$$

Aus Gleichung 3-34 bzw. 3-35 wird ersichtlich, daß obiges Modul eine zeitvariante Modul-Übergangs- bzw. -Fehlerrate aufweist. In Bild 3.9 sind beide Lösungen nebst Approximationsfehler dargestellt. Abschnitt 3.2 war zu entnehmen, daß zeitvariante Übergangsraten nicht in gewöhnliche Markov-Ketten eingebunden werden können. Zeitvariante Übergangsraten würden lediglich eine numerische Lösung der C-K-Gl ermöglichen. Somit schließt sich hier die unmittelbare Modellierung eines Übergangs vom Zustand 0 in den Zustand 3 aus.
Diese Grenze der Markov-Ketten-Modellierung stellt gleichzeitig eine Limitierung der hierarchischen Modellierung dar. Da jedoch in Systembeispiel 1 ohnehin der Zwischenzustand „Verfügbarkeitskritische Leckage in einem Bremskreis“ von Interesse war, bedeutete die Modellierung des Übergangs vom Zustand 0 zum Zustand 3, über den Zustand 2, keinen Mehraufwand.
In Bezug auf die hierarchische Modellierung besteht die Möglichkeit einen in die Markov-Kette einzubindenden Fehlerbaum in zwei oder mehrere Fehlerbäume mit zeitinvarianten Modul-Fehlerraten aufzusplitten.
Grundsätzlich kann jedoch angemerkt werden, daß eine zeitvariante Übergangsrate meist durch Einführung von „Zwischen- bzw. Hilfszuständen“ in zeitinvariante Raten überführbar ist. Hierfür sei auf [Rei88] verwiesen.

Dieser Modellierungs-Mehraufwand stellt die „Grenze“ bzw. das Defizit der Markov-Ketten-Modellierung bzw. hierarchischen Modellierung dar.

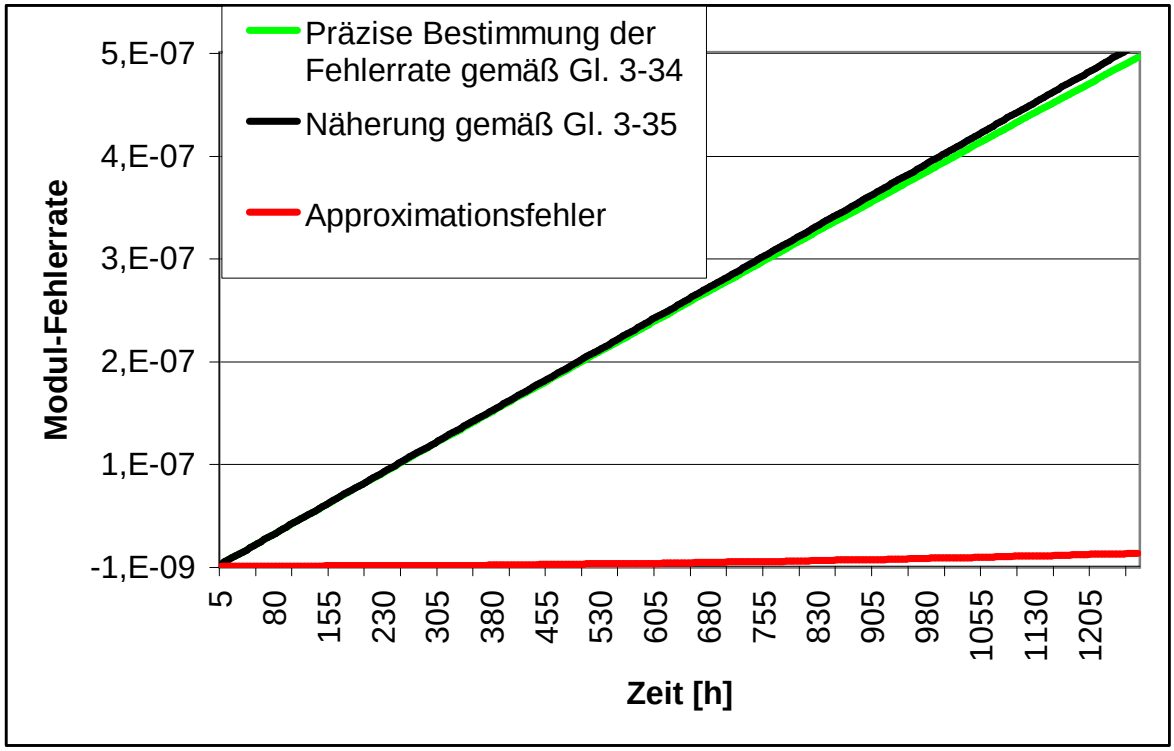


Bild 3.9: Darstellung der zeitvarianten Modul-Fehlerrate (Gl. 3-34), Näherung (Gl. 3-35) sowie des Approximationsfehlers

3.3.2 Einbindung von Markov-Ketten in FTAs

Eine weitere Möglichkeit der hierarchischen Modellierung sieht die Einbindung von Markov-Ketten in Fehlerbäume vor. Wie sich in Kap. 5 anhand der für die Fehlerbäume des D-b-W zu erstellenden Pareto-Diagramme zeigen wird, wirken sich nicht alle System-komponenten gleichermaßen dominant auf die F/V/S/W aus. Um den Modellierungsaufwand zu reduzieren, werden Markov-Ketten nur für die D-b-W-Komponenten erstellt, die sowohl auf die Verfügbarkeit, wie auch Sicherheit einen gravierenden Einfluß haben. Im Sinne der hierarchischen Modellierung werden diese Komponenten zu Submodulen zusammengefaßt.

Damit lassen sich die in den Abschnitten 3.2 bzw. 3.3.1 und 3.3.2 skizzierten Ansätze der hierarchischen Modellierung wie in Bild 3.10 dargestellt fusionieren. Durch diese Vorgehensweise lassen sich die Vorteile der Fehlerbaumanalyse und Markov-Ketten-Modellierung vereinen.

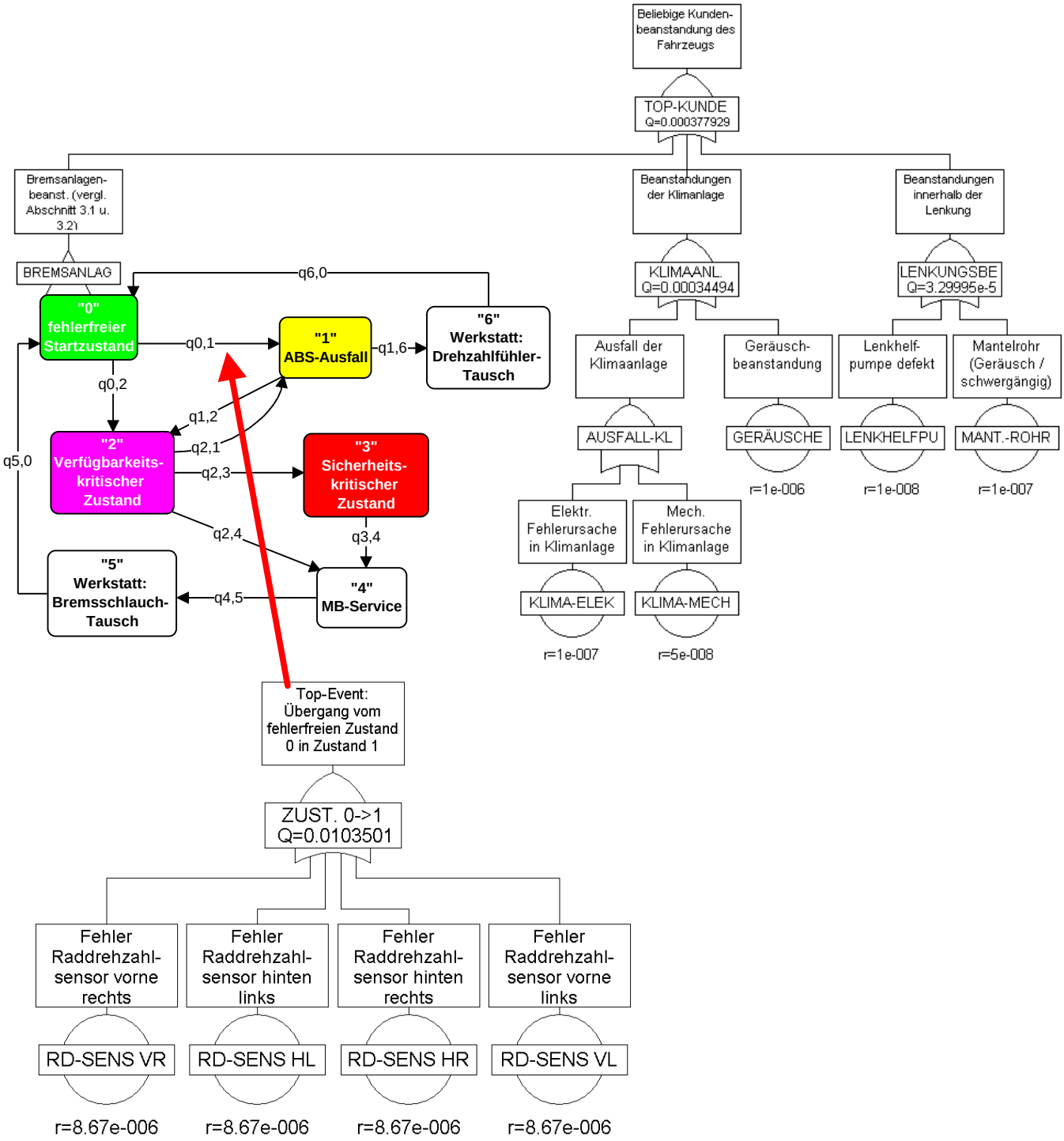


Bild 3.10: Hierarchische Modelle basierend auf Fehlerbäumen und Markov-Ketten

3.4 Zusammenfassung Kap. 3

Im vorliegenden Kapitel wurden mit der Fehlerbaum- und Markov-Ketten-Analyse zwei für die F/V/S/W-Bewertung zukünftiger Kfz-Systeme geeignete Methoden vorgestellt. Hauptanliegen war es, die für Automobilsysteme geeigneten Zuverlässigkeitskenngrößen und deren Quellen aufzuzeigen.

Grundsätzlich ist zu betonen, daß die Bewertung der Methoden zur Analyse komplexer Kfz-Systeme nicht als Aufforderung zur Anwendung einer Methode bei gleichzeitiger Unterlassung anderer Zuverlässigkeits- bzw. Sicherheitsanalysemethoden verstanden werden soll.
Sämtliche F/V/S-Analysemethoden weisen Vor- und Nachteile auf. Es ist die Aufgabe des Benutzers, die für die spezifische Aufgabe geeigneten Methoden zu bestimmen und diese mit dem Wissen um die zugrundeliegenden Theorien korrekt anzuwenden.
Oftmals erweist es sich als sinnvoll, verschiedene Analysemethoden parallel oder miteinander verknüpft einzusetzen. Erstere Vorgehensweise bietet die Möglichkeit, durch die Diversität der Methoden die Korrektheit der erlangten Ergebnisse zu untermauern bzw. auf Fehler innerhalb der Analyse aufmerksam zu werden. Die in Abschnitt 3.3 präsentierte Verknüpfung der Fehlerbäume mit Markov-Ketten zu „hierarchischen Modellen“ bietet die Möglichkeit, Defizite der beiden Methoden zu umgehen bzw. zu kompensieren. So können sowohl stochastische Abhängigkeiten komplexer Systeme, wie auch vielkomponentige Systeme, mit vertretbarem Aufwand untersucht werden.

4 Das System Drive-by-Wire: Funktion und Fehlermoden

Wie bereits in Kap. 3 erwähnt, ist es zwingend, für die F/V/S/W-Analyse eines komplexen Systems detailliertes System-Know-how aufzubauen. Neben den Leistungsumfängen, d.h. der korrekten bzw. erwünschten Funktion, zählen hierzu Wechselwirkungen zwischen den einzelnen Subsystemen und Komponenten, wie auch die Fehlermoden der Komponenten und deren Zuverlässigkeitskenngrößen.
In diesem Sinne soll an dieser Stelle das Applikationsbeispiel Drive-by-Wire (D-b-W) vorgestellt werden. Mit Blick auf den Wettbewerb innerhalb der Automobilindustrie wird das System D-b-W nur in der Detaillierung vorgestellt, die für die F/V/S/W-Analyse zwingend erforderlich ist. In einem frühen Entwicklungs- oder gar Forschungsstadium wird eine tiefergehende Kenntnis der Ziel-Hardware etc. ohnehin nicht vorliegen. Dem Zuverlässigkeitsingenieur mag diese Detaillierung ein Anhaltspunkt dafür sein, welches Maß an System-Know-how er sich bei der Analyse eines für ihn neuen Systems aneignen muß.
Im weiteren Verlauf der Arbeit werden die in Kap. 3 vorgestellten Methoden zur Bewertung der Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit auf dieses System angewandt.

4.1 Übersicht

Beim D-b-W handelt es sich um ein modulares Regler-Konzept, welches durch Eingriff in die Lenkung das Fahrzeug über den gesamten Fahrdynamikbereich stabilisiert. Damit stellt dieses in der Forschungsabteilung F1M/I entwickelte System eine konsequente Weiterentwicklung des seit 1995 in der S- und SL-Klasse der Mercedes-Benz AG als Serienausstattung befindlichen ESP [Mer94, Bos95] dar.
Die in diesem Kapitel beschriebenen Leistungsumfänge des D-b-W-Konzepts wurden mit Ausnahme der Sicherheitssoftware ohne Mitwirken des Autors entwickelt. Details hierzu finden sich in [Böt93, Sui94].
Im weiteren Verlauf dieses Kapitels sollen die für die F/V/S/W-Analyse der Sicherheits-software des D-b-W relevanten Merkmale des Systems diskutiert werden.
Derzeit ist ein A-Muster des D-b-W-Konzepts in einem Pkw-Testträger der aktuellen Mercedes-Benz S-Klasse realisiert. Hierzu wurde das in Bild 4.1 dargestellte Fahrzeug mit den skizzierten Elementen bestückt. Es soll jedoch betont werden, daß die hier dargestellten Elemente mit Ausnahme der Kupplung, Lenkmotoren und des zweiten Querbeschleunigungsgebers in ähnlicher Form bereits zum ESP-Serienumfang gehören. Details sind den folgenden Abschnitten zu entnehmen.

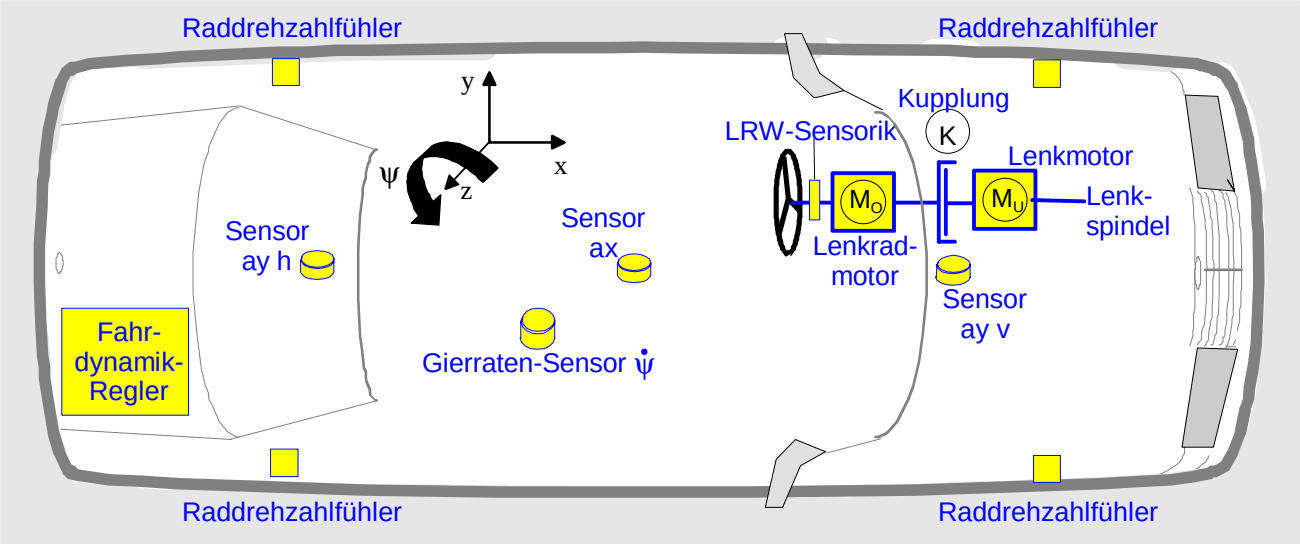


Bild 4.1: Für das D-b-W-Konzept erforderliche Sensorik, Aktorik und Reglermodul

A) Aufgetrennte Lenkung T-Elster-Aktuatorik:
Unterschreiten die von der Fahrbahn auf die Reifen übertragbaren Seitenkräfte einen tolerierbaren Wert, wird im Rahmen des Konzeptes D-b-W kurzzeitig eine der Destabilisierung der Fahrdynamik entgegenwirkende Lenkwinkeländerung an den Vorderrädern herbeigeführt. Dieser aktive Eingriff in die Fahrdynamik führt nicht zur Abweichung des Fahrzeugs von der vom Fahrer angestrebten Trajektorie. Jedoch müssen zu dieser Form der Fahrdynamikstabilisierung mitunter vom fahrerseitig gewählten Lenkradwinkel deutlich abweichende Lenkwinkel am Rad gestellt werden. Dies führt zur Notwendigkeit, eine mechanische Entkopplung obiger Größen vorzunehmen, was durch die Auftrennung der Lenkspindel realisiert wird.
Mit Blick auf die Systemsicherheit wird diese Trennung mittels einer mechanischen Kupplung (Magnet-Kupplung) im nichtelektronischen Notlauf automatisch rückgängig gemacht [Win93] bzw. [Wei93].
Die D-b-W-Aktuatorik umfaßt neben der Kupplung die in Bild 4.1 skizzierten Elektromotoren M_U und M_O.
Mittels Motor M_U wird der vom D-b-W-Fahrdynamikregler ermittelte Sollenkwinkel via Lenkspindel an der Vorderachse gestellt.
Wie Fahrversuche ergaben, benötigt der Fahrzeugführer zum Steuern des Fahrzeugs eine permanente haptische Rückwirkung des Fahrzeugverhaltens auf dem Straßenbelag [Ste96] *(Kraftschlußpotential, Seitenkräfte bzw. Momentenbilanz am Rad)*. Hierzu wird im elektronischen Betrieb bei offener Kupplung via Motor M_O ein synthetisches Moment auf das Lenkrad beaufschlagt. Dieses Moment wird in Abhängigkeit des vom Fahrer gestellten Lenkradwinkels und der aktuellen Fahrzeuggeschwindigkeit variiert. Eine Weiterentwicklung dieses Aktorikkonzeptes, als Steer-by-Wire bezeichnet, wurde im Rahmen der Diplomarbeit [Ste96] bereits auf Zuverlässigkeit und Sicherheit hin analysiert.

B) Fahrdynamik-Sensorik
Wie in Abschnitt A angedeutet, wird der vom Fahrer gestellte Lenkradwinkel sensoriell erfaßt. Aus Sicherheitsgründen ist die hierfür verwandte Sensorik teils diversitär konzipiert (siehe Abschnitt 4.2.1.1).
Neben des Lenkradwinkels fließen in den D-b-W-Regler die folgenden in Abschnitt 4.2.1 detailliert zu diskutierenden Sensorinformationen ein:

- Gierrate und -beschleunigung
- Quer- u. Längsbeschleunigung
- Raddrehzahlen

C) Reglermodul, Degraded-Modes
Sämtliche in Bild 4.1 skizzierten Sensorinformationen werden zur Bestimmung der aktuellen Fahrdynamik herangezogen. Aus diesen Sensordaten wird eine Soll-Giergeschwindigkeit bestimmt, die via M_U als Lenkwinkel an der Vorderachse gestellt wird.
Mit Blick auf die Verfügbarkeit der elektronisch geregelten Fahrdynamikstabilisierung wurde der D-b-W-Regler modular konzipiert. Bei Fehlfunktion bzw. Ausfall eines Sensors kann in Abhängigkeit der weiterhin nutzbaren Information eine Degradation des D-b-W-Reglers eingeleitet werden. Diese modulare Struktur wird in der Literatur als Degraded Modes bezeichnet.
Der D-b-W-Regler wird in Abschnitt 4.2.3 in dem für die F/V/S/W-Betrachtung erforderlichen Maß detailliert.

D) Elektronische Fahrdynamikregelung / Rückfallebenen (Notlaufstrategie)
In Abschnitt C wurde bereits die in Abhängigkeit der Sensorinformation einzuleitende Degradation des D-b-W-Reglers angesprochen. Neben diesen elektronischen Moden ist auch eine mechanische Rückfallebene vorgesehen, in die das System im Falle schwerwiegender Fehler überführt wird. So führt beispielsweise der Total-Ausfall des Bordnetzes

(Energieversorgung) zu einem automatischen Übergang in die auch als Notlauf bezeichnete Rückfallebene. Hierbei wird durch Schließen der Kupplung der physikalische Durchgriff des Fahrers auf die Räder hergestellt. Damit befindet sich das Fahrzeug hinsichtlich seiner Fahrdynamik in einem vollmechanischen Betrieb, wie er in heutigen Fahrzeugen ohne Servounterstützung vorzufinden ist. Dieser Zustand wird gemäß Straßenverkehrsordnung aus Sicht des elektronischen D-b-W-Betriebs als sicherer Zustand bezeichnet.

4.2 Für die F/V/S/W-Betrachtung erforderliche Detaillierung der D-b-W-Komponenten

Der Regelkreis des D-b-W setzt sich aus den für die Erfassung der Fahrdynamik relevanten Sensoren, der Regler-Software und -Hardware, der Lenkaktorik T-Elster und weiteren elektrischen Komponenten (Verkabelung, Energieversorgung etc.) zusammen.
Jede dieser Komponenten ist als Kandidat für eine Fehlfunktion bzw. einen Ausfall des Gesamtsystems D-b-W zu betrachten, weswegen im folgenden die für die F/V/S/W-Betrachtungen relevanten Leistungsmerkmale zu diskutieren sind:
Zu diesen Leistungsmerkmalen gehören:

I. Funktionsprinzip der Komponente, örtliche Anordnung im Gesamtsystem.
II. Kenndaten wie Wertebereich, Auflösung etc.
III. Fehlermoden der Komponente und deren Auftrittshäufigkeit.
IV. Auswirkungen des Fehlermodes auf das Gesamtsystem D-b-W.

Im weiteren Verlauf des aktuellen Kapitels werden die Spezifika I-III der Minimal-Struktur (siehe unten) des D-b-W diskutiert. Das D-b-W nicht unmittelbar tangierende Funktionalitäten bzw. auch im herkömmlichen Fahrzeug verwandte Komponenten und Systeme, wie beispielsweise die Motorsteuerung, Fahrwerk etc. sollen an dieser Stelle von den Betrachtungen ausgegrenzt werden. Entsprechende Details sind [Bos95] zu entnehmen.

Die im weiteren Verlauf dieses Kapitels vorzustellenden D-b-W-Umfänge werden als Minimal-System bezeichnet. Diese Einschränkung bezieht sich auf den Umstand, daß hier lediglich die für die Funktion der höchsten Reglerstufe erforderlichen Elemente des D-b-W berücksichtigt werden. In Kap. 6 werden der Sicherheit bzw. Verfügbarkeit zuträgliche Redundanzstrukturen vorgestellt, die somit zur Erweiterung der D-b-W-Hard- und Software beitragen.

4.2.1 Detaildiskussion der Sensorik

Im folgenden werden die für die höchste D-b-W-Reglerstufe benötigten Sensoren detailliert. Die hierbei im Fokus stehende Fehlermodenbetrachtung sieht im Sinne der in Abschnitt 3.3.1 beschriebenen Modularisierungsstrategie folgende Vereinfachung vor:

> Kabel, Stecker, Kontakte, A/D-Wandler etc., die zur Übertragung der Sensorinformation an den D-b-W-Regler dienen bzw. die Sensoren energetisch versorgen, werden im jeweiligen Modul „Sensor“ zusammengefaßt. Dies führt zu einem Übergang von der HW-orientierten zur informationsorientierten F/V/S/W-Betrachtung. Die mit dieser Modularisierung einhergehende Zunahme der Fehlerhäufigkeit bzw. -rate des Sensormoduls wurde entsprechend der in Abschnitt 3.3.1 beschriebenen hierarchischen Modellierung berücksichtigt. Die im folgenden aufgeführten Fehlerraten entsprechen somit bereits den Ergebnissen der Modulfehlerraten.

4.2.1.1 Lenkradwinkelerfassende Sensorik

Der Fahrerlenkwunsch ist die maßgebliche Eingangsgröße der als Führungsgröße des D-b-W-Reglers dienenden Soll-Giergeschwindigkeit des Fahrzeugs (siehe Abschnitt 4.2.3.1.1). Aus diesem Grund wurde bereits im Minimal-System eine teils diversitäre Sensorik zur Erfassung des Lenkradwinkels implementiert.

Beim Starten des Fahrzeugs wird der aktuelle Lenkradwinkel mittels des bereits im ESP serienmäßig verwandten fail-silent Absolut-Winkelgebers erfaßt. Da seine Auflösung während des Fahrbetriebs nicht für die D-b-W-Applikation ausreicht, wird hier der Fahrerlenkwunsch inkrementell mittels eines hochauflösenden Induktiv-Sensors detektiert. Inwieweit diese Sensorkonfiguration zu einer Fehlersicherheit oder gar Fehlertoleranz der Lenkwinkelinformation führt, wird in Kap. 5 diskutiert. Es soll jedoch bereits vorweggenommen werden, daß der Absolutwinkelgeber bei kurzzeitiger Fehlfunktion des Inkrementalgebers auch während des Fahrbetriebs zu dessen Initialisierung verwandt wird. Die Fail-Silency des Absolutwinkelgebers ermöglicht darüberhinaus im Rahmen seiner Auflösung bzw. Genauigkeit eine permanente Überwachung des Inkrementalgebers. Im Rahmen des D-b-W-Sicherheitskonzeptes führt jeder erkannte Fehler innerhalb der Lenkradwinkelsensorik zum Übergang in die Rückfallebene, d.h. Schließen der Kupplung.

4.2.1.1.1 Absolut-Winkelgeber

Funktionsprinzip des Sensors:

Der Absolut-Winkelgeber besteht aus Gabellichtschranken und einer Graycodescheibe, deren Codespur in diese Lichtschranken eintaucht. Die Ausformung der Codescheibe in Verbindung mit der Anordnung der Gabellichtschranken ergibt für jeden Lenkradwinkelwert einen eindeutigen Graycode, so daß Fehler in der Codescheibe oder der Ausfall von Lichtschranken sicher erkannt werden. Zwei unabhängig arbeitende Mikrocontroller, die sich gegenseitig überwachen, lesen die aktuellen Zustände der Lichtschranken ein und berechnen anhand einer Codetabelle den zugehörigen Lenkradwinkelwert. Durch die Auslegung des Lenkwinkelsensors mit digitaler Signalerfassung, redundanten Mikrocontrollern und dynamischer Schnittstelle wird ein hohes Maß an inhärenter Sicherheit bei diesem Sensor erreicht.

Funktion im D-b-W:

- Permanente Überwachung des Inkrementalwinkelgebers auf Fehlfunktionen, die zu Abweichungen hinsichtlich des inkrementell bestimmten Lenkwinkels führen, die größer sind, als die Genauigkeit des Absolut-Winkelgebers.
- Initialisierung des Inkrementalwinkelgebers beim Starten des Fahrzeugs und temporären Fehlfunktionen (Aussetzern) des Inkremental-Lenkradwinkelsensors.

Meßbereich: +/- 720°

Auflösung: 1,25°

Overall-Error: <0,5% des aktuellen Winkels (max. +/-3,6°).

Besonderheit: Fail-Silent durch Zweiprozessorarchitektur mit Selbsttestroutine.

Fehlermoden und deren relative Häufigkeit:

1. Fehlerhaftes Ausgangssignal	45,3%
2. Kurzschluß	18,6%
3. Leerlauf	10,7%
4. Keine Funktion	8,9%
5. Wackelkontakt / temporäre Unterbrechung der Funktion	8,8%
6. Mechanischer Fehler	7,6%

Tabelle 4.1: Häufigkeitsverteilung potentieller Fehlermoden des LRW-Sensors entnommen aus [FMD-91], Sensor (Summary)

An dieser Stelle ist zu erwähnen, daß in [FMD-91] kein dem vorliegenden Sensorprinzip entsprechender Sensor aufgeführt ist. Aus diesem Grund soll hier exemplarisch auf eine Garantie- und Kulanzstatistik zurückgegriffen werden. Mit Blick auf die Vertraulichkeit dieser Daten werden die Fehlermoden der Felddatenerfassung jedoch anschließend nicht mit relativen Beanstandungshäufigkeiten multipliziert.

1. Elektrischer Fehler	84,6%
2. Kontaktfehler / Unterbrechung	6,4%
3. Kontakt / Steckverbindung aufgeweitet	3,7%
4. Schlecht eingestellt	2,8%
5. Schadhaft etc.	2,5%

Tabelle 4.2: Häufigkeitsverteilung potentieller Fehlermoden des LRW-Sensors abgeleitet aus Kfz-Felddaten

Es ist festzuhalten, daß sich die Fehlermoden aus [FMD91] und Kfz-Garantie- und Kulanzstatistiken im wesentlichen aufeinander abbilden lassen. Fahrzeughersteller und Vertragswerkstätten klassifizieren mit Blick auf die G/K-Kostenverantwortlichkeit im wesentlichen nach:

Fehlerklassifikation	Verantwortlichkeit / Ursache
1. Elektrischer Fehler	Bauteile-Lieferanten
2. Kontaktfehler	Fahrzeugherstellerseitiger Einbau bzw. Zulieferer-Defizit
3. Schlecht eingestellt	Fahrzeughersteller, Montagefehler
4. Schadhaft / mechanischer Defekt	Werkstattpersonal / verursacht beim Ausbau oder im Zuge einer Verunfallung des Fahrzeugs

Tabelle 4.3: Vom Fahrzeughersteller bzw. werkstattseitig vorgenommene Fehlerklassifikation nebst Verantwortlichkeiten und Ursachenforschung.

Die in Tabelle 4.3 dargestellte Detaillierung reicht nicht aus, um auf die Fehlerschwere bzw. -auswirkungen zurückzuschließen. Eine entsprechend ausreichende Detaillierung auf Bauteileebene ist Befundungsergebnissen der Zulieferer oder dem öffentlich zugänglichen [FMD91] zu entnehmen.

Betrachtet man Tabelle 4.1 und 4.2, so lassen sich folgende Pendants identifizieren:

FMD91	≈	Kfz-Felddaten
Fehlerhaftes Ausgangssignal + Kurzschluß + Leerlauf + keine Funktion = 83,5%	≈	Elektrische Fehler + schlecht eingestellt = 87,4%
Wackelkontakt / temporäre Unterbrechung der Funktion = 8,8%	≈	Kontaktfehler / Unterbrechung + Kontakt/Steckverbindung aufgeweitet = 10,3%
Mechanischer Fehler = 7,6%	≈	Schadhaft = 2,5%

Tabelle 4.4: Pendants zwischen den in Tabelle 4.1 aufgeführten [FMD91]-Daten und Kfz-Feldbeanstandungen des deutschen Marktes

Es läßt sich also eine hohe Korrelation zwischen den [FMD91]-Daten und den Kfz-Feldbeanstandungen des deutschen Marktes feststellen. Mit Blick auf die Vertraulichkeit wird daher im weiteren Verlauf der Arbeit ausschließlich das öffentlich zugängliche [FMD91]-Datenmaterial verwandt.

Abbildung der [FMD91]-Fehlermoden auf Hard-, Softfailures und temporäre Fehler
In Tabelle 4.5 wird durch die unterschiedliche Kritikalität der Systemauswirkungen bereits deutlich, daß erst durch die Fehlermodenaufschlüsselung der Komponenten die F/V/S/W-Unterscheidung ermöglich wird. Folglich stellt sich die Frage, wie weit die verschiedenen Fehlermoden einer Komponente zusammengefaßt bzw. unterschieden werden können und müssen. Wie sich im weiteren Verlauf dieses Kapitels zeigen wird, kann die **Si**cherheits-**S**W (SIS, Abschnitt 4.2.3.1.2) zwischen Hardfailures, Softfailures und temporären Fehlern unterscheiden. Entsprechend sind die Komponenten-Fehlermoden in gleichem Maße aufzuschlüsseln. Eine höhere Detaillierung würde zu einem enormen Anstieg des Modellierungsaufwandes, aber für die F/V/S/W-Analyse keinen Mehrwert bringen. Nach Feststellung der Eignung der in [FMD91] aufgeführten Fehlermoden erfolgt für den Absolutwinkelgeber folgende Klassifikation.

Fehlermode	Abk.	Fehlerbild und **System-Auswirkung**	α Proz. Anteil an 100% Komp.Fehler
Hardfailure	**HF**	Fehlerbild: Unplausibilitäten: Sensorausfall, Verlassen des Meßbereichs z.B.: Kurzschluß, Leerlauf, keine Funktion Sys.-Auswirkung: SIS erkennt Fehler und degradiert Regler (w.c. **Verfügbarkeitsverlust**)	45,8 (ermittelt für LRW-Sens.)
Softfailure	**SF**	Fehlerbild: Im Meßbereich liegendes fehlerhaftes Ausgangssignal z.B.: Drift / Offset Sys.-Auswirkung: ggf. erkennt SIS Fehler nicht. (w.c. **Sicherheitsrelevanz durch unplausiblen Reglereingriff**)	45,3
Temporäre Fehler	**TF**	Fehlerbild: Temporäre Unterbrechung der Funktion bzw. des Sensorsignals für weniger als 6 Rechenzyklen (siehe Abschnitt 4.2.3.1.2) Sys.-Ausw: SIS leitet keine Fehlerlokalisation /-behandlung ein (Fehlerzähler) (w.c. **Sicherheitsrelevanz durch unplausiblen Reglereingriff**)	8,9

Tabelle 4.5: Häufigkeitsverteilung potentieller Fehlermoden des LRW-Sensors klassifiziert nach Hard- u. Softfailures sowie temporären Hardfailures

Im weiteren Verlauf dieser Arbeit soll für sämtliche Sensoren hinsichtlich der Fehlermoden von der in Tabelle 4.5 aufgeführten Häufigkeitsverteilung ausgegangen werden.

Ausfallrate des absolut messenden LRW-Sensors

Für die Kap. 5ff. vorzunehmende quantitative F/V/S/W-Analyse des D-b-W-Systems bedarf es der Angabe der relativen Auftretenshäufigkeit obiger Fehlermoden. Grundvoraussetzung für die herkömmliche Markov-Ketten-Analyse basierend auf der geschlossenen Lösung der Chapman-Kolmogorov-Gleichung (siehe Abschnitt 3.2.1.1) ist die Existenz konstanter Ausfall- bzw. Übergangsraten. Inwieweit diese Voraussetzung von elektronischen bzw. elektrischen Bauteilen, auf die sich die weiteren Betrachtungen beschränken sollen, erfüllt wird, soll nunmehr exemplarisch analysiert werden.
In [NPR95] findet sich für den absoluten LRW-Sensor folgender Stellvertreter:
[Sensor, Light, Rotary Motion, Mil, AIC]

$$\lambda_{Sensor,AIC} = \frac{3{,}9443 \cdot 10^{-6}}{h} \qquad \text{Gl. 4-1}$$

Hierbei wird von einer zeitinvarianten Ausfallrate ausgegangen. Wie in Kap. 3.1.2.8 erläutert, muß diese aus der Luftfahrt gewonnene Ausfallrate auf Automobil-Belange umskaliert werden.
Ausgehend von einer durchschnittlichen Einsatzdauer eines Flugzeuges von 6 Stunden pro Tag ergibt sich die jährliche Nutzungsdauer von 2.190 Stunden. Will man obige Zuverlässigkeitskenngröße in eine Automobil-Ausfallrate überführen, ist folgende Umskalierung vorzunehmen:

$$\lambda_{LRW-Sensor_{GM}} = \lambda_{Sensor,AIC} \cdot \frac{2.190h}{300h} \cong \frac{2{,}9 \cdot 10^{-5}}{h} \qquad \text{Gl. 4-2}$$

Daß diese Ausfallrate im weiteren Verlauf zur Beschreibung des Fehlerverhaltens des LRW-Sensors verwandt werden kann, wird im folgenden Abschnitt nachgewiesen.

Wie in Kapitel 3.1.2.8 erläutert, werden die im [NPR95] aufgeführten GM-Ausfallraten ebenfalls mit einem Zeitfaktor multipliziert. Bei Sensoren wird von einer permanenten Nutzung während des Fahrbetriebs von jährlich durchschnittlich 300 Stunden ausgegangen, womit für die in Gl. 4-2 aufgeführte Ausfallrate der Zeitfaktor Z_1 verwandt wird.

Zeitfaktor : Z_1

Resultierende Fehlerwahrscheinlichkeit innerhalb eines 1 Jahr alten Pkw:
Hieraus ergibt sich eine Auftrittswahrscheinlichkeit der Fehlfunktion des absoluten LRW-Sensors nach einem Jahr von:

$$F_{LRW-ABS_{1Jahr}}(t = 300h) = 1 - e^{-\lambda_{LRW-Sensor_{GM}} \cdot 1300h}$$
$$= 1 - e^{-2{,}9 \cdot 10^{-5} \cdot 300} = 8{,}7 \cdot 10^{-3} \qquad \text{Gl. 4-3}$$

Fehleranzahl in [ppm i.d.1.J] = 8700

Entsprechend würden von einer Mio. produzierten Fahrzeugen, die mit obigem Sensor ausgestattet sind, binnen des ersten Jahres Feldeinsatz 8.700 Fzg. einen Sensordefekt aufweisen.

4.2.1.1.2 Nachweis der Zulässigkeit der Exponentialapproximation des Fehlerverhaltens des Lenkradwinkelsensors

Neben der Frage, ob obige Ausfallrate das Fehlerverhalten LRW-Sensor wiedergibt, ist zu klären, ob das Fehlerverhalten des im Fahrzeug eingesetzten Sensors exponentialverteilt anzunehmen ist.
Hierzu wird an dieser Stelle exemplarisch die Verteilungsfunktion des LRW-Sensors mittels Felddaten diskutiert. Mit Blick auf Tabelle 4.2 wird an dieser Stelle die Verteilungsfunktion des dominanten Fehlermodes „elektrischer Fehler“ mittels des Software-Tools Weibull-Smith analysiert. Grundlagen zur Bestimmung der Weibull-Verteilung sind [NWH94] sowie der Dokumentation des Tools entnommen.

Mit Blick auf die Vollständigkeit der Felddaten wurden Garantie-Beanstandungen (1. Jahr nach Zulassung) in den Jahren ‘94 und ‘95 gefertigter mit LRW-Sensor bestückter Fahrzeuge analysiert.

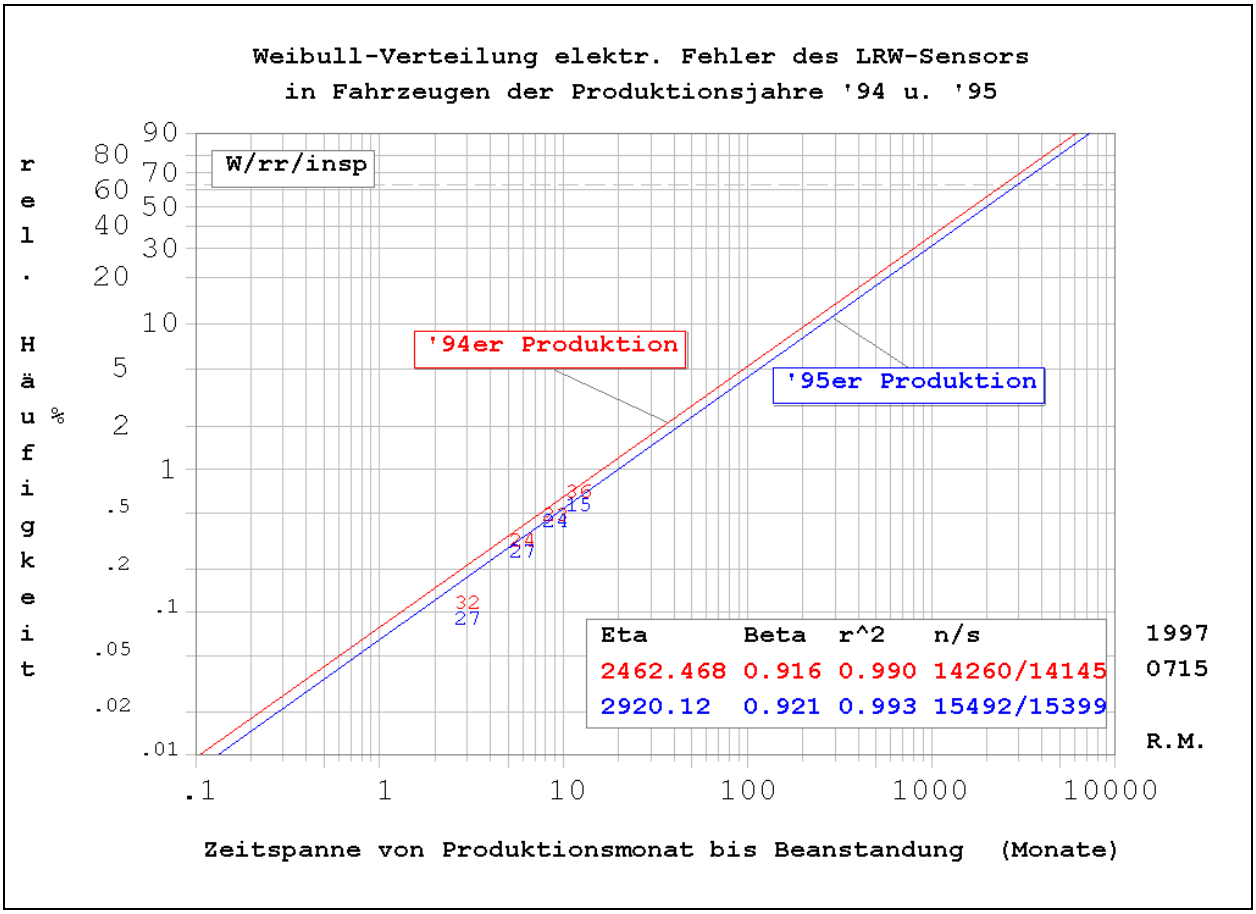


Bild 4.2: Weibull-Graph des Fehlermodes „elektrischer Fehler“ des absoluten LRW-Sensors

Diskussion des Bildes 4.2:
Es zeigt sich, daß für die beiden Produktionsjahre nahezu identische Verteilungsfunktionen des Fehlermodes „elektrischer Fehler“ zu verzeichnen sind. Die Konfidenz der zweiparametrigen Weibull-Verteilung beider Fehlerverhalten kann als sehr gut betrachtet werden. Hierfür ist der Curve-Fitting-Parameter (r^2) von nahezu 1 ein sehr gutes Indiz.
Im Mittel beider Produktionsjahre ergibt sich ein Formparameter β von 0,92 sowie eine charakteristische Lebensdauer von 2691 Monaten.
Damit gestaltet sich die Weibull-Verteilung des Fehlermodes „elektrischer Fehler“ wie folgt:

$$F_{LRW-Sensor}(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}} = 1 - e^{-\left(\frac{t}{2.691\text{Monate}}\right)^{0.92}}$$

$$\Rightarrow \lambda(t) = \frac{f(t)}{1-F(t)} = \frac{dF(t)/dt}{1-F(t)} = \frac{\beta}{\eta} \cdot \left(\frac{t}{\eta}\right)^{\beta-1}$$

Gl. 4-4

Hieraus bestimmt sich eine Auftretenswahrscheinlichkeit obigen Fehlers innerhalb des ersten Jahres von:

$$F_{LRW-Sensor}(12\text{Monate}) = 1 - e^{-\left(\frac{12\text{Monate}}{2.691\text{Monate}}\right)^{0.92}} = 6{,}85 \cdot 10^{-3} \cong 6852\text{ppm}$$

Gl. 4-5

Berücksichtigt man den Umstand, daß gemäß Tabelle 4.2 dieser Fehlermode 84,6% der Gesamtbeanstandungshäufigkeit ausmacht, so ergibt sich die Gesamtbeanstandungshäufigkeit von 8100ppm. Dieser Wert korreliert in hohem Maß mit dem gemäß [NPR95] bestimmten Wert aus Gl. 4.3. Aus diesem Grund soll im weiteren Verlauf der Arbeit Gl. 4.3 als zeitinvariante Ausfallrate des LRW-Sensors verwandt werden.

Im folgenden soll exemplarisch die Ausfallrate λt) über variierendem Formparameter β aus Gleichung 4-4 dargestellt werden.

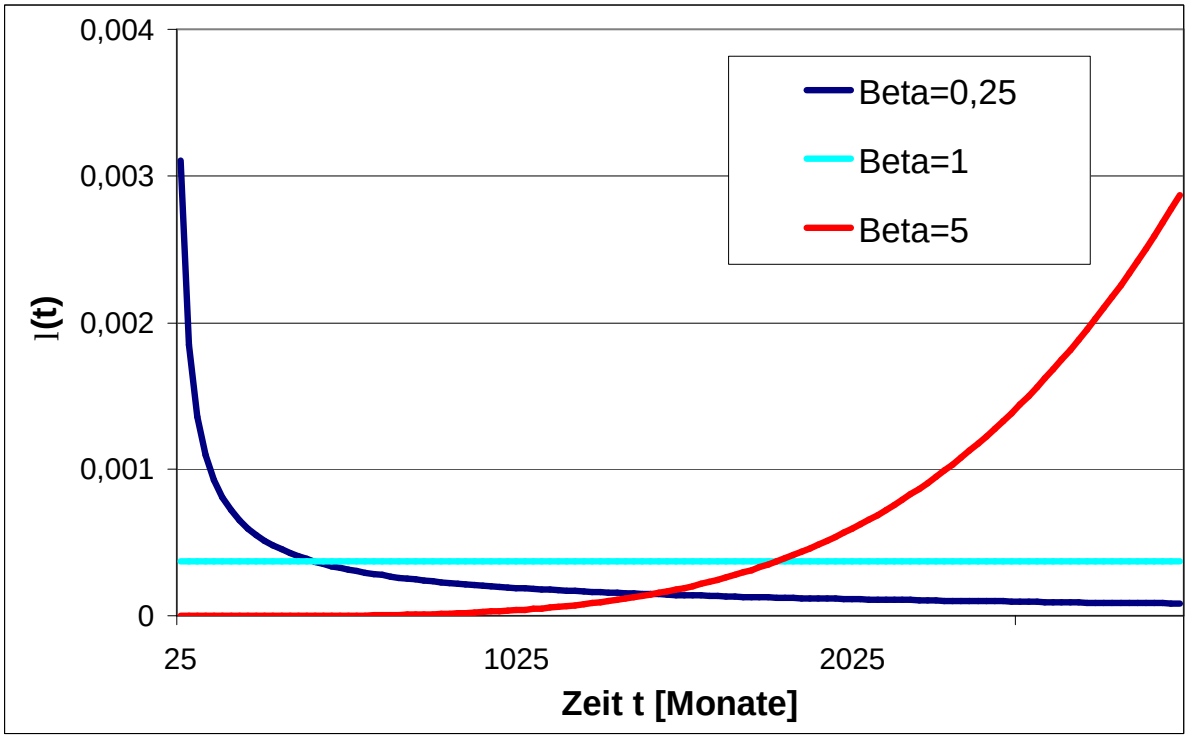


Bild 4.3: Ausfallrate λ(t) über variierendem Formparameter β (charakt. Lebensdauer=2691 Monate)

Obiger Darstellung ist zu entnehmen, daß die Weibullverteilung stark vom Formparameter β abhängt. Einen Spezialfall stellt hier die Weibullverteilung mit β=1 dar. In diesem Fall geht Gleichung 4-4 in die Exponentialverteilung über, wie sie näherungsweise in Bild 4-3 ermittelt wurde und insbesondere für das Ausfallverhalten elektrischer Bauteile bezeichnend ist. Die Ausfallrate ist konstant über der Zeit und entspricht dem Kehrwert der charakteristischen Lebensdauer η.

Eine Weibullverteilung mit $\beta<1$ hingegen weist eine über der Zeit abnehmende Ausfallrate auf. Entsprechend steigt hier die Beanstandungshäufigkeit zu einem frühen Zeitpunkt rapide an, wohingegen sie zu späteren Zeitpunkten kaum mehr zunimmt. Dieser Sachverhalt ist bezeichnend für Frühausfälle, mitunter zurückzuführen auf falsch-, d.h. unterdimensionierte Bauteileparameter.
Eine Weibullverteilung mit $\beta>1$ weist eine über der Zeit anwachsende Ausfallrate auf. Entsprechend wächst die Beanstandungshäufigkeit anfangs nur sehr langsam an, wohingegen sie zu späteren Zeitpunkten steil ansteigt. Diese Ausfallverhalten ist bezeichnend für verschleißdominierte mechanische Bauteile.

Zusammenfassende Bemerkungen zur Weibull-Verteilungsbestimmung

Die analysierten Felddaten weisen eine Ausfallsteilheit β von nahezu 1 auf. Im weiteren Verlauf dieser Arbeit soll daher das Ausfallverhalten des LRW-Sensors durch eine Exponentialverteilung angenähert werden. Obige Ausführungen dienten also der Verifikation, daß diese für die FTA, aber vor allem für die MKA, wichtige Voraussetzung zulässig ist.
Es ist zu betonen, daß dieser Nachweis rein exemplarisch zu verstehen ist. Streng genommen muß er für jedes Element bzw. jede Übergangsrate nachgewiesen werden. Hierbei ist zu beachten, daß die Weibull-Verteilung für jeden Fehlermode isoliert vorzunehmen ist, da gemäß dem zentralen Grenzwertsatz ein Moden-Mix nicht exponentialverteilter Fehlermoden die Ausfallsteilheit des Gesamtfehlerverhaltens gegen 1 laufen läßt [NWH94, Len95]. Weiterhin ist es wichtig, ausreichende Felddaten beanstandeter Bauteile (in der Größenordnung von 20 oder mehr Beanstandungen) vorliegen zu haben.
Obiger Nachweis kann ebenso für nicht elektronische/elektrische Bauteile erfolgen. Sollte sich hierbei eine Ausfallsteilheit abweichend von 1 ergeben, so ist eine geeignete Modellierung dieses Übergangsverhaltens mittels Semi-Markov-Ketten [Sah96, Rei88, Gae77] anzustreben. Diese Thematik soll jedoch nicht zum Umfang der vorliegenden Arbeit zählen. Da jedes System und die in ihm verwandten Komponenten andere Fehlermoden, Fehlerwahrscheinlichkeiten und Verteilungsfunktionen aufweisen, muß obige Vorgehensweise als Methodik verstanden werden, mit der der Leser „eigene“ Systeme analysieren kann.
Es sei abschließend darauf hingewiesen, daß es sich bei obigen Felddatenbeanstandungen nicht zwangsläufig um Fehlfunktionen der Bauteile handelt. Jedoch liegen nicht für sämtliche beanstandeten Bauteile Befundungsergebnisse vor. Daher wurden mit Blick auf die statistisch repräsentative Aussage lediglich Beanstandungsdaten analysiert.

4.2.1.1.3 Inkremental-Sensor

Funktionsprinzip des Sensors:
Hierbei handelt es sich um einen hochauflösenden Induktiv-Sensor der inkrementell Winkeländerungen am Lenkrad erfaßt. Der absolute Lenkradwinkel wird mittels eines einschrittigen Codes bestimmt, der mit mehreren Hall-Elementen gleichzeitig abgetastet wird [Bos94].

Funktion im D-b-W:

- Die Sensorinformation fließt in die via Vorfilter bestimmte Regeleingangsgröße $\dot{\psi}_{Soll}$ ein.
- Darüberhinaus wird der Sensorwert sowohl im Regler, der T-Elster, wie auch dem Schwimmwinkelbeobachter genutzt.

Meßbereich: maximal detektierbare Winkelgeschwindigkeit: 1700°/sek

Auflösung: $1{,}7 \cdot 10^{-3}$ °

Overall-Error: keine Angabe

Fehlermoden und deren relative Häufigkeit:
Wie in Abschnitt 4.2.1.1.1 diskutiert, soll für die Sensorik von der in Tabelle 4.5 aufgeführten Fehlermodenverteilung ausgegangen werden.

Ausfallrate des inkrementell messenden LRW-Sensors:
Im Falle des inkrementellen LRW-Sensors konnte hinsichtlich der Fehlerhäufigkeit auf herstellerseitige Spezifikationen zurückgegriffen werden. Via MTBF von ca. 120.000 Stunden ergibt sich eine Ausfallrate des Sensors von:

$$\lambda_{LRW-Inkr.} = \frac{8{,}33 \cdot 10^{-6}}{h} \qquad \text{Gl. 4-6}$$

Zeitfaktor : Z_1

Resultierende Fehlerwahrscheinlichkeit innerhalb eines 1 Jahr alten Pkw:

$$F_{LRW-Inkr.\,1Jahr}(t = 300h) = 1 - e^{-\lambda_{LRW-Inkr.} \cdot 1300h} = 1 - e^{-8{,}33 \cdot 10^{-6} \cdot 300} = 2{,}5 \cdot 10^{-3} \qquad \text{Gl. 4-7}$$

Fehleranzahl in [ppm i.d.1.J] = 2500

4.2.1.2 Gierratensensor

Funktionsprinzip des Sensors:
Bei dem Gierratensensor handelt es sich um einen schwingenden Zylindergyrometer, bei dem ein Metallzylinder in eine amplitudengeregelte Resonanzschwingung versetzt wird. Die durch Einwirkung der Corioliskraft hervorgerufene Verschiebung der Schwingungsknoten wird durch einen Servokreis zurückgeregelt. Die hierfür notwendige Stellgröße ist ein direktes Maß für die Drehgeschwindigkeit des Fahrzeugs. Weitere Details finden sich in [Bos94].

Funktion im D-b-W:

- Der Sensor liefert die für die Bestimmung der Regeldifferenz des D-b-W-Reglers notwendige Ist-Gierrate des Fahrzeugs.
- Darüberhinaus wird durch Ableitung des Ausgangssignals die ebenfalls in den Regler einfließende Gierbeschleunigung gewonnen.
- Weiterhin stellt die Gierrate eine wichtige Eingangsgröße des in Abschnitt 4.2.3.1 zu detaillierenden Schwimmwinkelbeobachters dar. Dieser liefert seinerseits mit dem Schwimmwinkel eine weitere Eingangsgröße des D-b-W-Reglers.

Meßbereich: +/- 50°/sek.

Auflösung: 1°/sek.

Maximal-Streuung des Ausgangssignals: ≤ 7°/sek.

Besonderheit:
Der Sensor verfügt über eine Selbsttestroutine. Hierbei wird dem Sensor für die Dauer von 19ms additiv ein Sprungsignal von +28°/sek. überlagert. Vor dem Selbsttest, der nicht permanent erfolgt, wird der letzte Gierratenwert, der sich aus der Fahrzeugdynamik und einem eventuell vorhandenen Fehler zusammensetzt, eingefroren. Aufgrund der Kürze der Überlagerung des Testsignals kann näherungsweise davon ausgegangen werden, daß sich die Fahrdynamik innerhalb des betrachteten Zeitfensters nur in vernachlässigbarer Form ändert. Die maximale Streuung des Ausgangssignale beträgt ≤7°/sek.. Damit muß sich im fehlerfreien Zustand des Sensors das neue Ausgangssignal aus der Summe des eingefrorenen Wertes und der Sprungantwort zusammensetzen. Nachteilig erweist sich, daß der Selbsttest mit Blick auf den Meßbereich nur bei Vorliegen eines Ausgangssignals von -50°/sek bis +22°/sek ausführbar ist. Berücksichtigt man darüberhinaus obige Streuung des Sensorsignals, so reduziert sich das überwachbare Fenster auf -50°/sek bis +15°/sek. Somit kann der Selbsttest nicht in allen Fahrsituationen angestoßen werden.
Neben obigem Selbsttest ist weiterhin eine Erkennung von Leitungsbruch (Leerlauf) und Kurzschlüssen möglich (<=0,2 V bzw. >=4,8 V).

Fehlermoden und deren relative Häufigkeit: siehe Tabelle 4.5, Seite 86

Ausfallrate des Drehratensensors:
Im Falle des Drehratensensors konnte erneut ein Vergleich zwischen [NPR95]-Daten und Felddaten hergestellt werden. Aufgrund der wie schon beim LRW-Sensor festgestellten hohen Korrelation der Ergebnisse, wird im folgenden die ([NPR95], Gyros, Integrating (Summary), Unk, GM) entnommene Ausfallrate verwandt:

$$\lambda_{Drehrate} = \frac{24{,}75 \cdot 10^{-6}}{h}$$ Gl. 4-8

Zeitfaktor : Z_1

Resultierende Fehlerwahrscheinlichkeit innerhalb eines 1 Jahr alten Pkw:

$$F_{Drehrate.1Jahr}(t = 300h) = 1 - e^{-\lambda_{Drehrate} \cdot 1300h} = 1 - e^{-24{,}75 \cdot 10^{-6} \cdot 300} = 7{,}43 \cdot 10^{-3}$$ Gl. 4-9

Fehleranzahl in [ppm i.d.1.J] = 7430

4.2.1.3 Längs- u. Querbeschleunigungssensorik

Funktionsprinzip des Sensors:
Die Beschleunigungssensoren basieren auf einem Feder-Masse-System, wobei die Auslenkung der Feder durch eine Magnet-Hallelement-Anordnung sensiert wird. Die Auslenkung ist ein direktes Maß für die auftretende Beschleunigung, der systembedingt Neigungseinflüsse aus der Fahrzeugumgebung überlagert sein können. Dieser, vor der Weiterverarbeitung des Sensorsignals im Regler, zu eliminierende Kopplungsanteil wird mittels des in Abschnitt 4.2.3.1.1 zu diskutierenden Schwimmwinkelschätzers bestimmt und vom Sensorsignal subtrahiert.

Funktion im D-b-W:

- Die für die D-b-W-Regelung benötigte Querbeschleunigungsinformation des Fahrzeugschwerpunkts berechnet sich aus geometrischen Zusammenhängen der beiden Querbeschleunigungssensoren a_{yv}, a_{yh} [Sti95]:

$$a_{y_{SP}} = \frac{a_{y_v} \cdot l_{a_{y_h}} + a_{y_h} \cdot l_{a_{y_v}}}{l_{a_{y_{ges}}}}$$ Gl. 4-10

- Darüberhinaus fließen Längs- und Querbeschleunigung in den Schwimmwinkelbeobachter ein.
- Weiterhin kann aufgrund der örtlichen Anordnung der zwei Querbeschleunigungssensoren aus ihnen die Gierbeschleunigung des Fahrzeugs bestimmt werden. In Gl. 4-10 entspricht $l_{ayv,h}$ dem Abstand vom Fahrzeugschwerpunkt zum vorderen bzw. hinteren Querbeschleunigungssensor (siehe Bild 4.1); $l_{ayv,h}$ gibt den Abstand zwischen beiden Sensoren wieder. Damit stellt sie eine diversitäre Information der via Gierratensensor gewonnenen Gierbeschleunigung dar, die entweder zur Überwachung letzteren oder als kalte Redundanz dienen kann.

Meßbereich: +/- 1,5g, wobei in der D-b-W-Applikation bedingt durch die A/D-Wandlung eine Begrenzung auf +/-1g erfolgt.

Auflösung: 0,125 m/s^2 (LSB)

Bandbreite: 0-300 Hz

Meßfehler bezogen auf den maximalen Meßwert: 1%

Fehlermoden und deren relative Häufigkeit: siehe Tabelle 4.5

Ausfallrate der Beschleunigungssensoren:
Der in [NPR95] aufgeführte Beschleunigungsgeber aus dem Avionik-Bereich weist, insbesondere nach einer zeitlichen Transformation gemäß Gl. 4.2 (abs.-LRW), eine mit Kfz-Feldbeanstandungsstatistiken in keinster Weise korrelierende Fehlerhäufigkeit auf. Aus diesem Grund wird an dieser Stelle auf Feldbeanstandungsdaten vergleichbarer Sensoren zurückgegriffen.

$$\lambda_{\text{Beschl.}} = \frac{8{,}5 \cdot 10^{-6}}{\text{h}} \qquad \text{Gl. 4-11}$$

Zeitfaktor : Z_1

Resultierende Fehlerwahrscheinlichkeit innerhalb eines 1 Jahr alten Pkw:

$$F_{\text{Beschl.}_{1\text{Jahr}}}(t = 300\text{h}) = 1 - e^{-\lambda_{\text{Beschl.}} \cdot 1300\text{h}} = 1 - e^{-8{,}5 \cdot 10^{-6} \cdot 300} = 2{,}55 \cdot 10^{-3} \qquad \text{Gl. 4-12}$$

Fehleranzahl in [ppm i.d.1.J] = 2550

4.2.1.4 Raddrehzahlsensoren

Funktionsprinzip der Sensoren:
Die eingesetzten Raddrehzahlsensoren sind identisch mit den für ABS bzw. ASR bereits in Serieneinsatz befindlichen Gebern [Bos94]. Beim Testträger wird die Drehzahl sämtlicher Räder induktiv bzw. über Hall-Sensoren erfaßt (Vierkanal-ABS).

Funktion im D-b-W:

- Die sensoriell erfaßte Raddrehzahl stellt eine wichtige Eingangsgröße des Schwimmwinkelbeobachters dar.
- Die vom Schwimmwinkelbeobachter unter Verwendung der Raddrehzahlen geschätzte Längsgeschwindigkeit des Fahrzeugs fließt sowohl in das Vorfilter, wie auch in den modularen D-b-W-Regler ein.
  (Nur bei Schlupffreiheit und Geradeauslauf entspricht die Fahrzeuglängs-geschwindigkeit der Radumfangsgeschwindigkeit v = ω*r).

Meßbereich: 2,75km/h bis 300km/h

Auflösung: in (1/Bit) 1,2 km/h

Meßfehler: keine Angabe

Besonderheit:
Es soll bereits an dieser Stelle angemerkt werden, daß die eigentlich für das D-b-W-Konzept relevante Fahrzeuglängsgeschwindigkeit bei erkannten Fehlfunktionen innerhalb der Raddrehzahlsensorik auch ohne Schwimmwinkelbeobachter über simple kinematische Zusammenhänge geschätzt werden kann. Die Frage, welche der für diese „schlechtere“ Schätzung relevanten Raddrehzahlinformationen benötigt werden, soll in Kap. 5 u. 6 diskutiert werden.

Fehlermoden und deren relative Häufigkeit: siehe Tabelle 4.5, Seite 86. Details finden sich in [Coz90, S. 78].

Ausfallrate der Raddrehzahlsensoren:
Wie schon beim Beschleunigungsgeber findet sich in [NPR95] auch für die ABS-Sensorik kein geeigneter Stellvertreter. Eine Auswertung von Felddaten ergibt folgende Ausfallrate je Drehzahlfühler [Mah96_2]

$$\lambda_{Rd-Zahl} = \frac{8{,}67 \cdot 10^{-6}}{h} \qquad \text{Gl. 4-13}$$

Zeitfaktor : Z_1

Resultierende Fehlerwahrscheinlichkeit eines der vier Raddrehzahlsensoren innerhalb eines 1 Jahr alten Pkw: Siehe hierzu auch Gl. 3-17

$$F_{Rd-Zahl-Gesamt_{1Jahr}}(t = 300h) = 1 - \prod_{i=1}^{4}(1 - F_i) = 1 - e^{-\sum_{i=1}^{4}\lambda_i \cdot t} \approx 4 \cdot \lambda_{Rd-Zahl} \cdot 1 \cdot 300h = 10^{-2} \qquad \text{Gl. 4-14}$$

Fehleranzahl innerhalb einer der vier Raddrehzahlsensoren in [ppm i.d.1.J] = 10400

4.2.1.5 Weitere Sensorik /zukünftige Sensorik

Sensoren, die nicht unmittelbar zur Erfassung der Fahrdynamik bzw. als Eingangsgrößen des D-b-W-Konzepts basierend auf Lenkungseingriffen dienen, sollen mit Blick auf die zunehmende Komplexität der Systemanalyse im weiteren Verlauf der Arbeit nicht weiter berücksichtigt werden.
Als Ausnahme sind jedoch der Bremslichtschalter, das Drosselklappenpotentiometer und der Bremsdrucksensor in die F/VS/W-Analyse einzubeziehen. Diese Geber dienen im weiteren Verlauf der Arbeit zur Erzeugung funktionaler Redundanzen. Mit Blick auf die Verfügbarkeit einer via funktionaler Redundanz erlangten Information muß auch die Fehlfunktion obiger Sensoren berücksichtigt werden. Da im D-b-W für diese Sensoren mit Ausnahme der Hardfailure-Erkennung keine Überwachungsfunktionen vorgesehen sind, müssen lediglich die folgenden beiden Fehlermoden unterschieden werden:

1. Potentieller Softfailure: Fehlerhaftes Ausgangssignal, welches nicht erkennbar ist, sowie temporäre Unterbrechungen der Funktion bzw. kurzfristiger Wegfall der Sensorinformation	54,2%
2. Hardfailure: Völliger Wegfall der Sensorinformation bzw. Verlassen des Meßbereichs bzw. Unplausibilität des Sensorsignals (Kurzschluß, Leerlauf, keine Funktion, mechanischer Fehler)	45,8%

Tabelle 4.6: Häufigkeitsverteilung potentieller Fehlermoden des Bremslichtschalters, Drosselklappenpotentiometers und Bremsdrucksensors klassifiziert nach Hard- u. Softfailures

Funktionsprinzip obiger Sensoren: siehe [Bos95]

Funktion im D-b-W:

- Die Sensoren werden in Serienfahrzeugen im Rahmen der Motorsteuerung sowie des ESPs verwandt.
- In Kap. 6 werden die funktionalen Redundanzen diskutiert, die unter Zuhilfenahme obiger Sensoren formulierbar sind.

Meßbereich, Auflösung, Meßfehler: Für die vorliegende Arbeit nicht von Bedeutung.

Zeitfaktor der Sensoren: Z_1

Relative Fehlerhäufigkeit und Ausfallrate des Bremslichtschalters:
Eine Felddatenauswertung ergibt hier eine Fehlerhäufigkeit von:

$$F_{BLS_{1Jahr}}(t = 300h) = 1 - e^{-\lambda_{BLS} \cdot 1 \cdot 300h} = 3{,}6 \cdot 10^{-3}$$

$$\Rightarrow \lambda_{BLS\approx} \frac{F_{BLS_{1Jahr}}(t = 300h)}{300h} = \frac{12 \cdot 10^{-6}}{h}$$

Gl. 4-15

Fehleranzahl in [ppm i.d.1.J] = 3600

Ausfallrate des Bremsdrucksensors:
Hier wurde auf [NPR95, Transducer, Pressure, Summary, Unk, GM] zurückgegriffen, wobei die dort in Ausfälle pro Millionen Meilen Laufleistung aufgeführte Ausfallrate in eine Rate pro Stunde überführt werden muß:

Geht man von einer Durchschnittsgeschwindigkeit von 15Meilen/h aus (Empfehlung vom RAC. In Deutschland wo die Geschwindigkeitsbegrenzung in aller Regel höher ist, als in den USA, geht man von 50km/h aus), benötigt man für die Bewältigung von 1Mio. Meilen:

$$t_{Durchschnitt} = \frac{10^6 \text{Meilen}}{15 \text{Meilen}/h} = 66.667h$$

Gl. 4-16

Damit ließe sich die Ausfallrate/Meilen wie folgt in Ausfälle/h ausdrücken:

$$\lambda\left[\frac{1}{h}\right] = \frac{\lambda\left[\frac{1}{\text{Meilen}}\right]}{66.667\,h}$$

Gl. 4-17

Wendet man Gl. 4-17 nunmehr auf obige NPRD-Angabe an, so ergibt sich die folgende Ausfallrate eines Drucksensors:

$$\lambda_{Br.-Druck-Sensor}\left[\frac{1}{h}\right] = \frac{0{,}0961}{66.667\,h} = \frac{1{,}44 \cdot 10^{-6}}{h}$$

$$\Rightarrow F_{Br.-Druck-Sensor_{1Jahr}}(t = 300h) = 1 - e^{-\lambda_{Br.-Druck-Sensor} \cdot 1 \cdot 300h} = 432{,}5 \cdot 10^{-6}$$

Gl. 4-18

Fehleranzahl in [ppm i.d.1.J] = 433

Ausfallrate des Drosselklappenpotentiometers:
An dieser Stelle soll exemplarisch eine mit Felddaten korrelierende Ausfallrate aus [MIL82] verwandt werden. In [MIL82, Seite 5-259] findet sich eine Formel zur Herleitung der Ausfallrate eines veränderten Schichtwiderstandes. Folgende Kfz-spezifischen Parameter flossen in die Formel ein: mittlere Temperatur von 100°C [Rat96]; mittlere Belastung von 60%. Weitere Angaben zu den Umgebungsbedingungen, denen Kfz-Systeme während des Fahrzeugeinsatz ausgesetzt sind, finden sich in [Ste96, Seite 71]

$$\lambda_{\text{Drosselklappenpotentiometer}}\left[\tfrac{1}{h}\right] = \frac{0{,}12 \cdot 10^{-6}}{h} \qquad \text{Gl. 4-19}$$

$$F_{\text{Drosselklappenpotentiometer}_{1\text{Jahr}}}\left(t = 300h\right) = 1 - e^{-\lambda_{\text{Dr.–Klappenpoti}} \cdot 1 \cdot 300h} = 36 \cdot 10^{-6} \qquad \text{Gl. 4-20}$$

Fehleranzahl in [ppm i.d.1.J] = 36

4.2.2 Diskussion der Aktuatorik
Fehler bzw. Ausfälle der T-Elster müssen zuverlässig erkannt und im worst case durch Schließen der Kupplung behandelt werden. Da sowohl im Minimal-System, wie auch in den erweiterten Systemen (Kap. 6) die gleiche Aktorik eingesetzt wird, kann sie für die vergleichende Systemanalyse außen vorgelassen werden. Diese Ausgrenzung der Aktorik aus den F/V/S/W-Betrachtungen wirkt einer unnötigen Komplexitätszunahme der Markov-Graphen entgegen. In [Ste96] wurden jedoch Moden und Auftrittshäufigkeiten von Fehlfunktionen elektronisch geregelter Lenksysteme ausführlich diskutiert, weswegen die vorliegende Arbeit schwerpunktmäßig Fehler innerhalb der informationserzeugenen Einheiten und deren FELB-Strukturen analysiert.

4.2.3 Fahrdynamikregler (HW/SW)
Im folgenden soll eine Konkretisierung des in Bild 4.1 skizzierten Fahrdynamik- oder auch D-b-W-Reglers erfolgen. Hierbei wird zwischen Softwarealgorithmen zur Realisierung der D-b-W-Funktionalität, einer Sicherheitssoftware zur Überwachung der Korrektheit der Systemfunktion und der verwandten HW-Plattform unterschieden. Es sollen nur die Software- und Hardwareelemente hinsichtlich ihres Fehlerverhaltens diskutiert werden, die Inputs der D-b-W-Regelung darstellen. Die Regelungssoftware bzw. die HW-Plattform und Aktorik werden mit Blick auf die vergleichende Analyse der funktionalen und analytischen Redundanzkonzepte nicht weiter betrachtet.

4.2.3.1 Software-Algorithmen
In Bild 4.4 sind die für die Realisierung der D-b-W-Funktionalität erforderlichen Softwaremodule skizziert. Diese im weiteren Verlauf der Arbeit als D-b-W-Software bezeichneten Algorithmen sollen gemäß der in sie einfließenden Sensorinformationen in folgende Module unterteilt werden:

a) D-b-W-Software-Module
- a.1) Vorfilter
- a.2) modularer ψ-Regler
- a.3) Schwimmwinkel-Beobachter
- a.4) T-Elster-Software

b) Sicherheitssoftwaremodul (SIS)

Im weiteren werden diese Module in dem für die F/V/S/W-Analyse erforderlichen Maß vorgestellt.

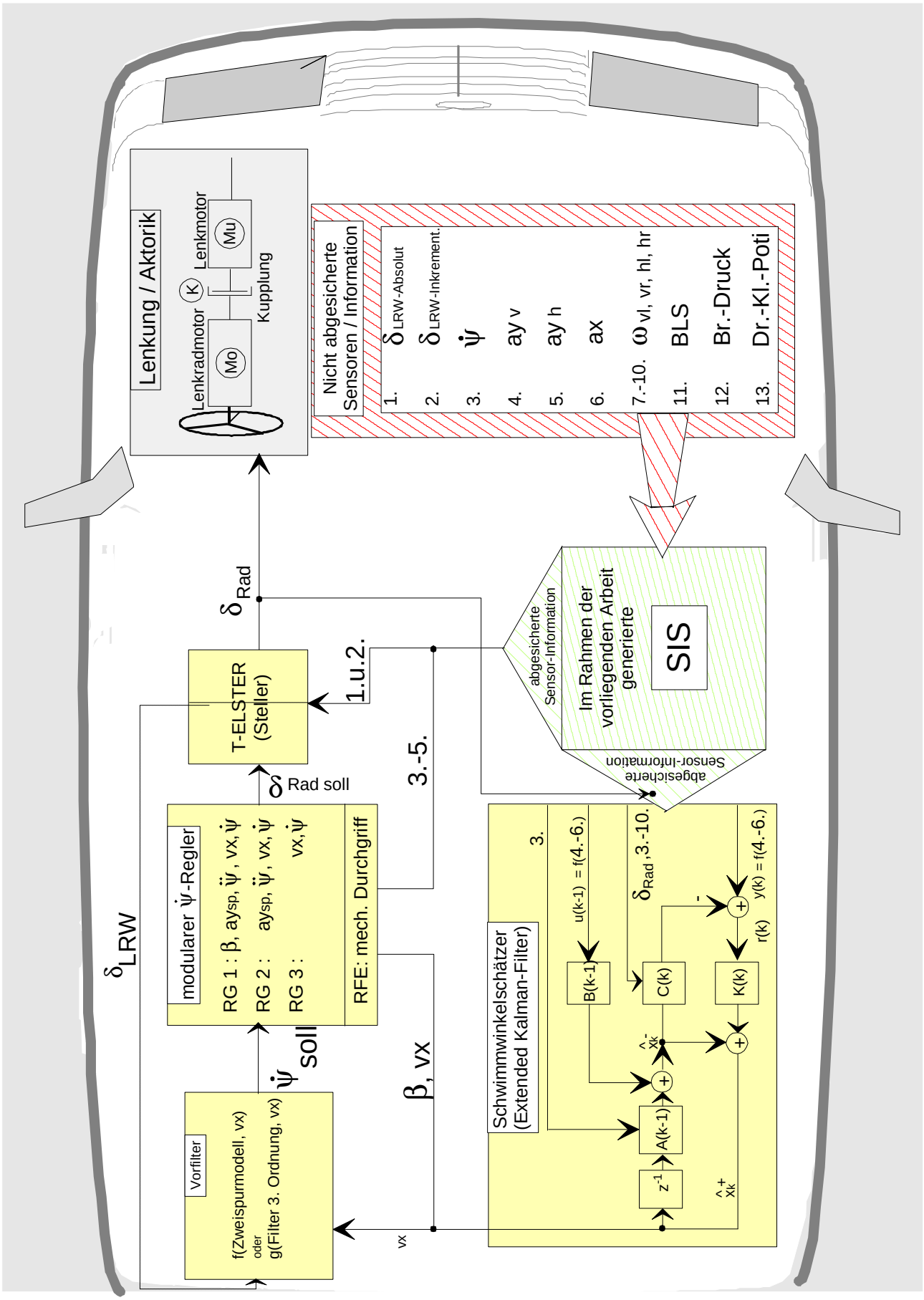


Bild 4.4: Darstellung der für die D-b-W-Funktionalität relevanten Software-Module nebst Minimal-Sensorik

Wie bereits im Falle der Aktorik, sollen Software-Fehler innerhalb der D-b-W-Software-Module im Rahmen dieser Arbeit nicht weiter betrachtet werden. Aus diesem Grund beschränkt sich die folgende Diskussion der D-b-W-Module auf deren Funktion, sowie mögliche Degradationsmechanismen, die in Abhängigkeit der zur Verfügung stehenden Sensorinformation eingeleitet werden können.

Die anschließend folgende Diskussion der Sicherheitssoftware beschränkt sich auf die zur Überwachung der in Abschnitt 4.2.1 detaillierten Sensorfehler relevanten Algorithmen. Softwarefehler, wie etwa Programmier- oder Compilerfehler sollen mit Blick auf Abschnitt 3.1.2.4 in dieser Arbeit nicht betrachtet werden.

4.2.3.1.1 D-b-W-Software-Module

Vorfilter

Die Reglereingangsgröße $\dot{\psi}_{soll}$ des im folgenden zu diskutierenden $\dot{\psi}$-Reglers wird über den vom Fahrer vorgegebenen Lenkradwinkel δ_{LRW} mittels des Vorfilters (Bild 4.4) generiert. Das Vorfilter bedient sich hierzu wahlweise eines Zweispurmodells bzw. eines Filters 3. Ordnung des Fahrdynamikverhaltens. In beiden Fällen benötigt das Vorfilter die Längsgeschwindigkeitsinformation v_x (hier können die Sensoren 11-13 unterstützend genutzt werden).
Die in das Vorfilter einfließende Führungsgröße δ_{LRW} wird im Modul T-Elster gewonnen. Dieses Modul bedient sich hierfür der Lenkradwinkelsensoren.

Modularer $\dot{\psi}$-Regler

Der in Bild 4.4 skizzierte modulare $\dot{\psi}$-Regler generiert in Abhängigkeit der ihm zugeführten Information einen Sollwert des Lenkwinkels $\delta_{Rad\ Soll}$. Die im Vorfilter generierte Sollgiergeschwindigkeit $\dot{\psi}_{Soll}$ dient als Regeleingangsgröße. Zur Formulierung von $\delta_{Rad\ Soll}$ benötigt der $\dot{\psi}$-Regler neben der Regeleingangsgröße weitere sensoriell bzw. beobachterseitig erfaßte Informationen über die aktuelle Fahrzeugdynamik.

Im folgenden werden die 3 elektronischen Regelstufen RG 1,2 und 3 diskutiert:

Regelstufe RG 1:
Arbeiten alle Sensoren bzw. der Schwimmwinkelbeobachter fehlerfrei, so kann der $\dot{\psi}$-Regler in der hinsichtlich der Regelgüte höchsten Stufe „RG 1“ arbeiten.

Regelstufe RG 2:
RG 2 benötigt neben der Regeleingangsgröße Informationen über die bereits oben angesprochene Quer- und Gierbeschleunigung sowie die Fahrzeuggeschwindigkeit über Grund und die Gierrate.
Kann der vom Schwimmwinkelbeobachter generierte Wert nicht verwandt werden bzw. liegt dieser nicht vor, sind jedoch die soeben aufgezählten Sensorinformationen vorhanden, so muß auf den von der Regelgüte her niederwertigeren Regler „RG2“ umgeschaltet werden.
Eine sensorische Ursache für diesen Verlust ist das Versagen des Längs-beschleunigungssensors. Weitere Ursachen werden in Kap. 5 diskutiert. Diese Fehlfunktionen zu detektieren, ist Bestandteil der vorliegenden Arbeit. Kann auf die Beobachterinformationen nicht länger zurückgegriffen werden, ist die Fahrzeug-geschwindigkeit über Grund aus den verbleibenden Sensorinformationen zu bestimmen. Hierfür sind geeignete Strategien zu formulieren und in das SIS-Gesamt-konzept zu integrieren. Zur Bestimmung können neben den bereits in Reglermodul 1 verwandten Sensoren die Sensoren 11-13 (siehe Bild 4-4) genutzt werden.

Regelstufe RG 3:

Ausgehend von RG 2 führt ein Fehler in einem der Querbeschleunigungssensoren zur Notwendigkeit in RG 3 zu degradieren. Diese Reglerstufe benötigt neben der Reglereingangsgröße lediglich eine Information über die Fahrzeuglängsgeschwindigkeit.

In obigen Kurzbeschreibungen der Reglerstufen wurden bereits einige Ursachen für die Notwendigkeit einer Reglerdegradation skizziert. Im Verlauf des Kapitels 5 folgen weitere Ursachen. Es sollen an dieser Stelle noch zwei mögliche Fehlerszenarien skizziert werden, welche zum Übergang in die RFE (mech. Rückfallebene) führen. Bei Fehlfunktion des Gierratensensors oder vollständigem Verlust der Raddrehzahlinformationen muß die Kupplung geschlossen werden. Details zum Fahrdynamikregler sind [Böt93, Bos94, Mer94, Mar94_2] zu entnehmen.

Der Schwimmwinkel-Schätzer (Extended-Kalman-Filter)
Gemäß Bild 4.4 stellt der **S**chwimm**w**inkel**s**chätzer (SWS) die wichtigen Eingangsgrößen Fahrzeuglängsgeschwindigkeit und Schwimmwinkel für den D-b-W-Regler zur Verfügung.

Funktionsprinzip des Schätzers sowie Funktion im D-b-W:

- Neben einer Giergeschwindigkeitsregelung fußt D-b-W auf einer Schwimmwinkelbegrenzung. Dieses Fahrdynamikstabilisierungskonzept wurde bereits in [Bos94] und [Bos95] diskutiert. Da sich der Schwimmwinkel nicht mit vertretbarem Aufwand messen läßt, wird in der Literatur auf Schwimmwinkelschätzer zurückgegriffen [Zom92, Patentschriften DE 40 30 704 A1, DE 42 00 061 A1]. Für D-b-W wurde ein Schwimmwinkelschätzer basierend auf einem extended-Kalman-Filter entwickelt [Sui94]. Der Schwimmwinkel wird über die Schätzgrößen Fahrzeuglängs- und quergeschwindigkeit bestimmt.
- In [Mah94] wird der SWS zu einem Kalman-Filterbankkonzept zur Erfassung von Fehlern innerhalb der Querbeschleunigungssensorik erweitert. Auf diese Strategie der analytischen Redundanz soll jedoch mit Blick auf den Umfang der Arbeit nicht weiter eingegangen werden.

Struktur des Schwimmwinkelschätzers:
Die Struktur des Schwimmwinkelschätzers basiert auf einem in [Lof90], [And79] und [Kre80] ausführlich diskutierten, zwangslinearisierten und damit „extended“ Kalman-Filter. Mit Verweis auf Bild 4.4 werden im folgenden lediglich das lineare Systemmodell sowie das noch nicht linearisierte Beobachtungsmodell dargestellt. Für weitere Details soll auf [Zom92, Sui94] verwiesen werden.

Systemmodell

$$\underline{\hat{x}}_k^- = A(k-1)\cdot \underline{\hat{x}}_{k-1}^+ + B(k-1)\cdot \underline{u}(k-1)$$
$$\begin{pmatrix} v_y \\ v_x \\ \mu_H \\ \Phi \end{pmatrix} = f(\psi_{sensoriell}, a_{y_{v,h}-sensoriell}, a_{x-sensoriell}, \text{diversen Fzg.-Parametern}) \qquad \text{Gl. 4-21}$$

Hierin entspricht

- μH dem Kraftschlußbeiwert des Luftreifens auf der Straßendecke [Bos95] und potential,
- Φ der Fahrbahnquerneigung.

Nichtlineares Beobachtungsmodell

$$\underline{y}_k = h(\underline{x}, \underline{u}, k,)$$
$$\begin{pmatrix} a_{y_{v,h}-\text{sensoriell}} \\ a_{x-\text{sensoriell}} \\ \ddot{\psi}_{\text{sensoriell}} \end{pmatrix} = h(a_{y_{v,h}-\text{sensoriell}}, a_{x-\text{sensoriell}}, \dot{\psi}_{\text{sensoriell}}, \delta_{\text{Rad}_{\text{Aktor}}}, \omega_{\text{Rad}}, \text{diversen Fzg.-Parametern})$$

Gl. 4-22

Aus der geschätzten Längs- und Quergeschwindigkeit wird anschließend der Schwimmwinkel gewonnen:

$$\beta = \arctan\left(\frac{-v_y}{v_x}\right) \approx -\frac{v_y}{v_x}$$

Gl. 4-23

Fehlermoden und deren relative Häufigkeit:

- **Auswirkungen von Sensorfehlern / Verlust der Beobachtbarkeit:**
  Obigen Gleichungen des Schwimmwinkelschätzers ist zu entnehmen, daß sowohl im System- wie auch im Beobachtungsmodell in sämtlichen Gleichungen Sensordaten als Eingangsgrößen dienen. Damit wird deutlich, daß ein Sensorfehler zur Fehlfunktion des Schwimmwinkelbeobachters führen kann. Die Frage der Robustheit des nichtlinearen Schätzermodells gegen Fehler von Eingangsgrößen bzw. Modellunsicherheiten soll im Rahmen dieser Arbeit jedoch nicht behandelt werden. In [Zom92] erfolgte eine Detailanalyse der Beobachtbarkeit des SWS. Für den weiteren Verlauf der Arbeit sei von der vereinfachenden Annahme ausgegangen, daß im Falle des Fehlers bzw. Ausfalls eines im SWS verwandten Sensorsignals die Beobachtbarkeit der Schätzgrößen verloren geht, was zu einem nicht tolerierbaren Schätzfehler führt. Weiterhin sei davon ausgegangen, daß dieser Verlust der Beobachtbarkeit nur in dem Maße erkannt wird, wie der entsprechende Sensorfehler erkennbar bzw. lokalisierbar ist. Im Rahmen der Fehlerbehandlung des Sensors wird die Degradation des D-b-W-Reglers eingeleitet, was dem Wegschalten des SWS gleichkommt. Andere Ursachen für den Verlust der Beobachtbarkeit seien nicht betrachtet.
- **Schätzfehler**, beispielsweise verursacht durch Modellierungsfehler des zu beschreibenden Systemverhaltens sollen in dieser Arbeit nicht betrachtet werden.
- **Softwarefehler**, wie beispielsweise Programmierfehler, Spezifikationsfehler etc. sollen mit Verweis auf Abschnitt 3.1.2.4 nicht als Ursache für ein Versagen des SWS betrachtet werden.

Relative Häufigkeit obiger Fehlermoden:
Da sich die betrachteten Fehlermoden auf die Auswirkungen der sensoriellen Eingangsgrößen des SWS beschränken, bestimmt sich die Fehlerhäufigkeit über ein nvn-Modell der n in das SWS einfließenden Sensorsignale (siehe Kap. 3 und 5).

Zeitfaktor : Z_1

Fehleranzahl in [ppm i.d.1.J]: siehe Kap. 5

T-Elster-Software
Die T-Elster-Software umfaßt die in Abschnitt 4.1 diskutierten Leistungsumfänge des aktiven Lenkungseingriff sowie den Sicherheitskernel „Schließen der Kupplung“ im Notlauf. Fehlfunktionen der dem Bereich Aktorik zuzuordnenden hochsicherheits-

relevanten T-Elster-Software sollen an dieser Stelle mit Verweis auf die definierten Top-Events nicht weiter betrachtet werden.

4.2.3.1.2 Minimal-Sicherheitssoftware

Im folgenden wird die SIS (**Si**cherheits**s**oftware) des Minimal-Systems diskutiert. Hierbei beschränkt sich die Betrachtung im wesentlichen auf FELB-Algorithmen zur Überwachung der in Abschnitt 4.2.1 beschriebenen Sensorik.

4.2.3.1.2.1 Minimal-SIS zur Sensor-FELB

Funktionsprinzip und Aufbau der Minimal-Sicherheitssoftware im D-b-W:

Im letzten Abschnitt wurden Gründe für eine Degradation des $\dot{\psi}$-Reglers skizziert. Hierbei wurde davon ausgegangen, daß ein Fehler bzw. Verlust der für die aktuelle Reglerstufe notwendigen Information erkannt und die Degradation im Sinne der Fehlerbehandlung eingeleitet wird.

Aus obigen Ausführen wird auch deutlich, daß im Sinne der Systemsicherheit und maximalen Verfügbarkeit, obige Fehler zuverlässig erkannt, lokalisiert und behandelt werden müssen. Genau diese Aktionen sollen durch das in Bild 4.4 skizzierte SIS-Modul gesteuert werden. In dieses Modul werden die „nicht abgesicherten“ Sensorinformationen eingespeist und an den D-b-W-Regler bzw. die Kupplung die als fehlerfrei identifizierten Sensordaten und die erforderlichen Degradationsmeldungen weitergeleitet.

Im Rahmen der Minimal-SIS soll auf funktionale und analytische Redundanzkonzept verzichtet werden. Sie sind Bestandteil der erweiterten FELB und werden somit erst in Kap. 6 vorgestellt.

Die im folgenden zu detaillierende SIS-Struktur ist mit Blick auf die Aufgabenstellung der „FELB“ ist die SIS in ein Fehlererkennungs-, -lokalisations-, und -behandlungsmodul unterteilt. Sie basiert auf den Arbeiten [Mah94, Sti95].

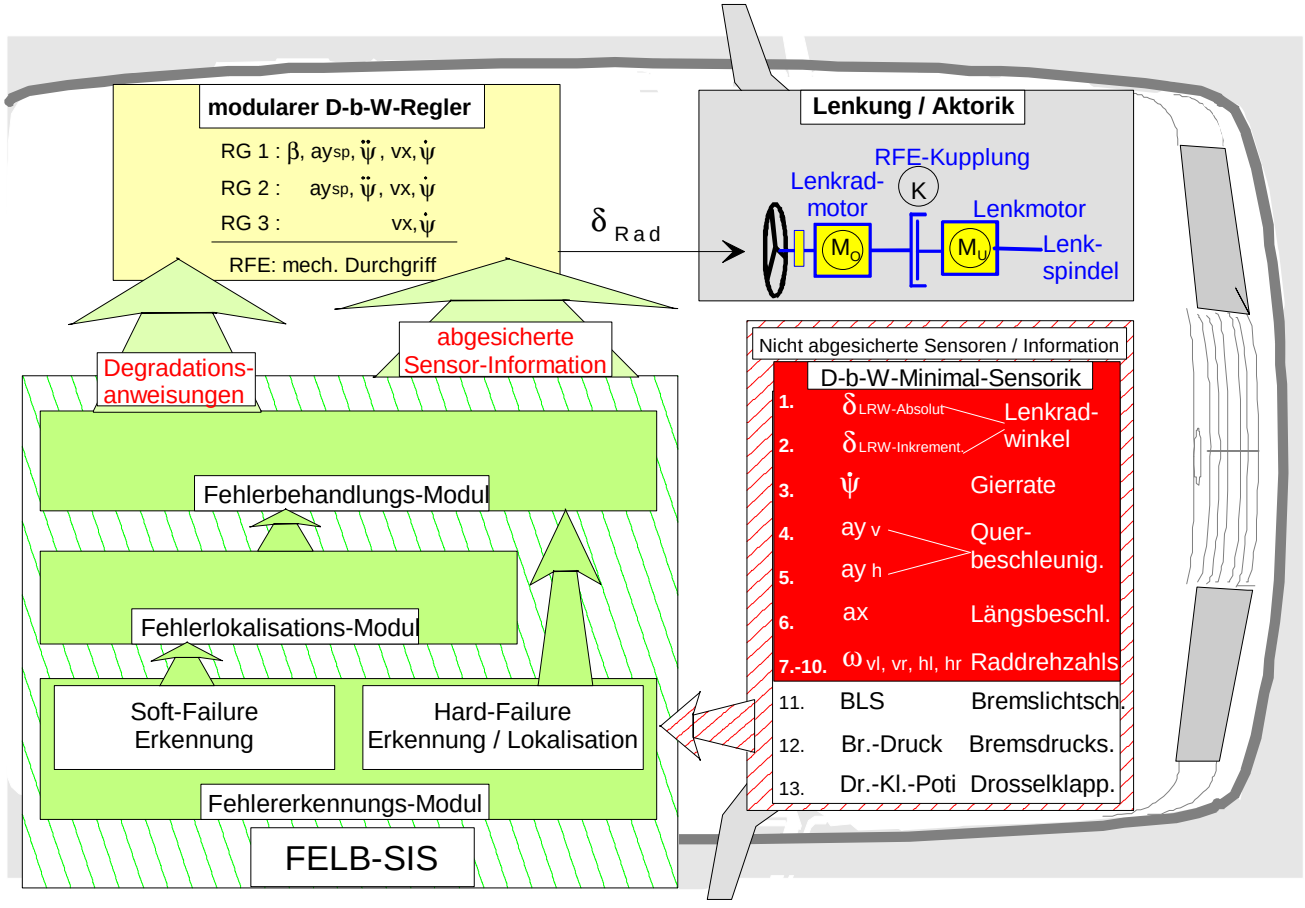


Bild 4.5 Modularisierung der SIS zur Sensor-FELB

Die Fehlererkennung wird wie auch die übrigen D-b-W-Algorithmen innerhalb der Zykluszeit von 10ms einmal durchlaufen. Erst bei Vorliegen einer Fehlermeldung wird das Fehlerlokalisations- bzw. -behandlungsmodul durchlaufen.
Mit der zyklisch durchgeführten Fehlererkennung ist zumindest formal die Forderung aus Abschnitt 2.3.1 nach der kontinuierlichen Überwachung der sicherheitsrelevanten Sensorik erfüllt. Wie sich im Bereich Softfailure-Erkennung zeigen wird, können Softfailures nur innerhalb der Gierraten- und Lenkradwinkelsensorik detektiert werden. Daher reicht die hier dargestellte Minimal-SIS nicht zur umfassenden Überwachung sämtlicher möglichen Sensorfehler aus.

Sensor-Fehlererkennungsmodul
Wie Bild 4.5 zu entnehmen ist, wird innerhalb des Fehlererkennungsmoduls zwischen Hardfailure-Erkennung/Lokalisation und Softfailure-Erkennung unterschieden.

Hardfailure-Erkennung/Lokalisation

Zum Leistungsumfang der Hardfailure-Erkennung zählen die Plausibilitätsprüfungen auf:

- Leitungsbruch und Kurzschluß,
- Meßbereichsüberschreitung des Sensorsignals,
- unplausible Gradienten.

Da für die Detektion obiger Defekte keine weiteren Sensorinformationen benötigt werden, kommt die Erkennung eines Hardfailures der Lokalisation der Fehlerquelle gleich.

Das folgende Flußdiagramm gibt anhand der Meßbereichsüberschreitungsalgorithmik exemplarisch den Aufbau der Hardfailure-Erkennungssoftware wider. Weitere Details finden sich in [Mah94, Sti95].

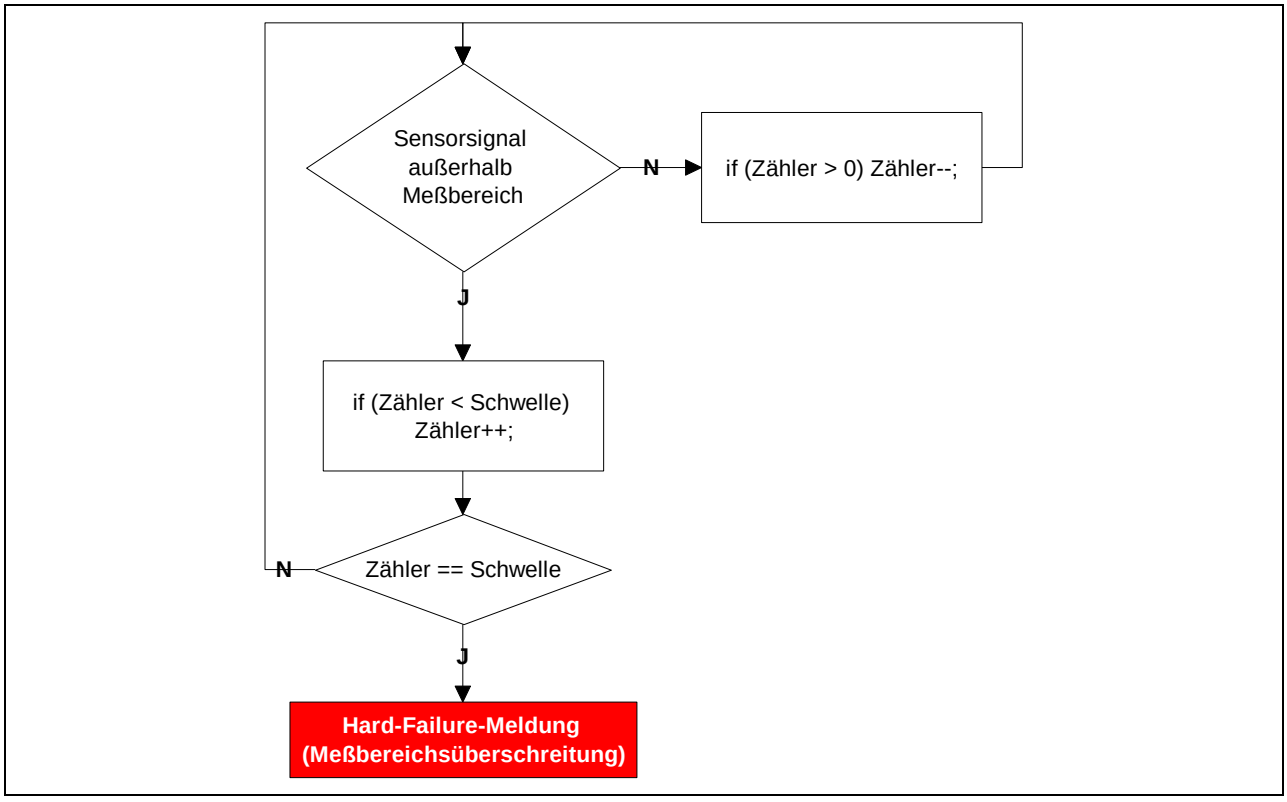


Bild 4.6 Flußdiagramm der Meßbereichsüberwachung innerhalb des Moduls Hard-Failure-Erkennung

Wie Bild 4.6 zu entnehmen ist, wird durch die Zählerstrategie eine Robustheit der Fehlererkennung gegen Ausreißer geschaffen. In [Sti95] wurden Meßbereich und die geeignete Zählerschwelle identifiziert. Es konnten optimale Ergebnisse mit der Schwelle = 6 erzielt werden. Hieraus resultiert eine zeitliche Verzögerung von 60ms vom Zeitpunkt des Auftretens eines permanenten Hardfailures bis zu seiner Lokalisation. Eine weitere zeitliche Verzögerung von 100ms resultiert aus der Notwendigkeit, sämtliche Sensorsignale via Tiefpaßfilterung zu glätten.
[Bos90] und [Kub84] beschreiben weitere Strategien zur Hardfailure-Erkennung innerhalb von Kfz-Sensoren.

Softfailure-Erkennungen

Hinsichtlich der Softfailure-Erkennung muß zwischen den einzelnen Sensoren unterschieden werden. An Softfailure-Erkennungen existieren im Minimal-System nur

- der herstellerseitig vorhandene Selbsttest des Gierraten-Sensors,
- die Selbstüberwachung des absoluten Lenkradwinkelsensors,
- die mit überprüfter Fehlerfreiheit des absoluten Lenkradwinkelsensors vornehmbare Überwachung des inkrementellen Lenkradwinkelsensors. Hierfür wird das Absolutwinkelsignal tiefpaßgefiltert und anschließend differenziert. Die Differenz beider Signale wird als Fehlerindikator des inkrementellen Winkelgebers interpretiert. Der Fehlermeldung geht eine Schwellwert- und Zählerstrategie wie in Bild 4.6 skizziert voraus.

Da im weiteren Verlauf der F/V/S/W-Betrachtungen Software-Fehler nicht berücksichtigt werden, spielen Struktur und Komplexität der für obige Softfailure-Erkennungen erforderlichen Algorithmen nur im Sinne der in die Algorithmen einfließenden zusätzlichen Sensordaten eine Rolle. Auf die Frage der Fehlererkennungsraten wird in Abschnitt 4.2.3.1.2.4 eingegangen.

Softfailures der hier nicht aufgeführten D-b-W-Sensoren können im Minimal-System nicht erkannt werden. Da sich hiermit auch die Lokalisation und Behandlung ausschließen, fließen die fehlerhaften Sensorsignale in die D-b-W-Regelung ein. Inwieweit der Regler gegen derartige Fehler robust ist, soll im Rahmen der vorliegenden Arbeit nicht untersucht werden. Vielmehr wird mit Blick auf die Sicherheitsrelevanz davon ausgegangen, daß nicht erkennbare Fehler zum Eintritt des sicherheitsrelevanten Top-Events C führen. Im Zustandsraum entspricht dies einem Übergang in den hochsicherheitsrelevanten Zustand „white-space“. Diese Namensgebung spiegelt die noch ungewissen Auswirkungen des Fehlerszenarios wider.

Mit Verweis auf [Sti95] und [Wei93] soll an dieser Stelle nicht weiter auf die Softfailure-Erkennung eingegangen werden.

Sensor-Fehlerlokalisationsmodul

Wie bereits beschrieben, wird das Fehlerlokalisationsmodul nur aktiviert, wenn seitens des Fehlererkennungsmoduls eine Softfailuremeldung erfolgte.
In der hier zu betrachtenden Minimal-SIS kommen jedoch Hard- und Softfailure-Erkennung der Lokalisation des fehlerhaften Sensors gleich. Damit kann in Kap. 5 auf die Betrachtung der Auswirkungen einer Aktion des Fehlerlokalisationsmoduls verzichtet werden.

Sensor-Fehlerbehandlungsmodul
Auf die im Sinne der Fehlerbehandlung einzuleitenden Degradationen des modularen D-b-W-Reglers wird im Rahmen der in Abschnitt 5.1.1 zu analysierenden Maßnahmen zur Kompensation von Sensorfehlern eingegangen.

4.2.3.1.2.2 HW-FELB

In [Ric88, Seite 20ff] sind diverse Verfahren zur Erkennung von Fehlern innerhalb von Mikroprozessoren skizziert (watch dogs etc.). Mit Verweis auf dieses Werk und Blick auf Bild 4.7 sei davon ausgegangen, daß die zweikanalige D-b-W-HW-Struktur die Fail-Safe-Eigenschaft besitzt. Damit können Fehler innerhalb eines der beiden Kanäle zuverlässig erkannt und durch Schließen der Kupplung behandelt werden [Wei93].
Es sei jedoch kritisch angemerkt, daß die SIS-HW im Minimal-System nur einkanalig ausgelegt ist. Weist der Rechner einen Fehler auf, kann dies hochsicherheitskritische Folgen haben. Gemäß [VDI88] stellt diese HW-Struktur eine Verletzung der Forderung dar: „Die Überwachungseinrichtungen selbst dürfen nicht durch Fehler unbemerkt ausfallen."
Da diese Struktur jedoch zur Veranschaulichung der Thematik völlig ausreicht und bereits in der B-Musterphase der D-b-W-Systementwicklung durch eine geschlossene Steuergeräte-Architektur ersetzt wird, soll in dieser Arbeit von obiger Struktur ausgegangen werden.

4.2.3.1.2.3 FELB-Übergangsraten

In [Kur96] wurde eine Herleitung für die mittlere Fehlererkennungs-, -lokalisations und -behandlungszeit vorgenommen. Hierbei wurde in Abhängigkeit der für das jeweilige FELB-Modul verwandten Source Lines of Code (SLOC) eine mittlere CPU-Zeit bestimmt, deren Kehrwert im Sinne einer Reparaturrate als konstante Übergangsrate verwandt wurde. Abweichend von dieser Vorgehensweise sei mit Blick auf Abschnitt 4.2.3.2 davon ausgegangen, daß die Zykluszeit auf allen Transputerplattformen 10ms betrage und daß innerhalb dieser Zeitspanne das bzw. die relevanten FELB-Module einmal ablaufen können. Demzufolge bestimmen sich die FELB-Übergangsraten als Kehrwert des Produktes der Zykluszeit und der für die Entscheidung (Fehler erkannt, lokalisiert oder behandelt) benötigten Rechendurchläufe, nebst des Anteils, der sich aus der Tiefpaßfilterung ergibt.

Hardfailure-Erkennungsrate :

$$\varepsilon_{Hard} = \frac{1}{6 \cdot Zykluszeit + 100ms} = 22.500\,{}^{1}\!/_{h} \qquad \text{Gl. 4-24}$$

Softfailure-Erkennungsrate:

Gierratensensor
Es sei davon ausgegangen, daß der Selbsttest zyklisch einmal pro Sekunde angestoßen wird. Auch hier sei zur Vermeidung von Fehlalarms aufgrund von Ausreißern eine Zählerstrategie wie in Abschnitt 4.2.3.1.2.1 gewählt.
Hieraus ergibt sich die Softfailure-Erkennungsrate des Gierratensensors von:

$$\varepsilon_{Soft-Gierraten-Sensor} = 600\,{}^{1}\!/_{h} \qquad \text{Gl. 4-25}$$

Kritisch ist jedoch anzumerken, daß diese Rate nur unter der Voraussetzung erzielt wird, daß die Gierrate des Fahrzeugs innerhalb des für den Selbsttest zulässigen Meßbereichs liegt (siehe hierzu Abschnitt 4.2.1.2).
Weiterhin gilt einschränkend, daß durch obige Zähler die temporären Fehler nicht erkannt werden können. Die Frage der Robustheit des D-b-W-Reglers gegen diese

weniger als 6 Zyklen (60ms) vorliegenden Fehler wird im Rahmen der vorliegenden Arbeit nicht untersucht.

Absoluter Lenkradwinkelsensor
Hinsichtlich der Fehlererkennungsrate sei von der des Gierratensensors ausgegangen:

$$\varepsilon_{Soft-LRW-Abs.-Sensor} = 600\,1/h \qquad \text{Gl. 4-26}$$

Positiv ist hier anzumerken, daß dieser Selbsttest unabhängig vom Fahrmanöver durchgeführt werden kann. Hinsichtlich der temporären Fehler bzw. Aussetzer sei auf obige Anmerkungen zum Gierratensensor verwiesen.

Inkrementeller Lenkradwinkelsensor
Mit Verweis auf Abschnitt 4.2.3.1.2.1 bestimmt sich die Fehlererkennungsrate ebenfalls aus dem Kehrwert der 6-fachen Zykluszeit.

$$\varepsilon_{Soft-LRW-Inkr.-Sensor} = 600\,1/h \qquad \text{Gl. 4-27}$$

Fehlerlokalisationsrate:
Wie bereits in Abschnitt 4.2.3.1.2.1 beschrieben, kommt in der hier zu betrachtenden Minimal-SIS die Hard- und Softfailure-Erkennung der Lokalisation des fehlerhaften Sensors gleich. Damit kann bei der Minimal-SIS auf die Angabe einer Fehlererkennungsrate verzichtet werden.

Fehlerbehandlungsraten:
Wie in Abschnitt 3.2.1.2 soll auch hier zwischen der Onboard- und Offboard-Fehlerbehandlung unterschieden werden. Entsprechend sind folgende Übergangsraten zu definieren:

Onboard Fehlerbehandlungsrate $\zeta_{Onboard}$:
Sie setzt sich aus dem Kehrwert der Zeitspanne für:

- die Ausführung der Degradationsanweisung an den D-b-W-Regler bzw. die T-Elster
- die Umsetzung der Degradationsanweisung im Regler bzw. der Kupplung (Datenkommunikation, Neuinitialisierung der Reglerparameter etc.).

An dieser Stelle sei davon ausgegangen, daß obige Aktionen binnen eines Rechenzyklusses erfolgen. Damit entspricht die Onboard-Fehlerbehandlungsrate $\zeta_{Onboard}$:

$$\zeta_{Onboard} = 360.000\,1/h \qquad \text{Gl. 4-28}$$

Hinsichtlich sämtlicher hier aufgeführter Übergangsraten ist kritisch anzumerken, daß sie bei der Zustandsraummodellierung in Verbindung mit den Fehlerraten aus Abschnitt 4.2.1 zu steifen Markov-Ketten führen. Jedoch kann gerade bzgl. der enorm großen Fehlerbehandlungsrate Abhilfe geschaffen werden. Wie sich in Kap. 5 zeigen wird, folgt auf die erfolgreiche Fehlererkennung zwangsläufig die Fehlerbehandlung. Daher kann als Übergangsrate die Summe der beiden Raten angegeben werden. Dies führt zu einer Reduzierung der Steifheit der Markov-Kette.

Offboard Fehlerbehandlungsrate:

Hier sei gegenüber den in Bild 3.8 aufgeführten Übergangsraten folgende Zusammenfassung vorgenommen:

Bei Aufleuchten der gelben Warnlampe steuert der Fahrer binnen ca. 3 Stunden die Werkstatt an.

$$\nu_{Fahrer-Reaktion-gelbeWarnlampe} = \frac{1}{t_{Offboard} + t_{Fahrer-Reaktion-gelbeWarnlampe}} = \frac{1}{10ms + 3h} \approx \frac{1}{3h}$$

Gl. 4-29

Bei Aufleuchten der roten Warnlampe parkiert der Fahrer binnen ca. 5 Minuten das Fahrzeug:

$$\nu_{Fahrer-Reaktion-roteWarnlampe} \approx \frac{1}{5\,min}$$

Gl. 4-30

Ferner wird das Fahrzeug im Anschluß an Gl. 4-30 binnen ungefähr einer Stunde durch den MB-Service in die Werkstatt überführt.

$$\nu_{MB-Service} = \frac{1}{t_{Offboard} + t_{Fahrer-Reaktion-roteWarnlampe} + t_{MB-Service}} = \frac{1}{10ms + 5\,min + 1h} \approx \frac{1}{1h}$$

Gl. 4-31

Reparaturrate:

Obwohl die endgültige Architektur des D-b-W-Systems derzeit noch nicht vorliegt, sei davon ausgegangen, daß jeder Defekt innerhalb Sensorik und Rechnern durch Tauschen der defekten Einheit innerhalb weniger Minuten behoben werden kann. Als Zeitspanne vom Eintreffen des Fahrzeugs in der Werkstatt bis zur Rückgabe an den Kunden sei von 6 Stunden ausgegangen. Dies wird dem Umstand gerecht, daß die eigentliche Reparatur nicht unmittelbar mit dem Eintreffen des Fahrzeugs in die Werkstatt eingeleitet werden kann.

$$\mu = \frac{1}{6h}$$

Gl. 4-32

4.2.3.1.2.4 Fehlermöglichkeiten der SIS

- In Abschnitt 3.2.1.2.2 wurde bereits deutlich, daß mit Ausnahme der in dieser Arbeit nicht diskutierten Softwarefehler, die meisten Fehlfunktionen der SIS auf Sensorfehler oder den Ausfall des SIS-Rechners zurückzuführen sind. So versagt beispielsweise die Softfailure-Überwachung des inkrementellen Lenkwinkelsensors, wenn der Absolutwinkelgeber fehlerhaft arbeitet. Damit handelt es sich hier um Common-Cause-Fehler.
- Eine weitere Fehlerursache stellen die bereits in Abschnitt 4.2.3.1.2.1 beschriebenen Lücken in der Überwachung des jeweiligen Fehlerphänomens, wie das bereits beschriebene Unvermögen, mittels der Minimal-SIS Softfailures der Beschleunigungs- bzw. Raddrehzahlgeber zu detektieren, dar.

Beide Fehlermöglichkeiten führen zu den bereits in Abschnitt 3.2.1.2.2 beschriebenen Mißalarm, Mißlokalisation oder -behandlung.

4.2.3.1.2.5 Auftrittshäufigkeit eines SIS-Fehlers

Mit Blick auf obige Fehlermoden, bedarf es hier keiner Angabe einer Fehlerhäufigkeit der SIS. In Kap. 5 und 6 werden die entsprechenden Zustände aufgrund hardwarebasierter Zustandsübergänge und somit -raten eingenommen.
Diese Betrachtungsweise berücksichtigt auch den Umstand, daß komplexere SIS-Strukturen, wie sie in Kap. 6 vorgestellt werden, auf eine größere Anzahl von Informationen benachbarter Sensoren zurückgreifen. Damit hängt die Verfügbarkeit dieses komplexen SIS-Moduls von einer größeren Anzahl von Fehlerraten ab.

4.2.3.2 HW-Plattform / örtliche Verteilung der Software-Algorithmen / Energieversorgung

4.2.3.2.1 HW-Struktur, örtliche Verteilung der D-b-W-Funktionalität:

Wie in Bild 4.7 skizziert, läßt sich die für das System D-b-W verwandte Rechner-HW vereinfacht als fehlersichere zweikanalige Transputer-Struktur darstellen. Neben diesen beiden identischen Kanälen wird ein weiterer Transputer als HW-Plattform für die Sicherheitssoftware verwandt. Die dargestellte „Sensorik“ umfaßt die in Abschnitt 4.2.1 beschriebenen Geber. Der zur gezielten Verfälschung und damit Verifikation der Leistungsfähigkeit der Sicherheitssoftware skizzierte Sensorfehlersimulator wird in Abschnitt 4.2.3.2.3 skizziert.
Defaultmäßig werden die Ergebnisse des HW-Kanal 1 auf die Aktuatorik durchgeschaltet. Erkennt die SIS eine signifikante Abweichung der Ergebnisse beider HW-Kanäle, wird die Kupplung geschlossen. Selbiges erfolgt als Reaktion auf Fehlfunktionen der sicherheitsrelevanten Giergeschwindigkeits- bzw. Lenkradwinkelsensorik.
Auf eine weitere Detaillierung hinsichtlich Systembus, CPU, RAM/ROM, E/A-Bausteinen etc. soll an dieser Stelle verzichtet werden.

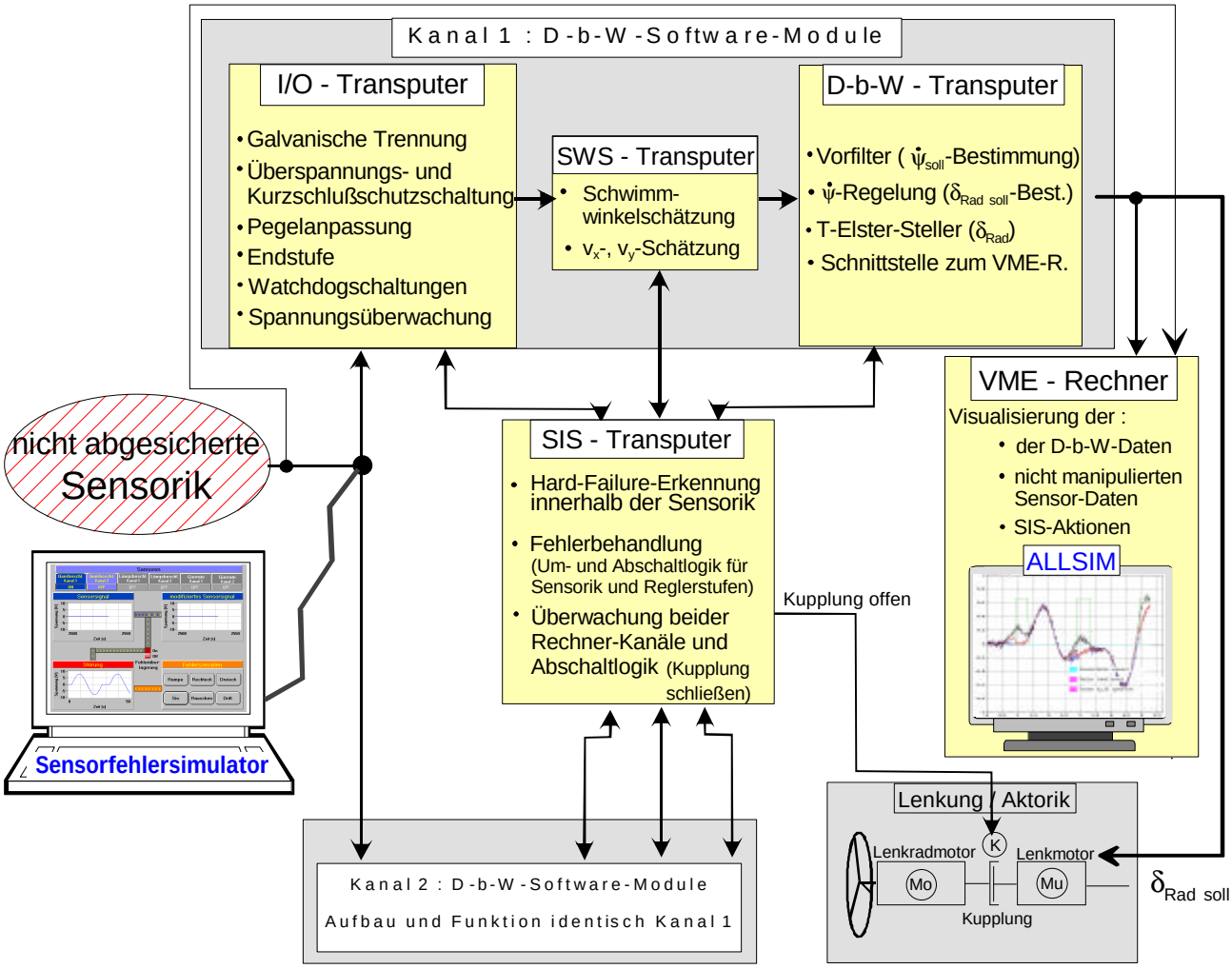


Bild 4.7: Transputer-Konfiguration für die D-b-W-Software-Module und Sicherheitssoftware

Die in Bild 4.7 dargestellten Transputer sind vom Typ T805-30MHz, 4 MB. Diese Konfiguration ist jedoch historisch bedingt und könnte gemäß heutigem Entwicklungsstand

besser durch Power-PCs realisiert werden. Der VME-Rechner dient zur Visualisierung von Meßwerten des Fahrzeugverhaltens und Ausgabe der SIS-Ergebnisse. Als Visualisierungsoberfläche wurde das Software-Tool ALLSIM verwandt, welches in Abschnitt 4.2.3.2.3 skizziert wird. Auf eine weitere Detaillierung hinsichtlich Transputer-Links etc. soll an dieser Stelle mit Verweis auf [Wei93] und [Win93] verzichtet werden.

Zykluszeit: Die verwandten Transputer erlauben eine Zykluszeit von 2ms. Jedoch werden sämtliche in dieser Arbeit vorgestellten D-b-W-Umfänge innerhalb einer Zykluszeit von 10ms abgearbeitet.

Fehlermoden und deren relative Häufigkeit:
In Analogie zu Abschnitt 4.2.3.1, sollen an dieser Stelle lediglich Fehlfunktionen der SIS- und SWS-Hardware betrachtet werden. Spätestens bei Erreichen des B-Muster-Standes wird die Transputer-Plattform durch eine Steuergeräte-Konfiguration ersetzt. Für Steuergeräte sicherheitsrelevanter Kfz-Systeme wurden in [Mah96_2 und Ste96] Zuverlässigkeits- und Sicherheitsanalysen durchgeführt.
Fehlermoden von Mikrorechnern und deren Auftrittshäufigkeiten können [Ric88, S. 4-6 und Coz90, S. 79] entnommen werden.

- Hardfailure (Ausfall): Aufgrund der hochgradig sequentiellen Arbeitsweise eines Mikroprozessors führen Fehler meist zu seinem Totalausfall, selbst wenn der Fehler oder die Störung nur kurzfristig aufgetreten ist.
- Softfailure (fehlerhaftes Signal): Störungen auf den Adreß-, Daten- oder Steuerleitungen führen zu Fehlinterpretationen durch den Mikroprozessor und somit zur fehlerhaften Ablauffolge der Befehle.

In [FMD-91] findet sich keine geeignete quantitative Aufspaltung der Fehlermoden. Mit Blick auf die Sicherheitsrelevanz des Systems D-b-W soll jedoch davon ausgegangen werden, daß sämtliche Fehler des SIS-Transputers zum Eintritt des Top-Events C führen. Einfachfehler der D-b-W-Transputer führen zum Eintritt des Top-Events B. Aufgrund dieser Eindeutigkeit, bedarf es keiner weiteren Betrachtung der Häufigkeitsverteilung der einzelnen Fehlermoden.

Ausfallrate eines Mikrorechners:
Da auch dem [NPR95] keine entsprechende Angabe zu entnehmen ist, wird auf eine Angabe aus [Mey91] zurückgegriffen.

$$\lambda_{\text{Transputer}} = \frac{10^{-6}}{\text{h}}$$ Gl. 4-33

Zeitfaktor : Z_1

Resultierende Fehlerwahrscheinlichkeit innerhalb eines 1 Jahr alten Pkw:

$$F_{\text{Transputer}_{1\text{Jahr}}}(t = 300\text{h}) = 1 - e^{-\lambda_{\text{Transputer}} \cdot 1 \cdot 300\text{h}} = 1 - e^{-10^{-6} \cdot 300} = 3 \cdot 10^{-4}$$ Gl. 4-34

Fehleranzahl in [ppm i.d.1.J] = 3000

4.2.3.2.2 Bordnetz / Datenübertragung

Bordnetz

Fehlermoden des Bordnetzes (Energieversorgung), deren Auftrittshäufigkeit und Auswirkungen wurden in [Mah96_2] und [Ste96] diskutiert. Aus diesen Arbeiten erfolgte die Empfehlung, hochsicherheitsrelevante Kfz-Systeme wie D-b-W mit einem voll-redundanten Bordnetz zu versorgen. Mit Verweis auf den Umstand, daß durch eine Zweikanaligkeit des gesamten Bordnetzes im Testträger Einfachfehler robust kompensierbar sind, soll die Energieversorgung an dieser Stelle nicht weiter diskutiert werden.

Datenübertragung

Der in Abschnitt 4.2.1 diskutierte Bremslichtschalter, das Drosselklappenpotentiometer und die Bremsdruck-, Raddreh- und Lenkwinkelsensorik, sowie die Motordrehzahl werden via CAN an die SIS bzw. D-b-W-HW geführt. Fehlfunktionen, die vorrangig im Bereich der Schnittstellen auftreten können, sind durch die Zuordnung der Stecker- u. Kontaktfehler zu den jeweiligen „Sendeelementen“ berücksichtigt.

4.2.3.2.3 Testumgebung

Sensorfehlersimulator

Sensorfehler stochastischer Natur treten zeitlich gesehen nur sehr selten auf (siehe MTBF). So konnten nach Implementierung einer erweiterten Version der in [Sti95] entwickelten SIS während einer zweiwöchigen Dauerlaufuntersuchung lediglich Offsetfehler während der Initialisierungsphase des Systems innerhalb der Quer-beschleunigungssensoren identifiziert werden. Diese stationären Fehler sind auf den Transport des Testträgers zur Teststrecke und damit verbundene Referenzierungsfehler zurückzuführen. Die anschließende Kalibrierung behob den Fehler. Weitere Fehler-meldungen konnten nicht verzeichnet werden.

Um aber die Qualität der FELB ermitteln zu können, sind die in Abschnitt 3.2.1.2.2 bzw. 4.2.3.1.2 beschriebenen Fehlerphänomene der FELB auszuschließen.
Zu diesem Zweck wurde im Rahmen der Diplomarbeit [Wet96] ein Sensorfehlersimulator entwickelt. Dieser Simulator ermöglicht es, im Testträger den Sensorsignalen gezielt beliebige Fehlerszenarien zu überlagern. Der Entwurf berücksichtigte die Forderung nach Echtzeitfähigkeit sowie der Unveränderheit des zu prüfenden Systems D-b-W-HW inklusive SIS. Letztere Eigenschaft wurde gefordert, da beispielsweise eine einfach zu realisierende Erweiterung der SIS um einen softwarebasierten Sensorfehlersimulator einer Veränderung des zu prüfenden Systems gleichkommt. Die nachträgliche Eliminierung des Simulators würde den gerade erfolgten F/V/S-Nachweis der SIS wieder in Frage stellen.

Allsim

Um sowohl im Fahrzeug, wie auch im Labor die SIS entwickeln und testen zu können, wurde das Software-Tool ALLSIM verwandt.

4.3 Vorteile des D-b-W-Konzeptes / System-Anforderungen

Wie bereits erwähnt, handelt es sich beim D-b-W um die konsequente Weiterentwicklung der bereits in Serie befindlichen Fahrdynamikstabilisierung ESP.

Vorzüge des D-b-W gegenüber ESP

- Durch den Lenkeingriff erstreckt sich die Fahrdynamikstabilisierung bis weit in den fahrdynamischen Grenzbereich hinein. Damit bietet D-b-W einen gegenüber ESP erweiterten Leistungsumfang.
- Einen weiteren, durch die Auftrennung des mechanischen Durchgriffs der Lenkung bereits angedeuten Vorteil bietet die Integration des D-b-W-Reglers in eine elektronische Lenkung (Steer-by-Wire, [Ste96]). Der hiermit ermöglichte Wegfall der Lenksäule führt zur Reduzierung des Risikos der Fahrzeuginsassen, im Falle des Frontalaufpralls durch die sich in den Fahrzeuginnenraum schiebende Lenksäule verletzt zu werden.
- Neben der Reduzierung des Verletzungsrisikos bietet der Wegfall der Lenksäule auch wirtschaftlichen Nutzen. So kann beispielsweise auf kostenintensive Links- bzw. Rechtslenker-Umbauten im Motorraum verzichtet werden.
- Weiterhin kann die für die Führung des Fahrzeugs erforderliche Lenkwunschvorgabe des Fahrzeugs über einen Joy-Stick getätigt bzw. sensiert werden. Hierdurch ließe sich auf das im Crash-Fall ebenfalls verletzungsträchtige Lenkrad verzichten.
- Weitere Vorteile sind in [Ste96] aufgeführt.

Anforderungen an das System

- Durch die Auftrennung des mechanischen Lenkdurchgriffs des Fahrers auf die Räder nimmt die Sicherheitsrelevanz des Systems immens zu. Damit wachsen die Anforderungen an die Bauteile, aber auch den Entwicklungsprozeß des Systems.
- Gefährliche Einfachfehler, die aufgrund des Alterns der Systemkomponenten nicht auszuschließen sind, müssen zuverlässig erkannt und in der Art behandelt werden, daß sie für Fahrzeuginsassen, Fahrzeug und andere Verkehrsteilnehmer keine Gefahr darstellen [VDI88].
- Gegen Fehler, die nicht erkennbar und somit nicht behandelbar sind, muß das System robust sein. Der Nachweis über die Robustheit des noch im Forschungs-stadium befindlichen Systems muß noch erbracht werden. Bis zum Erfolg dieses Nachweises ist davon auszugehen, daß nicht entdeckbare Fehler sicherheitsrelevant sind und somit zum Eintritt des Top-Events C führen.

4.4 Abschließende Bemerkungen zu Kapitel 4

Die bisher skizzierten Komponenten des Systems Drive-by-Wire wurden nach funktionalen Gesichtspunkten konzipiert und sind bis auf die Lenkradwinkelerfassung und den Gierratensensor nur eingeschränkt fehlersicher bzw. fehlertolerant.
Es ist nochmals zu betonen, daß es sich bei dem hier beschriebenen System um einen Testträger in A-Muster-Stand handelt. Damit erklären sich gewisse Unschärfen hinsichtlich der Struktur von Steckverbindungen etc.
Jedoch soll auch betont werden, daß durch die Betrachtung der Funktion bzw. Information, eine Detaillierung bis auf Komponenten- bzw. Bauteileebene nicht zwingend erforderlich ist. Aus diesem Grund wurden hier konstruktive Maßnahmen zur Vermeidung der Kurzschlußfestigkeit bzw. Verpolungssicherheit etc., die in [Wei93] ausführlich beschrieben sind, nicht diskutiert.

Mit Blick auf die Sicherheitsrelevanz des Systems muß es das Ziel sein, schon in der Forschungsphase in den Entwicklungsprozeß in der Form einzugreifen, daß neben der Funktionalität auch Aspekte der System-Verfügbarkeit bzw. -Sicherheit berücksichtigt werden.

Durch die bereits angesprochene Zuordnung der Kabel, Kontakte, A/D-Wandlern etc. zu den jeweiligen Sensoren lassen sich die Fehlerbäume und Markov-Ketten in den folgenden Kapiteln erheblich reduzieren.

Es ist nochmals hervorzuheben, daß die Bewertung der Qualität von Redundanzkonzepten, wie sie im weiteren Verlauf der Arbeit erfolgt, maßgeblich von den Zuverlässigkeitsparametern Fehlermode und dessen Auftrittsverhalten beeinflußt wird. Da die im aktuellen Kapitel aufgeführten Zuverlässigkeitsparameter im wesentlichen aus [NPR95], [FMD91] und [Mah96_2] abgeleitet wurden, sind diese Daten als Stellvertreter des tatsächlichen Fehlerverhaltens zu verstehen. Die Frage der Übertragbarkeit auf Kfz-Systeme sowie die Gültigkeit der Markov'schen Bedingung muß streng genommen für jede Systemkomponente isoliert analysiert werden. Die hierfür geeignete Vorgehensweise wurde in Abschnitt 4.2.1.1. vorgestellt.

Aufgrund obiger Problematik soll die vorliegende Arbeit mit Schwerpunkt auf die Möglichkeit einer detaillierten Modellierung der F/V/S/W eines komplexen Systems verstanden werden. Es sei damit dem Leser überlassen, mittels der in den Kap. 3 und 4 zur Verfügung gestellten Methodik Systeme zu analysieren und vertraulich zu behandelnde systemimmanente Zuverlässigkeitskenngrößen in die Analyse einzuspeisen.

5 F/V/S/W-Analyse des Minimal-Konzeptes

Im vorliegenden Kapitel erfolgt die F/V/S/W-Analyse des in Kap. 4 vorgestellten Minimal-Systemkonzeptes des **D**rive-**b**y-**W**ire (D-b-W). Ziel hierbei ist die geschlossene Modellierung obiger Qualitätsparameter. Hierfür werden die in Kap. 3 vorgestellte FTA und die hierarchische Modellierung eingesetzt.
Die somit zu ermittelnde F/V/S/W des Minimal-Systems soll im Sinne des Abschnittes 2.2.3 als F/V/S/W-Maßstab des in Kapitel 6 vorzustellenden erweiteren Systementwurfs dienen.
Mit Blick auf Kap. 4 fließen nur die Zuverlässigkeitskenngrößen in die quantitative FTA bzw. hierarchischen Modelle ein, die innerhalb der festgelegten Systemgrenzen liegen. Außerhalb liegende Elemente wie Software bzw. deren Fehler und das Bordnetz, werden der Vollständigkeit halber im Rahmen der FTA qualitativ aufgeführt.

5.1 Auswirkungen der Fehlermöglichkeiten aus Kap. 4

Gemäß Kap. 3 ist eine wesentliche Voraussetzung der detaillierten quantitativen F/V/S/W-Analyse, die Auswirkungen der in Kap. 4 vorgestellten Fehlermoden auf das Gesamtsystemverhalten zu bestimmen. Hierzu soll eine abgewandelte Form der in [Oco90, Mey86] beschriebenen FMEA verwendet werden. Mit Verweis auf Abschnitt 2.2.1 (Sicherheitsmaßstab: gefährliche Einfachfehler müssen erkannt und ihr kritischer Einfluß auf das Systemverhalten ausgeschlossen werden), sollen hier Einfachfehler der innerhalb der Systemgrenzen berücksichtigten Sensorik und Rechnerhardware sowie mögliche Reaktionen der FELB auf diese analysiert werden. Durch die Berücksichtigung der in Kap. 3 und 4 beschriebenen Fehlermöglichkeit der FELB ergibt sich folglich eine Zweifachfehlerbetrachtung, womit auch der Forderung „ein Versagen der FELB muß erkannt werden“ nachgegangen wird (siehe hierzu Abschnitt 5.3).

In Anhang E befindet sich die Tabelle „Auswirkungen der Fehlermöglichkeiten der D-b-W-Komponenten des Minimal-Systems auf das Systemverhalten“. In dieser Tabelle wurden gemäß Kap. 4.2 die Fehlermoden Hardfailure, Softfailure und temporärer Fehler für jede innerhalb der betrachteten Systemgrenzen befindliche Komponente diskutiert. Hierbei wurde hinterfragt, inwieweit bei Auftreten des jeweiligen Fehlers die Fehlererkennung, die Fehlerlokalisation und Fehlerbehandlung möglich ist und in welcher Zeit die jeweilige FELB-Aktion nach Auftreten des Fehlers erfolgt. Darüberhinaus wurde die Systemreaktion hinsichtlich ihrer Verfügbarkeits- bzw. Sicherheitsrelevanz unterschieden. Ferner wurde eine Zuordnung des betrachteten Fehlers zu einem der vier Top-Events vorgenommen (vergleiche Abschnitt 3.1.1). Da sämtliche Fehler automatisch einem „Auftreten eines beliebigen Systemfehlers“ gleichkommen, wurde der Eintritt des Top-Events D nicht explizit in der Tabelle vermerkt.

Diese Tabelle entspricht der bereits in Kap. 3 erwähnten „Quasi-FMEA“ des Systems und stellt eine wesentliche Voraussetzung für die Erstellung der qualitativen Fehlerbäume sowie die hierarchischen Modelle dar.

Zur Verdeutlichung der Vorgehensweise soll an dieser Stelle ein Auszug aus der Tabelle „Auswirkungen der Fehlermöglichkeiten der D-b-W-Komponenten des Minimal-Systems auf das Systemverhalten“ aus Anhang E dargestellt werden.

Fehler in Komp.	Fehler-mode	FE-Maß-nahme und FE-Rate	FL-Maß-nahme und FL-Rate	FB-Maß-nahme und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Abs. LRW-Sensor	HF	HF-FE-Modul FE-R.: Gl. 4-24	FE kommt FL gleich	D-b-W in RFE überführen FB-R.: Gl. 4-28	Fehler wirkt sich verfügbarkeitskritisch aus. Bis zur FELB (6 Zyklen) auch sicherheitskritisch, da beispielsweise im Moment der Initialisierung des inkr. LRW-Sensors ein fehlerhafter Lenkwinkel weiterverarbeitet wird. Aufgrund der angenommenen 100%igen-FELB ist der Fehler jedoch nach der FB nicht mehr als sicherheitskritisch anzusehen. Dieser transiente Sachverhalt kann in der FTA nur bedingt über die Modellierung temporärer Fehler berücksichtigt werden. **Top-Event: B** Im Rahmen der Detailanalyse via hierarchischer Modellierung (Abschnitt 5.3) wird die Reaktionszeit der FELB über einen „sicherheitsrelevanten“ Zwischenzustand modelliert, der nach der Fehlererkennungszeit (siehe Gl. 4-24) wieder verlassen wird. Der sicherheitsrelevante Zustand ist also nicht absorbierend (Hier sieht man also bereits einen wesentlichen Vorzug der detaillierten dynamischen Modellierung mittels MKA). Weitere Kommentare zur FB: Nach der Onboard-FB Offboard-FB einleiten: • Rote Warnlampe aktivieren • Ablegen der Fehlermeldung im Diagnosespeicher • $\nu_{Fahrer\text{-}Rot}$: Gl. 4-30 • MB-Service und Offboard-Reparaturrate gemäß Gl. 4-31 und 4-32

Tabelle 5.1: Auszug aus der in Anhang E aufgeführten „Auswirkungen der Fehlermöglichkeiten der D-b-W-Komponenten des Minimal-Systems auf das Systemverhalten“

Wie den Spalten 1 und 2 zu entnehmen ist, wurde hier der Hardfailure (HF) des absolutmessenden Lenkradwinkelsensors (siehe Abschnitt 4.2.1.1.1) diskutiert.

Spalte 3 und 4: Bei Auftreten des Fehlers erfolgt seine Erkennung (FE, **F**ehler**e**rkennung) über das Hardfailure-Erkennungsmodul (siehe Abschnitt 4.2.3.1.2.1). Die Erkennungszeit beträgt gemäß **F**ehler**e**rkennungs**r**ate FE-R aus Gl. 4-24 160ms. Die Hardfailure-Erkennung kommt der **F**ehler**l**okalisation (FL) gleich. Die fehlerhafte Komponente ist eindeutig identifiziert.

Spalte 5: D-b-W wird binnen eines Rechenzyklusses von 10ms (**F**ehler**b**ehandlungs**r**ate FB-R) in die Rückfallebene überführt.

In Spalte 6 befinden sich neben der Klassifikation nach Verfügbarkeits- und Sicherheitsrelevanz bzw. Top-Event-Zugehörigkeit des betrachteten Fehlers weitere für die Onboard- bzw. Offboard-FELB wichtigen Kommentare.

5.2 FTAs des Minimal-Konzeptes

Nachdem in Abschnitt 5.1 die Auswirkungen der in Kap. 4 skizzierten Fehlermoden diskutiert wurden, folgen nunmehr die FTAs der in Kap. 3 abgeleiteten Top-Events.

Da die in „Fault-Tree+“ erzeugten Fehlerbäume nicht mit akzeptabler Auflösung in das Textverarbeitungsprogramm einbindbar sind, befinden sich die entsprechenden Graphen und Tabellen in Anhang E-N der vorliegenden Arbeit. Es sei im folgenden davon ausgegangen, daß sämtliche im Anhang graphisch bzw. tabellarisch dargestellten Fehlerbäume mit den in Kap. 3-5 diskutierten Hintergründen im wesentlichen selbsterklärend sind. Die Fehlerbäume werden qualitativ durch die Grafiken beschrieben. Die quantitative Analyse erfolgt in Form der in diesen Abschnitt eingebundenen Pareto-Diagramme. Q entspricht in sämtlichen Fehlerbäumen der Fehlerwahrscheinlichkeit bzw. Auftrittswahrscheinlichkeit der Top-Events. Als Missionsdauer wurde mit Verweis auf die Abschnitte: 3.1.2.3 und 3.1.2.8 der Zeitraum des ersten Betriebsjahres ab Zulassung, d.h. effektiv 300 Betriebsstunden angesetzt.

5.2.1 Fehlerbaum Top-Event A des Minimal-Systems

Zur Erinnerung sei an dieser Stelle nochmals angemerkt, daß zum unerwünschten Ereignis „Top-Event A“ die Komponentenfehler führen, die eine Degradation des D-b-W-Reglers von der höchsten Regelgüte in eine niedrigere erforderlich machen. Weitere Details finden sich in Abschnitt 3.1.1.1 bzw. 4.2.3.1.
Die graphische Darstellung und damit qualitative Fehlerbaumanalyse des Top-Events A findet sich in Anhang F1. Sämtliche Komponentenfehler fließen mit den in Kap. 4 definierten Fehlerraten in Oder-Gatter des Fehlerbaums ein. Es wurde hierbei bewußt eine Modularisierung im Sinne des Schwimmwinkelschätzers vorgenommen. Wie der Darstellung zu entnehmen ist, fließen sämtliche übrigen Komponentenfehler, die für Top-Event A verantwortlich sind, auch gleichzeitig in das Gatter des Schwimmwinkelschätzers ein. Entsprechend trägt die Fehlerwahrscheinlichkeit des Schwimmwinkelschätzers gemäß Absorptionsgesetz rechnerisch nicht zur Erhöhung der Auftrittswahrscheinlichkeit des Top-Events A bei. Es soll jedoch betont werden, daß der Schwimmwinkelschätzer auch aufgrund anderer Komponentenfehler ausfällt bzw. Schätzfehler aufweist. Da die hierfür ursächlichen Fehler jedoch unmittelbar zum Top-Event B oder C führen, sind sie nicht im Fehlerbaum des Top-Events A aufgeführt.
Grundsätzlich wird deutlich, daß der Schwimmwinkelschätzer ein sehr fehleranfälliges Konstrukt darstellt. Diese Aussage kann bereits als erstes Indiz für die Fehleranfälligkeit analytischer Kanäle, auf dem einer der beiden in Kap. 6 vorzustellenden FELB-Ansätze basiert, gewertet werden. Details zur F/V/S/W eines analytischen Kanals folgen in Kap. 6.

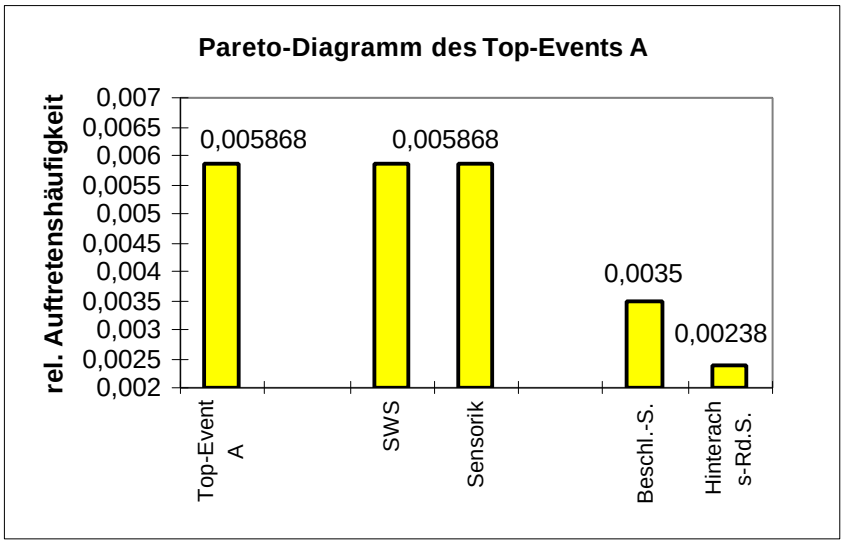


Bild 5.1: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events A

Dem Pareto-Diagramm ist zu entnehmen, daß von 1Mio. einjährigen, mit D-b-W ausgestatteten Pkw innerhalb der Missionsdauer von 300 Stunden 5.868 Fahrzeuge eine Degradation der Fahrdynamikregelung auf die Reglerstufe 2 oder 3 erfahren haben.
Den Fragen, wieviele Fahrzeuge genau zum Zeitpunkt $t_{Mission}$ = 300 Stunden in der Regelstufe 2 oder 3 unterwegs sind bzw. einen entsprechenden Fehler aufweisen, der jedoch noch nicht erkannt wurde, wird in Abschnitt 5.3 nachgegangen.

Weitere Kommentare zum Fehlerbaum des Top-Events A:
Anhand Tabelle 5.1 bzw. Anhang E und dem qualitativen Fehlerbaum in Anhang F1 wird deutlich, daß sämtliche das Top-Event tangierenden Komponentenfehler in ODER-Gatter einfließen. Die Top-Event-A-Fehlerrate entspricht folglich der Summe der einzelnen Fehlerraten, wobei hier jedes Element unabhängig von der Häufigkeit seiner Aufführung im Fehlerbaum, nur einmal gezählt wird.
Es ist mit Verweis auf Abschnitt 2.1 und 3.1.1 wichtig zu betonen, daß es sich bei obiger Auftretenswahrscheinlichkeit des Top-Events A lediglich um die zu erwartende rel. Häufigkeit der Notwendigkeit einer Degradation von der höchsten Reglerstufe auf eine der beiden niedrigeren, ebenfalls elektronischen Reglerstufe RG 2 oder 3 handelt. Die Frage der Systemverfügbarkeit und -sicherheit wird in Abschnitt 5.2.2 bzw. 5.2.3 und 5.3 diskutiert. Wie sich in den folgenden Pareto-Diagrammen der Top-Events B und C zeigen wird, besteht deutlich häufiger die Notwendigkeit, D-b-W in die Rückfallebene zu überführen bzw. ist es nicht möglich, einen Fehler zuverlässig erkennen zu können, als die Möglichkeit, D-b-W in RG 2 bzw. 3 zu überführen. Erst eine Verbesserung der FELB bzw. eine Erhöhung der Informationsredundanz kann dieses Verhältnis zugunsten der Systemverfügbarkeit ändern.
Abschließend soll angemerkt werden, daß die in Anhang F aufgeführten Rauten der qualitativen Berücksichtigung in dieser Arbeit nicht weiter detaillierter Systemumfänge, wie beispielsweise Softwarefehler, dienen. Damit bietet die FTA die Möglichkeit, trotz des Unvermögens, das Ausfallverhalten von Software mathematisch modellieren zu können, auf die Fehlereinflüsse bzw. Schnittstellen der Software im Systemkontext hinzuweisen. Sollten sich später Modelle finden, um auch das zeitliche Fehlerverhalten von Software zu modellieren, kann dieses Verhalten zu einem späteren Zeitpunkt in die FTA eingebunden werden.

5.2.2 Fehlerbaum Top-Event B des Minimal-Systems

Unter Top-Event B sind die Komponentenfehler zusammengefaßt, die eine Überführung des Systems D-b-W in die mechanische Rückfallebene erfordern. Top-Event B entspricht somit der Unverfügbarkeit des Systems D-b-W. Weitere Details finden sich in Abschnitt 3.1.1.2 bzw. Kap. 4.

Die graphische Darstellung und damit qualitative Fehlerbaumanalyse des Top-Events B findet sich in Anhang F2. Wie bereits in Abschnitt 5.2.1 angedeutet, führen im Minimal-System deutlich mehr Komponentenfehler zur Notwendigkeit, das D-b-W in die RFE zu überführen. Mit Blick auf die Systemverfügbarkeit ist diese Aussage negativ zu bewerten. Andererseits verdeutlicht diese Tatsache, daß es sich beim D-b-W um ein sicherheits-relevantes System handelt, bei dem nicht unterdrückbare Fehler zumeist kritische Folgen haben könnten. Daher ist eine mitunter „verfrühte“ RFE-Überführung anzuraten.

Wie in Tabelle 5.1 bzw. Anhang E erläutert, finden sich im aktuellen Fehlerbaum verstärkt die Modularisierungen im Bereich der beiden Kanäle der „Vorfilter“ bzw. „ψ-Regler“. Wird eine Abweichung der beiden Kanäle voneinander erkannt, muß das System degradiert werden. Mit Blick auf das Absorptionsgesetz (siehe Abschnitt 3.1.2.6) sind einige Gatter in Anhang F2 in reduzierter Form dargestellt.

Um die Fehleranfälligkeit des ψ-Reglers zu veranschaulichen, wurde trotz Absorptions-gesetz in der qualitativen FTA das jeweilige Vorfilter als Ursache für einen Fehler des Reglers berücksichtigt.

In Abschnitt 5.3 werden die hier generierten Fehler-Module in die hierarchischen Modelle eingebunden. Dies kann als Benefit der FTA gewertet werden.

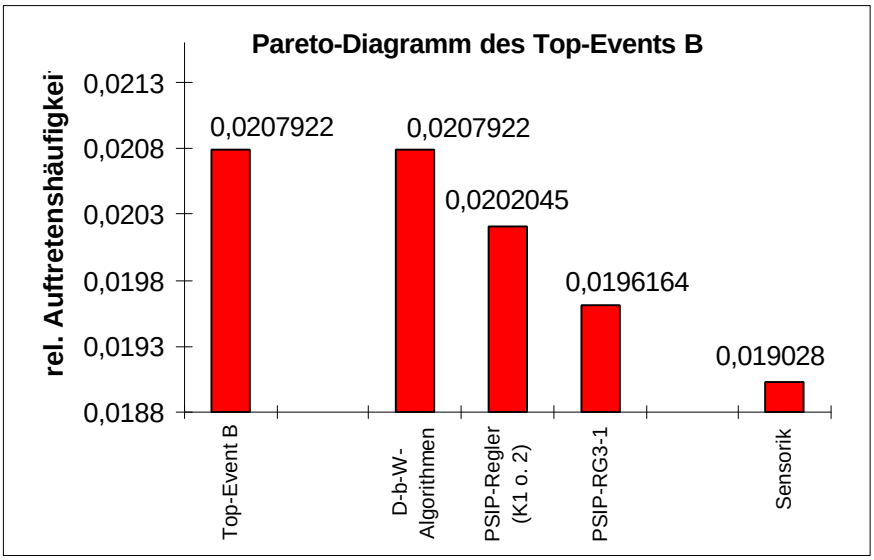


Bild 5.2: Pareto-Diagramm dominanter Gatter des Fehlerbaums des Top-Events B

In Bild 5.2 sind unter den Balken:

- D-b-W-Algorithmen: Fehler innerhalb der D-b-W-Software, aber auch -HW zusammengefaßt, die zu einem erkennbaren Fehler innerhalb der D-b-W-Algorithmik führen, der seinerseits eine Degradation in RFE erfordert.
- PSIP-Regler (K1 o. K2) : Fehler im ersten oder zweiten Kanal des ψ-Reglers (siehe Bild 4.4 und 4.7).
- PSIP-RG3-1: Fehler in Reglerstufe RG3 des ersten Kanals des ψ-Reglers.

Diskussion von Bild 5.2

Bild 5.2 ist zu entnehmen, daß von 1Mio. einjährigen, mit D-b-W ausgestatteten Pkw innerhalb der Missionsdauer von 300 Stunden 20.792 Fahrzeuge eine Degradation der Fahrdynamikregelung in die mech. Rückfallebene erfahren haben.

Es gilt festzuhalten, daß 97% der Top-Event-B-Fehler in Zusammenhang mit einer Fehlfunktion innerhalb eines der beiden $\dot{\psi}$-Regler stehen. Dieser Umstand ist damit zu begründen, daß in die entsprechenden Gatter, mit Ausnahme der SWS-Transputer, sämtliche am Top-Event B beteiligten Fehlermoden einfließen.

Im folgenden gilt es weiter zu differenzieren, welche Komponentenfehler die Reglerfehler dominieren.

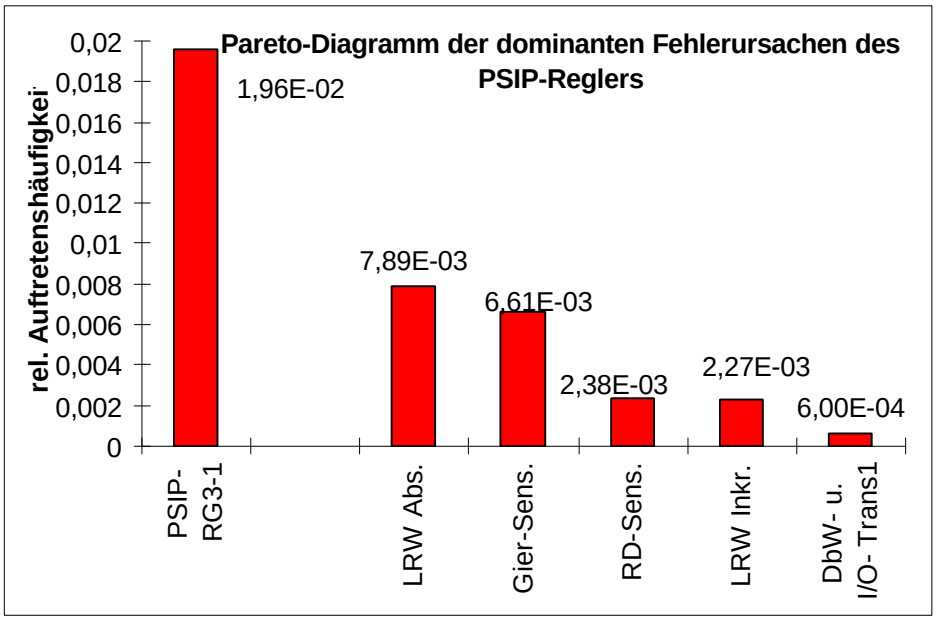


Bild 5.3: Pareto-Diagramm der dominanten Gatter des Kanals 1 der Reglerstufe RG3 des $\dot{\psi}$-Reglers

Diskussion von Bild 5.3

Wie Bild 5.3 zu entnehmen ist, wird die Häufigkeit der Notwendigkeit das D-b-W-System aufgrund eines $\dot{\psi}$-Regler-Fehlers in die RFE zu überführen durch Fehler des absoluten LRW-Sensors und des Gierratensensors dominiert.

5.2.3 Fehlerbaum Top-Event C des Minimal-Systems

Unter Top-Event C sind die Komponentenfehler zusammengefaßt, die sicherheitsrelevanter Natur sind. Weitere Details finden sich in Abschnitt 3.1.1.3 bzw. Kap. 4. Die graphische Darstellung und damit qualitative Fehlerbaumanalyse des Top-Events C findet sich in Anhang F3.
Es kann mit Blick auf Bild 5.4 zusammengefaßt werden, daß mit Ausnahme des Top-Events D die meisten Fehlfunktionen des D-b-W-Minimal-Systems zum Eintritt des Top-Events C führen. Dies spiegelt sich in der Komplexität des Fehlerbaums (qualitative FTA) des Top-Events C wider.
So führen:

- 11 Basic-Events (Fehlermoden) zum Eintritt des Top-Events A,
- 17 Basic-Events zum Eintritt des Top-Events B,
- 26 Top-Events zum Eintritt des Top-Events C.

Dennoch tritt Top-Event C nicht so häufig wie Top-Event B auf. Grund hierfür ist der Umstand, daß die für das Auftreten des Top-Events C schwerpunktmäßig ursächlichen temporären Fehler gemäß Tabelle 4.5 nur 8,8% der Gesamtfehlerwahrscheinlichkeit der Sensorik ausmachen.
Die hohe Anzahl von Fehlermoden, die zum Eintritt des Top-Events C führen, unterstreicht wiederum die Tatsache, daß es sich beim D-b-W um ein sicherheitsrelevantes System handelt, bei dem Fehler, die nicht aus dem System durch Wegschalten eliminiert werden, kritische Folgen haben könnten.
Die hohe Anzahl sicherheitskritischer Fehlermoden ist auf den Umstand zurückzuführen, daß innerhalb des Minimal-Systems nur wenige Fehler erkennbar oder gar lokalisierbar sind. Würde das System über die Minimal-Struktur hinaus weitere redundante Informationen zur Verfügung stellen, könnte häufiger eine Degradation auf die RFE erfolgen. Diese Strategie der Erhöhung der Systemverfügbarkeit bei gleichzeitiger Erhöhung der Systemsicherheit wird in Kap. 6 diskutiert. In Analogie zu Bild E2 wird auch in Bild E3 der Umstand berücksichtigt, daß der Gierratensensor-Selbsttest nicht in allen Fahrsituationen ausgeführt werden kann. Ansonsten finden sich auch hier verstärkt die Modularisierungen im Bereich der beiden Kanäle des Vorfilters bzw. ψ-Reglers. Mit Ausnahme der Sensorik sind diese beiden Module zweikanalig aufgebaut. Somit können Fehler nur dann nicht durch den Vergleich beider Informationskanäle erkannt werden (Top-Event C), wenn sie gleichzeitig in beide Kanäle einfließen.

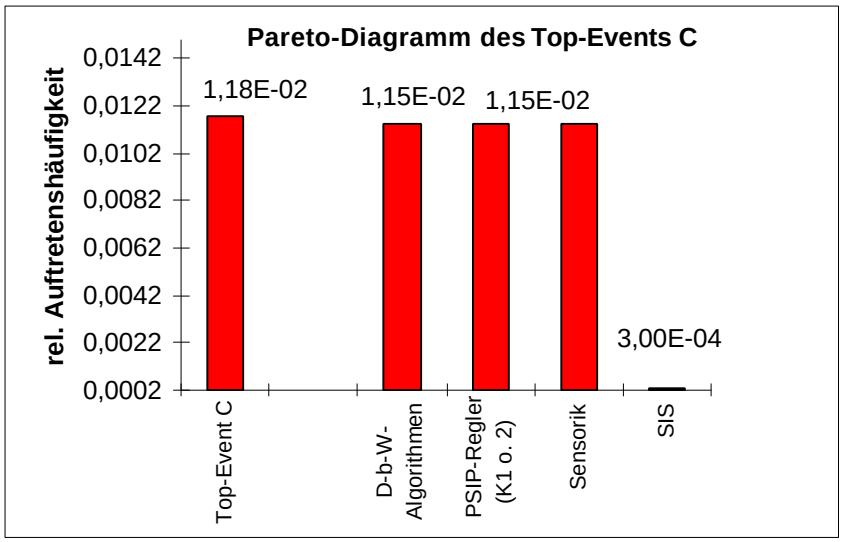


Bild 5.4: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events C

Unter dem Gatter „SIS“ sind Fehler innerhalb des einkanaligen SIS-Transputers bzw. seiner Software zusammengefaßt.

Diskussion von Bild 5.4

Bild 5.4 ist zu entnehmen, daß von 1Mio. einjährigen, mit D-b-W ausgestatteten Pkw innerhalb der Missionsdauer von 300 Stunden ca. 11.800 Fahrzeuge einen Fehler aufweisen, der vom System nicht erkannt werden kann und somit potentiell sicherheitsrelevant ist.

Es gilt festzuhalten, daß sämtliche Fehler auf eine Fehlfunktion innerhalb des Fahrdynamikreglers (D-b-W-Algorithmen oder SIS) zurückzuführen sind. Durch die oben angesprochene Zweikanaligkeit, sind die D-b-W-Algorithmenfehler fast ausschließlich auf Sensorfehler zurückzuführen.

Im folgenden gilt es weiter zu differenzieren, welche Komponentenfehler das Gatter SENSORIK im Fehlerbaum des Top-Events C dominieren.

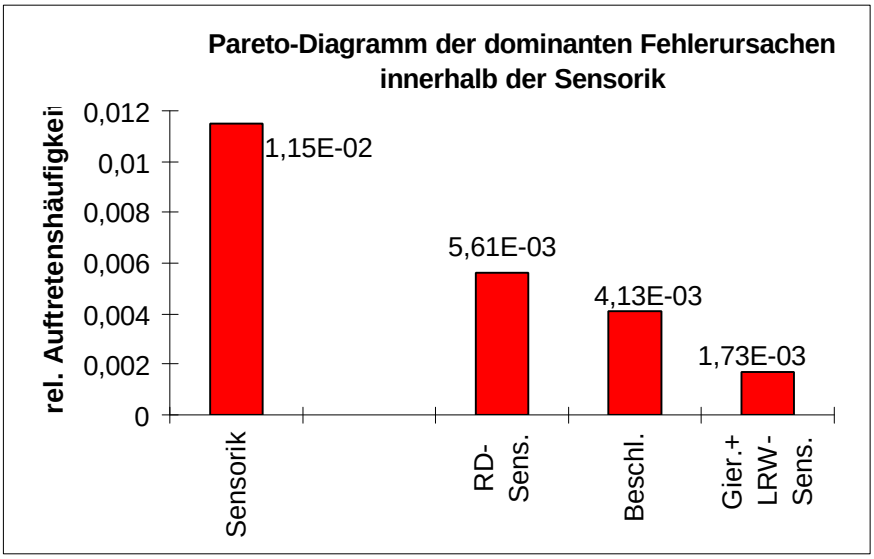


Bild 5.5: Pareto-Diagramm dominanter Komponentenfehler des Gatters SENSORIK des Top-Events C

Diskussion von Bild 5.5
Wie Bild 5.5 zu entnehmen ist, werden die zu Top-Event C führenden Sensorikfehler durch die Fehler der Raddrehzahlsensorik (Rd-Sens.) und der Beschleunigungssensorik (Beschl.) dominiert. In Summe machen sie 86% der sicherheitsrelevanten Sensorik-Fehler aus. Vergleicht man diese Verteilung mit der in Bild 5.3 für das Top-Event B dargestellten Verteilung, so weichen beide deutlich voneinander ab. In Bild 5.3 dominierten die LRW- und Gierratensensorik. Grund für die hier nun genau umgekehrten Verhältnisse ist der Umstand, daß für Top-Event C im wesentlichen nur temporäre Fehler der beiden letztgenannten Sensorarten ursächlich sind. Die Raddrehzahlsensorik und Beschleunigungssensorik verfügt im Minimal-System jedoch über keinerlei Überwachungslogik zur Detektion von Softfailures. Wäre eine entsprechende Überwachung möglich, würde dies zu einer Senkung der Auftretenshäufigkeit des Top-Event C auf 0,00336 führen. Damit würden von obigen 1Mio. Fahrzeugen innerhalb der Missionsdauer von 300 Stunden nur noch 3360 Fahrzeuge einen sicherheitsrelevanten nicht erkennbaren Sensorfehler aufweisen. Dies entspricht einer relativen Senkung der Fehlerhäufigkeit von 71%.

> **Bereits die Überwachbarkeit der Softfailures der Raddrehzahlsensorik würde eine Senkung der Häufigkeit des Top-Event-C auf 0,0068 bewirken. Diese gegenüber der Häufigkeit des Top-Event-C aus Bild 5.4 erreichbare Senkung um 42% soll mittels der in Kap. 6 vorzustellenden erweiterten FELB-Strategien erzielt und diskutiert werden.**

Weitere Kommentare zum Fehlerbaum des Top-Events C:
Mit Verweis auf Bild F3 sei festgehalten, daß im Gegensatz zum Top-Event A und B (Bild F1, F2) Fehlfunktionen des Bordnetzes nicht im Fehlerbaum des Top-Event C berücksichtigt wurden. Ursache hierfür ist der Umstand, daß durch die angenommene Vollredundanz des Bordnetzes Fehler innerhalb desselben zuverlässig erkannt werden können.

5.2.4 Top-Event D des Minimal-Systems

Gemäß Abschnitt 3.1.1.4 fließen in Top-Event D sämtliche innerhalb der betrachteten Systemgrenzen möglichen Komponentenfehler ein. Unter der Annahme, daß diese Komponentenfehler dem Kunden früher oder später auffallen bzw. ihm durch die FELB kommuniziert werden, stellt Top-Event D indirekt ein Maß für die Kundenzufriedenheit dar.
Da der qualitative Fehlerbaum für dieses Top-Event lediglich einer graphischen Darstellung der in Abschnitt 5.1 bzw. der Tabelle in Anhang E aufgeführten Fehlermöglichkeiten des Systems entspricht, wurde auf eine Einbindung in diese Arbeit verzichtet. Vielmehr soll an dieser Stelle lediglich das Endergebnis, sprich die Fehlerwahrscheinlichkeit des Gesamtsystems benannt werden.
Für das Minimal-System ergibt sich die Gesamtfehlerwahrscheinlichkeit von 4,15%. Hierbei soll angemerkt werden, daß Sensoren wie der Bremslichtschalter, Bremsdrucksensor und das Drosselklappenpotentiometer nicht zum Systemumfang hinzugerechnet wurden.
Von 1Mio. einjährigen, mit D-b-W ausgestatteten Pkw wiesen innerhalb der Missionsdauer von 300 Stunden ca. 41.500 Fahrzeuge einen Fehler auf, der den Kunden früher oder später zum Aufsuchen der Werkstatt veranlassen wird. Es soll betont werden, daß die in Abschnitt 5.2.1 bis 5.2.3 diskutierten Fehler jeweils Teilmengen der Top-Event-D-Fehler darstellen. Setzt man die in Abschnitt 5.2.4 bestimmte Auftretenswahrscheinlichkeit eines sicherheitsrelevanten Fehlers von 1,18% in Relation zu obigen 4,15%, so bedeutet dies statistisch betrachtet, daß im D-b-W-Minimal-System nahezu jeder dritte Fehler (28,4%) sicherheitsrelevanter Natur ist.
Dieses Verhältnis muß durch die in Kap. 6 vorzustellenden erweiterten FELB-Konzepte unbedingt abgesenkt werden.

5.2.5 Kritische Pfade des Systems / Zwischenbilanz der F/V/S/W-Analyse mittels FTA

In den Abschnitten 5.2.1-5.2.4 wurde deutlich, daß erst durch die Unterscheidung der Fehlermoden der einzelnen Komponenten eine Differenzierung nach Fehlerhäufigkeit, Degradation der Regelgüte, Verfügbarkeit und Sicherheit innerhalb des Fehlverhaltens des D-b-W-System ermöglicht wurde.
Diese Differenzierung fußte maßgeblich auf der Fähigkeit der Sicherheitssoftware und -schaltung, gewisse Fehlermoden erkennen, lokalisieren und behandeln zu können. So ergab die Pareto-Analyse, daß die Auftretenshäufigkeit des sicherheitsrelevanten Top-Events C durch die Softfailures der Raddrehzahl- und Beschleunigungssensorik dominiert wird. Da die Einführung von FELB-Strategien zur Erkennung, Lokalisation und Behandlung von Softfailures innerhalb der Raddrehzahlsensorik zu einer Senkung der Auftretungshäufigkeit des Top-Event C um 42% führen würde, werden in Kap. 6 entsprechende FELB-Konzepte vorgestellt und hinsichtlich ihrer Auswirkungen auf die Qualitätsparameter diskutiert.
Gleichzeitig ist kritisch anzumerken, daß bedingt durch die gegenüber der Sensorik geringe Fehlerhäufigkeit der Transputerhardware eine zweikanalige Rechnerarchitektur nur geringfügige Vorzüge hinsichtlich der Senkung der Top-Event B- bzw. C-Häufigkeit bietet.
Wie Abschnitt 5.2.4 verdeutlichte, ist statistisch betrachtet mit ca. 28% der möglichen Fehler im Minimal-System ein enorm hoher Anteil der Fehler sicherheitsrelevanter Natur. Dieser Anteil muß durch eine Verbesserung der Fehlererkennung, -lokalisation und –behandlung minimiert werden. Dies wird in Kap. 6 durch die erweiterten FELB-Konzepte verdeutlicht.

Als wesentlicher Vorteil der FTA ist zu erwähnen, daß die Systemanalyse mit geringem Aufwand vorgenommen werden konnte.

Nachteilig ist die getrennte Analyse des Fehlerverhaltens nach Fehlerhäufigkeit, Degradation der Reglergüte, Verfügbarkeit und Sicherheit. Um die Einflüsse einer Soft-FELB der Raddrehzahlsensorik, wie sie in Kap. 6 vorgestellt wird, auf die vier Top-Events analysieren zu können, sind entsprechend 8 verschiedene Fehlerbäume miteinander zu vergleichen. Hier schafft die MKA bzw. hierarchische Modellierung Abhilfe, die neben der geschlossenen Analyse der Qualitätsparameter auch eine Modellierung des Faktors Wirtschaftlichkeit erlaubt.
Dennoch wird sich in Abschnitt 5.3 zeigen, daß erst durch die erstellten Fehlerbäume eine geschickte Modellierung des Systemverhaltens im Zustandsraum ermöglicht wird. So lassen sich beispielsweise fast sämtliche nicht entdeckbaren und damit sicherheits-relevanten Top-Event-C-Fehler in einem Zustand „Top-Event C“ zusammenfassen. Diese dem Begriff der hierarchischen Modellierung zuzuordnende „Clusterungen“ führt zu einer immensen Reduzierung der Zustandsraumkomplexität.

5.3 Hierarchische Modellierung des Minimal-Systems

Abschnitt 5.2 war zu entnehmen, daß sich die Einführung einer Softfailure-FELB der Raddrehzahlsensorik positiv auf die Systemsicherheit auswirkt. Bevor in Kap. 6 entsprechende FELB-Konzepte diskutiert werden, gilt es mittels der nun folgenden hierarchischen Modellierung den Faktor Garantie- und Kulanz-Kosten des Minimal-Systems abzuleiten. Neben der Wirtschaftlichkeitsaussage bietet die hierarchische Modellierung weiterhin den Vorzug der detaillierten geschlossenen Analyse der Degradationshäufigkeit, Verfügbarkeit und Sicherheit des D-b-W-Systems sowie die Möglichkeit, die in Abschnitt 3.2.1.2 eingeführten „heilenden“ Zuverlässigkeitskenngrößen in die Systemanalyse einzubeziehen. Erst durch die Einführung dieser Zuverlässigkeits-kenngrößen läßt sich das dynamische Systemverhalten in den Degraded-Modes (RG 2, 3 und der RFE) analysieren.
In Tabelle 5.2 findet sich ein Auszug der für die Aufstellung des Zustandsraummodells wichtigen Systemgrößen. Die gesamte Tabelle findet sich in Anhang G. Die hier aufgeführten Informationen orientieren sich an den in Abschnitt 3.2.3.2 „Kurzanleitung zur Aufstellung von Markov-Ketten“ als essentiell identifizierten Systemkenngrößen.
So sind in den beiden ersten Spalten die für die Zustandsraummodellierung erforderlichen Systemzustände nebst Kurzbeschreibung des Zustands aufgeführt.
Spalte 3 und 4 beinhalten die aus dem jeweiligen Zustand i in einen Folgezustand j führenden Übergänge mit den entsprechenden Übergangsraten $q_{i,j}$.
Somit liegen hier alle für die Aufstellung und Lösung der Chapman-Kolmogorov-Differentialgleichung (siehe Abschnitt 3.2.1) erforderlichen Systemgrößen vor.

Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
0	D-b-W in Reglerstufe RG1 • Fehlerfreier Startzustand • Zustand in Bild 5.6 farblich grün hervorgehoben • Startaufenthaltswahr-scheinlichkeit = 1	$q_{0,1}$	Fehler- bzw. Ausfallrate, die sich über einen Fehlerbaum mit der Veroderung aus folgenden Eingangsgrößen zusammensetzt (siehe auch Kap. 4): • HF absolut LRW-Sensor • HF inkr. LRW-Sensor • HF Gierratensensor • HF beide Raddrehzahlsensoren der Vorderachse $q_{0,1} = \lambda_{Modul} = 36{,}375 \cdot 10^{-6}\ \frac{1}{h}$ Entspricht mit Ausnahme der Sensor-Softfailures dem Gatter SENSORIK des Top-Events B (siehe Anhang F2).

Tabelle 5.2: Auszug aus der in Anhang G befindlichen Tabelle „Für die Zustandsraum-modellierung des D-b-W Minimal-Systems erforderliche Kenngrößen“

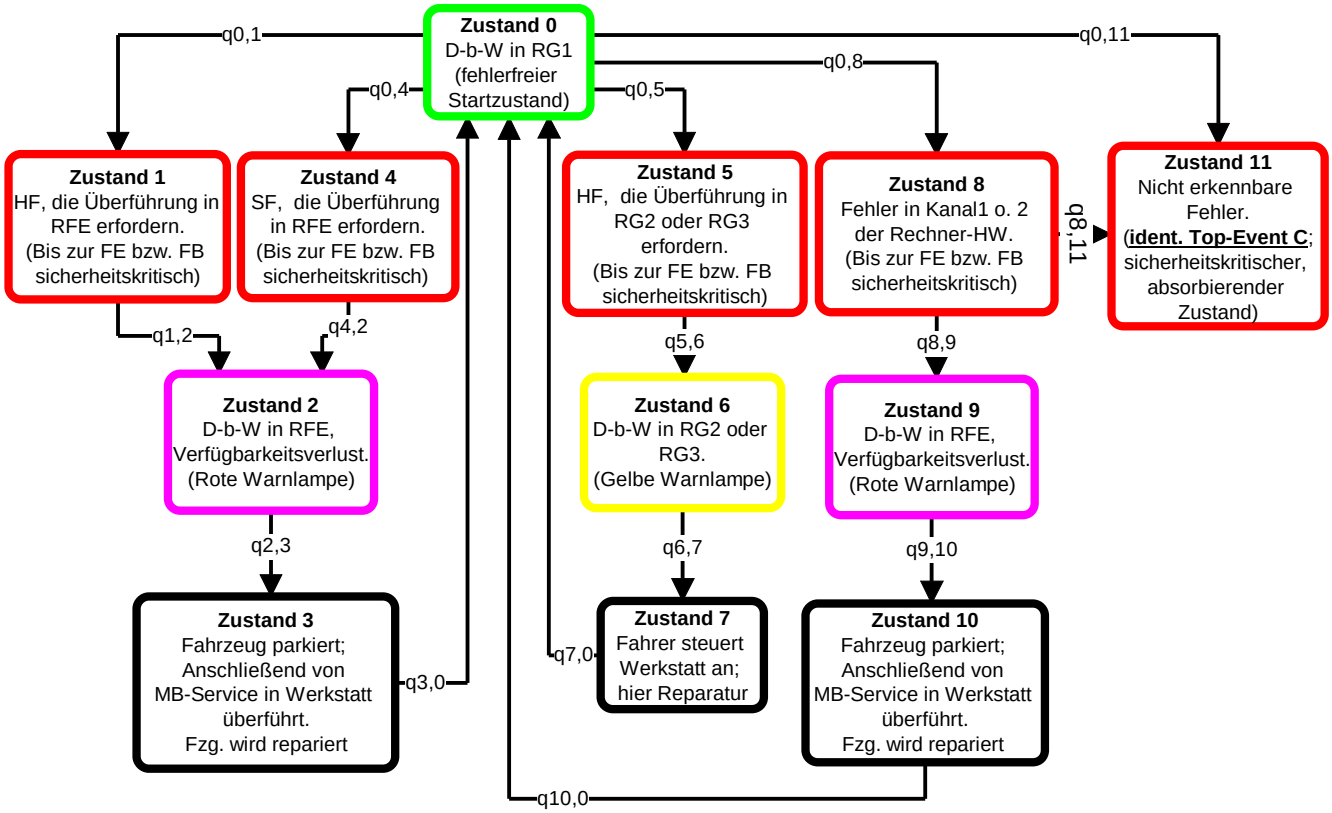


Bild 5.6: Markov-Kette des Systems D-b-W

Kommentare zu den Zuständen und Zustandsübergängen:
Bild 5.6 stellt das aus der Tabelle in Anhang G hervorgehende Zustandsraummodell dar. Hierbei entspricht Zustand 0 dem fehlerfreien Betriebszustand des Minimal-Systems D-b-W. Je nach Fehlerart degradiert das System von diesem Startzustand in die Zustände 1, 4, 5, 8 oder 11. Mit Ausnahme des absorbierenden Zustandes 11 handelt es sich bei obigen Zuständen um Zwischenzustände, die durch die folgende Onboard-Fehlererkennung bzw. -lokalisation und –behandlung verlassen werden. Da sich das System bis zur eigentlichen Fehlererkennung bzw. -lokalisation und -behandlung in einem fahrdynamisch kritischen Zustand befinden kann, wird davon ausgegangen, daß obige Zustände sicherheitskritischer Natur sind, weswegen sie rot umrandet sind. In Zustand 11 führen sämtliche in Top-Event C mündende Fehler (vergleiche Abschnitt 5.2.3). Im Sinne der pessimistischen Analyse wurde davon ausgegangen, daß ein von der FELB nicht entdeckbarer Fehler die potentielle Gefahr einer Verunfallung in sich birgt. Daher wurde Zustand 11 als absorbierend modelliert. Diese Annahme bewirkt, daß die Markov-Kette ergodisch ist. **Gemäß Abschnitt 3.2.1.2.1 ist der Umstand, daß ausgerechnet der einzig absorbierende Zustand sicherheitsrelevant ist, für die Systemsicherheit des Systems äußerst ungünstig.**
Wie bereits erläutert, werden die Zustände 1, 4, 5 und 8 nach erfolgter onboardseitiger Erkennung bzw. Lokalisation und Behandlung des Fehlers in die Zustände 2, 6 bzw. 9 verlassen. In den Zuständen 2 und 9 wird das System in der mech. Rückfallebene betrieben (vergleiche Abschnitt 5.2.2, Top-Event B) und der Fahrer mittels roter Warnlampe zum sofortigen Parkieren und Überführen des Fahrzeugs in die Werkstatt aufgefordert. Im Zustand 6 wird das System in der Reglerstufe 2 bzw. 3 betrieben, womit dieser Zustand Top-Event A zuzuordnen ist.
In den Folgezuständen 3, 7 und 10 wird das Fahrzeug in die Werkstatt überführt bzw. dort repariert. Hier wurde zwischen drei Zuständen unterschieden, um zwischen erforderlichem Abschleppen, unterschiedlichen Reparaturen, den hiermit einhergehenden Zeitaufwänden

und Kosten differenzieren zu können. Da der Fahrer in allen drei Zuständen auf das Automobil verzichten muß, handelt es sich hierbei im Sinne der Funktion „Mobilität des Fahrers“ um verfügbarkeitskritische Zustände. Durch die Abschlepp- und Reparaturkosten wird der Aspekt der Wirtschaftlichkeit in das Zustandsraummodell integriert.
Nach Instandsetzung wird das fehlerfreie Fahrzeug an den Kunden zurückgegeben, womit auch das System D-b-W wieder im fehlerfreien Zustand 0 betrieben werden kann.

Weitere Anmerkungen zu den Zuständen und Zustandsübergängen aus Bild 5.6
Mit Ausnahme des Zustands 11 sind sämtliche Zustände der Markov-Kette des D-b-W-Systems rekurrent, was bedeutet, daß jeder Zustand in einer endlichen Zeit wiederholt eingenommen wird. Die skizzierten Zustandsübergangsmodule basieren auf den in Abschnitt 3.3.1 erläuterten Einbindungen von Fehlerbäumen in Markov-Ketten.
Vergleicht man obige Anzahl von Zuständen mit der Anzahl der in die Analyse einfließenden D-b-W-Komponenten, so sind deutlich die komplexitätsreduzierenden Effekte der hierarchischen Modellierung zu erkennen. Wie in Abschnitt 3.2. erläutert, wäre bei einer Anzahl von n Komponenten mit bis zu 2^n Zuständen zu rechnen. Es ist wichtig zu betonen, daß erst durch die in Abschnitt 5.2 vorgenommenen FTAs das Wissen um die Möglichkeiten der Modellreduzierung vorlag. Beispielsweise konnte auf die Einbindung des Zustands „Fehler innerhalb Reglermodul“ verzichtet werden, da die hierfür ursächlichen Sensor- und Transputerfehler bereits im Zustandsraummodell berücksichtigt sind. Genauso wurden Zusammenfassungen von Fehlererkennungs- und –behandlungsraten vorgenommen. Neben der Reduzierung der Zustandsraumkomplexität wird durch die resultierende Zunahme der Reaktionszeiten die Problematik der Steifigkeit von Markov-Ketten kompensiert.

Modellierung der Markov-Kette, Chapman-Kolmogorovgleichung
Auf eine Darstellung der Chapman-Kolmogorovgleichung soll mit Verweis auf Abschnitt 3.2.1.2 verzichtet werden. Ferner findet sich in Anhang H die für Bestimmung der Aufenthaltswahrscheinlichkeiten in den einzelnen Systemzuständen mittels des Tools MKV erstellten Markov-Ketten des Minimal-Systems.

Stationäre Lösung:

Aufgrund des absorbierenden Zustandes 11 ist für $t\rightarrow\infty$ die Aufenthaltswahrscheinlichkeit in diesem Zustand gleich 1. Diese Lösung ist jedoch nicht als „interessant“ zu bezeichnen. Aus Sicht des Automobil-Herstellers interessiert vielmehr die resultierende Aufenthaltswahrscheinlichkeit in Zustand 11 mit Erreichen der mittleren Betriebsdauer von 3000 Stunden (10 Jahren Nutzung).

$$\pi_{11}(t = 3000h) \approx F(t = 3000h) = 1 - e^{-q_{0,11} \cdot 3.000h} = 0{,}11167 \qquad \text{Gl. 5-1}$$

Damit befinden sich bei einer angenommenen Produktionsmenge von 1Mio. Fahrzeugen nach 3000 Stunden Nutzungsdauer 111670 Fahrzeuge im sicherheitskritischen Zustand. Diese Aussage impliziert die Unschärfe, daß ein verunfalltes Fahrzeug fortwährend im sicherheitskritischen Zustand verweilt, was nicht zwangsläufig der Fall ist.

Diskussion der F/V/S/W des Minimal-Systems D-b-W

Da das System, wie oben dargestellt bzw. in Anhang G erläutert, lediglich über einen wenig interessanten stationären Zustand ($\pi_{11}(t\rightarrow\infty)=1$) verfügt, erscheinen aus Sicht des Autors bereits die Aufenthaltswahrscheinlichkeiten in den einzelnen Systemzuständen zum Zeitpunkt t=300h als aussagekräftig für die System-Verfügbarkeit, -Sicherheit etc.

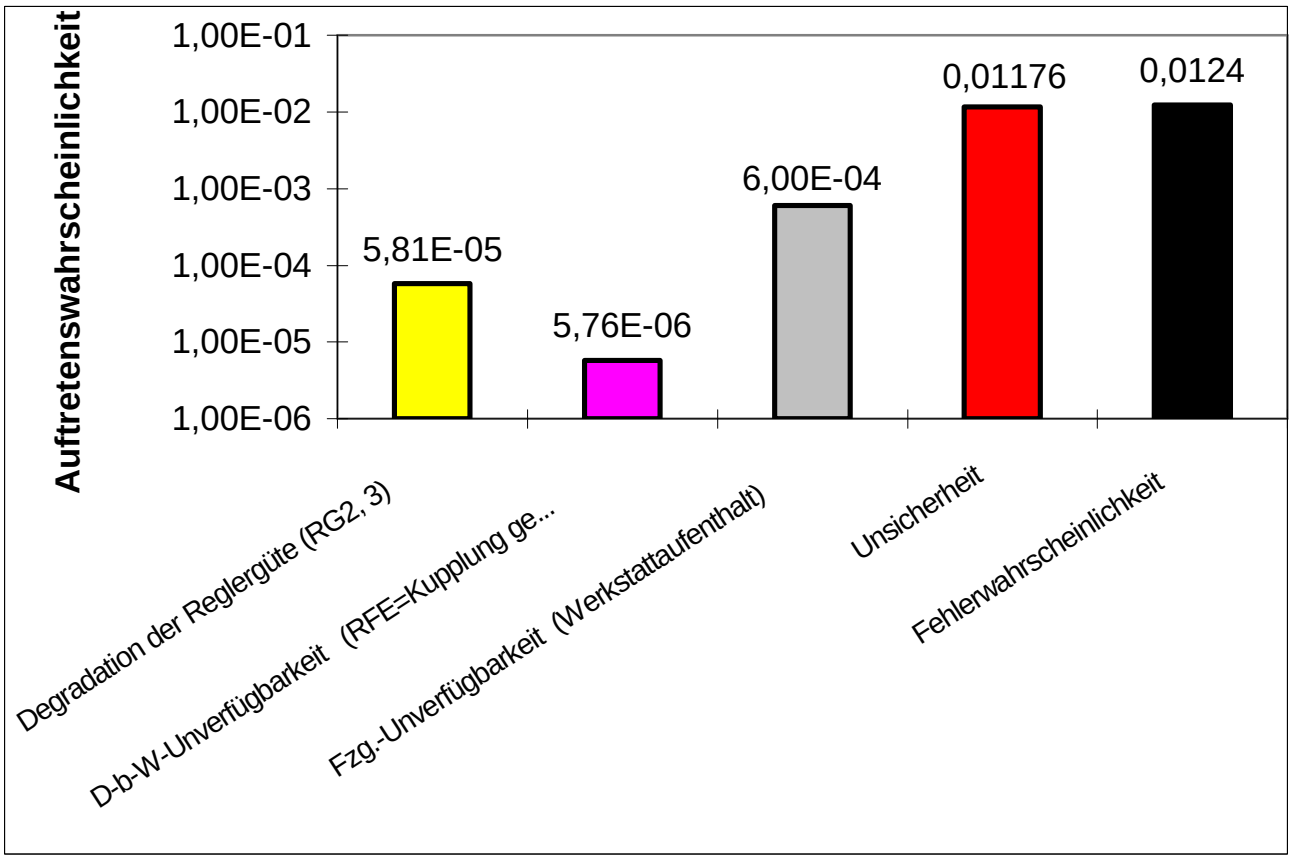


Bild 5.7: Fehlerwahrscheinlichkeit, Unverfügbarkeit und Unsicherheit des D-b-W-Minimal-Systems für t=300h

Die Fehlerwahrscheinlichkeit F(t=300h) = 0,0124 entspricht der Wahrscheinlichkeit, daß der Zustand 0 zum Zeitpunkt t=300h verlassen wird. Als Komplement entspricht die Aufenthaltswahrscheinlichkeit im Zustand 0 (0,98757) der Fehlerfreiheit des Systems zum Zeitpunkt t=300h. Ausgehend von 1 Mio. ein Jahr alter, mit D-b-W ausgestatteter Pkw würden 12.428 dieser Fahrzeuge einen Fehler aufweisen, der zum Verlassen des Zustands 0 führt.

Die Unverfügbarkeit bezieht sich hier auf die Unverfügbarkeit der elektronischen D-b-W-Funktionalität während des Fahrbetriebs. Hierbei befindet sich das Fahrzeug in der RFE, ist somit also sicher. Die Unverfügbarkeit bestimmt sich folglich aus der Summe der Aufenthaltswahrscheinlichkeiten in den Zuständen 2 und 9 (P(RFE(t=300h)) = 5,76E-6). Ausgehend von der Annahme, daß alle Fahrzeuge innerhalb des ersten Betriebsjahres eine Missionsdauer von 300 Stunden aufweisen, sind zu diesem Zeitpunkt 6 Fahrzeuge im Sinne obiger Definition nicht verfügbar.

Weiterhin interessieren den kommerziellen Autoverleiher, aber auch den Endkunden die Standzeiten der Fahrzeuge bzw. die Unverfügbarkeit des Fahrzeugs. Als wichtige Größe ist hierfür die Wahrscheinlichkeit für den Werkstattaufenthalt bzw. das „Nicht zur Verfügungstehen des Fahrzeugs“ zu benennen. Sie setzt sich aus den Aufenthalts-wahrscheinlichkeiten in den Zuständen 3, 7 und 10 zusammen und soll im weiteren

Verlauf der Arbeit als „Unverfügbarkeit des Fahrzeugs“ = P(Werkstatt) = 0,0006 bezeichnet werden. Ausgehend von der Annahme, daß alle Fahrzeuge innerhalb des ersten Betriebsjahres eine Missionsdauer von 300 Stunden aufweisen, sind zu diesem Zeitpunkt 600 Fahrzeuge im Sinne obiger Definition nicht verfügbar.

Die Unsicherheit, als aus Sicht des Autors für den Konzept-Entscheid wichtigste Kenngröße, bestimmt sich aus der Summe der Aufenthaltswahrscheinlichkeiten in den Zuständen 1, 4, 5, 8 und 11. In diesen Zuständen befindet sich das Fahrzeug im Einsatz und Fehler können entweder nicht erkannt werden (Zustand 11 = Fehlalarm = $(1\text{-}S_{11})$ = 0,0117635) bzw. noch nicht erkannt bzw. behandelt werden (Verbleibende Zustände = Mißalarm bzw. -behandlung = $(1\text{-}S_{\text{ohne Zustand 11}})$ = 5,81E-8). Diese Unterscheidung ist mit Blick auf die im folgenden Abschnitt bzw. Kap. 6 zu diskutierenden Verbesserungsvorschläge wichtig. Die sehr kleinen Mißalarm- bzw. –behandlungswahrscheinlichkeiten sind auf die kurzen Reaktionszeiten der FELB-SIS zurückzuführen. Im Vergleich hierzu ist die Wahrscheinlichkeit des Fehlalarms aufgrund des Unvermögens das ursächliche Fehlerphänomen zu erkennen ca. um den Faktor 200.000 größer.

Damit bot die Markov-Ketten-Analyse die Möglichkeit, nachzuweisen, daß das Hauptaugenmerk der Minimierung der Aufenthaltswahrscheinlichkeit im Zustand 11 (Top-Event C) liegt, und eine Reduzierung der Zykluszeiten, die in der Literatur häufig als Verbesserungsmaßnahme vorgeschlagen wird [siehe beispielsweise Wal86], nur untergeordneten Einfluß hat.

Hier sei bezugnehmend auf Abschnitt 3.2 nochmals betont, daß die Ursachen für die Fehlfunktionen in einer unzureichenden SIS bzw. in dem Folgefehler innerhalb des SIS-Transputers liegt. Wobei durch letztere Fehlfunktion das Voting bzw. eine Fehlerbehandlung ausgeschlossen wird. In Abschnitt 3.2 wurde weiterhin die Anzahl der Fahrzeuge bestimmt, die innerhalb des ersten Betriebsjahres in den bzw. die sicherheitsrelevanten Zustände eintreten. Hierfür wurde auf eine Näherung zurückgegriffen. Da das Hauptanliegen der Kap. 5 und 6 ist, eine vergleichende Analyse zwischen dem Minimal-System und dem erweiterten System vorzunehmen, kann auf diese Größe verzichtet werden.

Auch die Garantie- und Kulanz-Kosten sollen nicht für das gesamte Betriebsjahr, sondern mit Blick auf die vergleichende Analyse lediglich für den Zeitpunkt t = 300h ermittelt werden. Folglich bestimmen sie sich aus dem Produkt der Reparatur- und Abschleppkosten mit der Anzahl der in den entsprechenden Zuständen zum Zeitpunkt t =300 h befindlichen Fahrzeugen.

Anmerkung: Die HW-Kosten des auszutauschenden Elementes werden in der Berechnung nicht berücksichtigt. Grund hierfür ist der Umstand, daß in der aktuellen Entwicklungsphase des D-b-W-Systems die Serienkosten noch nicht vorliegen. Durch den Vergleich mit den anfallenden G/K-Kosten der erweiterten FELB aus Kap. 6 wird dieses Manko jedoch kompensiert. Die resultierende Differenz an G/K-Kosten kann für die Mehrkosten der erweiterten FELB-HW eingesetzt werden. Zwar bestünde auch das aus kaufmännischer Sicht berechtigte Interesse, die Materialkosten zwecks Gewinnmaximierung möglichst gering zu halten, jedoch soll bereits eine Reduzierung der Aufenthaltswahrscheinlichkeit in den sicherheitsrelevanten Zuständen als anzustrebendes Ziel ausreichen.

- G/K-Kosten Zustand 3 = π_3 * 1E6 Fzg. * Kosten für (Abschleppen und Reparatur) = 885.638 DM.
- G/K-Kosten Zustand 7 = π_7 * 1E6 Fzg. * Kosten für Reparatur = 174.447 DM
- G/K-Kosten Zustand 10 = π_{10} * 1E6 Fzg. * Kosten für Abschleppen und Reparatur = 62.235 DM.

Damit ergeben sich in der Summe G/K-Kosten 1 Mio. ein Jahr alter Fahrzeuge ausgestattet mit D-b-W und verursacht durch dessen Systemfehler von 1.122.320 DM.

Über diese G/K-Kosten hinaus besteht die Möglichkeit, im Sinne der pessimistischen Analyse davon auszugehen, daß alle Fahrzeuge, die einen nicht entdeckten Fehler aufweisen (Zustand 11), verunfallen. Würde man diese Fahrzeuge mit Kosten von 75.000 DM pro Fahrzeug kalkulieren, so würde dies zu folgenden weiteren Kosten führen:

- Fahrzeug-Kosten = π_{11} * 1E6 * 75.000 DM = 882.262.500 DM

Jedoch soll letztere Rechnung unbedingt als worst-case-Rechnung verstanden werden, da wie bereits erläutert, nicht entdeckte Fehler nicht zwangsläufig zu einer Verunfallung des Fahrzeugs führen. Auf die Thematik der Regreß- bzw. Schmerzensgelder und des Imageverlusts soll und kann hier mit Verweis auf Abschnitt 2.3 (Sicherheitsmaßstab) nicht weiter eingegangen werden.
Dennoch ist obigen Rechnungen zu entnehmen, daß die Senkung der Aufenthaltswahrscheinlichkeit im sicherheitsrelevanten Zustand indirekt zu einer erheblichen Senkung der „Feldkosten“ führen würde. Wobei hier wie bereits oben gesagt, auf den wirtschaftlich schwer bezifferbaren Einfluß des Image-Verlustes der Automobil-Marke nicht eingegangen werden soll.

Abschließend sollen die MKV-Ergebnisse mit den FTA-Ergebnissen aus Abschnitt 5.2 verglichen werden:

- In Abschnitt 5.2 wurden keine „heilenden“ Zuverlässigkeitskenngrößen verwandt. Wäre Zustand 5 absorbierender Natur, entspräche seine Aufenthaltswahrscheinlichkeit der Top-Event A-Häufigkeit. Umgekehrt würde die Berücksichtigung der Übergangsrate $q_{5,6}$ als Reparaturrate der Top-Event-A-Komponenten dazu führen, daß Top-Event A der in Bild 5.6 bestimmten Aufenthaltswahrscheinlichkeit in Zustand 5 entspräche. Jedoch würde die Fehlerbaumanalyse damit suggerieren, daß das System nach Auftreten der Fehlfunktionen bereits nach weniger als 200ms in den fehlerfrei Zustand zurückgeführt würde. Somit entstünde durch die Fehlerbaumanalyse und die hiermit bestimmte Auftrittswahrscheinlichkeit des Top-Events der Eindruck, daß alle betroffenen Fahrer trotz gelber Warnlampe das Fahrzeug unverändert weiterbenutzen würden bzw. die Degradierung auf RG 2 oder 3 zwar erforderlich sei, aber nicht vorgenommen wird. Die Überführung in einen „degraded-mode“ Zustand ist somit mittels der statischen FTA nicht modellierbar. Sie erlaubt lediglich, daß Systemverhalten in einem Betriebszustand zu analysieren. Demzufolge weist Zustand 5 gegenüber der in Abschnitt 5.2 bestimmten Top-Event A-Häufigkeit nach 300 Stunden Missionsdauer eine um nahezu Faktor 6.4 Mio. niedrigere Aufenthaltswahrscheinlichkeit auf. Dennoch erwies sich die FTA als äußerst hilfreich, um eine der Zustandsraumexplosion entgegenwirkende geschickte Modularisierung der D-b-W-Komponentenfehler vornehmen zu können.
- Top-Event B sollte sich in den Zuständen 1 und 8 widerspiegeln. Jedoch ist auch hier die deutlich größere Top-Event B-Wahrscheinlichkeit auf die oben beschriebenen Defizite der FTA zurückzuführen.
- Mit Top-Event C gibt die FTA uneingeschränkt die Aufenthaltswahrscheinlichkeit in Zustand 11 wieder. Der Umstand, daß die Top-Event-C-Häufigkeit relativ um 1,4% von der Aufenthaltswahrscheinlichkeit abweicht, ist ebenso auf obige Rechengenauigkeiten zurückzuführen.

5.4 Zusammenfassung des Kapitels 5

5.4.1 Abschlußbemerkungen zur F/V/S/W-Modellierung

Im vorliegenden Kapitel wurden die Vorzüge und Defizite der FTA, MKA bzw. hierarchischen Modellierung anhand der Systemanalyse des D-b-W-Minimal-Systems veranschaulicht. Zwar erweist sich die Modellierung des Systemverhaltens im Zustandsraum als aufwendiger als die Erstellung eines Fehlerbaumes, jedoch sind insbesondere komplexe dynamische Systeme, die über degraded-modes verfügen, erst durch die Zustandsraummodellierung analysierbar. Ein weiterer Vorzug der hierarchischen Modellierung liegt in der Möglichkeit, eine geschlossene Analyse der drei Qualitätsparameter F/V/S sowie der Wirtschaftlichkeit vorzunehmen.
Weiterhin war es ein Anliegen dieses Kapitels, zu verdeutlichen, daß erst unter Ausnutzung der Erkenntnisse der FTA aus Abschnitt 5.2 die komplexe Zustandsraumdarstellung in ein vertretbar kleines hierarchisches Modell überführt werden konnte.
So liessen sich beispielsweise fast sämtliche nicht entdeckbaren und damit sicherheitsrelevanten Fehler in einem Zustand „Top-Event C“ zusammenfassen. Über die Zustände „Gelbe Warnlampe“ und „Rote Warnlampe“ ließen sich entsprechend nahezu alle zu den Top-Events A und B beitragenden Fehler bündeln. Obige, dem Begriff der hierarchischen Modellierung zuzuordnenden „Clusterungen“, führen zu einer immensen Reduzierung der Zustandsraumkomplexität. Wie bereits in Abschnitt 5.2.4 erwähnt, wurde somit erst durch die FTA eine vertretbare MKA ermöglicht.
Eine weitere Möglichkeit die Modellierungskomplexität der MKA zu reduzieren, besteht in der Beschränkung des Zustandsraummodells (siehe hierarchischen Modellierung). Denn neben der Möglichkeit, die FTA zur Bestimmung der Zustandsübergänge der MKA zu nutzen, kann auch die MKA zur Bestimmung der Fehlerraten der FTA genutzt werden. Diese Strategie macht insbesondere dann Sinn, wenn das zu analysierende System wenig vernetzt, aber vielkomponentig ist. Wenn andererseits in gewissen Teilbereichen des Systems interessante Abhängigkeiten bestehen, die den Einsatz der MKA erfordern oder lohnenswert machen, können für diese Teilbereiche MKAs durchgeführt werden und dann in die weniger komplexen FTAs eingebaut werden.
Da es sich bei dem zu analysierenden System jedoch um ein nicht zu aufwendiges handelte und die oben beschriebene Einbindung der FTA in die MKA bereits zu einer erheblichen Reduzierung der Zustandsraumkomplexität führte, wurde diese Strategie hier nicht angewendet.

Damit läßt sich also zusammenfassen, daß die Analyse-Reihenfolge

1. „veränderte“ FMEA als Grundlage für die FTA und die hierarchische Modellierung
2. die FTA zwecks Modulbildung für die hierarchische Modellierung
3. und zuletzt die auf der MKA basierende hierarchische Modellierung

eine Bestimmung sämtlicher relevanter Qualitätsparameter eines komplexen Systems mit vertretbarem Aufwand ermöglicht.

Neben der Fusion beider Analysemethoden in Form hierarchischer Modelle, liefern FTA und MKA auch einander ergänzende Informationen über die Qualitätsparameter des zu analysierenden Systems. So beantwortet die FTA die Frage: „wieviele Fahrzeuge innerhalb des betrachteten Betriebszeitraumes in einen betreffenden Zustand eintreten, wohingegen die MKA die Frage beantwortet, wieviele Fahrzeuge sich zum betreffenden Zeitpunkt (Ende des Betriebszeitraumes) in diesem Zustand befinden.

5.4.2 Abschlußbemerkungen zur F/V/S/W des D-b-W-Minimal-Systems, Verbesserungsvorschläge

Es ist zu betonen, daß die vorliegenden F/V/S/W-Ergebnisse maßgeblich durch die Wahl der verwendeten, in Bild 3.8 skizzierten, Zuverlässigkeitskenngrößen bestimmt sind. Oftmals sind jedoch die Zuverlässigkeitskenngrößen mit einer derart großen Unsicherheit behaftet (siehe Abschnitt 3.1.2.3.5), daß die oben diskutierten Näherungsfehler bei der Bestimmung der Garantie- und Kulanz-Kosten als vernachlässigbar anzusehen sind.
Wie sich in den Abschnitten 5.2 und 5.3 zeigte, kann die Sicherheit des Systems D-b-W erhöht werden, indem die „unerkennbaren" Komponentenfehler bzw. deren Auftretenswahrscheinlichkeit reduziert wird.
So ergab die Pareto-Analyse aus Abschnitt 5.2, daß die sicherheitsrelevante Top-Event C Häufigkeit bzw. Aufenthaltswahrscheinlichkeit in Zustand 11 durch die Softfailures der Raddrehzahl- und Beschleunigungssensorik dominiert wird. Da die Einführung von FELB-Strategien zur Erkennung, Lokalisation und Behandlung von Softfailures innerhalb dieser Sensorik zu einer Senkung der Auftretungshäufigkeit des Top-Event C um 70% führen würde, sollte die Installation einer entsprechenden FELB dringend empfohlen werden.
Um die Einflüsse einer Soft-FELB der Raddrehzahl- und Beschleunigungssensorik auf alle drei Qualitätsparameter analysieren zu können, soll das in Abschnitt 5.3 abgeleitete hierarchische Modell mit dem in Kap. 6 für das erweiterte FELB zu entwickelnden Modell verglichen werden.

Verbesserungsvorschläge:

- Maßnahmen zur Senkung der Fehlerwahrscheinlichkeit des Gesamtsystems
  - Senkung der Ausfallraten der Systemkomponenten durch Einsatz qualitativ hochwertigerer Bauelemente. Da diese Strategie sowohl ihre technologischen wie auch wirtschaftlichen Grenzen hat, ist sie nicht beliebig anwendbar. Durch eine Pareto-Analyse lassen sich jedoch unzuverlässige Bauteile identifizieren, deren „Veredelung" einen maximalen Effekt auf die Senkung der Fehlerwahrscheinlichkeit des Systems verspricht.
  - Mit Blick auf den Umstand, daß das hier analysierte D-b-W-Konzept bereits das Minimal-System darstellt, sollte die Strategie einer Senkung der Gesamtfehlerwahrscheinlichkeit durch Reduzierung der Systemkomponenten hier nicht verfolgt werden (siehe negative Auswirkungen auf die Systemsicherheit).
- Maßnahmen zur Steigerung der Systemsicherheit (Wechselwirkungen auf die übrigen Qualitätsparameter)
  - Wie bereits in Abschnitt 5.2.3 erläutert, impliziert die Minimal-HW ein hohes Maß an nicht erkennbaren und somit nicht behandelbaren Sensorfehlern. Mit Blick auf die noch ausstehenden Robustheitsuntersuchungen und die Sicherheitskritikalität des Systems wird davon ausgegangen, daß alle nicht erkennbaren Fehler sicherheitskritische Auswirkungen auf den D-b-W-Regler und somit das Fahrzeug haben können. Damit stellt die Senkung der nicht erkennbaren Sensorfehler (Top-Event C bzw. Zustand 11 aus Abschnitt 5.3) eine sinnvolle Strategie zur Erhöhung der Systemsicherheit dar. Ebenso lassen sich hierdurch die Garantiekosten maßgeblich senken (siehe Tabelle 5.3). In Kap. 6 werden FELB-Strategien zur Erkennung von Softfailures innerhalb der Raddrehzahl- und Beschleunigungssensorik diskutiert und die Auswirkungen dieser Maßnahmen auf die übrigen drei Qualitätsparameter untersucht.
    Natürlich stellt auch die Robustheit gegen die nicht erkennbaren Fehler eine Möglichkeit dar. Da aber dieser Nachweis derzeit nicht vorliegt, soll diese Maßnahme hier nicht berücksichtigt werden.

    - Eine weitere Möglichkeit zur Erhöhung der Systemsicherheit liegt in der Senkung der Fehlererkennungs- bzw. -lokalisations- und –behandlungszeiten. Hierdurch können die in Abschnitt 5.3 beschriebenen sicherheitskritischen Zwischenzustände 1, 4, 5 und 8 schneller verlassen werden und das System in sichere Zustände überführt werden. Allerdings müßte diese Maßnahme entweder durch eine schnellere Rechner-HW oder verbesserte bzw. mitunter komplexere Algorithmen erzwungen werden, wobei auch letztere Strategie ein Mehr an Rechenleistung impliziert. Damit wirken sich beide Maßnahmen negativ auf die Produktkosten aus. Mit Blick auf den Umstand, daß mit zunehmendem Reifegrad die Rechner-HW eher kleiner und somit weniger leistungsfähig sein wird und in Abschnitt 5.3 gezeigt wurde, daß eine Verkürzung der Fehlererkennungszeit nur eine untergeordnete Rolle spielt, erscheint die Strategie der Senkung der Fehlererkennungsraten nicht praktikabel.

- Maßnahmen zur Steigerung der Systemverfügbarkeit (Wechselwirkungen auf die übrigen Qualitätsparameter):
    - Die Systemverfügbarkeit läßt sich weitestgehend durch die Maßnahmen zur Senkung der Gesamtfehlerwahrscheinlichkeit bzw. Steigerung der Systemsicherheit erhöhen.
    - Darüberhinaus wirkt sich die Erhöhung des Redundanzgrades positiv auf die Systemverfügbarkeit aus.
    - Ebenso kann durch Verkürzung der Instandsetzungszeiten die Systemverfügbarkeit erhöht werden.

- Maßnahmen zur Senkung der Kosten (Wechselwirkungen mit den Qualitätsparametern)
    - In den letzten Jahren wurde im deutschen Automobilbau, aufgrund des zunehmenden Wettbewerbsdruckes, verstärkt nach Wegen zur Senkung der Entwicklungs-, Produktions- und Produktkosten gesucht. Leider zeigte sich in der jüngsten Vergangenheit, daß diese Einsparungen vor Markteinführung mit oftmals großen Imageverlusten beim Feldeinsatz verbunden waren. Aus Sicht des Autors sollte die Qualität des Produktes und somit die Kundenzufriedenheit im Vordergrund zukunftsweisender Entwicklungen, wie D-b-W, stehen. Aus diesem Grund sollen hier keine unmittelbaren Maßnahmen zur Senkung der Kosten diskutiert werden. Jedoch ermöglicht die Einführung analytischer bzw. funktionaler Redundanzkonzepte eine Einsparung an HW-Redundanzen. Wie sich in Kap. 6 zeigen wird, wirkt sich dies indirekt positiv auf die Produktkosten sowie G/K-Kosten aus.

Vergleicht man die Pareto-Diagramme Bild 5.1, Bild 5.3 und vor allem Bild 5.5, so wird deutlich, daß die kritischen Pfade des Minimal-Modells in Bezug auf die Fehlerwahrscheinlichkeit, Degradationswahrscheinlichkeit, Verfügbarkeit und vor allem die Sicherheit durch die Senkung der Fehlerhäufigkeit der Raddrehzahlsensorik herbeiführen läßt. Entsprechende Ansätze und deren Auswirkungen auf die F/V/S/W werden in Kap. 6 diskutiert.
Abschließend soll nochmals betont werden, daß die in Kap. 5 für das Minimal-System bestimmten Qualitätsparameter im weiteren als Qualitätsmaßstäbe betrachtet werden sollen. Die im folgenden Kapitel vorzustellenden FELB-Erweiterungen sollen dazu beitragen, daß das entsprechend optimierte D-b-W obige Qualitätsmaßstäbe übertrifft.

6 F/V/S/W-Analyse der erweiterten FELB

Wie sich in Kap. 5 zeigte, besteht hinsichtlich der Fehlererkennung, -lokalisation und –behandlung mit Blick auf das Bestreben, die Sicherheitsrelevanz des D-b-W-Konzeptes zu senken, das Ziel, die Raddrehzahlsensorik und Beschleunigungssensorik auf Softfailures überwachen zu können.
In [Mah94, Sti95, Ben97] wurden Überwachungsstrategien der Beschleunigungssensorik basierend auf Kalman-Filtern, -Bänken und funktionalen Redundanzen vorgestellt.
Um den Umfang dieser Arbeit nicht übergebührend zu strapazieren, sollen im weiteren Verlauf die in obigen Werken vorgestellten Maßnahmen zur Überwachung der dominanten Softfailures in den Raddrehzahlsensoren diskutiert werden. Hierbei handelt es sich um funktionale Redundanzkonzepte [Sti95, Mah95] bzw. ein robustes Kalman-Filter [Ben97]. Auf FELB-Konzepte, die auf Selbsttests basieren, wurde bewußt verzichtet, da dem Autor kein praxistaugliches Konzept zur Selbstüberwachung von Raddrehzahlsensoren bekannt ist.
Ziel des vorliegenden Kapitels ist es somit, den Benefit der FELB-Erweiterungen hinsichtlich F/V/S/W in Relation zum Minimal-System aus Kap. 5 zu bewerten.
Da in heutigen sicherheitsrelevanten Kfz-Applikationen vornehmlich HW-Redundanz eingesetzt wird, soll auch der hier zu verzeichnende F/V/S/W-Benefit einer zweikanaligen Raddrehzahlkonzeptes diskutiert werden. Genau mit diesem, den „Stand der Technik“ repräsentierenden, Redundanzkonzept soll die folgende Diskussion beginnen.

6.1 Erweiterung der FELB hinsichtlich der Raddrehzahlsensor-überwachung

6.1.1 Zweikanalige Raddrehzahlsensorik

Exemplarisch wurde im D-b-W-Testträger zur Verifikation der Raddrehzahlinformationen eine vollredundante Sensorik installiert. Diese Vollredundanz impliziert eine unabhängige Energieversorgung und analoge Übertragung der Sensorinformation zur D-b-W-Transputer-HW.

Sensorfehlererkennung
Die vollredundante Raddrehzahlsensorik ermöglicht eine Erkennung von Einfachfehlern innerhalb der beiden Sensor-Kanäle. Hierfür werden die beiden Sensorinformationen im SIS-Transputer durch einen softwarebasierten Voteralgorithmus, wie er in [Sti95, Mah95] realisiert wurde, verglichen. Um einen Fehlalarm zu vermeiden, führen erst Differenzen innerhalb beider Sensorsignale, die größer sind als 4m/s, d.h. 14,4 km/h, zum Inkrementieren des Fehlerzählers. Das Fehlererkennungsflag wird, wie in Abschnitt 4.2.3.1.2.1 erläutert, nach sechsmaligem Inkrementieren des Fehlerzählers gesetzt.
Damit können durch die zweikanalige Raddrehzahlsensorik auch in gewissem Umfang Softfailures erkannt werden. Inwieweit die D-b-W-Reglersoftware gegen die verbleibenden, nicht erkennbaren Softfailures robust ist, wäre zu untersuchen. Mit Blick auf die geringen Realisationschancen eines Serien-Systems mit vollredundanter Raddrehzahlsensorik wurde hierauf in der vorliegenden Arbeit verzichtet.
Im weiteren Verlauf der Arbeit wird vereinfachend davon ausgegangen, daß sämtliche sicherheitsrelevanten Softfailures durch das vorliegende Redundanzkonzept erkannt werden können.
Hardfailures werden, wie in Kap. 4 bzw. 5 bereits erläutert, nachwievor innerhalb des Hard-Failure-Erkennungsmoduls identifiziert.

Sensorfehlerlokalisation
Wie bereits in Abschnitt 2.4 erläutert, erlaubt eine zweikanalige Struktur nicht unmittelbar eine eindeutige Lokalisation beliebiger Einfachfehler. Um eine saubere Abgrenzung zu den in den folgenden Abschnitten vorzustellenden funktionalen bzw. analytischen Redundanzkonzepten zu gewährleisten, wird davon ausgegangen, daß die zweikanalige Raddrehzahlsensorik keine Fehlerlokalisation ermöglicht.

Sensorfehlerbehandlung
Im Anschluß an die Fehlererkennung innerhalb der Raddrehzahlsensorik der Vorderachse erfolgt die Degradation auf die mechanische Rückfallebene (siehe auch Zustand 2, RFE in Abschnitt 5.3), bei Fehlererkennung innerhalb Hinterachs-Sensorik auf Reglerstufe RG 2.

Fehlererkennungsrate
Mit Blick auf obige Zählerstrategie soll von einer Fehlererkennungsrate von 600 1/h ausgegangen werden, was der in Gl. 4-26 bestimmten Rate entspricht. Wie sich bereits in Kap. 5 zeigte, würde eine weitere Verkürzung der FELB-Reaktionszeiten nur unwesentlich zur Verbesserung der System-F/V/S beitragen.

Onboard Fehlerbehandlungsrate
In Analogie zum Minimal-System, sei auch hier von der Onboard-Fehlererkennungsrate von 360.000 1/h ausgegangen (siehe Gl. 4-28).

Werkstatterreichens- bzw. Offboard Fehlerbehandlungsrate
Bei Fehlern innerhalb der Hinterachsraddrehzahlsensorik muß der Fahrer durch Aktivierung der gelben Warnlampe über die Degradation auf RG2 informiert werden. Damit setzt sich die Fehlerbehandlungsrate aus den Gl. 4-29 und 4-32 zusammen. womit sich eine Fehlerbehandlungsrate von 1/9 1/h ergibt.
Bei Fehlern innerhalb der Vorderachsraddrehzahlsensorik erfolgt die Aktivierung der roten Warnlampe. Die Fehlerbehandlungsrate setzt sich somit aus den Gl. 4-30, 31 und 32 zusammen, womit sie ungefähr 1/7 1/h beträgt.

Mißalarm, -lokalisation und -behandlung
Ein Mißalarm kann, wie bereits angedeutet, aufgrund Softfailures auftreten, die unterhalb der Detektionsschwelle von 4m/s liegen. Zwecks Vereinfachung wird jedoch, wie bereits geschildert, davon ausgegangen, daß sämtliche relevanten Softfailures erkennbar sind. Bedingt durch den Umstand, daß wie schon innerhalb der Minimal-Sensorik, auch hier temporäre Fehler nicht erkannt werden können, wird obige Unschärfe kompensiert.
Weitere Ursachen für den Mißalarm sind Fehler innerhalb der SIS-HW. Mißlokalisation und -behandlung sind als Folgeerscheinung des Mißalarms möglich.

Fehler- bzw. Ausfallrate
Wie bereits in Kap. 5 diskutiert, können Mißalarm, -lokalisation und -behandlung in der vorliegenden Arbeit schwerpunktmäßig auf Sensorfehler bzw. Überwachungslücken innerhalb der SIS zurückgeführt werden. Damit reduziert sich die Fehlerrate auf die Sensorfehlerraten (siehe Kap. 4) bzw. Wahrscheinlichkeiten, die auf Fahrdynamik-szenarien basieren (siehe Abschnitt 5.2 und 6.1.2).

6.1.2 Funktionales Redundanzkonzept zur Überwachung der einkanaligen Raddrehzahlsensorik

In [Mah95] wurde für die Raddrehzahlsensorik des D-b-W-Testträgers eine SIS entwickelt, die auf funktionalen Redundanzen basiert.

Sensorfehlererkennung
Hierfür wurden die einkanaligen Sensorinformationen jedes Rades in den Fahrzeugschwerpunkt transformiert und somit ein 4v4-Voting zur Erkennung von Fehlern innerhalb der Sensoren generiert. Für die Transformation wurde neben zeitinvarianten Parametern der Fahrzeuggeometrie (Radstand und Spurbreite) der absolut sensierte Lenkradwinkel (Ackermannwinkel) in die Modellierung aufgenommen.
Diese äußerst simple Transformationsmodellierung ist nur zulässig, solange der Radschlupf gering bzw. an allen vier Rädern nahezu gleich ist. Damit versagt diese SIS bei µ-Split, übermäßigem Antriebs- oder Bremsschlupf. In heutigen ABS-Sicherheitssoftwaremodulen wird aus diesem Grund eine aufwendige Fallunterscheidung vorgenommen und die Fehlerdetektionsschwelle entsprechend angepaßt.
Zur Veranschaulichung der Problematik der an die Fahrdynamik gekoppelten Fehlererkennung wurde in [Mah95] bei Drosselklappenwinkeln größer 30° (erhöhter Antriebsschlupf an den Hinterrädern) bzw. Aktivierung des Bremslichtschalters (Bremsschlupf), die Überwachung der Raddrehzahlsensorik abgeschaltet. Auf eine Schätzung des Kraftschlußpotentials an den einzelnen Rädern wurde verzichtet.
Damit läßt sich zusammenfassen, daß die auf obiger simplen funktionalen Redundanz basierende Raddrehzahlsensorüberwachung eine fahrdynamik- und fahrbahn- bzw. witterungsabhängige Fehlererkennung zuläßt.
Mit Ausnahme obiger „Überwachungslücken“ können selbst nach Erkennung des ersten Fehlers innerhalb eines der Sensoren die verbleibenden Raddrehzahlsensoren weiterhin überwacht werden. Hierbei beschränkt sich die in [Mah95] entwickelte SIS auf die Erkennung des ersten und zweiten Sensorfehlers.
Im weiteren Verlauf dieses Kapitels werden bei der F/V/S/W-Analyse des funktionalen Redundanzkonzeptes die Überwachungslücken der Sensoren mitberücksichtigt. Ebenso werden Fehler der Lenkradwinkelsensorik, des Bremslichtschalters bzw. des Drosselklappenpotentiometers, die zu einem Versagen der SIS führen, in der F/V/S/W-Analyse mitmodelliert. Idealisiert wird davon ausgegangen, daß sämtliche Räder über das gleiche Haftreibpotential verfügen.
Wie Testfahrten ergaben, können mit obiger SIS Sensorfehler größer 5m/s (18km/h) erkannt werden. Damit liegt diese Sensitivität im Bereich der Softfailure-Erkennung aus Abschnitt 6.1.1. Hinsichtlich der Fehlerzählerstrategie etc. sei ebenfalls auf Abschnitt 6.1.1 verwiesen.

Um in den Abschnitten 6.2-6.5 wahrscheinlichkeitstheoretische Aussagen zur Erkennung von Softfailures mittels des funktionalen Redundanzkonzeptes vornehmen zu können, sollen an dieser Stelle die Bedingungen für das „Nicht-Erkennen“ eines Fehlers, d.h. das Auftreten von Überwachungslücken mathematisch aufgearbeitet werden:

Wie bereits geschildert, funktioniert die Softfailure-Überwachung (Einfach- bzw. Zweifachfehler) der Raddrehzahlsensorik nicht, wenn entweder:

A) der absolute LRW-Sensor nicht korrekt funktioniert,
B) das Drosselklappenpotentiometer nicht korrekt funktioniert,
C) der sensierte Drosselklappenwinkel größer 30° ist,
D) der Bremslichtschalter nicht korrekt funktioniert
E) oder das BLS-Signal einen Fahrerbremswunsch anzeigt.

In Analogie zum Gierratensensor (siehe Anhang E) soll nunmehr für die Bedingungen C) und E) ein gemeinsames Übersetzungsverhältnis formuliert werden:

Zu C: Die Wahrscheinlichkeit für einen Drosselklappenwinkel größer 30° während des Fahrens wird für ein Automatikgetriebe, wie es im W140-Testträger serienmäßig ist, mit 30% angenommen.

Zu E: Die Wahrscheinlichkeit für die Aktivierung der BLS bestimmt sich gemäß Abschnitt 2.2 und des Umstandes, daß jede der während der durchschnittlichen Lebensdauer von 10 Jahren getätigten 250.000 Bremsungen im Mittel 2 Sekunden andauert, zu:

$$p_{BLS-Aktiv}(\text{innerhalb } t = 3000h) = \frac{250.000 \cdot 2s}{3.000h \cdot 3.600\,{}^{s}\!/_{h}} = 0{,}0463 \qquad \text{Gl. 6-1}$$

Analog zum Fehlermoden-Faktor α (Gl. 3-13), kann Gl. 6.1 kann als über der gesamten Missionsdauer des Fzgs. zeitinvariantes Übersetzungsverhältnis für nicht erkennbare Softfailure-Anteile der Raddrehzahlsensorik genutzt werden. Gleiches gilt für die Drosselklappe. Da eine gleichzeitige übermäßige Motor- bzw. Drosselklappenaktivität und Bremsenaktivität in aller Regel vom Fahrer unerwünscht ist bzw. fahrdynamisch nicht sinnvoll ist, schließen sich obige Wahrscheinlichkeiten aus. Somit sind beide Wahrscheinlichkeiten für die Gewinnung des Gesamt-Übersetzungsverhältnisses zu addieren. Folglich sind bereits allein aufgrund von Fahrdynamikmanövern 34,63% der auftretenden Raddrehzahl-Einfach- bzw. Zweifach-Softfailures nicht erkennbar.
Hieraus ergibt sich in Analogie zum Gierratensensor (Anhang E):

1. Eine auf Einfach- bzw. Zweifachfehler überwachbare Softfailure-Rate der Raddrehzahlsensoren.

$$\begin{aligned} &\lambda_{SF-Rd.Sensor-überwachbar} \\ &= \text{Softfailureanteil}(\lambda_{Rd-Zahl}) \cdot \left(1 - \left(p_{BLS-Aktiv} + p_{DR>30^0}\right)\right) \\ &= 0{,}453 \cdot \lambda_{Rd-Zahl} \cdot (1 - 0{,}3463) = \lambda_{Rd-Zahl} \cdot 0{,}296 \end{aligned} \qquad \text{Gl. 6-2}$$

Anmerkung:
Obige Faktoren resultieren aus Tabelle 4.5 (Softfailure-Häufigkeitsverteilung) bzw. dem Komplement der „Nicht-Überwachbaren“ Rd.-Sensorfehler.

2. Eine auf Einfach- bzw. Zweifachfehler <u>nicht</u> überwachbare Softfailure-Rate der Raddrehzahlsensoren.

$$\lambda_{SF-Rd.Sensor-nicht\,überwachbar} = Softfailureanteil(\lambda_{Rd-Zahl}) \cdot \left(P_{BLS-Aktiv} + P_{DR>30^0}\right) = 0{,}453 \cdot \lambda_{Rd-Zahl} \cdot 0{,}346 = \lambda_{Rd-Zahl} \cdot 0{,}157$$

Gl. 6-3

Zu dem in Gl. 6.3 bestimmten, „nicht überwachbaren“ Softfailure-Anteil kommen weiterhin die Wahrscheinlichkeiten für das Versagen des absoluten LRW-Sensors, des Drosselklappenpotentiometers und des Bremslichtschalters. Diese Fehlerereignisse schließen sich jedoch nicht gegenseitig aus und sollen als stochastisch unabhängig von Fahrmanövern, Witterungsverhältnissen etc. angesehen werden. Somit können die entsprechenden Fehlerraten obiger Sensoren (siehe Abschnitt 4.2.1) innerhalb der in Abschnitt 6.2 folgenden Fehlerbaumanalysen mit den Raddrehzahlsensorraten entsprechend „verodert“ werden.

Sensorfehlerlokalisation
Im Gegensatz zur HW-Redundanz aus Abschnitt 6.1.1 erlaubt die funktionale Redundanz eine Lokalisation von Einfach- und Zweifachfehlern innerhalb der Raddrehzahlsensorik. Wie bereits bei der Fehlererkennung, ist auch hier zwingende Voraussetzung, daß die in die Modellierung einfließenden übrigen Fahrdynamiksensoren korrekt funktionieren und der bzw. die Raddrehzahlsensorfehler nicht mit Überwachungslücken zusammenfallen.

Sensorfehlerbehandlung
Streng genommen könnte bereits nach der Fehlererkennung ein Ausblenden der D-b-W-Eingriffe in die Lenkung erfolgen. Es wird jedoch vereinfachend davon ausgegangen, daß erst nach der Fehlerlokalisation eine Degradation innerhalb der D-b-W-Struktur vorgenommen wird. Im Anschluß an die Lokalisation eines Einfachfehlers erfolgt eine Degradation auf RG2. Ein zweiter Fehler führt aus Sicherheitsgründen unmittelbar zum Abschalten des D-b-W in die RFE.

Fehlererkennungsrate
Strenggenommen hängt die Erkennungsrate von der Charakteristik des Sensorfehlers und der Art der Fehlererkennungsstrategie (Schwellwerthöhe, Zählerstrategie etc.) ab. Diese der Entscheidungstheorie zuordenbare Thematik wird ausführlich in [Wal89] diskutiert, soll aber nicht Bestand der vorliegenden Arbeit sein. Vereinfachend wird mit Blick auf die in Abschnitt 4.2.3.1.2.1 beschriebene Zählerstrategie ebenfalls von einer mittleren Fehlererkennungsrate gemäß Gl. 4-26 von 600 1/h ausgegangen.

Fehlerlokalisationsrate
Wie bei der Fehlererkennungsrate wird auch hier eine mittlere Fehlerlokalisationsrate von 600 1/h verwandt.

Onboard Fehlerbehandlungsrate
In Analogie zum Minimal-System, sei auch hier von der Onboard-Fehlererkennungsrate von 360.000 1/h ausgegangen (siehe Gl. 4-28).

Werkstatterreichens- bzw. Offboard Fehlerbehandlungsrate
Bei Einfachfehler muß der Fahrer durch Aktivierung der gelben Warnlampe über die Degradation auf RG2 informiert werden. Damit setzt sich die „Offboard Fehlerbehandlungsrate“ aus den Gl. 4-29 und 4-32 zusammen, womit sich eine Offboard-Fehlerbehandlungsrate von 1/9 1/h ergibt. Dem zweiten erkannten Fehler folgt die Aktivierung der roten Warnlampe. Die entsprechende Übergangsrate setzt sich somit aus den Gl. 4-30, 31 und 32 zusammen, womit sie ungefähr 1/7 1/h beträgt.

Mißalarm, -lokalisation und -behandlung
Ein Mißalarm bzw. die -lokalisation kann wie bereits angedeutet, aufgrund Softfailures auftreten, die unterhalb der Detektionsschwelle von 5m/s liegen. Wie schon in Abschnitt 6.1.1, wird auch hier davon ausgegangen, daß die sicherheitsrelevanten Fehler unter der Voraussetzung, daß sie nicht durch eine Überwachungslücke tangiert sind, erkannt werden. Weitere Ursachen für den Mißalarm sind im Bereich Sensorfehlererkennung bzw. Abschnitt 6.1.1 beschrieben.
Mißbehandlung ist infolge der Mißlokalisation möglich.

Fehler- bzw. Ausfallrate
Wie bereits in Kap. 5 diskutiert, können Mißalarm, -lokalisation und -behandlung in der vorliegenden Arbeit schwerpunktmäßig auf Sensorfehler bzw. Überwachungslücken innerhalb der SIS zurückgeführt werden. Als weitere Ursache sind obige Wahrscheinlichkeiten für das Vorliegen einer Überwachungslücke, bei gleichzeitigem Vorhandensein eines zu detektierenden Sensorfehlers, zu nennen. Auswirkungen der erhöhten Softwarekomplexität der SIS sollen mit Verweis auf den Umstand, daß Softwarefehler in dieser Arbeit nicht quantitativ mitmodelliert werden, vernachlässigt werden.

6.1.3 Analytisches Redundanzkonzept zur Überwachung der einkanaligen Raddrehzahlsensorik

In [Mah94] und [Ben97] wurden auf Kalman-Filtern basierende und somit analytische Redundanzkonzepte zur Überwachung der D-b-W-Sensorik entwickelt. Mit Blick auf die Pareto-Analyse des sicherheitsrelevanten Top-Events C aus Abschnitt 5.2 soll nunmehr die in [Ben97] entwickelte robuste analytische Redundanz zur Überwachung der Raddrehzahlen skizziert werden.
Die „Robustheit“ dieser Redundanz bezieht sich auf den Umstand, daß eine minimale Sensibilität gegenüber unbekannten Eingangsgrößen und maximale Sensibilität gegenüber den zu detektierenden Sensorfehlern angestrebt wurde.

Struktur der analytischen Redundanz
In [Ben97] konnte ein „vereinfachendes“ lineares Fahrzeugmodell für die Entwicklung des Kalman-Filters verwendet werden. In Analogie zur Darstellung des Schwimmwinkelschätzers in Abschnitt 4.2.3.1.1, soll auch hier nur die Struktur des FELB-Schätzers dargestellt werden. Hierbei beschränkt sich die Darstellung auf den Zustands- und Meßvektor sowie die Aufführung der übrigen in den Schätzer einfließenden Informationen.

Systemmodell: Zustandsvektor

$$\underline{x} = \begin{pmatrix} \omega_{Rad-Vl} \\ \omega_{Rad-VR} \\ \omega_{Rad-HR} \\ \omega_{Rad-Hl} \\ v_x \\ \theta_{Straße} \\ dM_{Rad-VL} \\ dM_{Rad-VR} \\ dM_{Rad-HR} \\ dM_{Rad-HL} \end{pmatrix} \qquad \text{Gl. 6-4}$$

In Gl. 6.4 entspricht

- $\theta_{Straße}$ der Straßenlängsneigung,
- dM der an jedem Rad wirkenden Differenz aus Antriebs- und Bremsmoment.

  Beide Größen wurden als Zustandserweiterungen ohne eigene Dynamik in den Zustandsvektor aufgenommen. Durch diese Zustandserweiterungen können Modellierungsfehler in gewissem Umfang kompensiert werden, was der Robustheit dieses FELB-Filters zuträglich ist.

Weitere in das Systemmodell einfließende Informationen:

- Gegenüber der Prädiktion zeitlich unmittelbar vorhergehende Filterschätzwerte der Längs- und Quergeschwindigkeit, entnommen aus dem SWS.
- Sensierte Gierrate
- Sensierter absoluter Lenkradwinkel
- Sensierte Längsbeschleunigung
- M_A (aus Kennfeld, siehe auch Drosselklappenwinkel, Gang etc.) und M_B (aus Bremsdrucksensor (Abschnitt 4.2.1.5) und näherungsweise konstanter Bremskraftverteilung an den Achsen.).
- Trägheitsmoment, Reifenradius, Längssteifigkeit der Räder
- Näherungen/Vereinfachungen:
  - Konstanter Haftreibwert
  - Fzg.-Schwerpunkt auf Fahrbahnhöhe (kein Fahrzeugnicken und -wanken, keine Achs- und Radlastveränderungen
  - Vernachlässigung der Seitenkräfte und des Querschlupfes

Meßvektor des Beobachtungsmodells

$$\underline{y} = \begin{pmatrix} \omega_{RD-Sensor-VL} \\ \omega_{RD-Sensor-VR} \\ \omega_{RD-Sensor-HR} \\ \omega_{RD-Sensor-HL} \\ ax_{sensoriell} \end{pmatrix} \qquad \text{Gl. 6-5}$$

In die Beobachtungsmatrix einfließende Informationen

- Gegenüber der Prädiktion zeitlich unmittelbar vorhergehende Filterschätzwerte der Längsgeschwindigkeit, entnommen aus dem SWS.
- Sensierter absoluter Lenkradwinkel
- Reifenradius, Fahrzeugmasse, Längssteifigkeit der Räder
- Näherungen/Vereinfachungen: siehe Systemmodell.

Aus obigen Darstellungen wird deutlich, daß die hier skizzierte analytische Redundanz einen deutlich höheren Modellierungsaufwand aufweist, als die funktionale oder gar HW-Redundanz. Die Beobachtbarkeitsanalyse in [Ben97] ergab, daß das System trotz der getätigten Näherungen und Zustandserweiterungen vollständig beobachtbar ist, also alle Zustandsgrößen geschätzt werden können.
Dennoch können sämtliche in das Kalman-Filter einfließenden fehlerhaften Informationen, siehe insbesondere die Verwendungen von Schätzwerten des SWS, der in Kap. 5 bereits als wenig zuverlässig identifiziert wurde, ursächlich für das Auftreten eines Schätzfehlers sein. Damit ist Abschnitt 6.2 bereits vorwegzunehmen, daß die Verfügbarkeit einer derart komplexen analytischen Redundanz nicht sehr hoch ist.

Sensorfehlererkennung
Aufgabe obiger Filterstruktur ist es, Fehler innerhalb der Raddrehzahlsensorik zuverlässig erkennen und lokalisieren zu können. Die Detektion und Lokalisation eines Sensorfehlers erfolgt über die Auswertung der erzeugten Residuen (Differenz aus Meß- und Zustandsgröße). In [Ben97] wurde zur Erhöhung der Robustheit dieser FELB-Struktur eine spezielle Verstärkung dieses Residuums entwickelt, die es ermöglicht, Einfachfehler innerhalb der Raddrehzahlsensorik zu erkennen und zu lokalisieren, die kleiner 1m/s sind. Mehrfachfehler können nicht zuverlässig erkannt werden, da nach dem ersten Fehler innerhalb der Raddrehzahlsensorik der für die Schätzung der Längs- und Quergeschwindigkeit verwendete Schwimmwinkelschätzer fehlerhafte Werte liefert. Demzufolge ist nach Erkennung auf Sensorfehler D-b-W in die RFE zu überführen.
Hinsichtlich der Fehlerzählerstrategie etc. sei auf Abschnitt 6.1.1 verwiesen.

Sensorfehlerlokalisation
Die analytische Redundanz erlaubt eine Lokalisation von Einfachfehlern innerhalb der Raddrehzahlsensorik. Im Gegensatz zur funktionalen Redundanz ergaben die Untersuchungen in [Ben97], daß durch Wahl einer adaptiven Schwellwertstrategie Sensorfehler über den gesamten Fahrdynamikbereich zuverlässig erkannt und lokalisiert werden können. Allerdings zeigte sich auch, daß im Mittel für Erkennung und Lokalisation von Softfailures Zeiten bis zu 1 Sekunde verstreichen können.
Im weiteren Verlauf der Untersuchungen wird deshalb von einer zusammengefaßten „FEL“-Zeit, d.h. **F**ehler**e**rkennungs- und –**l**okalisationszeit, von 1 Sekunde ausgegangen.
Genau wie bei der funktionalen Redundanz wird auch hier vereinfachend davon ausgegangen, daß erst mit der Fehlerbehandlung eine Degradation innerhalb der D-b-W-Struktur vorgenommen wird. Demnach ist erst mit der Fehlerbehandlung die Sicherheitsrelevanz des Sensorfehlers hinsichtlich der Fahrdynamik eliminiert.

Sensorfehlerbehandlung
Im Anschluß an die Lokalisation eines Einfachfehlers erfolgt aus Sicherheitsgründen unmittelbar eine Abschaltung des D-b-Ws in die RFE.

Fehlererkennungsrate
Siehe auch Kommentare aus Abschnitt 6.1.2 bzw. Fehlerlokalisationsrate.

Fehlerlokalisationsrate
Wie oben beschrieben, wird mit der zusammengefaßten Fehlererkennungs- und -lokalisationsrate gerechnet:

$$FEL - R. = 3.600\ {}^{1}\!/\!_{h} \qquad \text{Gl. 6-6}$$

Onboard Fehlerbehandlungsrate
In Analogie zum Minimal-System sei auch hier von der Onboard-Fehlerbehandlungsrate von 360.000 1/h ausgegangen (siehe Gl. 4-28).

Werkstatterreichens- bzw. Offboard Fehlerbehandlungsrate
Bei Einfachfehlern muß der Fahrer durch Aktivierung der roten Warnlampe über die Degradation auf RFE informiert werden. Die Fehlerbehandlungsrate setzt sich somit aus den Gl. 4-30, 31 und 32 zusammen, womit sie näherungsweise 1/7 1/h beträgt.

Mißalarm, -lokalisation und -behandlung
Mit Verweis auf die Struktur der analytischen Redundanz, sind „Überwachungslücken“ aufgrund von fehlerhaft in das Filter einfließenden Informationen zu berücksichtigen.
Vereinfachend wird hier davon ausgegangen, daß jede beliebig fehlerhafte sensorielle Information zum Versagen der FELB führt. Durch diese pessimistische Annahme soll die Vereinfachung kompensiert werden, daß beispielsweise Modellierungsfehler verursacht durch fehlerhaft geschätztes Kraftschlußpotential, im weiteren vernachlässigt werden.
Inwieweit das Versagen der FELB erkannt werden kann, hängt davon ab, ob die entsprechend ursächliche fehlerhafte Information überwachbar war.

Fehler- bzw. Ausfallrate
Wie bereits in Kap. 5 diskutiert, können Mißalarm, -lokalisation und -behandlung in der vorliegenden Arbeit schwerpunktmäßig auf Sensorfehler zurückgeführt werden. Auswirkungen der erhöhten Softwarekomplexität der SIS sollen mit Verweis auf den Umstand, daß Softwarefehler in dieser Arbeit nicht quantitativ mitmodelliert werden, vernachlässigt werden.
Abschließend ist jedoch kritisch anzumerken, daß vor Serieneinsatzes eines analytischen Redundanzkonzeptes seine Stabilität nachzuweisen ist, was aufgrund des hier verwendeten nichtlinearen Beobachtungsmodells zum „Killer-Kriterium“ werden kann.

6.2 Auswirkungen der Fehlermöglichkeiten der jeweiligen FELB-Erweiterung

An dieser Stelle sollen nunmehr die wesentlichen, aufgrund der FELB-Erweiterungen verursachten Veränderungen hinsichtlich der Fehlermöglichkeiten des D-b-W-Systems zusammengefaßt werden. Die Darstellung aller Veränderungen gegenüber dem D-b-W-Minimal-System finden sich in der Tabelle in Anhang I. Unveränderte Fehlermöglichkeiten sind der Tabelle 5.1 bzw. Anhang E zu entnehmen.

6.2.1 Veränderte Auswirkungen der Zweikanaligkeit der Raddrehzahlsensorik

Die Verbesserung der Erkennbarkeit, Lokalisierbarkeit und Behandelbarkeit von Fehlern innerhalb des Systems D-b-W beschränkt sich in dieser FELB-Erweiterung ausschließlich auf die Raddrehzahlsensorik.
So führte beim Minimal-System ein erkannter Einfachfehler innerhalb der Hinterachs-Raddrehzahlsensorik zur Degradierung der Reglergüte (Top-Event A), innerhalb der Vorderachssensorik zur Überführung des Systems in die RFE (Top-Event B = Verfügbarkeitsverlust). Softfailures konnten hier überhaupt nicht erkannt werden, was zum sicherheitskritischen Top-Event C führte.
Dahingegen können mittels der zweikanaligen Raddrehzahlsensorik der erweiterten FELB Hard- und Soft-Einfachfehler innerhalb der üblichen Reaktionszeiten (siehe Anhang I1) erkannt und behandelt werden. Dabei sieht die Fehlerbehandlung eines Hardfailures jedoch ausschließlich einen Ausschluß der fehlerhaften Sensorinformation vor, womit nachwievor die volle D-b-W-Funktionalität gewährleistet ist. Der Fahrer wird über den Defekt via gelber Warnlampe informiert.
Da Softfailures im zweikanaligen System nicht eindeutig lokalisiert werden können, führt ihr Auftreten innerhalb der Vorderachssensorik zur Überführung in die Rückfallebene. Bei Auftritt eines Softfailures innerhalb der Hinterachssensorik muß der Regler lediglich auf die Reglerstufe 2 degradiert werden.
Im Sinne der pessimistischen Analyse des sicherheitsrelevanten Systems D-b-W wird aber auch beim erweiterten System davon ausgegangen, daß sich das System bis zur eigentlichen Fehlerbehandlung in einem sicherheitskritischen Zwischenzustand befindet.

Innerhalb der zweikanaligen Raddrehzahlsensorik wirkt sich der Verlust beider Kanäle (Zweifachfehler) durch Hard- bzw. Softfailures auf die Funktionalität des Systems D-b-W aus, wie die Einfachfehler innerhalb des einkanaligen Minimal-Systems. Weitere Details hierzu finden sich in Anhang I1.
Lediglich beim Auftritt temporärer Fehler wird auch im zweikanaligen System davon ausgegangen, daß diese nicht erkennbar sind und sich das System im Sinne der pessimistischen Analyse in einem kritischen Zustand befindet. Dennoch soll angemerkt werden, daß bei Verwendung des Mittelwertes beider Sensorkanäle als weiterzuverarbeitende Information, eine gewisse Glättung auftritt, die den Einfluß temporärer Fehler mindert.

Als Zwischenergebnis gilt es also festzuhalten, daß aufgrund der Eigenständigkeit der vorliegenden FELB-Erweiterung durch redundante Raddrehzahlsensoren keine Wechselwirkungen zu den übrigen Systemkomponenten und deren Fehlermöglichkeiten existieren. Diese Unabhängigkeit kann als wesentlicher Vorteil der HW-Redundanz gewertet werden (siehe auch funktionale bzw. analytische Redundanz).
Abschließend sei angemerkt, daß über die in Anhang I1 aufgeführten Kombinationen von Raddrehzahlsensorfehlern hinaus weitere denkbar sind. Diese sind aber gemäß dem Absorptionsgesetz für die wahrscheinlichkeitstheoretischen Betrachtungen irrelevant.

6.2.2 Auswirkungen der funktionalen Redundanz der Raddrehzahlsensorik

Im Gegensatz zur HW-Redundanz wirkt sich die Einführung der funktionalen Redundanz in vielerlei Hinsicht auf das Gesamt-FELB-Konzept aus. In Analogie zu Abschnitt 6.2.1 sollen jedoch auch hier nur die wesentlichen Veränderungen gegenüber dem Minimal-System diskutiert werden. Die Liste sämtlicher Veränderungen findet sich in Anhang I2. Dort sind auch die Fehlererkennungs-, -lokalisations- und -behandlungsraten bzw. -zeiten aufgeführt, die jedoch im wesentlichen nicht von denen des Minimalsystems abweichen.
Als erster Unterschied gegenüber dem Minimal-System sind ähnlich wie bei der zweikanaligen Raddrehzahlsensorik (Abschnitt 6.2.1) die Reaktionen auf Hardfailures innerhalb der Vorderachs-Raddrehzahlsensorik zu nennen. Da hier die Längsgeschwindigkeit über die verbleibende korrekte Vorderradgeschwindigkeitsinformation und den funktionalen Zusammenhang (siehe Abschnitt 6.1.2) bei geringem Schlupf nachwievor bestimmbar ist, bewirkt der Fehler lediglich eine Degradierung auf Reglerstufe RG2. Erst wenn beide Vorderachssensoren defekt sind und diese Fehler erkannt wurden, muß das System in die Rückfallebene überführt werden.
Ein weiterer wesentlicher Unterschied gegenüber dem Minimal-System liegt in der Möglichkeit, Softfailures innerhalb der Vorder- und Hinterradsensorik erkennen und behandeln zu können. Einfachfehler innerhalb der Vorder- und Hinterachssensorik bewirken lediglich eine Degradierung der Reglergüte auf Reglerstufe 2. Darüberhinaus kann sogar der „zweite“ Softfailure im verbleibenden Achs-Sensor über die funktionale Redundanz erkannt werden. Betraf dieser Zweitfehler neuerlich die Vorderachse, muß D-b-W in die Rückfallebene überführt werden. Der zweite Softfailure in der Hinterachs-Raddrehzahlsensorik bedarf lediglich einer Überführung des D-b-W in Reglerstufe 2. In diesem Fall wird die Längsgeschwindigkeit über die korrekte Vorderachssensorik und den funktionalen Zusammenhang (siehe Querbeschleunigungssensorik) bei geringem Schlupf bestimmt.
Temporäre Fehler haben auch innerhalb der funktional redundanten Raddrehzahlsensorik sicherheitsrelevanten Charakter (Top-Event C)

Da die funktionale Redundanz im Gegensatz zum Minimalsystem auf Informationen des Bremslichtschalters und des Drosselklappenpotentiometers zurückgreift, wirkt sich diese Aufweitung der Systemgrenzen auch auf die Fehlerbetrachtungen aus.
So führt ein Hardfailure innerhalb des Bremslichtschalters oder des Drosselklappenpotentiometers zur Überführung des Systems in die Rückfallebene. Grund hierfür ist die durch den Verlust der funktionalen Redundanz verlorene Fähigkeit der FELB, Softfailures der Raddrehzahlsensorik erkennen zu können. Mit Blick auf das Minimal-System wäre es auch denkbar, nach Auftreten obiger Hardfailures die FELB abzuschalten und den Fahrer über den Verlust der Diagnose zu informieren. Jedoch scheint dieser vom Automobil-Hersteller veranlaßte „Blindflug“ aus juristischer und ethischer Sicht nicht akzeptabel. Hier wird deutlich, daß ein Mehr an Diagnose auch zu einem Mehr an Verantwortung des Systementwicklers bzw. Automobilherstellers führt. Ein verfrühtes Überführen D-b-Ws in die Rückfallebene und damit der Verlust der Verfügbarkeit, bedeutet ein Mehr an Sicherheit.
Da Softfailures und temporäre Fehler des Bremslichtschalters bzw. seiner Nachverarbeitung, wie auch des Drosselklappenpotentiometers nicht erkannt werden können, sei im Rahmen der pessimistischen Analyse davon ausgegangen, daß diese Fehler die Gefahr eines Mißalarms oder Fehlalarms der Raddrehzahlsensorik in sich bergen. Da es sich um schlafende Fehler handelt, wurden sie dem sicherheitskritischen Top-Event C zugeordnet.
Genau wie in Abschnitt 6.1.1 muß auch hier angemerkt werden, daß über die in Anhang I2 aufgeführten Kombinationen von Raddrehzahlsensorfehlern weitere denkbar sind. Diese sind aber gemäß dem Absorptionsgesetz für die wahrscheinlichkeitstheoretische Betrachtung irrelevant.

Als Zwischenergebnis gilt es also festzuhalten, daß aufgrund des Einfließens diverser Sensoren in das funktionale Redundanzkonzept zur Überwachung der Raddrehzahlsensoren gegenüber dem Minimal-System (Anhang E) viele Änderungen innerhalb der Fehlermöglichkeiten zu verzeichnen sind. Diese Aussage wird sich bei den qualitativen, wie auch quantitativen Fehlerbäumen des Abschnittes 6.3 bemerkbar machen.

6.2.3 Auswirkungen der analytischen Redundanz der Raddrehzahlsensorik

Auch in diesem Abschnitt sollen nur die wesentlichen Veränderungen hinsichtlich der Fehlerauswirkungen im D-b-W-System mit analytischer Redundanz gegenüber dem Minimal-System diskutiert werden. Die Liste sämtlicher Veränderungen findet sich in Anhang I3. Dort sind auch die Fehlererkennungs-, -lokalisations- und –behandlungsraten bzw. -zeiten aufgeführt, die jedoch im wesentlichen nicht von denen des Minimalsystems abweichen.
Als erster Unterschied gegenüber dem Minimal-System sind die FELB-Reaktionen auf Hardfailures der Querbeschleunigungssensoren zu nennen. Da durch einen Ausfall obiger Sensoren die analytische Redundanz zur Überwachung der Raddrehzahlsensoren ausfiele, wird hier mit Verweis auf die Argumentationen in Abschnitt 6.2.1 (Ausfall der funktionalen Redundanz) D-b-W auch in diesem Fall in die Rückfallebene überführt. Analog hierzu wird auch bei Hardfailures des Längsbeschleunigungssensors, wie auch bei Auftreten eines Hard- wie auch Softfailures eines Raddrehzahlsensors degradiert.
Ein zweiter Hardfailure oder Softfailure innerhalb der Raddrehzahlsensorik würde, bedingt durch den vorausgehenden Ausfall der analytischen Redundanz, verursacht durch einen obiger Erstfehler, nicht erkannt werden. Entsprechend führen diese Fehler zum sicherheitskritischen Top-Event C.
Temporäre Fehler der Raddrehzahlsensorik können auch über das analytische Redundanzkonzept nicht erkannt werden und führen somit ebenfalls zum Top-Event C.
Im Gegensatz zu sämtlichen bisher diskutierten FELB-Konzepten, fließt in die analytische Redundanz die Information des Bremsdrucksensors, wie auch der aktuelle Getriebegang ein. Hardfailures dieser Informationsquellen führen zum Ausfall der analytischen Redundanz und somit zur Überführung D-b-Ws in die Rückfallebene (Top-Event B). Gleiches gilt für Hardfailures des Drosselklappenpotentiometers.
Softfailures, wie auch temporäre Fehler obiger drei Sensoren können durch die FELB nicht erkannt werden, womit sie zu Top-Event C führen.
Der Bremslichtschalter gehört nicht zum Systemumfang des mit analytischer Redundanz versehenen D-b-Ws.
Durch obige Ausführungen deutet sich bereits an, wie fehleranfällig die komplexe analytische Redundanz ist. Diese Aussage wird sich bei den qualitativen wie auch quantitativen Fehlerbäumen des Abschnittes 6.3 konkretisieren. Insbesondere wird deutlich, daß aufgrund des Verlustes der Überwachbarkeit der Rd-Sensorik D-b-W häufig in die RFE überführt wird, was zum Verlust der Verfügbarkeit des Systems führt.
Ziel sollte es somit sein, eine möglichst ohne „allzuviel“ Fremdinformation auskommende Überwachung zu entwickeln, die dennoch eine fahrsituationunabhängige Überwachung der Sensorik erlaubt.
Genau wie in Abschnitt 6.1.1 muß auch hier angemerkt werden, daß über die in Tabelle 6.2 aufgeführten Kombinationen von Raddrehzahlsensorfehlern weitere denkbar sind. Diese sind aber gemäß dem Absorptionsgesetz für die wahrscheinlichkeitstheoretischen Betrachtungen irrelevant.
Positiv ist jedoch anzumerken, daß die analytische Redundanz mit Ausnahme des indirekten Einflusses der Gierratensensorik keine fahrdynamisch bedingten Überwachungslücken aufweist.

6.3 FTAs der FELB-Erweiterungen

Mit Blick auf die mathematische Korrektheit der Fehlerbaumanalyse, sind hier sämtliche relevanten Fehlerszenarien und nicht nur die Elemente, die sich gegenüber dem Minimal-System verändert haben, zu modellieren.

6.3.1 Auswirkungen der FELB-Erweiterungen auf Top-Event A

Die graphischen Darstellungen und damit qualitativen Fehlerbaumanalysen des Top-Events A für die Redundanzkonzepte aus Abschnitt 6.1 bzw. 6.2 finden sich in Anhang J.

6.3.1.1 Auswirkungen der Zweikanaligkeit der Raddrehzahlsensorik auf Top-Event A

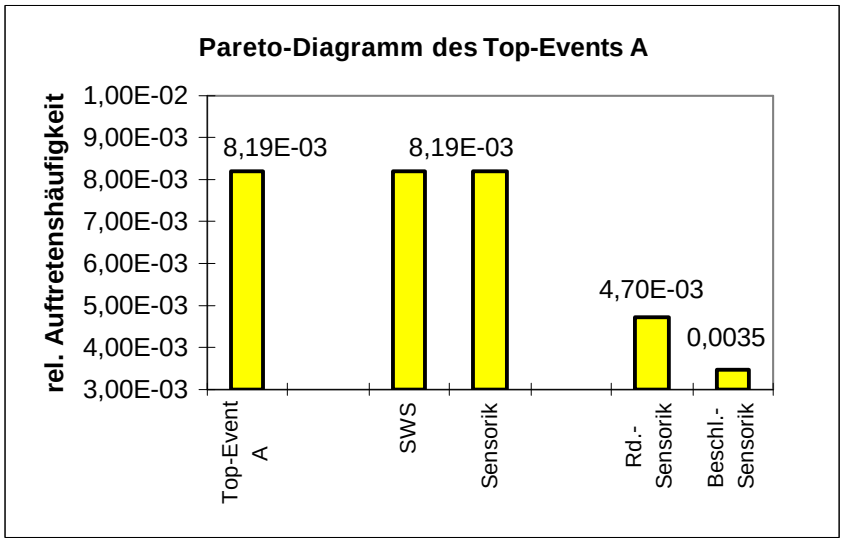


Bild 6.1: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events A der FELB-Erweiterung basierend auf redundanter Rd-Sensorik

Wie Bild 6.1 im Vergleich mit Bild 5.1 zu entnehmen ist, weist das D-b-W-System mit FELB-Erweiterung basierend auf HW-Redundanz der Rd-Sensorik eine Erhöhung der Top-Event A Häufigkeit von nahezu 40% gegenüber der des Minimal-Systems auf. Diese ist auf eine nahezu Verdoppelung des Anteils der Raddrehzahlsensoren am Top-Event A zurückzuführen. Zwar sollte die Robustheit gegenüber Einfach-Hardfailures der Raddrehzahlsensorik zu einer Senkung der Top-Event-A-Häufigkeit des HW-redundanten Systems führen, jedoch bewirkt die Zweikanaligkeit, daß nahezu doppelt soviele Softfailures der Raddrehzahlsensoren zum Eintritt des Top-Events führen, als es beim Minimal-System durch Hardfailures der Fall war.
Entsprechend würden nunmehr von 1Mio. einjährigen, mit D-b-W ausgestatteten Pkw innerhalb der Missionsdauer von 300 Stunden 8.190 Fahrzeuge eine Degradation der Fahrdynamikregelung auf die Reglerstufe 2 oder 3, begleitet von einer Fahrerwarnung durch Aktivierung der gelben Warnlampe, erfahren.
Wie sich in den Abschnitten 6.3.2 und 6.3.3 zeigen wird, ist die Erhöhung der Top-Event A-Häufigkeit mit einer Reduzierung der Top-Event C-Häufigkeit verbunden. Die Verfügbarkeit (Top-Event B) kann durch die verbesserte Diagnose nicht optimiert werden.

6.3.1.2 Auswirkungen der funktional redundanten Raddrehzahlsensorik auf Top-Event A

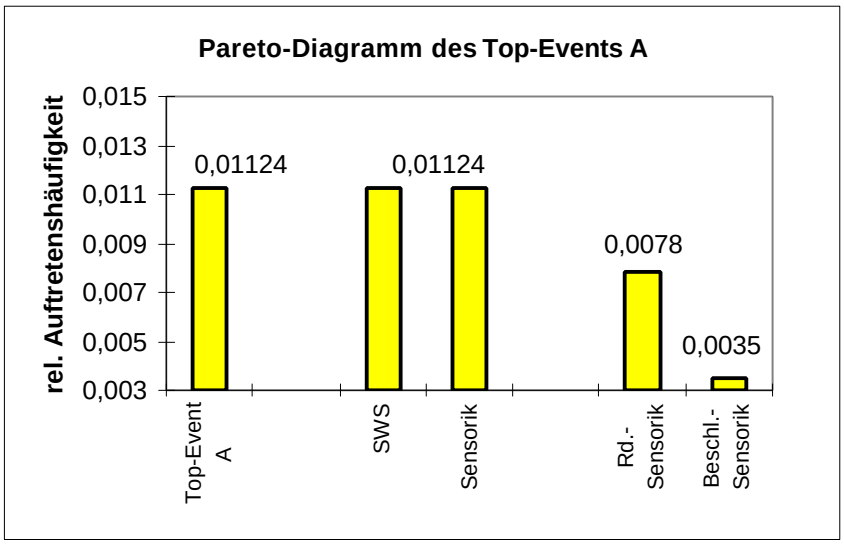


Bild 6.2: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events A der FELB-Erweiterung basierend auf funktional redundanter Rd-Sensorik

Wie Bild 6.2 im Vergleich mit Bild 5.1 zu entnehmen ist, weist das D-b-W-System mit FELB-Erweiterung basierend auf funktionaler Redundanz der Rd-Sensorik nahezu eine Verdoppelung der Top-Event A Häufigkeit auf. Dieser Umstand ist ausschließlich auf die Verbesserung der Überwachbarkeit der Rd-Sensorik zurückzuführen. Diese führte zu einer Aufnahme der überwachbaren Softfailure-Raten der Raddrehzahlsensoren in den Fehlerbaum des Top-Events A. Im Vergleich mit Bild 6.1 wird jedoch deutlich, daß die funktionale Redundanz aufgrund der Einsparung an HW-Redundanz eine höhere Top-Event-A-Häufigkeit aufweist. Grund hierfür liegt in der nunmehr fehlenden Robustheit gegenüber Einfach-Hardfailures der Raddrehzahlsensoren.
Entsprechend würden nunmehr von 1Mio. einjährigen, mit D-b-W ausgestatteten Pkw innerhalb der Missionsdauer von 300 Stunden 11.240 Fahrzeuge eine Degradation der Fahrdynamikregelung auf die Reglerstufe 2 oder 3 bzw. eine Fahrerwarnung durch Aktivierung der gelben Warnlampe erfahren.

6.3.1.3 Auswirkungen der analytisch redundanten Raddrehzahlsensorik auf Top-Event A

Wie Anhang I3 zu entnehmen ist, führen bedingt durch die analytisch redundante FELB-Erweiterung keinerlei Komponentenfehler zum Eintritt des Top-Event A. Die resultierende Top-Event A-Häufigkeit ist Null, womit sie als optimal bezeichnet werden kann. Um aber falschen Rückschlüssen über die Qualität des analytischen Redundanzkonzeptes vorzubeugen, soll Abschnitt 6.3.2 vorweggenommen werden, daß Top-Event B des analytischen Redundanzkonzeptes deutlich häufiger auftritt, als bei den übrigen Redundanzkonzepten bzw. dem Minimal-System.

6.3.2 Auswirkungen der FELB-Erweiterungen auf Top-Event B

Die graphischen Darstellungen und damit qualitativen Fehlerbaumanalysen des Top-Events B für die Redundanzkonzepte aus Abschnitt 6.1 und 6.2 finden sich in Anhang K.

6.3.2.1 Auswirkungen der Zweikanaligkeit der Raddrehzahlsensorik auf Top-Event B

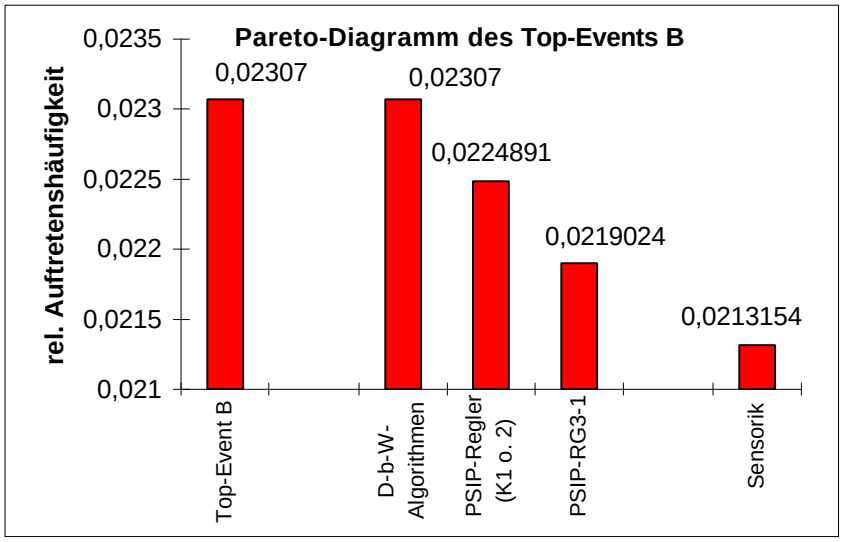


Bild 6.4: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events B der FELB-Erweiterung basierend auf redundanter Rd-Sensorik

Wie Bild 6.4 im Vergleich mit Bild 5.2 zu entnehmen ist, wirkt sich die HW-basierte FELB-Erweiterung geringfügig verschlechternd auf die Auftrittshäufigkeiten der relevanten Gatter des Fehlerbaums aus Anhang K aus. So nimmt die rel. Auftretenshäufigkeit des Top-Events B gegenüber Abschnitt 5.2.2 um 11% zu.
Damit beschränkt sich der Vorzug der HW-basierten FELB-Erweiterung ausschließlich auf einer Verbesserung der Systemsicherheit (siehe auch Abschnitt 6.3.3).

6.3.2.2 Auswirkungen der funktional redundanten Raddrehzahlsensorik auf Top-Event B

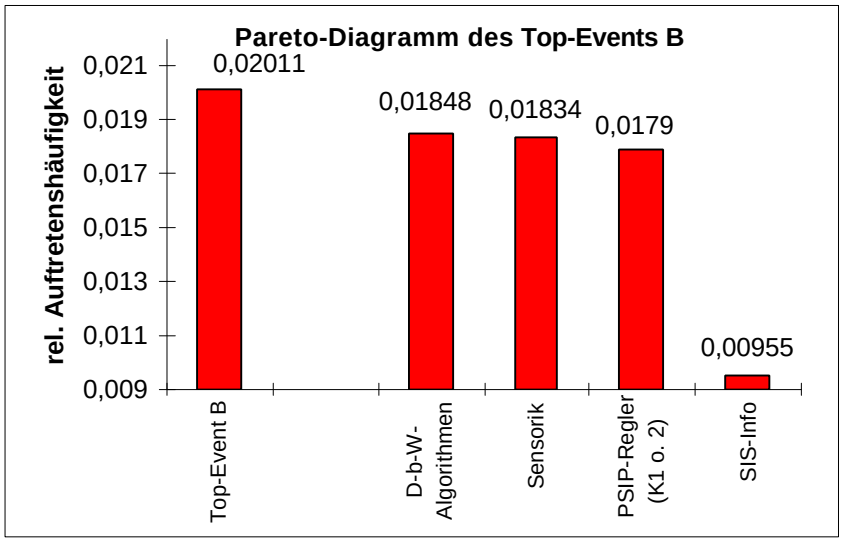


Bild 6.5: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events B der FELB-Erweiterung basierend auf funktional redundanter Rd-Sensorik

Wie Bild 6.5 im Vergleich mit Bild 5.2 zu entnehmen ist, wirkt sich die auf funktionaler Redundanz basierende FELB-Erweiterung kaum auf die Auftrittshäufigkeiten der relevanten Gatter des Fehlerbaums aus Anhang K aus. So nimmt die rel. Auftretens-häufigkeit des Top-Events B gegenüber Abschnitt 5.2.2 nur um 3,3% ab. Dennoch ist somit die Verfügbarkeit dieses Redundanzkonzeptes höher als die der HW-redundanten FELB-Erweiterung.
Es soll jedoch explizit auf das Gatter SIS-Info hingewiesen werden. Hier spiegeln sich die Sensor-Fehler wider, die zu einem Versagen der funktionalen Redundanzen der Raddreh-zahlsensorik führen. Der bisher im Gatter „Sensorik“ unberücksichtigte BLS führt gegenüber Bild 5.2 und 6.4 zum deutlichen Ansteigen der Gatter-Auftretenshäufigkeit.

6.3.2.3 Auswirkungen der analytisch redundanten Raddrehzahlsensorik auf Top-Event B

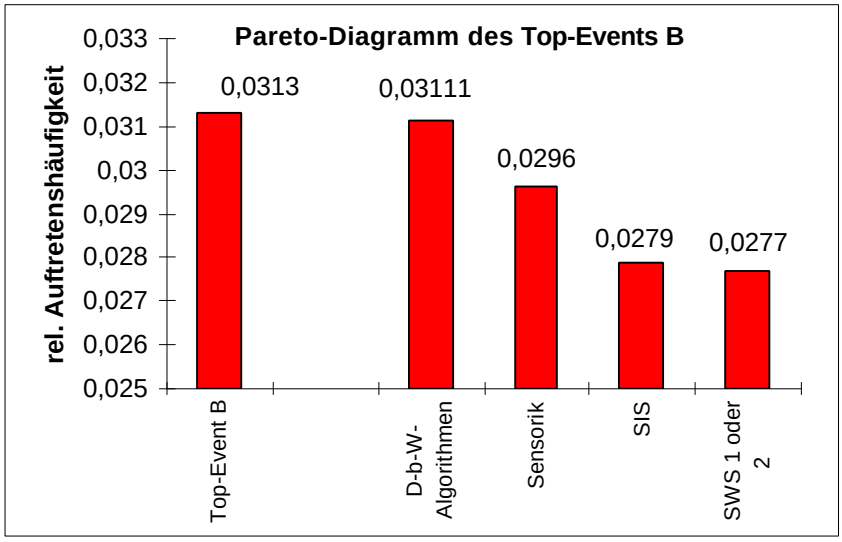


Bild 6.6: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events B der FELB-Erweiterung basierend auf analytisch redundanter Rd-Sensorik

Wie Bild 6.6 im Vergleich mit Bild 5.2 zu entnehmen ist, wirkt sich die auf analytischer Redundanz basierende FELB-Erweiterung massiv verschlechternd auf die Auftritts-häufigkeiten der relevanten Gatter des Fehlerbaums aus Anhang K aus. So nimmt die rel. Auftretenshäufigkeit des Top-Events B gegenüber Abschnitt 5.2.2 um 50,5% zu.
Entsprechend würden nunmehr von 1Mio. einjährigen, mit D-b-W ausgestatteten Pkw innerhalb der Missionsdauer von 300 Std. 31.300 Fahrzeuge eine Degradation der Fahrdynamikregelung in die RFE bzw. eine Fahrerwarnung durch Aktivierung der roten Warnlampe erfahren.
Ursache für diese Verschlechterung ist die Vielzahl der in Abschnitt 6.2.3 bzw. Anhang I3, wie auch im Fehlerbaum (Anhang K3) aufgeführten, zum Verlust der Überwachbarkeit der Rd-Softfailures führenden Fehlermöglichkeiten, denen ihrerseits durch eine Degradierung D-b-Ws in RFE begegnet wird.
Dem Pareto-Diagramm sind als signifikante Ursachen für den Eintritts des Top-Events B Fehler der Sensorik, insbesondere die Raddrehzahlsensorik zu entnehmen. Auch das ebenfalls dominante Gatter SIS der Raddrehzahlsensorik (SIS), in das die beiden Kanäle des Schwimmwinkelschätzers (SWS 1 oder 2) einfließen, wird somit von Sensorfehlern bestimmt.

6.3.3 Auswirkungen der FELB-Erweiterungen auf Top-Event C

Die graphischen Darstellungen und damit qualitativen Fehlerbaumanalysen des Top-Events C für die Redundanzkonzepte aus Abschnitt 6.1 bzw. 6.2 finden sich in Anhang L.

6.3.3.1 Auswirkungen der Zweikanaligkeit der Raddrehzahlsensorik auf Top-Event C

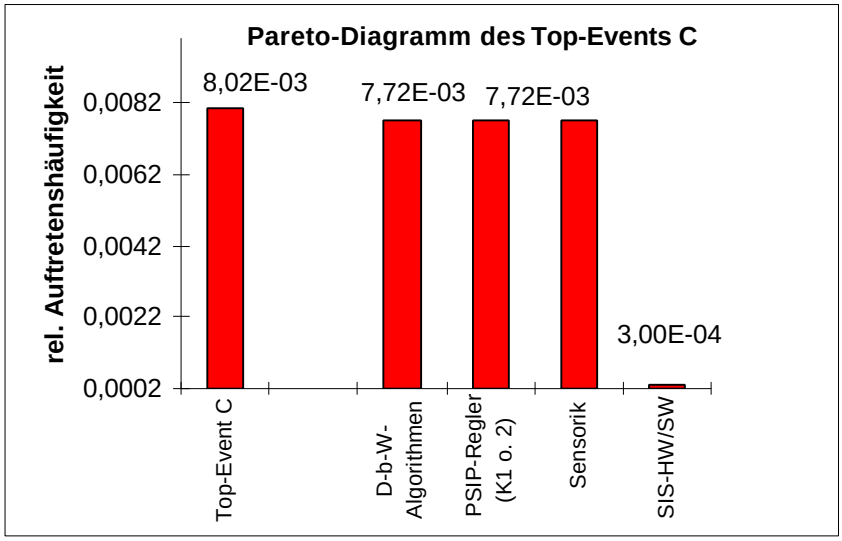


Bild 6.7: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events C der FELB-Erweiterung basierend auf redundanter Rd-Sensorik

Wie Bild 6.7 im Vergleich mit Bild 5.3 zu entnehmen ist, wirkt sich die HW-basierte FELB-Erweiterung positiv auf Auftrittshäufigkeiten des sicherheitsrelevanten Top-Events C aus. So nimmt die rel. Auftretenshäufigkeit des Top-Events C gegenüber Abschnitt 5.2.3 um 32% ab. Eine deutlichere Verbesserung war durch die herkömmliche HW-Redundanz nicht zu erwirken, da durch sie zwar nun einfache Softfailures innerhalb der Raddrehzahl-sensorik nicht mehr zum Eintritt des Top-Events C führen, sich die Anzahl temporärer Fehler innerhalb der Rd-Sensorik durch die Redundanz aber verdoppelt hat.

6.3.3.2 Auswirkungen der funktional redundanten Raddrehzahlsensorik auf Top-Event C

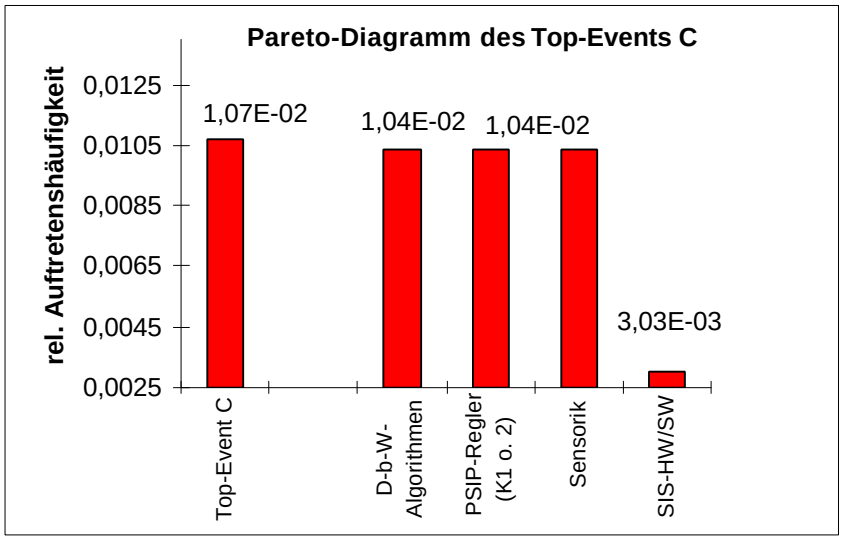


Bild 6.8: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events C der FELB-Erweiterung basierend auf funktional redundanter Rd-Sensorik

Wie Bild 6.8 im Vergleich mit Bild 5.3 zu entnehmen ist, wirkt sich die auf funktionaler Redundanz basierende FELB-Erweiterung zwar positiv auf Auftrittshäufigkeiten des sicherheitsrelevanten Top-Events C aus. Jedoch nimmt die rel. Auftretenshäufigkeit des Top-Events C gegenüber Abschnitt 5.2.3 lediglich um 9,6% ab. Eine deutlichere Verbesserung war bedingt durch die Überwachungslücken innerhalb der Softfailure-Erkennung der Raddrehzahlsensoren nicht möglich. Leider führte der für die Überwachungslücken maßgebliche Anteil der SIS-Info-Fehler (siehe Anhang L) auch dazu, daß die vorliegende Top-Event-C-Häufigkeit deutlich höher ist, als die der HW-Redundanz (vergleiche Bild 6.7).

6.3.3.3 Auswirkungen der analytisch redundanten Raddrehzahlsensorik auf Top-Event C

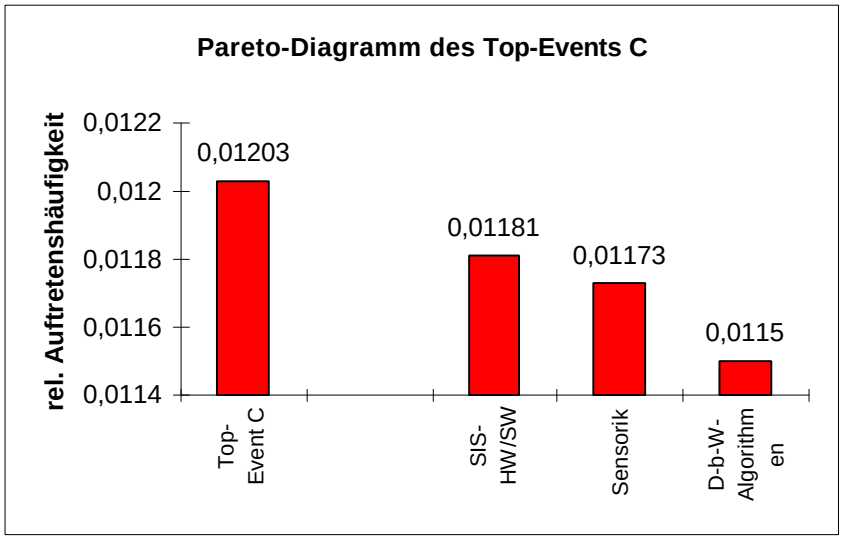


Bild 6.9: Pareto-Diagramm der dominanten Gatter des Fehlerbaums des Top-Events C der FELB-Erweiterung basierend auf analytisch redundanter Rd-Sensorik

Wie Bild 6.9 im Vergleich mit Bild 5.3 zu entnehmen ist, wirkt sich die auf analytischer Redundanz basierende FELB-Erweiterung sogar geringfügig verschlechternd auf die Systemsicherheit aus. So nimmt die rel. Auftretenshäufigkeit des Top-Events C gegenüber Abschnitt 5.2.3 um 2% zu. Eine Verbesserung war, bedingt durch die Vielzahl von Informationen, die zur Generierung der analytischen Redundanz benötigt wurden und deren nicht erkennbare Fehler zum Top-Event C führen, nicht erzielbar.

6.3.4 Auswirkungen der FELB-Erweiterungen auf Top-Event D

In Analogie zu Abschnitt 5.2.4 bzw. 3.1.1.4 fließen in Top-Event D sämtliche innerhalb der betrachteten Systemgrenzen möglichen Komponentenfehler ein. Mit Verweis auf obige Abschnitte bzw. die in Anhang I aufgeführten Fehlermöglichkeiten der FELB-Erweiterungen beschränkt sich die Top-Event-D-Diskussion hier auf die Angabe der Auftretenshäufigkeit dieses Top-Events.

Gemäß Abschnitt 5.2.4 ergab sich für das Minimal-System die Gesamtfehler-wahrscheinlichkeit von 4,15%.

Für das mit der HW-redundanten Raddrehzahlsensorik erweiterte D-b-W-System ergibt sich die Top-Event-D-Wahrscheinlichkeit von 5,14%. Diese Erhöhung um nahezu 25% gegenüber dem Minimal-System ist alleinig auf die Quasi-Verdoppelung der Fehler-wahrscheinlichkeit innerhalb der redundanten Raddrehzahlsensorik zurückzuführen.

Das mit funktional redundanter Raddrehzahlsensorik erweiterte D-b-W-System weist eine Top-Event-D-Wahrscheinlichkeit von 4,5% auf. Diese Erhöhung gegenüber dem Minimal-System ist auf die Einbeziehung des fehleranfälligen Bremslichtschalters und des Drosselklappenpotentiometers in die Systemgrenzen des erweiterten Systems zurückzuführen.

Lediglich das analytisch redundant erweiterte D-b-W-System weist mit einer Top-Event-D-Wahrscheinlichkeit von 4,19% eine mit dem Minimal-System vergleichbare Gesamtsystem-Fehlerwahrscheinlichkeit auf. Dies ist auf den Umstand zurückzuführen, daß gegenüber dem Minimal-System lediglich die relativ zuverlässigen Komponenten Drosselklappenpotentiometer und Bremsdrucksensor zum Systemumfang hinzukamen.

Grundsätzlich bestätigt sich hier jedoch die Aussage, daß mit zunehmender Anzahl an Systemkomponenten die Fehlerwahrscheinlichkeit des Gesamtsystems zunimmt. Entsprechend schneidet hier das Minimal-System am besten ab.

6.3.5 Die beste FELB-Erweiterung / Zwischenbilanz der F/V/S/W-Analyse mittels FTA

Ziel der Abschnitte 6.3.1-6.3.3 war es, basierend auf der einfach generierbaren Fehlerbaumanalyse, das hinsichtlich F/V/S optimale FELB-Konzept zu bestimmen.
Leider ergab die Analyse, daß keines der vorgestellten erweiterten FELB-Konzepte als hinsichtlich aller Qualitätsparameter optimal bezeichnet werden kann.
Da das Hauptaugenmerk auf die Systemsicherheit gerichtet ist, gefolgt von der Verfügbarkeit und Fehlerwahrscheinlichkeit, scheidet das hier vorgestellte analytische Redundanzkonzept aus. Seine gegenüber dem Minimalsystem geringfügig schlechtere Top-Event-C-Häufigkeit rechtfertigt nicht den Mehraufwand an Softwareentwicklung und Rechenleistung. Es soll angemerkt werden, daß analytische Redundanzen nur dann zum Einsatz kommen sollten, wenn die in die meist aufwendigen Modelle einfließenden Informationen abgesichert sind. Eine Absicherung kann beispielsweise durch Selbstüberwachung erfolgen. Anderenfalls eignen sich die auf Schätzerstrategien basierenden analytischen Kanäle lediglich zur Schätzung durch Sensoren nicht erfaßbarer Information, was eine Überwachung, fußend auf Redundanz, jedoch ausschließt.
Grundsätzlich sollte die mittels Schätzerstrategien gewonnene Information nicht sicherheitsrelevanter Natur sein, da aufgrund der im aktuellen Kapitel aufgezeigten Defizite hinsichtlich F/V/S der Schätzwert nicht als ausreichend verfügbar bezeichnet werden muß.
Vergleicht man HW-Redundanz und funktionale Redundanz, so müßte man sich hinsichtlich der Systemsicherheit für erstere entscheiden. Da absolut betrachtet beide nicht gravierend voneinander abweichen, erscheint die deutlich höhere Top-Event-A-Häufigkeit der HW-Redundanz als „Killer-Kriterium“ für dieses Konzept. Der Faktor Kosten wird bedingt durch HW-Mehraufwand ebenfalls zu Ungunsten dieser FELB-Erweiterung ausfallen.
Dementsprechend erscheint das funktionale Redundanzkonzept als bester Kompromiß, unter den hier vorgestellten FELB-Erweiterungen. Mit Blick auf die zu verzeichnenden Überwachungslücken, sollte eine Verbesserung der verwandten Modelle angeregt werden. Gleichzeitig sollte diese Optimierung der Modellierungsgüte nicht unter Zuhilfenahme zusätzlicher Sensorik geschehen, da diese zusätzliche Fehlerquellen darstellen.
Als Optimum hinsichtlich F/V/S erscheint dem Autor eine Fusion aus HW-Redundanz, gekoppelt mit funktionaler Redundanz.

6.4 Hierarchische Modellierung der funktional redundanten FELB-Erweiterung

Im weiteren Verlauf dieser Arbeit soll nunmehr untersucht werden, wie sich die im letzten Abschnitt als bester Kompromiß hinsichtlich F/V/S erwiesene FELB-Erweiterung basierend auf funktionaler Redundanz auf die G/K-Kostensituation des Gesamtsystems auswirkt. Hierzu erfolgt eine hierarchische Modellierung dieses Konzeptes, die anschließend mit der hierarchischen Modellierung aus Abschnitt 5.3 verglichen wird. Wie die FTA aus Abschnitt 6.3 ergab, tragen die Zweifachfehler der Raddrehzahlsensoren nur unmaßgeblich zum Fehlerverhalten des Gesamtsystems bei. Zwecks Vereinfachung der Zustandsraum-darstellung soll deshalb auf diese Fehlerdetaillierung verzichtet werden. Durch diese Vereinfachung läßt sich auch das um die funktionale Redundanz erweiterte System weitestgehend auf die Zustandsraumdarstellung des Minimal-Systems abbilden.
So konnte bis auf die Einführung des Zustandes 12, der ein Pendant zum Zustand 4 darstellt, der Zustandsvektor aus Abschnitt 5.3 übernommen werden. Ansonsten sind lediglich Veränderungen in den Übergangsraten ausgehend vom Startzustand „0“ zu verzeichnen, die mit der gegenüber dem Minimal-System erhöhten Überwachbarkeit des Systems und der hierfür erforderlichen Zusatzsensorik verbunden sind. Diese Übergangs-raten wirken sich in der im folgenden dargestellten Art auf die Zustandsaufenthalts-wahrscheinlichkeiten und somit die F/V/S/W des Systems aus.
Die tabellarische Darstellung der gegenüber dem Minimal-System veränderten Zustandsübergangsraten findet sich in Anhang M.

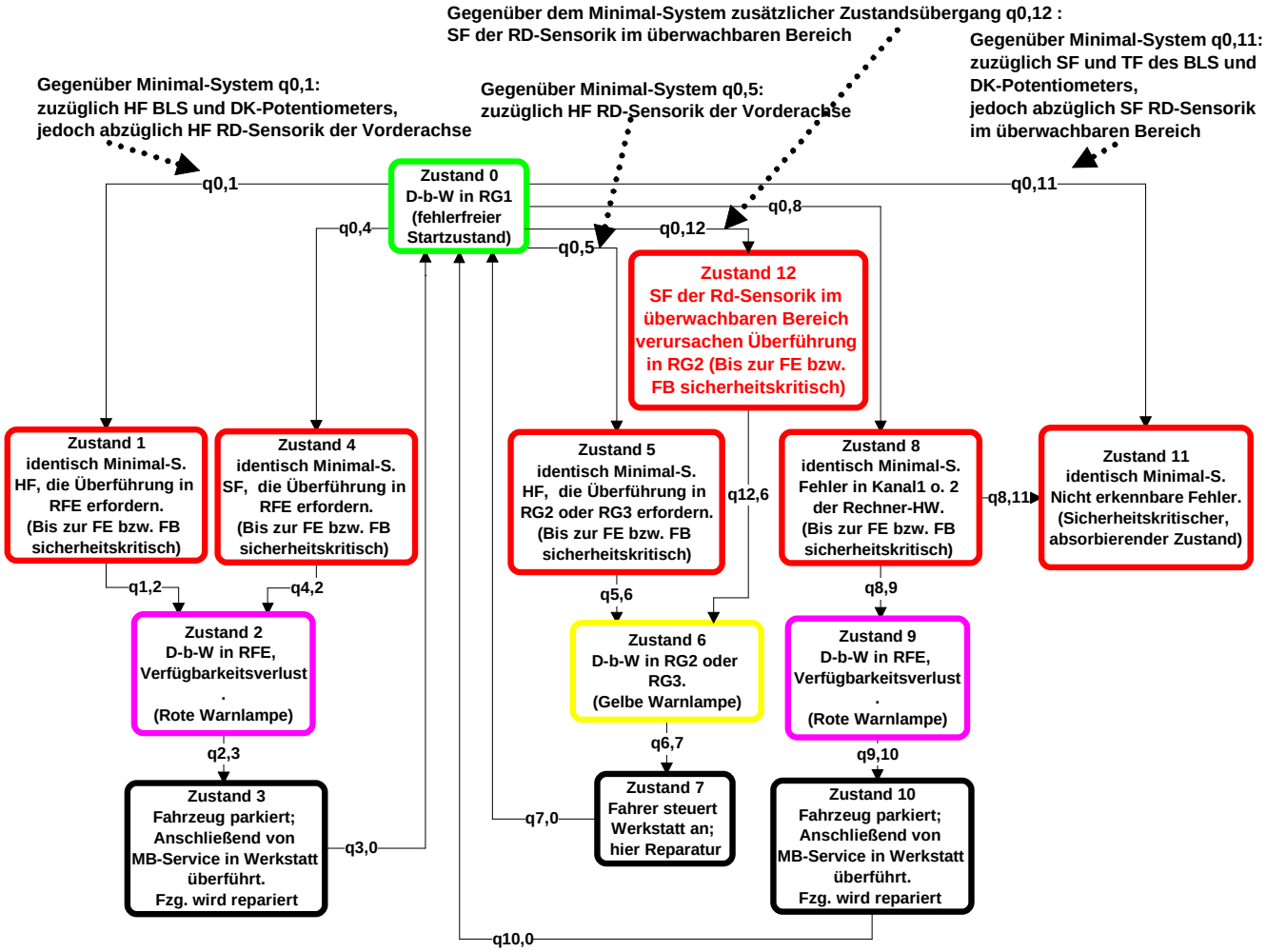


Bild 6.10: Markov-Kette des D-b-W-Systems mit funktional redundanter FELB-Erweiterung

Kommentare zu den Zuständen und Zustandsübergängen:
Hinsichtlich Kommentaren zu den Zuständen und Zustandsübergängen soll auf Bild 6.10, Abschnitt 5.3 und die Anhänge H und M verwiesen werden.

Modellierung der Markov-Kette mittels des Tools MKV
In Analogie zum Minimal-System befindet sich die mittels des Tools MKV bestimmte Lösung der Markov-Kette zum Zeitpunkt t=300h (1. Betriebsjahr eines mit D-b-W ausgestatteten Fzgs.) in Anhang N.
Entsprechend der Überlegung aus Abschnitt 5.3 gibt Gleichung 6-7 die resultierende Aufenthaltswahrscheinlichkeit in Zustand 11 mit Erreichen der mittleren Betriebsdauer von 3000 Stunden (10 Jahre Nutzung) wieder.

$$\pi_{11}(t = 3.000h) \approx F(t = 3.000h) = 1 - e^{-q_{0,11} \cdot 3.000h} = 0{,}101772 \qquad \text{Gl. 6-7}$$

Damit befinden sich bei einer angenommenen Produktionsmenge von 1Mio. Fahrzeugen nach 3000 Stunden Nutzungsdauer 101.772 Fahrzeuge im sicherheitskritischen Zustand. Vergleicht man diese Anzahl mit der des Minimalsystems (siehe Gl. 5-1), so liegt sie 8,9% unterhalb dieser. An dieser Stelle soll angemerkt werden, daß diese durch die FELB-Erweiterung erwirkte relative Verbesserung unterhalb derer nach Erreichen des ersten Betriebsjahres liegt (siehe Abschnitt 6.3.3.2). Ursache hierfür ist die Exponentialverteilung des Fehler- bzw. Ausfallverhaltens.
Bedingt durch den Umstand, daß der sicherheitsrelevante Zustand 11 absorbierender Natur ist, wirkt sich die FELB-Erweiterung mit zunehmender Missionsdauer weniger positiv auf die Systemsicherheit aus.

Diskussion der F/VS/W des D-b-W-Systems mit funktional redundanter FELB-Erweiterung

In Analogie zu Abschnitt 5.3 soll das D-b-W-System mit funktional redundanter FELB-Erweiterung hinsichtlich seiner F/V/S/W zum Zeitpunkt t=300h analysiert und mit den Ergebnissen des Minimal-Systems verglichen werden. In Bild 6.11 sind hierfür die Ergebnisse des Minimal-Systems jeweils links neben den Ergebnissen des erweiterten Systems dargestellt. Die numerischen Ergebnisse des Minimal-Systems sind jeweils schräg über den zugehörigen Balken dargestellt. Zur deutlicheren Abgrenzung sind die Balken des erweiterten Systems zusätzlich schwarz umrandet.

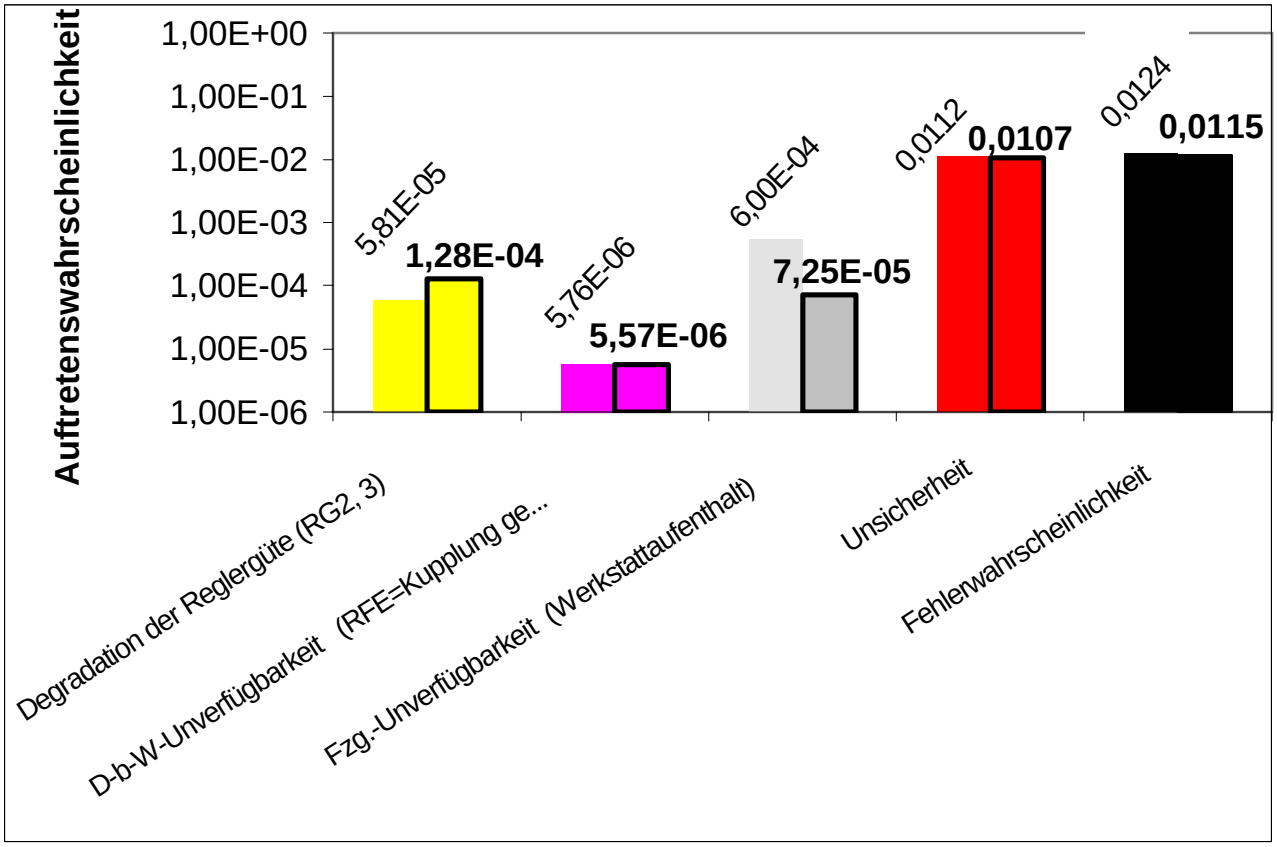


Bild 6.11: Vergleichende Darstellung der Fehlerwahrscheinlichkeit, Unverfügbarkeit und Unsicherheit des D-b-W-Minimal-Systems sowie des D-b-W-Systems mit funktional redundanter FELB-Erweiterung für t=300h

Die Fehlerwahrscheinlichkeit F(t=300h) = 0,0115 entspricht der Wahrscheinlichkeit, daß der Zustand 0 zum Zeitpunkt t=300h verlassen wird. Als Komplement entspricht die Aufenthaltswahrscheinlichkeit im Zustand 0 (0,98848) der Fehlerfreiheit des Systems zum Zeitpunkt t=300h. Ausgehend von 1 Mio. ein Jahr alter, mit D-b-W ausgestatteter Pkw würden 11.521 dieser Fahrzeuge, also 907 weniger als beim Minimal-System, einen Fehler aufweisen, der zum Verlassen des Zustands 0 führt. Dies entspricht einer Verbesserung um 7,3%.

Daß hier die Fehlerwahrscheinlichkeit zum Zeitpunkt t=300h niedriger ist, als die des Minimal-Systems, überrascht auf den ersten Blick. So ergab doch die FTA aus Abschnitt 6.3.4, daß die Top-D-Häufigkeit des mittels funktionaler Redundanz erweiterten Systems gegenüber dem Minimal-System um relativ 8,4% höher liegt. Um diesen scheinbaren Widerspruch aufzuklären, muß den noch folgenden Aussagen zur Unsicherheit des mittels funktionaler Redundanz erweiterten D-b-Ws vorweggegriffen werden. Wie sich zeigen wird, ist die Aufenthaltswahrscheinlichkeit im absorbierenden sicherheitskritischen Zustand 11 gegenüber dem Minimal-System absolut um 1,1E-3

niedriger. Bei einer Mio. Fahrzeugen entspricht dies ca. 1.100 Fahrzeugen. In Abschnitt 3.2 wurde deutlich, daß die Summe der Aufenthaltswahrscheinlichkeiten in sämtlichen Zuständen des Zustandsvektors 1 ist. Entsprechend führt die Absenkung der aus dem Verkehr gezogenen Fahrzeuge zu einer Erhöhung der Aufenthaltswahrscheinlichkeit im fehlerfreien Zustand 0, was seinerseits der Absenkung der Fehlerwahrscheinlichkeit entspricht.

In Analogie zu Abschnitt 5.3 wird auch hier zwischen der Unverfügbarkeit der elektronischen D-b-W-Funktionalität während des Fahrbetriebs und der Unverfügbarkeit des Fzgs. für den Fahrer unterschieden.

Die Unverfügbarkeit der elektronischen D-b-W-Funktionalität bestimmt sich analog zum Minimal-System aus der Summe der Aufenthaltswahrscheinlichkeiten in den Zuständen 2 und 9 (P(RFE(t=300h)) = 5,57E-6). Damit ist diese relativ zum Minimal-System um 3,2% niedriger.

Die Unverfügbarkeit des Fahrzeugs, auch als Aufenthaltswahrscheinlichkeit in der Werkstatt (P(Werkstatt)) bezeichnet, ergibt sich aus den Aufenthaltswahrscheinlichkeiten in den Zuständen 3, 7 und 10 zu 0,000725. Damit liegt hier die Unverfügbarkeit im Vergleich zum Minimal-System um 20,8% höher. Diese deutliche Verschlechterung ist auf den Anstieg der Aufenthaltswahrscheinlichkeit im Zustand 7, bedingt durch die Erkennbarkeit von SF der Rd-Sensorik zurückzuführen. Entsprechend befinden sich von den 1 Mio. ein Jahr alten, mit D-b-W ausgestatteten Fahrzeugen zum Zeitpunkt t=300h ca. 725 Fzg. in der Werkstatt.

Die Unsicherheit, als aus Sicht des Autors für den Konzept-Entscheid wichtigste Kenngröße, bestimmt sich aus der Summe der Aufenthaltswahrscheinlichkeiten in den Zuständen 1, 4, 5, 8, 11 und 12. Damit setzt sich die Unsicherheit bis auf den neu hinzugekommenen Zustand 12 aus den gleichen Zuständen wie beim Minimal-System zusammen. Die Aufenthaltswahrscheinlichkeit im absorbierenden, sicherheitsrelevanten Zustand 11 = Fehlalarm = $(1\text{-}S_{11})$ = 0,0106617) ist um 9,4% besser als beim Minimal-System. Die Aufenthaltswahrscheinlichkeit in den übrigen sicherheitsrelevanten Zuständen entspricht 8,433E-8.

In Summe liegt damit die Gesamtaufenthaltswahrscheinlichkeit in sämtlichen sicherheitsrelevanten Zuständen mit 0,01066178 relativ um 9,37% unterhalb derer des Minimal-Systems (vergleiche auch Top-Event C aus Abschnitt 6.3).

Auch die G/K-Kosten sollen in Analogie zu Abschnitt 5.3 zum Zeitpunkt t = 300h ermittelt werden. Folglich bestimmen sie sich aus dem Produkt der Reparatur- und Abschleppkosten mit der Anzahl der in den entsprechenden Zuständen zum Zeitpunkt t =300 h befindlichen Fahrzeugen.

- G/K-Kosten Zustand 3 = π_3 * 1E6 Fzg. * Kosten für (Abschleppen und Reparatur) = 853.554 DM.
- G/K-Kosten Zustand 7 = π_7 * 1E6 Fzg. * Kosten für Reparatur = 384.978 DM
- G/K-Kosten Zustand 10 = π_{10} * 1E6 Fzg. * Kosten für Abschleppen und Reparatur = 62.290 DM.

Damit ergeben sich in der Summe G/K-Kosten innerhalb des ersten Betriebsjahres von 1 Mio. Fahrzeugen, ausgestattet mit D-b-W inkl. funkt. redundanter FELB-Erweiterung, von 1.300.822 DM, was um 178.502 DM höher ist, als beim Minimal-System. Diese Kostensituation darf jedoch nicht als kaufmännisches „Killer-Kriterium“ für die FELB-Erweiterung betrachtet werden. Vielmehr muß, wie bereits in Abschnitt 5.3, berücksichtigt werden, wieviele Fahrzeuge durch die FELB-Erweiterung dem absorbierenden sicherheitsrelevanten Zustand 11 „entrinnen“.

Würde man pro Fahrzeug 75.000 DM ansetzen, so führt dies zu folgenden Kosten.

Fahrzeug-Kosten = P(11) * 1E6 * 75.000 DM = 799.627.500 DM und damit um 82.635 Mio. DM niedriger als im Minimalsystem.

Faßt man also obige Kosten zusammen, so belaufen sich die „Feld-Kosten“ des D-b-W-Systems mit funktional redundanter FELB-Erweiterung auf 800.928.322 DM. Eine Summe, die um ca. 82.46 Mio. DM bzw. 9,33% niedriger als beim Minimal-System ist.

Mit Blick auf das Bestreben, die Kundenzufriedenheit zu erhöhen, könnten obige Einsparungen als „Feld-“ bzw. Folge-Kosten in weitere Optimierungen des System-konzepts der HW etc. investiert werden. Dies würde unter Berücksichtigung der Überlegungen aus Kap. 5 und 6 zu einer weiteren Optimierung der System-Qualität führen.

6.5 F/V/S/W-Benefit gegenüber dem Minimal-System

Wie Abschnitt 6.3 zu entnehmen war, kann keine der hier vorgestellten FELB-Erweiterungen für sich allein verwandt als optimal hinsichtlich der drei Qualitätsparameter Fehlerwahrscheinlichkeit, Verfügbarkeit und Sicherheit bezeichnet werden.
Zwar erwies sich die HW-Redundanz hinsichtlich der Systemsicherheit gegenüber der funktionalen und analytischen Redundanz überlegen. Mit Blick auf die beiden weiteren Qualitätsparameter Fehlerhäufigkeit und Verfügbarkeit sowie den Faktor „Feld-“ bzw. Folgekosten (siehe insbesondere Abschnitt 6.4), muß jedoch die funktionale Redundanz als guter, wenngleich nicht optimaler Kompromiß vorgezogen werden. Für die hiermit einsparbaren Feld-Kosten können beispielsweise redundante Raddrehzahlsensoren an den Vorderrädern finanziert werden, die ihrerseits wieder erheblich zur Steigerung der Systemsicherheit und -verfügbarkeit beitragen werden (vergleiche Abschnitte 6.1 und 6.2).
Als Optimum bzgl. F/V/S/W erscheint dem Autor eine Fusion aus HW-Redundanz gekoppelt mit funktionaler Redundanz. Inwieweit sich diese hinsichtlich der Produkt- und Entwicklungskosten teure Lösung im Serieneinsatz durchsetzen wird, hängt von einer Vielzahl von Parametern ab, von denen bereits einige, wie etwa die Sicherheitsrelevanz des zu entwickelnden Systems, der Kundennutzen, die Kundenzufriedenheit und die „Feld“- bzw. Folgekosten, in dieser Arbeit angesprochen wurden.

6.6 Streuungen der Komponenten-Zuverlässigkeitskenngrößen und deren Auswirkung auf die System-Qualitätsmerkmale

Die in Abschnitt 4.2.1.1.2 (Bild 4.2) dargestellte Fehlerwahrscheinlichkeit des Lenkradwinkelsensors der Produktionsjahre 1994 und 1995 verdeutlicht, daß die Zuverlässigkeitskenngrößen in einem gewissen Bereich streuen. So ergibt sich für die `94er Produktion als Kehrwert der charakteristischen Lebensdauer eine Ausfallrate von 1,62E-5 1/h. Die Ausfallrate der `95er Produktion hingegen liegt bei 1,37E-5 1/h.

Der Schluß liegt nahe, daß obige Parameterstreuung zur Veränderung der System-Fehlerwahrscheinlichkeit, -Verfügbarkeit, -Sicherheit und –Wirtschaftlichkeit bzw. des jeweiligen kritischen Pfades führen kann. Aus diesem Grund muß es zukünftig das Ziel sein, neben der eigentlichen Angabe einer Verteilungsfunktion, ein Maß für die Konfidenz der statistischen Grössen beizusteuern. In [Ber90] wird hierfür ein Vertrauensbereichs eingeführt. Dieser Vertrauensbereich ist gekennzeichnet durch die Wahrscheinlichkeit, mit der eine Zufallsvariable in diesem Bereich liegt. So bedeutet beispielsweise ein 90%iger Vertrauensbereich, daß in 90 von 100 Fällen die beobachteten Werte in diesem Bereich auftreten. Auf diesem Wege kann ein Min- und Maxwert für die jeweilige Zuverlässigkeits-kenngröße benannt werden. Führt man anschließend innerhalb der Bandbreiten sämtlicher Komponenten-Zuverlässigkeitskenngrößen eine Monte-Carlo-Simulation durch, läßt sich die Streuung der Gesamt-System F/V/S/W bzw. des kritischen Pfades identifizieren.

Bzgl. der Konfidenz der in dieser Arbeit getätigten Aussagen kann zusammengefaßt werden, daß mit steigendem Stichprobenumfang n obiger Vertrauensbereich immer enger wird. Mit Blick auf den Umstand, daß die Pkw-Produktionsstückzahlen in aller Regel 100.000 Einheiten pro Jahr übersteigen, wird die Berücksichtigung der Parameterstreuung nur geringfügige Unterschiede bzgl. der Gesamtsystemqualitätsaussagen ergeben. Dennoch sollte es insbesondere bei Einführung von neuentwickelten Komponenten das Ziel sein, die Komponenten-Zuverlässigkeitskenngrößen schnellstmöglich durch Auswertung von Prüfstanduntersuchungen und Felddaten mit breiter statistischer Basis zu stützen.

An dieser Stelle muß abschließend jedoch nochmals betont werden, daß es das Hauptanliegen der vorliegenden Arbeit ist, eine Methodik zur geschlossenen Bewertung der System-F/V/S/W zur Verfügung zu stellen. Diesem Anspruch tut obige Streuung der Komponenten-Zuverlässigkeitskenngrößen keinen Abbruch. Die Methodik ist in vollem Umfang anwendbar. Eine Ergänzung um Vertrauensbereiche für die Zuverlässig-keitskenngrößen stellt lediglich eine sinnvolle Erweiterung der System-Analyse dar.

7 Zusammenfassung

7.1 Methoden und Tools zur Bewertung der F/V/S/W komplexer Kfz-Systeme

In der vorliegenden Arbeit wurde eine Methodik zur geschlossenen Bewertung der **F**ehlerhäufigkeit, **V**erfügbarkeit, **S**icherheit und **W**irtschaftlichkeit (F/V/S/W) komplexer sicherheitsrelevanter Kfz-Systeme entwickelt und anhand von Beispielen veranschaulicht. Diese Methodik fußt auf einer Fusion von Fehlerbäumen und Markov-Ketten zu hierarchischen Modellen.
Die hierarchische Modellierung erlaubt es, sowohl eine qualitative, wie auch quantitative Systemaussage mit vertretbarem Analyseaufwand zu generieren. Modifikationen innerhalb des Entwicklungsstandes können mit geringem Aufwand in die Systembetrachtungen integriert werden.

Die zentralen Aussagen der F/V/S/W-Analyse mittels hierarchischer Modelle sind:

- Identifikation der F/V/S/W-kritischen Fehler (-moden).
- Bestimmung der Auftretenswahrscheinlichkeit F/V/S-kritischer Ereignisse
- Bestimmung der Anzahl von Fahrzeugen, die während der Mission in F/V/S/W-kritische Systemzustände eintreten.
- Pareto-Analyse der F/V/S/W-kritischen Bauteile und Strukturen des Systems (kritische Pfade).
- Eine Modifikation dieser kritischen Pfade führt zu einer maximalen Verbesserung der F/V/S des Gesamtsystems unter Berücksichtigung des Faktors Wirtschaftlichkeit.
- Noch vor Umsetzung obiger Modifikationen kann die hierarchische Modellierung den Benefit hinsichtlich der Gesamtsystem-F/V/S/W mit geringem Aufwand quantisieren (vergleiche hierzu Kap. 5 und. 6).

Vorzüge der hierarchischen Modellierung gegenüber

a) statischen Methoden, wie der FTA (Fehlerbaumanalyse, **F**ault-**T**ree-**A**nalysis)
   - Systeme mit degraded Modes (Betriebsmoden unterschiedlichen Funktionsumfanges, in die das System infolge eines Fehlers degradiert werden kann) sind auch hinsichtlich ihres Übergangsverhaltens bewertbar.
   - Fehlererkennungs-, -lokalisations- und -behandlungsstrategien sowie die entsprechenden Reaktionszeiten sind modellierbar.
   - Berücksichtigung des Faktors Kosten in einem geschlossenen Modell mit F/V/S.

b) gegenüber der reinen Markov-Ketten-Analyse bzw. anderer zustandsraumorientierter Verfahren wie Petri-Netzen.
   - Reduzierung des Modellierungsaufwandes (Zustandsraumexplosion) durch Modulbildung basierend auf Fehlerbäumen.

Zwingende Voraussetzung für eine korrekte Applikation dieser Methodik auf zukünftige Systeme ist eine saubere Abgrenzung der in der Literatur häufig nicht differenzierten bzw. widersprüchlich behandelten Begrifflichkeiten Fehlerhäufigkeit, Zuverlässigkeit/Verfügbarkeit und Sicherheit. Aus diesem Grund erfolgte in Kap. 2 und 3 eine praxistaugliche Einführung in die Thematik der Zuverlässigkeits- und Sicherheitstheorie.
Wesentliche Etappenziele waren hier die:

- Aufarbeitung der Problematik des Sicherheitsziels bzw. –maßstabes.

- die Darstellung verschiedener FELB-Konzepte zur Erkennung, Lokalisation und Behandlung von Systemfehlern,
- die Präsentation für die F/V/S/W-Analyse geeigneter Methoden und Tools,
- die Präsentation eines Arbeitsplanes zur Bewertung der F/V/S/W
- sowie die Bereitstellung von Zuverlässigkeits- bzw. Sicherheitskenngrößen (Ausfallrate, Weibull-Parameter sowie die in dieser Arbeit definierten FELB-Raten,

die eine seriöse, mit vertretbarem Aufwand durchführbare Systemanalyse erlauben.

7.2 F/V/S/W des D-b-W-Systems

Um die Leistungsfähigkeit der hierarchischen Modellierung zu verifizieren, wurde das noch im Forschungsstadium befindliche Fahrdynamikstabilisierungssystem Drive-by-Wire auf seine F/V/S/W hin untersucht. Mit Blick auf den Wettbewerb innerhalb der Automobilindustrie wurde das hochinnovative System D-b-W in der vorliegenden Arbeit bewußt nur in einer Detaillierung vorgestellt, die für die F/V/S/W-Analyse zwingend erforderlich ist. In einem frühen Entwicklungs- oder gar Forschungsstadium wird eine tiefergehende Kenntnis der Ziel-Hardware etc. ohnehin nicht vorliegen. Dem Zuverlässigkeitsingenieur mag diese Detaillierung ein Anhaltspunkt dafür sein, welches Maß an System-Know-how er sich bei der Analyse eines für ihn neuen Systems aneignen muß.
Vor dem Hintergrund der Problematik eines absoluten Sicherheitsmaßstabes (siehe Abschnitt 2.3), wurde eine vergleichende Bewertung zwischen einem als Minimal-System bezeichneten Systemkonzept sowie mit FELB-Erweiterungen versehenen Systemkonzepten vorgenommen.
Als grundsätzliche Sicherheits-Anforderung an eine FELB-Struktur müssen gefährliche Einfachfehler zuverlässig erkannt und behandelt werden können. Die in dieser Arbeit vorgestellte Methodik der hierarchischen Modellierung ermöglicht die Identifikation dieser Fehler.
Wie sich zeigte, erwiesen sich Softfailures der Raddrehzahlsensorik als kritischer Pfad hinsichtlich der Sicherheit des Minimal-Systems.
Kap. 6 war zu entnehmen, daß eine redundante Raddrehzahlsensorik hinsichtlich der Systemsicherheit die beste FELB-Erweiterung darstellt. Die vorgestellte analytische Redundanz konnte hinsichtlich F/V/S/W nicht überzeugen. Grund hierfür war der Umstand, daß sie auf aufwendigen Modellen fußte, in die eine Vielzahl von Sensorinformationen einfließen. Folglich führten Fehlfunktionen dieser Elemente zum Versagen der Sensorüberwachung.
Mit Blick auf die Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit kann die funktionale Redundanz der Raddrehzahlsensoren als guter Kompromiß bezeichnet werden. Um die Qualität der funktionalen Redundanzüberwachung zu steigern, sollten die beim vorliegenden Konzept verdeutlichten Überwachungslücken minimiert werden. Hierzu ist die Modellierungsgüte zu optimieren. Für die mittels funktionaler Redundanz einsparbaren Feld-Kosten können beispielsweise redundante Raddrehzahlsensoren an den Vorderrädern finanziert werden, die ihrerseits wieder erheblich zur Steigerung der Systemsicherheit und -verfügbarkeit beitragen werden. Dennoch ist mit Verweis auf die Ergebnisse bei den analytischen und HW-Redundanzen eine Erhöhung der Systemkomponenten nur in Ausnahmefällen als sinnvoll zu betrachten, da hierdurch die Fehlerhäufigkeit und Kostensituation negativ beeinflußt wird.

Mit Blick auf obige FELB-Anforderungen ist zusammenzufassen, daß keine der FELB-Erweiterungen für sich alleine als optimal bezeichnet werden kann. Zwecks weiterer Optimierung erscheint dem Autor eine Fusion aus HW-Redundanz, gekoppelt mit funktionaler Redundanz als empfehlenswert. Diese Aussage darf jedoch nicht als pauschale Empfehlung verstanden werden. Vielmehr hängt die Qualität eines FELB-Konzeptes maßgeblich vom zu überwachenden System ab.
Inwieweit sich obige hinsichtlich der Produkt- und Entwicklungskosten teure Fusion beider Redundanz-Konzepte im Serieneinsatz durchsetzen wird, hängt von einer Vielzahl von Parametern an, derer bereits einige, wie etwa die Sicherheitsrelevanz des zu entwickelnden Systems, der Kundennutzen, die Kundenzufriedenheit und die „Feld“- bzw. Folgekosten, in dieser Arbeit diskutiert wurden.
Wie sich in der vorliegenden Arbeit bei der Betrachtung von temporären Fehlern und Mehrfachfehlern zeigte, kann eine 100%ige Erkennung bzw. Behandlung beliebiger Fehler nicht gewährleistet werden. Somit muß ergänzend zur Forderung nach der 100%igen Erkennung von gefährlichen Einfachfehlern das System zusätzlich in der Art ausgelegt sein, daß es robust gegen nicht erkennbare Fehler ist.
Der Nachweis dieser Systemeigenschaft ist vor Serieneinführung eines Massenproduktes wie des Automobils zu erbringen.
Es soll abschließend nochmals betont werden, daß das hier diskutierte Systembeispiel Drive-by-Wire den Reifegrad einer Machbarkeitsstudie aufweist. Bis zum Erreichen des Vorentwicklung- oder gar Serienentwicklungsstandes gewinnt das System gerade mit Blick auf die Systemsicherheit maßgeblich an Qualität. Dennoch konnte gerade dieses noch „unsichere“ System den Nutzen der vergleichenden F/V/S/W-Analyse verschiedener Systemkonzepte bzw. ähnlicher Systeme verdeutlichen. Außerdem wurde deutlich, daß die System-Qualität bereits in einem frühen Entwicklungsstadium berücksichtigt werden sollte.
Es ist jedoch ebenfalls zu betonen, daß von einer F/V/S/W-Vorhersage eines noch in Entwicklung befindlichen Systems nicht erwartet werden darf, daß sich diese Aussage letztendlich bis auf wenige Prozent mit dem in mehreren Jahren im Feld zu beobachtenden Feldausfall- bzw. Beanstandungsverhalten decken wird. Ziel muß es, insbesondere für sicherheitsrelevante Kfz-Systeme sein, die Größenordnung der zu erwartenden Qualität korrekt abzuschätzen.
Der „Unschärfe“ der Zuverlässigkeitsparameter neuentwickelter Komponenten bzw. der zu berücksichtigenden Umgebungsbedingungen und der aus der Unschärfe erwachsenden Annahmen kann in gewissem Umfang durch die „vergleichende“ F/V/S/W-Analyse ähnlicher Systeme begegnet werden.
Grundsätzlich geht die Tendenz in die Richtung, zukünftig bereits beginnend im Forschungsstadium Funktion und F/V/S/W-Belange parallel zu entwickeln. Auf diesem Wege werden sich die Entwicklungszeiten verkürzen, was dem Kunden durch die Optimierung des Preis-/Leistungsverhältnisses kommuniziert werden kann.

7.3 Ausblick

Wie sich in der vorliegenden Arbeit zeigte, bedarf es für eine verläßliche Beurteilung der F/V/S/W komplexer Kfz-Systeme der Erhöhung der Konfidenz, Detaillierung oder im Falle von Zuverlässigkeitsparametern für Software gar der grundsätzlichen Identifikation einzelner Komponentenzuverlässigkeiten.

- In diesem Sinne werden derzeit in enger Zusammenarbeit mit Zulieferern Zuverlässigkeitskenngrößen für Bauteile identifiziert und in geeignetem Format in Datenbanken abgelegt.
- Sollten zukünftige Arbeiten ergeben, daß Softwarefehler einen stochastischen Anteil aufweisen oder grundsätzlich eine Modellierung zulassen, können diese Fehler ebenfalls mit den verwandten bzw. entwickelten Methoden analysiert werden. Die Schnittstellen zur Einbindung der Software-Zuverlässigkeitskenngrößen wurden innerhalb der Fehlerbäume der hierarchischen Modelle in der vorliegenden Arbeit bereits geschaffen.
- Wenngleich in der vorliegenden Arbeit keine FELB-Erweiterung basierend auf Selbsttests untersucht wurde, ist deren Analyse mittels hierarchischer Modellierung dennoch möglich.
- Zwar wurde in dieser Arbeit nur jeweils ein Ansatz für die vorgestellten Redundanzkonzepte diskutiert, jedoch lassen sich die hier vorgenommen Überlegungen auch auf weitere funktionale und analytische FELB-Konzepte zur Überwachung der Gierraten- und Querbeschleunigungssensorik übertragen, die in [Mah94], [Mah95] und [Sti95] entwickelt wurden.

Damit soll abschließend nochmals betont werden, daß es das vorrangige Anliegen des Autors war, dem Entwicklungsingenieur ein praxistaugliches Werkzeug an die Hand zu geben, mit dem er beliebig komplizierte Überwachungsstrukturen hinsichtlich ihrer Qualitätsmerkmale Fehlerhäufigkeit, Verfügbarkeit, Sicherheit und Wirtschaftlichkeit bewerten kann.

8 Anhang

8.1 Anhang A: Literatur/Tools

[And79] Anderson, B., Optimal Filtering, Prentice-Hall-Information and System Sciences Series, 1979

[Ben97] Benzinger, M., Robustes Kalman-Filter zur Detektion von Sensorfehlern, Diplomarbeit, Daimler-Benz AG, 1997

[Ber90] Zuverlässigkeit im Maschinenbau, Bertsch, B., Lechner, G., Springer, 1990

[Bos90] Sensorschaltung, Offenlegungsschrift DE 40 17 843 A1, Offenlegungstag 05.12.91.

[Bos94] FDR - Die Fahrdynamikregelung von Bosch, A. van Zanten, ATZ Automobiltechnische Zeitschrift 96 (1994) 11

[Bos95] Kraftfahr Technisches Taschenbuch, Robert Bosch GmbH, 1995

[Böt93] Verfahren zur Bestimmung eines fahrsituationsabhängigen Lenkwinkels, Böttiger, F., Lorenz, R., Suissa, A., Patentschrift der Daimler-Benz AG, 1993

[Bro84] Bronstein-Semendjajew; Taschenbuch der Mathematik, Verlag Harri Deutsch, 1984

[Coz90] Untersuchung der Fehlertoleranz und Zuverlässigkeit eines Antiblockiersystems, G. Coza, Dissertation Technische Universität München, 1990

[DeL90] DeLaat, J.C.; Merrill, W.C., A Real Time Microcomputer Implementation of Sensor Failure Detection for Turbofan Engines, IEEE Control Systems Magazine, 1990

[Dhi88] Zuverlässigkeitstechnik: Einfluß des Menschen, B.S. Dhillon, VCH Verlagsgesellschaft, 1988

[FMD91] Failure Mode/Mechanism Distributions, Reliability Analysis Center, Department of Defense, USA, 1991

[FTA90] DIN 25 424, Fehlerbaumanalyse, Handrechenverfahren zur Auswertung eines Fehlerbaumes, Beuth Verlag, 1990

[Gae77] Zuverlässigkeit, Mathematische Modelle, W. Gaede, Carl Hanser Verlag, 1977

[Kon77] Definition und Berechnung der Sicherheit von Automatisierungssystemen, R. Konakovsky, Dissertation Universität Stuttgart, 1977

[Kre80] Krebs, V., Nichtlineare Filterung, R. Oldenbourg Verlag, München, 1980

[Kub84] Verfahren und System zum Ableiten von Radgeschwindigkeitsdaten für eine Kraftfahrzeug-Antirutsch-Steuerung, Kubo Jun, Nissan Motor Co, Offenlegungsschrift DE 3418235 A1.

[Kur96] Zuverlässigkeits- und Sicherheitsanalyse eines Sensorfehlererkennungs-, Lokalisations- und Behandlungsalgorithmus, Diplomarbeit bei der Daimler-Benz AG, A. Kurth, 1996

[Leh89] Computer-Aided Failure Mode and Effect Analysis of electronic circuits, M. Lehtela, Microelectron Reliability, Vol. 30, No. 4, 1990.

[Len95] Lenk, R.; Zuverlässigkeitsanalyse von komplexen Systemen am Beispiel Pkw-Automatikgetriebe, Dissertation, Uni-Stuttgart, 1995

[Lof90] Loffeld, O., Estimationstheorie I und II, Oldenbourg Verlag, 1990

[Mah94_1] Mahmoud, R.; Multisensorielles Data-Fusing mit Extended Kalman-Filtern, Universität-GH Siegen, Zentrum für Sensorsysteme, 1994

[Mah94_2] Mahmoud, R.; Intelligente Konzepte zur Gewährleistung von Systemsicherheit: Sensorsignalvalidierung mittels analytischer Redundanz, Bericht, Daimler-Benz, 1994

[Mah95] Mahmoud, R.; Sicherheitskonzepte und Sicherheitssoftware für die Sensorsysteme in Kfz-Applikationen, Projekt D-b-W, Daimler-Benz-AG, 1995

[Mah96_1] Mahmoud, R.; Markov-Ketten zur Evaluierung der Zuverlässigkeit und Sicherheit zukünftiger Kfz-Systeme, Technischer Bericht Nr. 96-0016, Daimler-Benz, 1996

[Mah96_2] Mahmoud, R.; Zwischenbericht zur vergleichenden Fehlerbaumanalyse zweier Bremssysteme, Technischer Bericht Nr. 96-0069, Daimler-Benz, 1996

[Mah97] Mahmoud, R.; Bewertung des Sicherheits-, Zuverlässigkeits-, Verfügbarkeits- und Wirtschaftlichkeitszuwachses von Redundanzkonzepten in Kfz-Systemen mittels Markov-Ketten, Technischer Bericht Nr. 97-0010, Daimler-Benz, 1997

[Mah97_2] Mahmoud, R.; Ergänzungen zur Qualitätssicherungsvereinbarung, Bericht, Daimler-Benz, 1997

[Mar94] Marx, D., Untersuchung zur Erkennung von Sensorfehlern mit Hilfe des Kalman-Filters, Bericht, Forschungsinstitut Mercedes-Benz, 1994

[Mar94_2] Marx, D., Vier-Rad Längsdynamikmodell zur Optimierung des Regleralgorithmus von Drive-by-Wire, Diplomarbeit, Forschungsinstitut Mercedes-Benz, 1994

[Mee92] Transiente Leistungsbewertung und Optimierung rekonfigurierbarer fehlertoleranter Rechnersysteme, H. de Meer, Arbeitsbericht Universität Erlangen/Nürnberg, 1992

[Mer94] Das neue Fahrsicherheitssystem Electronic Stability Program von Mercedes Benz, A. Müller, ATZ Automobiltechische Zeitschrift 96 (1994) 11

[Mey86] Meyna, A.; Handbuch der Sicherheitstechnik, Carl Hanser Verlag, 1985

[Mey91] Meyna, A.; Probabilistische Zuverlässigkeits- und Sicherheitsanalyse für die redundante Steuereinrichtung eines Antiblockiersystems, VDI-Bericht 1009, 1991

[MIL82] MIL-Handbook 217D, 1982

[MSR94] DIN V 19 250, Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, Beuth Verlag, 1994

[Neu96] System Software Reliability Training Course, A.M. Neufelder, Anaheim, 1996

[NWH94] New Weibull Handbook, R. Abernethy, North Palm Beach, Florida, 1994

[NPR95] Nonelectric Parts Reliability Data, Reliability Analysis Center, Department of Defense, USA, 1995

[NUR81] NUREG-0492; Fault Tree Handbook, U.S. Nuclear Regulatory Commision, 1981

[OCo90] O'Connor, P.D.T, Zuverlässigkeitstechnik, VCH-Verlag 1990,.

[Pro88] Prock, J. Signalvalidierung mittels analytischer Redundanz, 1988

[Rat96] Automotive Electronics, Reliability 2000, Okt. '96, R. Rathbone, R. Maier.

[Rei88] Zuverlässigkeitsstrukturen, Modellbildung-Modellauswertung, K. Reinschke, I. Usakov, Oldenbourg Verlag, 1988

[Ric88] Beitrag zur Untersuchung der Verfügbarkeitssicherung an einer Datenvermittlungseinrichtung, A. Richter, Dissertationsschrift Technische Universität Karl-Marx-Stadt, 1988

[Sah96] Sahner, Robin A., Trivedi Kishor; Performance and reliability analysis of computer systems, Kluwer Academic Publishers, 1996

[Sch73] Berechnung der Sicherheit von parallelredundanten Schaltwerken, Wolfgang Schneider, Dissertationsschrift, Technische Universität Braunschweig

[Sch78] Methoden zum Erreichen und zum Nachweis der nötigen Hardware-zuverlässigkeit beim Einsatz von Prozeßrechnern, H. Schüller, Dissertationsschrift, Technische Universität München, 1978

[Sch92] Schneeweiss, W.; Zuverlässigkeitstechnik - von den Komponenten zum System, Datakontext-Verlag, Köln

[Sin95] The Failure Rate of Software: does it exist ? N. Singpurwalla, IEEE Transactions on Reliability, 1995

[Ste96] Steigerwald, M.; Zuverlässigkeits- und Sicherheitsanalyse eines elektronisch geregelten Kfz-Lenksystems mit hydromechanischer Rückfallebene mittels FTA, Diplomarbeit, Daimler-Benz AG, 1996

[Sti95] Stiegler, M., Sensor-Fehlererkennung und -lokalisation mittels Redundanz-konzepten, Diplomarbeit, Daimler-Benz-AG, 1995

[Sui94] Suissa, A, Böttiger, F., Ein robustes Kalman-Filter zur indirekten Bestimmung des Schwimmwinkels und anderer Fahrdynamikgrößen eines Fahrzeugs, Technischer Bericht, Daimler-Benz AG, 1994

[Uhl97] Entwurf und Implementierung eines Software-Tools zur Aufbereitung von Basisdaten für Zuverlässigkeits- und Sicherheitsstudien zukünftiger Fahrzeugsysteme, Diplomarbeit, Daimler-Benz-AG, 1997

[Van93] Zustandsschätzerschemen zur Fehlererkennung, deren Zuverlässigkeit und Anwendung auf den spurgeführten Omnibus, D. van Schrick, Dissertations-schrift, Uni-GH-Duisburg

[VDE080] Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, DIN V VDE0801, 1990.

[VDI88] Trier, H.; Methode zur Planung von Systemsicherheit beim Einsatz von Elektronik im Kfz, VDI Bericht Nr. 687, Köln, 1988

[Vog93] Vogel, T., Systemsicherheit, Technischer Bericht, Daimler-Benz AG, 1993

[Wal86] Walker, Bruce K.; Approximate evaluation of reliability and availability via perturbation analysis, Department of Aeronautics & Astronautics; Massachusetts Institute of Technology, 1986

[Wei93] Weiß, G., Fehlertolerante Motoransteuerung, Diplomarbeit, Daimler-Benz AG, 1993

[Win93] Eine hierarchische, offene Elektronikstruktur für die flexible Auslegung übergeordneter Fahrzeugfunktionen, Dr. Winner, VDI-Bericht, 1993

[Zom92] Bestimmung des Schwimmwinkels mit regelungstechnischen Methoden, Z. Zomotor, Diplomarbeit, Daimler-Benz AG, 1992

[Zuv40] DIN 40041, Zuverlässigkeit, Begriffe, Beuth Verlag, 1990

Tools

- ALLSIM: Visualisierungsoberfläche zur Onboard-Darstellung von Echtzeitdaten im Fahrzeug bzw. Nachuntersuchung im Labor. Eigenentwicklung der Daimler-Benz AG
- Fault-Tree 7.0; Isograph/ITEM-Software, Hampshire, England
- MKV 2.0; Isograph/ITEM-Software, Hampshire, England
- Weibull-Smith; Fulton Findings, Torrance, Ca 90502, USA

8.2 Anhang B: Termini der Zuverlässigkeits- und Sicherheitstheorie

Die folgenden Definitionen sind in Kurzform [Sch77 bzw. VDE08] entnommen. Details hierzu finden sich außerdem in [Din40041].

Ausfall (failure): Die Beendigung der Fähigkeit einer Betrachtungseinheit, eine geforderte Funktion zu erfüllen. Der Ausfall ist ein Ereignis, im Gegensatz zum Fehler, der einen Zustand bezeichnet.

Ausfall- bzw. Fehlerwahrscheinlichkeit P: Wahrscheinlichkeit einer Betrachtungseinheit, bis zu einem vorgegebenen Zeitpunkt auszufallen bzw. einen Fehler aufzuweisen.

Ausfall- bzw. Fehlerwahrscheinlichkeitverteilung F(t): Zusammenhang zwischen der Ausfall- bzw. Fehlerwahrscheinlichkeit und der Zeit.

Ausfallrate l**(t)**: Bedingte Wahrscheinlichkeitsdichte dafür, daß ein Bauteil bis zum Zeitpunkt t+dt ausfällt, vorausgesetzt, es hat den Zeitpunkt t überlebt. Bei Exponential-verteilung des Ausfallverhaltens über der Zeit ist die Ausfallrate der Kehrwert des Erwartungswertes der Lebensdauer.

Common-Cause-Error: Ereignisse und Komponentenausfälle, die auf eine gemeinsame Ursache zurückzuführen sind.

Diversität: Redundante Implementierung einer Nutzfunktion durch mehrere verschieden-artige (z.B. unterschiedliche physikalische Prinzipien) entworfene Subsysteme.

Drift: Eine nicht sprunghafte („schleichende“) Abweichung des Istverhaltens einer Komponente vom (fehlerfreien), als tolerierbar spezifizierten, Sollverhalten über der Zeit.

Fail-Safe-Eigenschaft: Fähigkeit eines technischen Systems, beim Auftreten bestimmter Ausfälle im sicheren Zustand zu bleiben oder unmittelbar in einen anderen sicheren Zustand überzugehen.

Fehler (fault, defect, error, mistake): Im englischen Sprachgebrauch wird unterschieden zwischen

- fault: unzulässige Eigenschaft, die das Versagen einer Ausführungseinheit bewirken kann. So z. B. inadäquate Spezifikation, algorithmische Unzulänglichkeit, fehlerhafter Entwurf oder Auswirkung eines Hardwareausfalls aufgrund von Alterung.
- defect: unzulässige Abweichung eines Merkmals. Soll hier nicht weiter betrachtet werden.
- error: Abweichung zwischen dem berechneten Wert und dem wahren oder theoretisch richtigen Wert.
- mistake: Menschliche Handlung, die ein unerwünschtes Ereignis zur Folge haben kann. Soll nur als Ursache für das Auftreten eines Software-Faults berücksichtigt werden.

In der vorliegenden Arbeit werden die beiden im Englischen als fault und error bezeichneten „Fehlerarten“ verwandt.

Fehlerbaumanalyse (FTA, Fault Tree Analysis): Analytisches Verfahren, um Kombinationen von Komponentenausfällen zu finden, die zu einem Systemversagen führen und um diese bzgl. der Auftretenswahrscheinlichkeit zu bewerten.

Fehlersicherheit (fail-safe): siehe Abschnitt 2.3

Fehlertoleranz (fault tolerance): siehe Abschnitt 2.3

FELB/FDIR: **F**ehler**e**rkennung, -**l**okalisation und -**b**ehandlung / **f**ault **d**etection **i**dentification and **r**ecovery: siehe Abschnitt 2.3.

FMEA: siehe DIN 25 448

G/K: Garantie und Kulanz

Gefahr: Ist eine Sachlage, bei der das Risiko größer ist als das Grenzrisiko. Siehe auch Abschnitt 2.1

Grenzrisiko: Ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes. Es ist i.A. nicht quantitativ erfaßbar, sondern wird in der Regel indirekt durch sicherheitstechnische Festlegungen beschrieben. Oftmals wird es auch technisch historisch festgelegt. So wird eventuell der Absturz von 2 Flugzeugen pro Jahr mit je 50 Insassen als Grenzrisiko akzeptiert, wenn diese Zahlenwerte in der Vergangenheit nie unterboten werden konnten. Hier wird auch deutlich, daß diese Historie stark länder- bzw. kulturabhängig ist.

Hardfailure(s): Hierunter sind im weiteren Verlauf der Arbeit Fehlfunktionen der betrachteten Systemkomponenten zu verstehen, die zu einem massiven Abweichen der Funktionalität vom Sollverhalten führen.
Bei Sensoren fallen hierunter zum Beispiel Totalausfälle, Verlassen des plausiblen Wertebereichs bzw. Meßbereichs bedingt durch Offsets oder starke Drifterscheinungen.

Kanal: Liegt eine Information nicht redundant, also nur einmalig vor, spricht man von einer „Ein-Kanaligkeit“. Bei n vorhandenen gleichen Informationsträgern spricht man von n-Kanaligkeit bzw. (n-1)-facher Redundanz.

Lebensdauer: Für die einzelne, nicht instandsetzbare Betrachtungseinheit die beobachtete Zeitspanne vom Beanspruchungsbeginn bis zum Ausfallzeitpunkt.

Mittlerer Ausfallabstand (**MTBF**, **m**ean **t**ime **b**etween **f**ailure): Erwartungswert für den Abstand zwischen zwei Ausfallzeitpunkten. Bei konstanter Ausfallrate entspricht die MTBF dem Kehrwert der Ausfallrate - für nicht instandsetzbare Betrachtungseinheiten dem Erwartungswert der Lebensdauer.

MTTF (**m**ean **t**ime **t**o **f**ailure): Erwartungswert der Lebensdauer.

MTTFF (**m**ean **t**ime **t**o **f**irst **f**ailure): entspricht bei reparierbaren Systemen dem Erwartungswert der Zeit vom fehlerfreien Zustand bis zum ersten Fehler.

Qualität: Beschaffenheit einer Einheit bzgl. ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen. Oder Gesamtheit von Merkmalen und Merkmalswerten einer Einheit, bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse (Qualitätsanforderungen) zu erfüllen. Damit sind Fehlerfreiheit, Zuverlässigkeit/Verfügbarkeit und Sicherheit Qualitätsmerkmale.

Redundanz: Vorhandensein von mehr als für die Ausführung der vorgesehenen Aufgaben an sich notwendigen Mittel. Wird eine Komponente n-fach installiert, spricht man von (n-1)-facher Redundanz. Siehe auch Kanal/n-Kanaligkeit.

Risiko: siehe Abschnitt 2.1. Risiko = H*S, mit H = erwartete Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses; S = das beim Ereigniseintritt zu erwartende Schadensausmaß.

Sicherheit: Die Sicherheit einer Betrachtungseinheit ist ihre Fähigkeit, innerhalb der vorgegebenen Grenzen während einer gegebenen Zeitdauer keine Gefährdung der zu schützenden Einheit (Leben, Gesundheit, Maschinen usw.) zuzulassen. Darüberhinaus ist Sicherheit als die Sachlage definiert, bei der das Risiko nicht größer ist, als das Grenzrisiko. Damit ist die Sicherheit das Komplement der Gefahr.
Ein System ist hinsichtlich seiner Sicherheit noch funktionsfähig, wenn ein die Zuverlässigkeit beeinträchtigender Ausfall keine gefährlichen Auswirkungen haben kann.

Sicherer Zustand: Ein Zustand des Systems, von dem keine Gefahr ausgeht.

Sicherheitskenngrößen: siehe Zuverlässigkeitskenngrößen und Kap. 2, 3 und 5

Sicherheitskritischer Ausfall/Zustand: Ausfall/Zustand, der möglicherweise die Gefahr der Verletzung von Personen, beträchtlichem Sachschaden oder sonstige, nicht akzeptierbare Folgen mit sich bringt.

Softfailure(s): Hierunter sind Fehlfunktionen, nicht Ausfälle einer Komponente zu verstehen, die innerhalb der Spezifikationen liegen. Bei Sensoren fallen hierunter zum Beispiel geringfügige Abweichungen vom Sollverhalten, die jedoch nicht zum Verlassen des Meßbereichs bzw. zu unplausiblen Werten führen. Ursachen können geringfügige Offsets oder Drifterscheinungen sein. Siehe auch **Hardfailure(s)**.

Verfügbarkeit: Die Wahrscheinlichkeit, ein System zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand anzutreffen.

Zuverlässigkeit: Fähigkeit einer Betrachtungseinheit, innerhalb der vorgegebenen Grenzen denjenigen durch den Verwendungszweck bedingten Anforderungen zu genügen, die an das Verhalten ihrer Eigenschaften während einer gegebenen Zeitspanne gestellt werden. Die Zuverlässigkeit ist eine Wahrscheinlichkeit und Unterbegriff der Qualität. Teil der Qualität im Hinblick auf das Verhalten der Einheit während oder nach vorgegebenen Zeitspannen bei vorgegebenen Anwendungsbedingungen.

Zustand: Beschaffenheit einer Einheit zum Betrachtungszeitpunkt.

Zuverlässigkeitskenngrößen/-parameter: Größen zur Kennzeichnung der Wahrscheinlichkeitsverteilung der Zuverlässigkeit. Als „destruktiv“ werden Zuverlässigkeitskenngrößen bezeichnet, die das Ausfallverhalten beschreiben. Hieruntern fallen z.B. die Ausfallrate, -häufigkeit, MTBF, MTTF. Als „konstruktiv“ werden Zuverlässigkeitskenngrößen bezeichnet, die der Onboard- bzw. Offboard-Reparatur/Instandsetzung zuträglich sind (Fehlererkennungsrate, Reparaturrate etc.). Auch wenn beispielsweise die Übergangsrate in einen sicherheits- oder verfügbarkeitsrelevanten Zustand entsprechend als Sicherheits- oder Verfügbarkeitskenngröße bezeichnet werden könnte, sollen sie unter dem Begriff Zuverlässigkeitskenngröße zusammengefaßt werden.

8.3 Anhang C: Formelverzeichnis / Abkürzungen / Fahrzeugparameter

a_x	Längsbeschleunigung im Fahrzeugschwerpunkt (siehe Kap. 4)
a_y	Querbeschleunigung im Fahrzeugschwerpunkt (siehe Kap. 4)
a_{yh}	Querbeschl.-Sensor/-information im hinteren Teil des Fahrzeugs (siehe Kap. 4)
a_{ym}	Mittlere(r) Querbeschleunigungssensor/-information (siehe Kap. 4)
a_{ysp}	Querbeschleunigungsinformation im Fahrzeugschwerpunkt (siehe Kap. 4)
a_{yv}	Querbeschl.-Sensor/-information im vorderen Teil des Fahrzeugs (siehe Kap. 4)
A	Systemmatrix des Kalman-Filters (siehe Kap. 4)
B	Steuermatrix des Kalman-Filters (siehe Kap. 4)
BLS/BS	Redundanter **B**rems**l**icht**s**chalter (siehe Kap. 4)
C	Beobachtungsmatrix des Kalman-Filters (siehe Kap. 4)
CAN	Controll Area Network (siehe [Bos95])
CCF	Common-Cause-Failure (siehe Anhang B)
C-K-Gl	**C**hapman-**K**olmogorov-**Gl**eichung (Abschnitt 3.2.1.1)
D-b-W	Drive by Wire (Fahrdynamikregelungssystem, siehe Kap. 4)
DK	**D**rossel**k**lappe
DOD	Department of Defense (siehe Abschnitt 3.1.2.3.2)
ETA	**E**vent-**T**ree-**A**nalysis (Ereignisbaumanalyse)
F(t)	Fehler-, Ausfallwahrscheinlichkeit (siehe Abschnitt 2.2.1), rel. Häufigkeit
FB	Fehlerbehandlung (-smodul, siehe Abschnitt 2.3)
FDIR	**F**ault **D**etection **I**solation and **R**ecovery
FE	Fehlererkennung (-smodul, siehe Abschnitt 2.3)
FL	Fehlerlokalisation (-smodul, siehe Abschnitt 2.3)
FMD	**F**ailure-**M**ode/Mechanism and **D**istribution (siehe Abschnitt 3.1.2.3)
FMEA	**F**ailure **M**ode and **E**ffect **A**nalysis [DIN 25448]
F/V/S/W	Qualitätsparameter **F**ehlerwahrscheinlichkeit, **V**erfügbarkeit und **S**icherheit sowie die **W**irtschaftlichkeit im Sinne der Entwicklungs-, Garantie- und Kulanz-Kosten etc. eines Produktes/Systems. Siehe auch Abschnitt 2.1.
FTA	**F**ault-**T**ree-**A**nalysis (Fehlerbaumanalyse)
g	Gravitationskonstante [m/s^2]
G-/K-Kosten	**G**arantie- und **K**ulanz-Kosten
GLR	**G**eneralized **L**ikelihood-**R**atio. Stochastisches Verfahren zur Signalvalidierung mittels analytischer Redundanz [Pro88].
Generalized **L**ikelihood-**R**atio-Test (GLR) [Pro88]	
h	Hour, Stunde
HA	Hinterachs(e)
HF	Hardfailure(s)
HW	Hardware
i.O.	**I**n **O**rdnung (fehlerfrei)
$l_{h,v}$	Abstand Fahrzeugschwerpunkt zur Hinter- bzw. Vorderachse (siehe Kap 4)

$l_{a_{y_{v,h,ges}}}$	Entspricht näherungsweise dem Abstand vom Fahrzeugschwerpunkt zum vorderen, hinteren Querbeschleunigungssensor bzw. dem Abstand zwischen beiden Sensoren.
LSB	least significant bit
m	Fahrzeugmasse
MTBF	**M**ean **T**ime **B**etween **F**ailure (siehe Anhang B)
MTTD	**m**ean **t**ime **t**o **d**etect, siehe auch Fehlererkennungsrate ε, (siehe Abschnitt 3.2.1.2.2)
MTTL	**m**ean **t**ime **t**o **l**ocate, siehe auch Fehlerlokalisationsrate χ (siehe Abschnitt 3.2.1.2.2)
MTTO	**m**ean **t**ime **t**o rec**o**ver, siehe auch Onboard Fehlerbehandlungsrate ζ (siehe Abschnitt 3.2.1.2.2)
NPRD	**N**onelectric **P**arts **R**eliability **D**ata (siehe Abschnitt 3.1.2.3)
p	Zustands-Aufenthaltswahrscheinlichkeit zum Zeitpunkt t
p_i	Startwahrscheinlichkeit im Zustand i
p_m	Mittlere Zustands-Aufenthaltswahrscheinlichkeit innerhalb eines Jahres
PSIP	ψ (Gierrate)
ppm i.d.1.J.	ppm innerhalb des ersten Betriebsjahres
ppm/Jahr	relative Fehlerhäufigkeit bei einer Referenzmenge von 1Millionen Einheiten. Als Betrachtungszeitraum ist hier das erste Jahr nach Produktion/Zulassung des Fahrzeugs bzw. der Einheit gewählt worden. Diese Angabe darf nur bei Bauteilen konstanter Ausfallrate als „pro“ Jahr gelesen werden.
$\underline{Q}$	Intensitätsmatrix (siehe Chapman-Kolmogorov-Gleichung, Abschnitt 3.2). Um Verwechselungen mit der Unverfügbarkeit „Q“ zu vermeiden, wird diese Matrix unterstrichen dargestellt.
Q	Unverfügbarkeit
r	Radius [m], aber auch Fehlerrate [1/h], in den Tools FTA, MKV
R(t)	Zuverlässigkeit (siehe Abschnitt 2.2.3), rel. Häufigkeit
Rd	**R**ad**d**rehzahl (-sensor)
RFE	**R**ück**f**all**e**bene (Notlauf, Sicherer Zustand, siehe Abschnitt 4.1)
s	Sekunde
SF	Softfailure(s)
SIS	Die softwaremäßige Realisierung der FELB wird unabhängig von der Schwere des Fehlers, den das betreffende Modul erkennt, lokalisiert oder behandelt als **Si**cherheits**s**oftware (SIS) bezeichnet.
SW	Software
SWS	**S**chwimm**w**inkel**s**chätzer (siehe Abschnitt 4.2.3.1.1)
t	Betrachtungs- bzw. Missionsdauer [h] (siehe Abschnitt 3.1.2.8)
t_0	Ausfallfreie Zeit
$t_{Durchschnitt}$	durchschnittliche Missionsdauer/Jahr „$t_{Durchschnitt}$“ eines Pkw = 300 Stunden/Jahr (siehe Abschnitt 3.1.2.8)
TF	Temporäre Fehler (siehe Abschnitt 4.2.1.1.1)
VA	Vorderachs(e)
$Z_{1..3}$	Zeitfaktoren zur Berücksichtigung unterschiedlicher Komponentenoperations-dauern (siehe Abschnitt 2.2.7)

λ	Ausfallrate [1/h] (siehe Abschnitt 3.1.2.2)
$\lambda_{FE\text{-}Modul}$	Fehlalarmrate [1/h] (siehe Abschnitt 3.2.1.2.2)
$\lambda_{FL\text{-}Modul}$	Falschlokalisationsrate [1/h] (siehe Abschnitt 3.2.1.2.2)
$\lambda_{FB\text{-}Modul}$	Falschbehandlungsrate [1/h] (siehe Abschnitt 3.2.1.2.2)
β	Schwimmwinkel (siehe Kap. 4)
δ	Lenkwinkel am Rad (siehe Kap. 4)
δ_{LRW}	Lenkradwinkel (siehe Kap. 4)
ε	Fehlererkennungsrate [1/h] = 1/MTTD (**m**ean **t**ime **t**o **d**etect), (siehe Abschnitt 3.2.1.2.2)
χ	Fehlerlokalisationsrate [1/h] = 1/MTTL (**m**ean **t**ime **t**o **l**ocate), (siehe Abschnitt 3.2.1.2.2)
ζ	Onboard Fehlerbehandlungsrate [1/h] = 1/MTTO (**m**ean **t**ime **t**o rec**o**ver), (siehe Abschnitt 3.2.1.2.2)
μ	Reparaturrate [1/h] (siehe Abschnitt 3.2.1.2.2)
ν	Werkstatterreichensrate = 1/MTTS (**m**ean **t**ime **t**o reach **s**ervice) [1/h] (siehe Abschnitt 3.2.1.2.2)
$\pi(t)$	Zustandsaufenthaltswahrscheinlichkeitsvektor der Markov-Kette (siehe Abschnitt 3.2.)
$\pi_i(t)$	Aufenthaltswahrscheinlichkeit des Systems zum Zeitpunkt t im Zustand i (siehe Abschnitt 3.2.)
$\omega_{Rd\text{-}Sensor\text{-}VL}$	Sensierte Raddrehzahl des Rades vorne links [1/s] (siehe Kap. 4)
$\dot{\psi}$	Gierrate des Fahrzeugs [1/s] (siehe Kap. 4)

8.4 Anhang D: Vorteile und Nachteile verschiedener Fehlererkennungsstrategien

Plausibilitätskontrolle

Prinzipielle Vorteile:
- Robustheit, da nur Hardfailures detektiert werden müssen. Kurzschlüsse, Leerläufe oder massives Verlassen des Meßbereiches können, insbesondere bei Sensorik, bereits heute durch entsprechende Eingangsbeschaltungen detektiert werden.
- Mit geringem HW- bzw. SW-Aufwand realisierbar.

Prinzipieller Nachteil:In der Regel keine Überwachbarkeit von Softfailures möglich.

Eigenüberprüfung

Prinzipielle Vorteile:
- Ist meist darauf ausgerichtet, sowohl Hard- wie auch Softfailures zu detektieren.
- Arbeitet sehr zuverlässig.

Selbsttest

Prinzipielle Nachteile:
- Ist zumeist mit erheblichem HW-Aufwand im Sensor verbunden. Bedingt durch die Zunahme an HW-Komplexität steigt die Fehleranfälligkeit bzw. Fehlerhäufigkeit.
- Es ist sicherzustellen, daß die HW- bzw. SW-Umfänge, die der Komponente für die Fähigkeit des Selbsttests hinzugefügt wurden, auch überwachbar sind.
- Wie man in Kap. 5 feststellen wird, ist auch beim Selbsttest nicht absicherbar, daß alle Fehler erkannt werden.

Hardwareredundanz

Prinzipielle Vorteile:
- Mittels einfacher Redundanz können zuverlässig Hard- und Softfailures innerhalb eines der beiden Kanäle detektiert werden. Bei Verwendung diversitärer Redundanz sind sogar systematische Fehler detektierbar.
- Arbeiten sehr zuverlässig.

Prinzipielle Nachteile:
- Sind bedingt durch die n-Kanaligkeit der n-1-fachen Redundanz mit erheblichem HW-Aufwand (Platz, Gewicht, Geld) verbunden.
- Bedingt durch die Zunahme an HW-Komplexität steigt die Fehleranfälligkeit bzw. Fehlerhäufigkeit des resultierenden n-kanaligen Sensorsystems.
- Meist wird ein Voter benötigt [Vog93], der seinerseits fehlertolerant sein sollte, was zu einem weiteren Anwachsen an HW führt.

Fremdüberprüfung

Prinzipielle Vorteile:
- Bei entsprechender Modellgüte Bestimmbarkeit von Softfailures. Systematische Fehler sind somit auch erkennbar.
- Meist kann auf zusätzliche HW (Sensorik) verzichtet werden, was sich vorteilhaft auf Gewicht, Platz und Kosten auswirkt.
- Durch die Einsparung an HW kann die Gesamtsystemzuverlässigkeit erhöht werden.

Funktionale bzw. analytische Redundanz

Prinzipielle Nachteile:
- Modellierungsfehler schliessen die zuverlässige Detektion kleinster Softfailures aus.
- Um Softfailures erkennen zu können, sind komplexe Modelle vonnöten. Diese meist durch SW-realisierten Redundanzen weisen häufig Modellierungsfehler auf, die eine Detektion von Kleinstfehlern unmöglich macht.
- Mitunter hoher Entwicklungs- und Softwareaufwand.
- Jedoch kann für komplexe Systeme eine allgemeingültige Bewertung der FELB, basierend auf funktionalen bzw. analytischen Redundanzkonzepte, nach Meinung des Autors nicht applikationsunabhängig vorgenommen werden.
- Ein Nachweis der Zuverlässigkeit der Fehlererkennung bzw. Stabilität des Überwachungsalgorithmus ist, insbesondere bei Kalman-Filtern sehr aufwendig und kann für nichtlineare Modelle in aller Regel nicht eindeutig erfolgen.

8.5 Anhang E: Auswirkungen der Fehlermöglichkeiten der D-b-W-Komponenten auf das Systemverhalten des Minimal-Systems

Auswirkungen der in Kap. 4 detaillierten Fehlermöglichkeiten der D-b-W-Komponenten auf das Verhalten des betreffenden Systems.

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Abs. LRW-Sensor	HF	HF-FE-Modul FE-R.: Gl. 4-24	FE kommt FL gleich	D-b-W in RFE überführen FB-R.: Gl. 4-28	Fehler wirkt sich verfügbarkeitskritisch aus. Bis zur FELB (6 Zyklen) ist er auch sicherheits-kritisch, da beispielsweise im Moment der Initiali-sierung des inkr. LRW-Sensors ein fehlerhafter Lenkwinkel weiterverarbeitet wird. Aufgrund der angenommenen 100%igen-FELB ist der Fehler jedoch nach der FB nicht mehr als sicherheits-kritisch anzusehen. Dieser transiente Sach-verhalt kann in der FTA nur bedingt über die Modellierung temporärer Fehler berücksichtigt werden. **Top-Event: B** Im Rahmen der Detailanalyse via hierarchischer Modellierung (Abschnitt 5.3) wird die Reaktionszeit der FELB über einen „sicher-heitsrelevanten“ Zwischenzustand modelliert, der nach der Fehlererkennungszeit (siehe Gl. 4-24) wieder verlassen wird. Der sicherheitsrelevante Zustand ist also nicht absorbierend (Hier wird ein wesentlicher Vorzug der detaillierten dynamischen Modellierung mittels MKA ersichtlich). Nach der Onboard-FB Offboard-FB einleiten: • Rote Warnlampe aktivieren. Ablegen der Fehlermeldung im Diagnosespeicher • $\nu_{Fahrer\text{-}Rot}$: Gl. 4-30 • MB-Service und Offboard-Reparaturrate gemäß Gl. 4-31 und 4-32
	SF	Selbstüber-wachung FE-R.: Gl. 4-26	FE kommt FL gleich	Identisch HF	Siehe HF, jedoch führt eine veränderte Fehler-erkennungsrate aus dem sicherheitsrelevanten Zustand. **Top-Event: B**
	TF	Nicht möglich ⇒ Mißalarm	-	-	Mit Blick auf die Sicherheitsrelevanz des D-b-W wird im Sinne der pessimistischen Analyse davon ausgegangen, daß TF nicht erkennbar sind (Abschnitt 4.2). Bis zum Nachweis der Robustheit des D-b-W-Reglers gegen diese Fehler, wird ferner angenommen, daß sie sicherheitskritische Auswirkungen haben. **Top-Event: C** Zwar böte die MKA die Möglichkeit, den temporären Fehler in der Art zu modellieren, daß ein sicherheitskritischer Zustand über die TF-Rate eingenommen und nach spätestens 6 Zyklen wieder verlassen wird, jedoch muß bis zum Nachweis der Robustheit des Reglers davon ausgegangen werden, daß obiger Fehler im Sinne von Kap. 2 ein Risiko darstellt. Im Sinne der pessimistischen Analyse sei deshalb davon ausgegangen, daß sämtliche TF absorbierender Natur sind.

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Inkr. LRW-Sensor	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Überführen in RFE FB-R.: Gl. 4-28	Siehe HF des abs. LRW-S.
	SF	FE über abs. LRW-Sensor FE-R.: Gl. 4-27	Bei Fehler-freiheit des abs. LRW-Sensors: FE ≡ FL	Überführen in RFE FB-R.: Gl. 4-28	Siehe SF des abs. LRW-S. Strenggenommen muß hier die Fehlerfreiheit des abs. LRW-Sensors vorausgesetzt werden. Da sein Versagen jedoch im wesentlichen erkannt und durch RFE-Übergang behandelt wird, ist hier eine detaillierte Modellierung der zeitlichen Reihenfolge des Zweifachfehlers nicht notwendig.
	TF	Nicht möglich ⇒ Mißalarm	-	-	Siehe TF des abs. LRW-S.
Gier-raten-Sensor	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Überführen in RFE FB-R.: Gl. 4-28	Siehe HF des abs. LRW-S.
	SF	Selbstüber-wachung FE-R.: Gl. 4-25 Siehe jedoch Fahr-manöver-abhängig-keit	FE kommt FL gleich	Überführen in RFE FB-R.: Gl. 4-28	Sofern die Onboard-Fehlerbehandlung eingeleitet werden konnte (siehe Überwachbarkeit), folgt anschließend die offboard-Fehlerbehandlung (siehe HF des abs. LRW-S). Als Maß für die Aufenthaltswahrscheinlichkeit im „nicht überwachbaren Fahrdynamikbereich“ wird das zeitinvariante Verhältnis von ABS-Bremsungen zu herkömmlichen Bremsungen verwandt. $\ddot{U} = \frac{10.000\ \text{ABS} - \text{Br.}}{250.000\ \text{herk.Br.}} = 1/25$ Dieses Verhältnis wird im Sinne eines Zeitfaktors in die SF-Rate einbezogen (siehe Abschnitt 3.1.2.8): $\lambda_{\text{SF}-\text{Gier}-\text{S. nicht überwachbar}} = \ddot{U} \cdot \lambda_{\text{SF}-\text{Gier}-\text{S.}}$ $\lambda_{\text{SF}-\text{Gier}-\text{S. überwachbar}} = (1-\ddot{U}) \cdot \lambda_{\text{SF}-\text{Gier}-\text{S}}$ **Top-Event: B bzw. C** (im nicht überwachbaren Fahrdynamikbereich)
	TF	Nicht möglich ⇒ Mißalarm	-	-	Siehe TF des abs. LRW-S.

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
$a_{y\ v,h}$	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Überführen auf RG3 FB-R.: Gl. 4-28	Fehler führt lediglich zur Degradation in die Regelstufe RG3. Hier ist, wenn auch mit reduzierter Regelgüte, nachwievor elektronischer Regelbetrieb möglich. **Top-Event: A** Bzgl. der hierarchischen Modellierung etc. sei auf HF des absoluten LRW-Sensor verwiesen. Weitere Kommentare zur FB: • Längsgeschwindigkeit bei geringem Schlupf über: $v_X = \frac{v_{Rad_{vl}} + v_{Rad_{vr}}}{2} \cdot \cos\delta_{Rad}$ mit $v_{Rad_i} = \omega_{Rad_i} \cdot r_{dyn}$ Nach der Onboard-FB Offboard-FB einleiten: • Gelbe Warnlampe aktivieren • Ablegen der Fehlermeldung im Diagnosespeicher • $v_{Fahrer\text{-}Gelb}$: Gl. 4-29 • Offboard-Reparaturrate gemäß Gl. 4-32
	SF	Nicht möglich ⇒ Mißalarm	-	-	**Top-Event: C** In hierarchischer Modellierung Übergang in absorbierenden sicherheitskritischen Zustand.
	TF	Siehe SF	-	-	Siehe TF des abs. LRW-S.
a_x	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Degradation auf RG 2 FB-R.: Gl. 4-28	Fehler führt lediglich zur Degradation in die Regelstufe RG2. Hier ist, wenn auch mit reduzierter Regelgüte, nachwievor elektronischer Regelbetrieb möglich. **Top-Event: A** Weitere Details zur FELB siehe HF $a_{y\ v,h}$-Sensorik
	SF	Nicht möglich ⇒ Mißalarm	-	-	**Top-Event: C** In hierarchischer Modellierung Übergang in absorbierenden sicherheitskritischen Zustand.
	TF	Nicht möglich ⇒ Mißalarm	-	-	Siehe TF des abs. LRW-S. Auswirkungen des Fehlers auf Schwimmwinkelschätzer sind zukünftig zu untersuchen. Derzeit wird davon ausgegangen, daß TF nicht robust vom System abgefangen werden.
Vorder-Achs-Rd.Sen-soren	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	D-b-W in RFE überführen FB-R.: Gl. 4-28	D-b-W in RFE überführen, da die Längs-geschwindigkeit nicht ausreichend über die Raddrehzahlsensorik der angetriebenen Hinter-achse bestimmt werden kann (Schlupf). Fehler wirkt sich somit sowohl auf die Fehlerhäufigkeit, als auch auf die Verfügbarkeit negativ aus. **Top-Event: B** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF des abs. LRW-Sensors

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Hinter-Achs-Rd.Sen-soren	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Degradation auf RG 2 FB-R.: Gl. 4-28	Fehler wirkt sich weder verfügbarkeits- noch sicherheitskritisch aus, da die Längs-geschwindigkeit über die Vorderräder hin-reichend genau bestimmt werden kann. **Top-Event: A** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF $a_{y\,v,h}$-Sensorik
VA- u. HA-Rd.-Sen-soren	SF	FE im Minimal-System nicht möglich	-	-	**Top-Event: C** In hierarchischer Modellierung Übergang in absorbierenden sicherheitskritischen Zustand.
	TF	Nicht möglich ⇒ Mißalarm	-	-	Siehe TF des abs. LRW-S.
BLS, Brems-Drucks., u. Drossel-klappen-poten-tiometer.	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Im Minimal-System: gelbe Warnlampe FB-R.: Gl. 4-28	Solange der Schwimmwinkel-Schätzer korrekt funktioniert, wirken sich die hier beschriebenen Fehlfunktionen nicht negativ auf das D-b-W-System aus. Im Minimal-System hat diese Sensorik keine Auswirkungen auf das System-verhalten, weswegen es keiner Onboard-Degradation bedarf. Fehler wirkt sich nur auf die Fehlerhäufigkeit aus. Geht man davon aus, daß der SW-Schätzer durch einen Sensorfehler ausfällt, würde es sich hier bereits um den zweiten Sensorfehler handeln. Dies übersteigt die angestrebte Betrachtungstiefe, weswegen die Zuverlässigkeitskenngrößen nicht in die quantitative F/V/S/W-Analyse des Minimal-Systems eingespeist werden. **Top-Event: Qualitativ Top-D zuordenbar, aber hier außerhalb Betrachtungstiefe** Weitere Details zur Offboard-FB siehe HF $a_{y\,v,h}$-Sensorik.
	SF/TF	Nicht möglich ⇒ Mißalarm	-	-	Mit Verweis auf obige Kommentare zu HF der Sensorik außerhalb der Betrachtungstiefe. **Top-Event: Qualitativ Top-D zuordenbar, aber hier außerhalb Betrachtungstiefe**

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare

Vorfilter (psip-Regler)-Infor-mation (2v2-Voting)	CCF	Für das Versagen des Vorfilters ursächliche Fehler müssen erkannt werden. Wie sich jedoch im Falle der Sensoren zeigt, ist dies nur bedingt der Fall.	Nicht möglich (siehe 2v2-Voting)	Überführen in RFE	Vorfilterinformation kann aufgrund folgender Fehler ausfallen (SW-Fehler außerhalb der Systemgrenzen):
					• δ_{LRW}-Information von der T-Elster. Deren Fehlermoden:
					  • T-Elster-HW (siehe unten: Transputer-HW); T-Elster-SW
					  • LRW-Sensorik-Fehler (siehe oben)
					• vx-Informationswegfall. Hier Fehlermoden gemäß Absorptionssatz vordere Raddreh-zahlsensorik (da SWS auch aufgrund dieser Fehler ausfällt)
					Im Fehlerbaum (siehe Anhang F) werden die beiden Kanäle des Vorfilters als Gatter aufgeführt und tragen dort zur Veranschau-lichung der CCF-Thematik bei. Es wird deutlich, daß die Algorithmen vorrangig durch Fehl-funktionen der Sensorik ausfallen. Da diese nur einkanalig vorliegen, trägt die Zweikanaligkeit der Rechner-HW kaum zur V/S/W-Optimierung bei.
					Top-Event: B u. C (die beiden Kanäle des Vorfilters entsprechen Gattern im Fehlerbaum)
					Wie sich bei der FTA (Abschnitt 5.2) zeigt, sind die Vorfilter-Fehler nur durch Transputer- und vorrangig Sensorfehler bestimmt. Demzufolge wird mit Blick auf die Zustandsraum-komplexitätsreduzierung bei der hierarchischen Modellierung auf einen Zustand „Vorfilter-Fehler“ verzichtet.
					Anschließende Offboard-Fehler-Behandlung (siehe HF des abs. LRW-S).

Modular er $\dot{\psi}$-Regler-Infor-mation (Voting 2v2-Strategi e)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler, wobei hier neben SW-Fehlern folgende Fehlermoden im Sinne eines CCF zum Versagen eines der beiden Kanäle des Reglers führen können: • Vorfilterausfall (Ursachen, siehe oben) • D-b-W-Transputer (Rechnerplattform des Reglers) • Sämtliche Sensoren, die bereits im Gatter SENSORIK des betreffenden Fehlerbaums für den Eintritt des Top-Events ursächlich sein können **Top-Event: B u. C (die beiden Kanäle des Reglers entsprechen Gattern im Fehlerbaum)** Wie Vorfilter nicht in der hierarchischen Modellierung berücksichtigt. Anschließende Offboard-Fehlerbehandlung (siehe HF des abs. LRW-S).

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
SW-Schätzer-Infor-mation (Voting 2v2-Strategie)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	SW-Fehler liegen außerhalb der Systemgrenzen. Neben SW-Fehlern kann die SWS-Information aufgrund folgender Fehlermoden im Sinne eines CCF zum Versagen eines der beiden Kanäle des Reglers führen: • die entsprechenden Sensorinformationen (führen zu den dort beschriebenen RG-Degradationen) • bzgl. SWS-Transputer (siehe unten SWS-Transputer) **Top-Event: A (die beiden Kanäle des SWS spiegeln sich als Gatter im Fehlerbaum wider)** Wie Vorfilter nicht in der hierarchischen Modellierung berücksichtigt. Anschließende Offboard-Fehler-behandlung (siehe HF des abs. LRW-S).

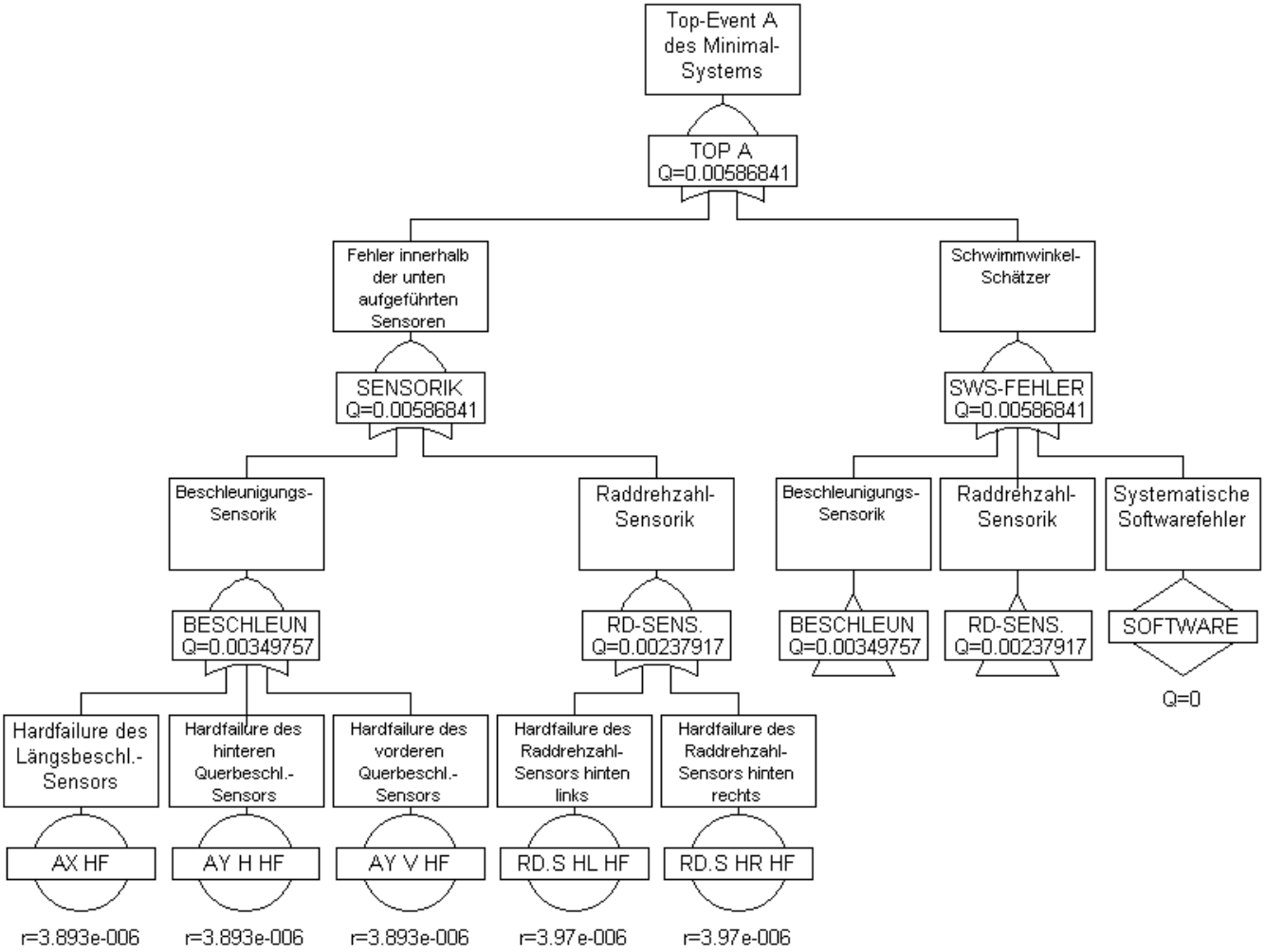
SIS-Infor-mation (ein-kanalig)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	SW-Fehler liegen außerhalb der Systemgrenzen
					Neben SW-Fehlern kann die SIS-Information aufgrund folgender Fehlermoden im Sinne eines CCF versagen:
					• SIS-Transputer (siehe unten SIS-Transputer)
					• Sensorfehler führen im Minimal-System nur im Sinne eines Mißalarms bzw. einer Mißbehandlung zum Versagen der SIS. Diese führen somit zum Eintritt des Top-Events C. In der hierarchischen Modellierung können diese Phänomene sehr anschaulich diskutiert werden (siehe Abschnitt 5.3)
					Top-Event: C (SIS-Gattern im Fehlerbaum)
					Die SIS ist jedoch nicht als explizites Gatter in der hierarchischen Modellierung berücksichtigt.
					Anschließende Offboard-Fehlerbehandlung (siehe HF des abs. LRW-S)
					Weitere Anmerkungen:
					• Da das HF-Modul der SIS auf „Selbstüber-wachung“ basiert, existieren hier keine Sensorfehler, die zum Versagen der SIS führen können.
					• Im Minimal-System beschränkt sich die Softfailure-Erkennung auf:
					  • Die Selbstüberwachung des Gierraten-sensors (dem Gierraten-S. zugeordnet)
					  • die Selbstüberwachung des absoluten Lenkradwinkelsensors
					  • die durch den absolut LRW-Sensor vornehmbare Überwachung des inkr. Lenkradwinkelsensors
					Die ersten beiden basieren somit ausschließlich auf SW und HW, womit auch nur diese Fehlermöglichkeiten vorliegen können. Beim dritten Element fließt außerdem noch der abs. LRW-Sensor ein.

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
SIS-Trans-puter	Gl. 4-32	Nicht möglich	Nicht möglich	Nicht möglich	Hochsicherheitsrelevanz, da Fehler aufgrund der Einkanaligkeit des SIS-Transputers nicht erkennbar. **Top-Event: C**
I/O-, SWS und D-b-W-Trans-puter (je zwei-kanalig)	Belie-biger Defekt Rate je Trans-puter: Gl. 4-32	Durch 1v2-Voting FE-R.: Gl. 4-25 (als Repräsentant)	Nicht möglich	D-b-W in RFE überführen FB-R.: Gl. 4-28	Einfachfehler in einem der beiden gleichen Rechnerkanäle wirken sich verfügbarkeitskritisch aus, bis zur FELB (siehe Gl. 4-32) auch sicherheitskritisch. Aufgrund der angenommenen 100%igen-FELB ist der Fehler jedoch nach der FB nicht mehr als sicherheitskritisch anzusehen. Zur Veranschaulichung wurden in die FTA, wie auch der hierarchischen Modellierung Zweifach-fehler der Transputer-HW mitmodelliert. **Top-Event: B (C bei Berücksichtigung von Zweifachfehlern)** Weitere Details zur hierarchischen Modellierung bzw. FB: siehe HF des abs. LRW-Sensors. Andere HW (VME, Sensorfehlersimulator etc.) gehört nicht zum D-b-W-Systemumfang und soll deshalb als außerhalb der Systemgrenzen betrachtet werden.
T-Elster-Aktorik (M_O, Kupp-lung, M_U)	Belie-biger Defekt	Außerhalb System-grenze	Außerhalb Systemgren ze	Außerhalb Systemgren ze	Bzgl. der Top-Events außerhalb der System-grenzen Mit Blick auf die Zustandsraumkomplexität und den Umstand, daß die T-Elster auch im erweiterten Konzept (Kap. 6) nicht verändert wird, soll auf eine Einbindung der T-Elster in die hierarchische Modellierung verzichtet werden.
Fahr-werk, Reifen etc.	Belie-biger Defekt	Außerhalb System-grenze	Außerhalb System-grenze	Außerhalb System-grenze	Bzgl. der Top-Events außerhalb der System-grenzen Mit Blick auf die Zustandsraumkomplexität und den Umstand, daß am Fahrzeug auch im erweiterten Konzept (Kap. 6) nicht verändert wird, soll auf eine Einbindung dieser Elemente in die hierarchische Modellierung verzichtet werden.
Voll-redun-dantes zwei-kanalig. Bord-netz	Belie-biger Defekt	Siehe Kommentar	Nicht vorgesehen	Siehe Kommentar	Top-Event: D (als qualitatives 2v2-Gatter) B (als qualitatives 1v2-Gatter) nicht C, da ein zeitgleicher Zweifach-fehler hinsichtlich der Auftretenswahr-scheinlichkeit ausgeschlossen werden soll und davon ausgegangen wird, daß im Anschluß an den Einfachfehler eine Offboard-FB eingeleitet wird.

8.6 Anhang F: Fehlerbäume des Minimal-Systems

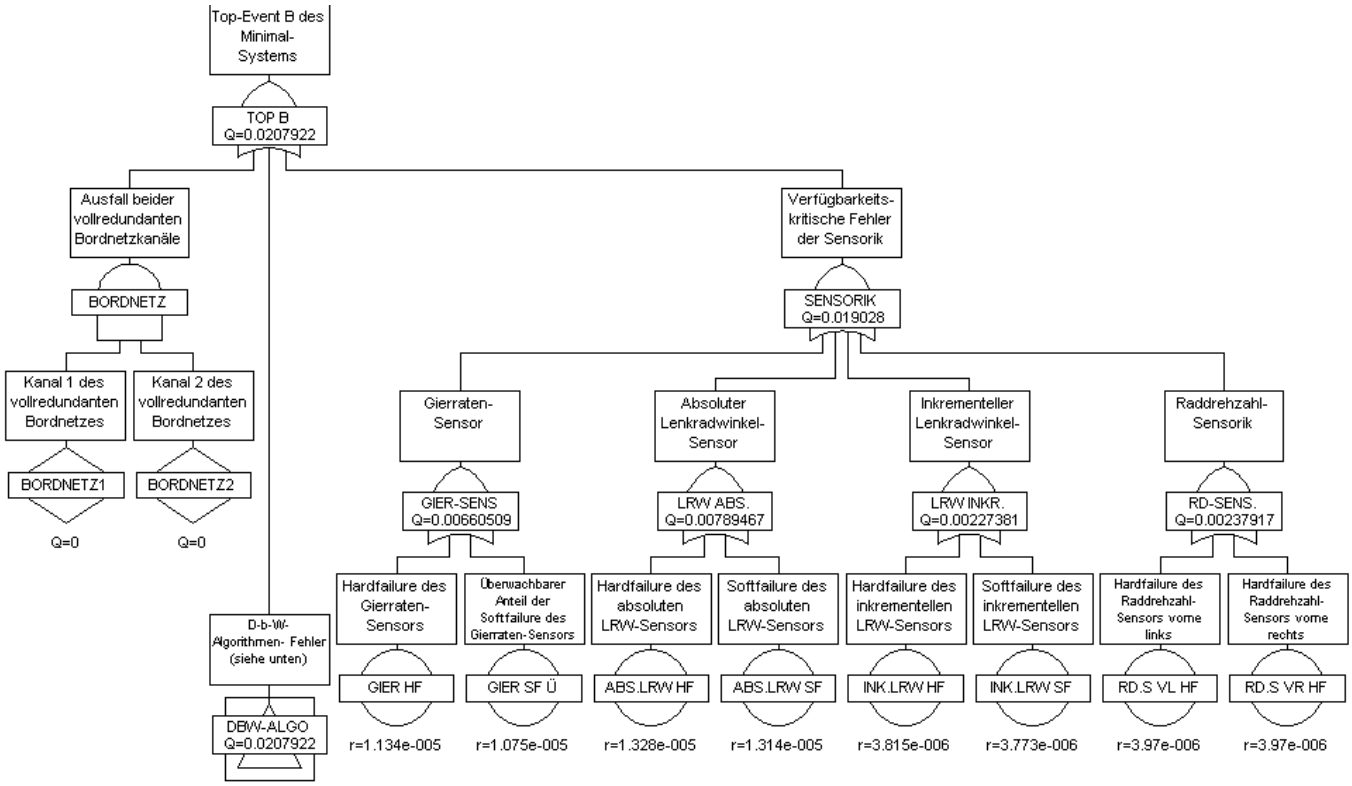
8.6.1 Anhang F1: Fehlerbaum des Top-Events A des Minimal-Systems

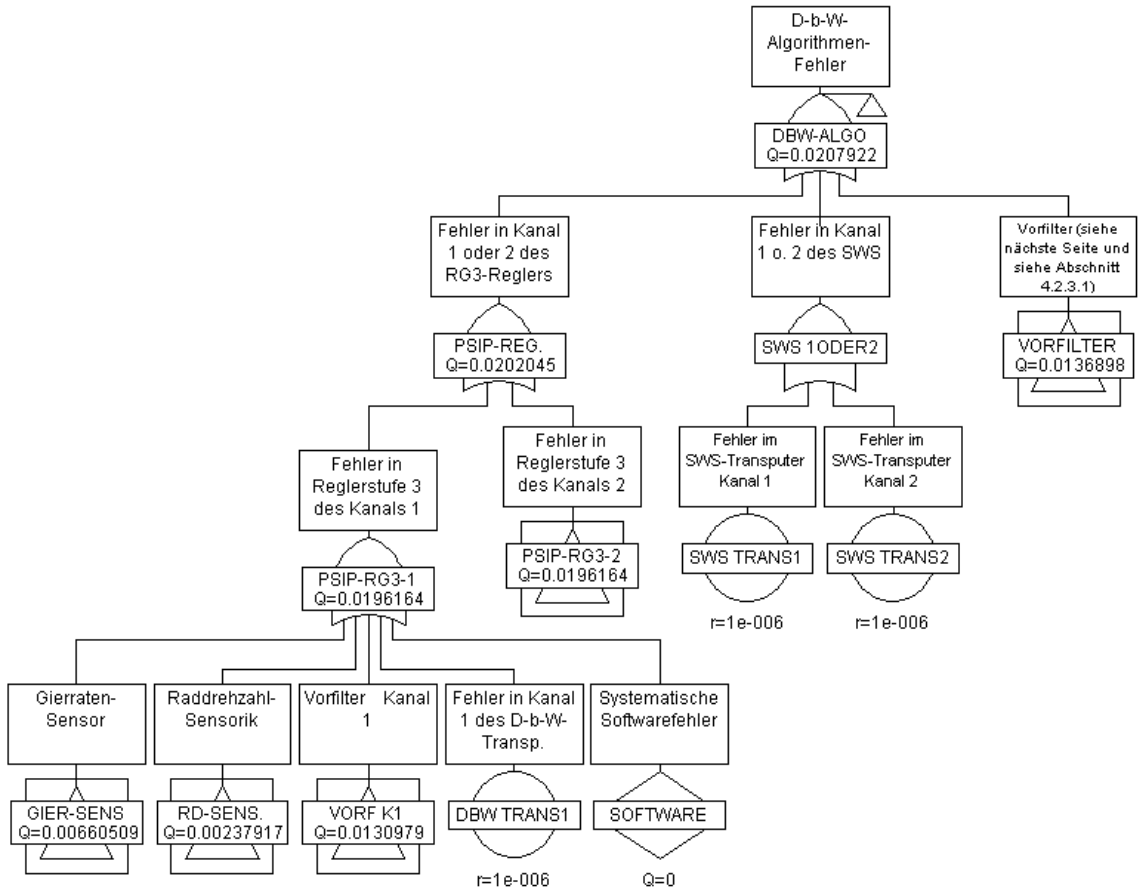
Anmerkung: Unter Top-Event A sind sämtliche Fehler zusammengefaßt, die zum Übergang des D-b-Ws von der höchsten Reglerstufe in die Reglerstufen 2 oder 3 führen (siehe Abschnitt 3.1.1.1).



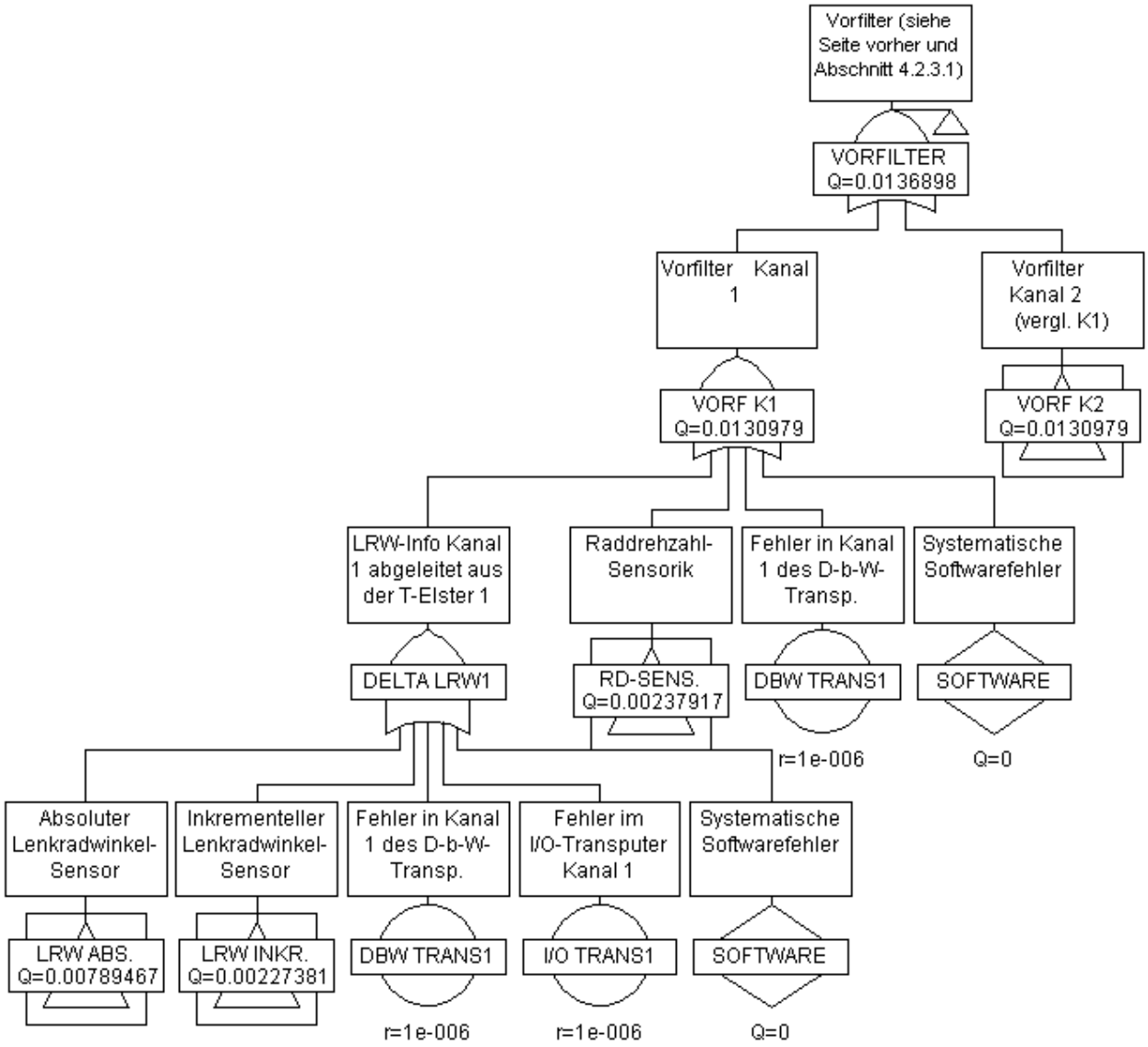
8.6.2 Anhang F2: Fehlerbaum des Top-Events B des Minimal-Systems

Anmerkung: Unter Top-Event B sind sämtliche Fehler zusammengefaßt, die zum Übergang des D-b-Ws in die Rückfallebene/Notlauf führen (siehe Abschnitt 3.1.1.2). Hierbei handelt es sich um die verfügbarkeitskritischen Fehler.



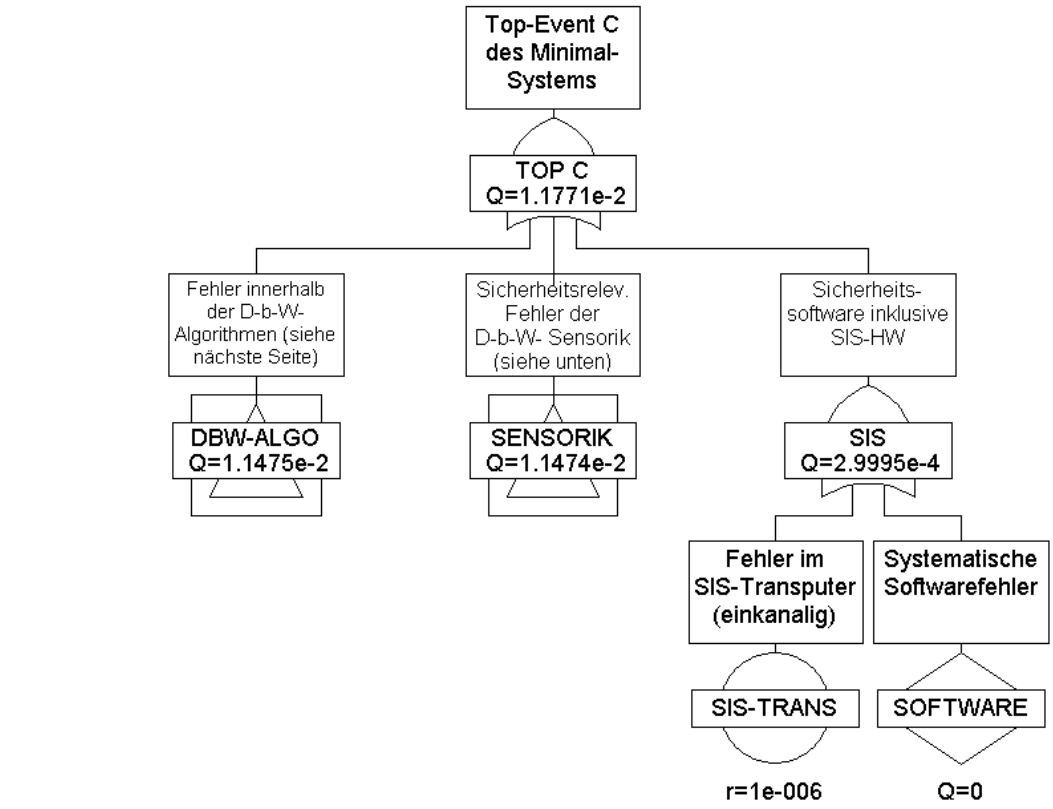


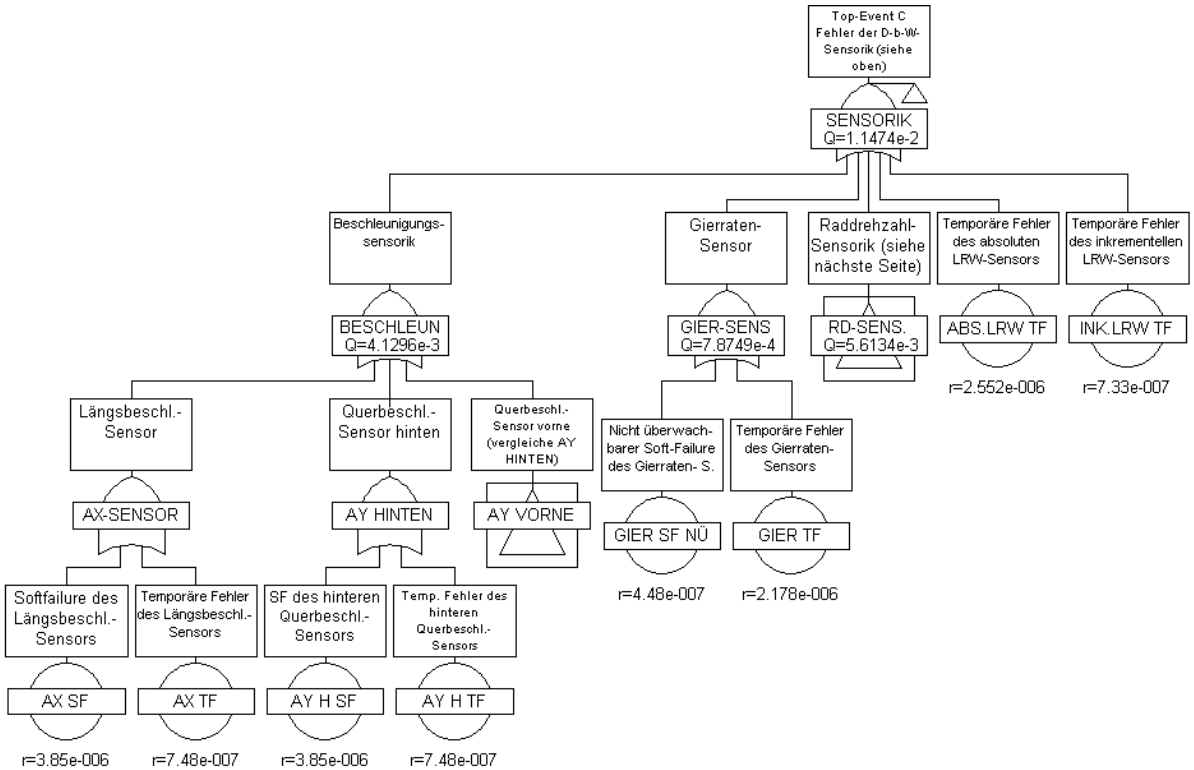
Fortsetzung des Fehlerbaums des Top-Events B des Minimal-Systems



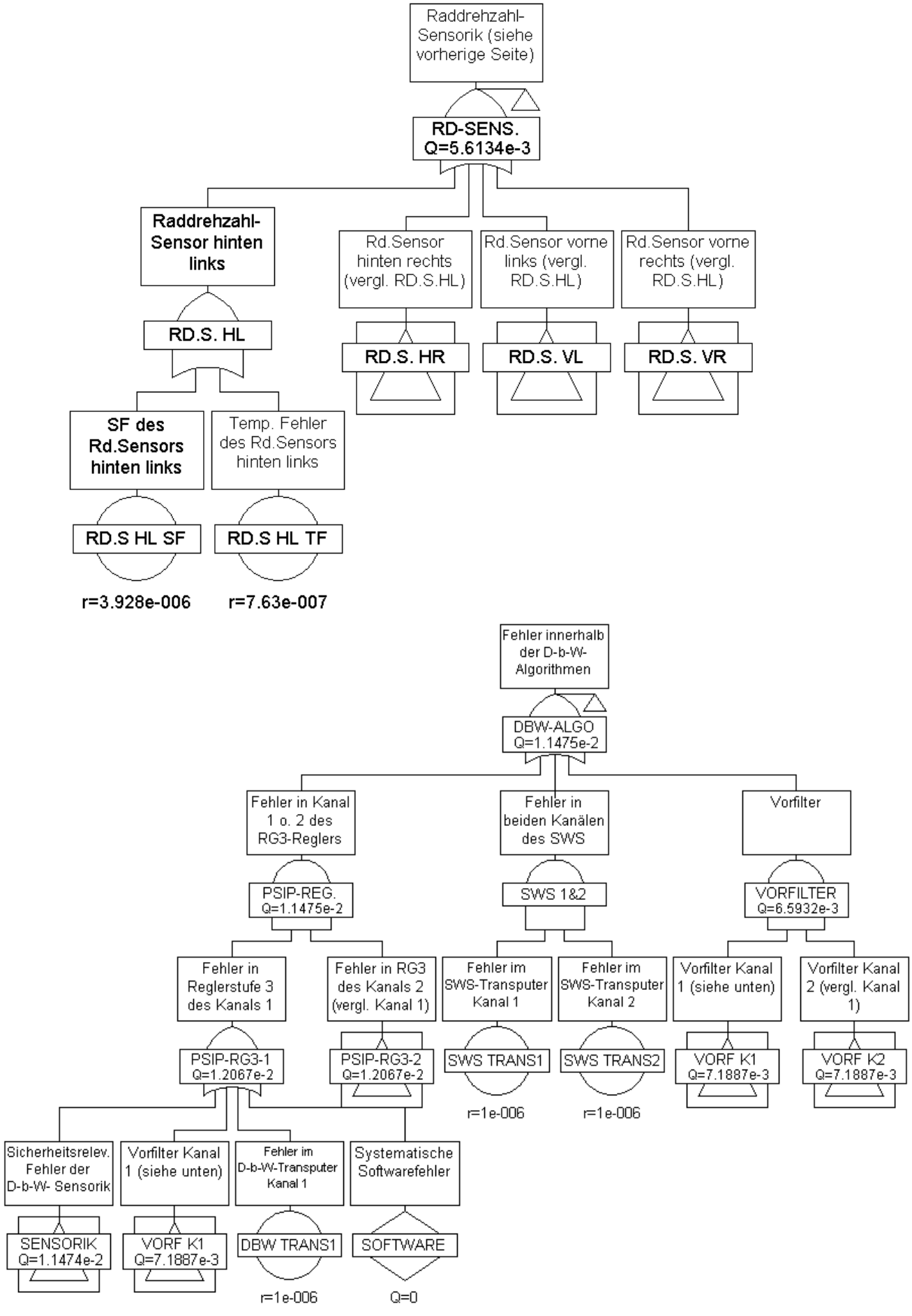
8.6.3 Anhang F3: Fehlerbaum des Top-Events C des Minimal-Systems

Anmerkung: Unter Top-Event C sind sämtliche sicherheitskritischen Fehler zusammengefaßt (siehe Abschnitt 3.1.1.3).

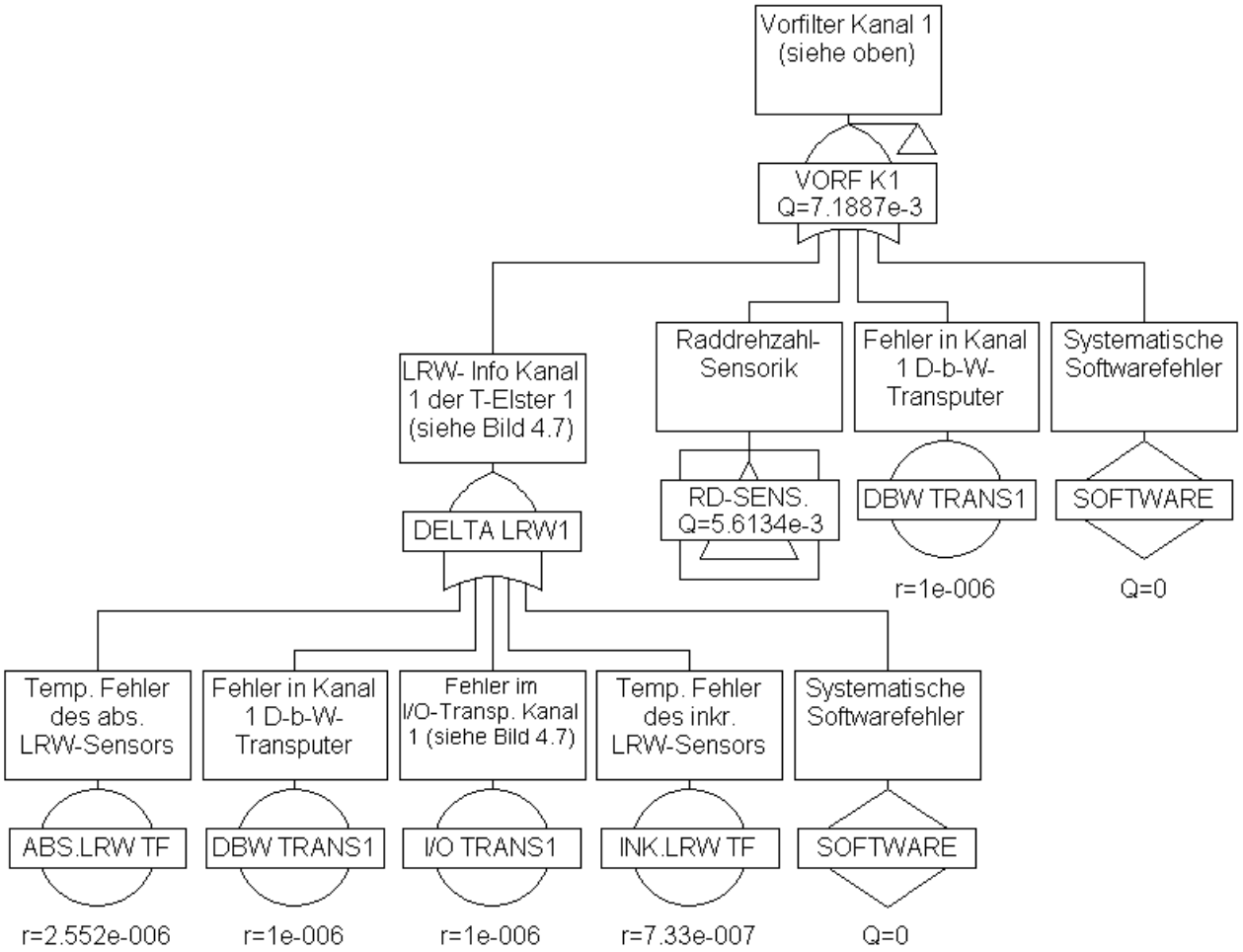




Fortsetzung des Fehlerbaums des Top-Events C des Minimal-Systems



Fortsetzung des Fehlerbaums des Top-Events C des Minimal-Systems



8.7 Anhang G: Für die Zustandsraummodellierung des D-b-W-Minimal-Systems erforderliche Kenngrößen

Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
0	D-b-W in Reglerstufe RG1 • Fehlerfreier Startzustand • Zustand in Bild 5.6 farblich grün hervorgehoben • Startaufenthaltswahr-scheinlichkeit = 1	$q_{0,1}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • HF absolut LRW-Sensor • HF inkr. LRW-Sensor • HF Gierratensensor • HF beide Raddrehzahlsensoren der Vorderachse $q_{0,1} = \lambda_{Modul} = 36{,}375 \cdot 10^{-6} \frac{1}{h}$ Entspricht mit Ausnahme der Sensor-Softfailures dem Gatter SENSORIK des Top-Events B (siehe Anhang F).
		$q_{0,4}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • SF absolut LRW-Sensor • SF inkr. LRW-Sensor • Überwachbare SF des Gierratensensors $q_{0,4} = \lambda_{Modul} = 27{,}663 \cdot 10^{-6} \frac{1}{h}$ Vergleiche hierzu auch Sensormodul Top-Event B. Entspricht den Sensor-Softfailures des Gatters SENSORIK des Top-Events B (Anhang F). Damit ergeben die Übergangsraten $q_{0,1}$ und $q_{0,4}$ die Fehlerrate des Gatters SENSORIK des Fehlerbaums des Top-Events B.
		$q_{0,5}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • HF Längs- und Querbeschleunigungssensorik • HF Rd-Sensorik der Hinterachse $q_{0,5} = \lambda_{Modul} = 19{,}62 \cdot 10^{-6} \frac{1}{h}$ Entspricht dem Gatter SENSORIK des Top-Events A (siehe Anhang F).
		$q_{0,8}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • Fehler in Kanal 1 oder 2 der Transputer-HW (I/O, SWS, D-b-W) $q_{0,8} = \lambda_{Modul} = 6 \cdot 10^{-6} \frac{1}{h}$ Diese Übergangsrate geht aus der Transputer-HW im Gatter D-b-W-Algo des Fehlerbaums des Top-Events B hervor (Vergleiche Anhang F).
		$q_{0,11}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • TF (abs. LRW + inkr. LRW + Gier-S. + Längs- und Querbeschleunigungssensorik + Rd-Sensorik) • SF Gierraten-S. im nicht überwachbaren Fahrdynamikbereich. • SF Beschleunigungs- und Rd-Sensorik. • Fehler in Transputer SIS $q_{0,11} = \lambda_{Modul} = 39{,}47 \cdot 10^{-6} \frac{1}{h}$ Diese Übergangsrate entspricht der Summe der Gatter-Übergangsraten „Sensorik“ und SIS des Fehlerbaums des Top-Events C (Vergleiche Anhang F).

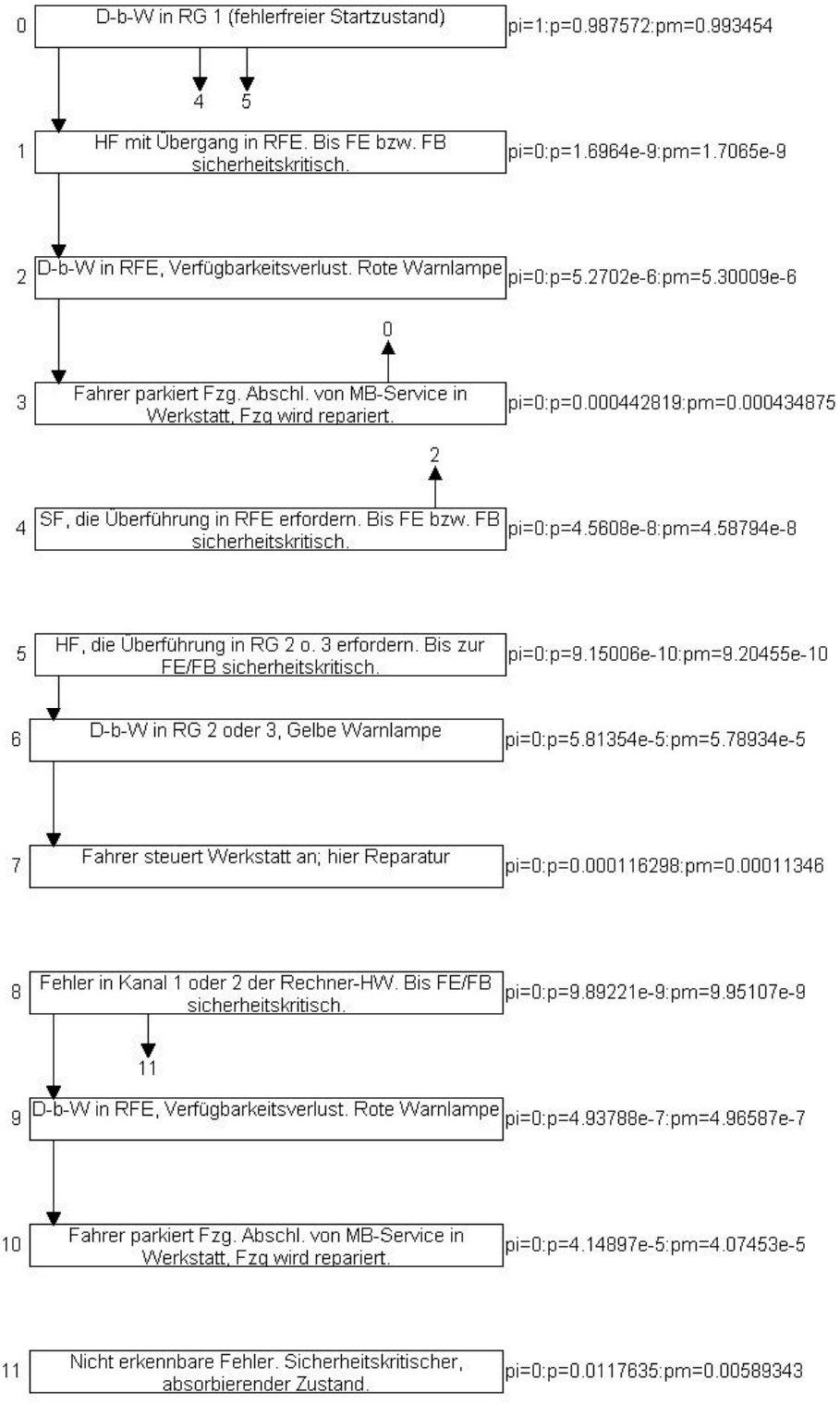
Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
1	HF-Fehler, die über HF-SIS-Modul erkannt werden können. • Bis zur FB sicherheitskritisch. • Zustand folglich farblich rot hervorgehoben • Startaufenthaltswahr-scheinlichkeit = 0	$q_{1,2}$	Da der Übergang in Zustand 2 nach Verstreichen der mittleren Fehlererkennungszeit und -behandlungszeit erfolgt, bestimmt sich die Übergangsrate aus dem Kehrwert der Summe beider Zeiten. Unter Verwendung von Gl. 4-24 und 4-28 ergibt sich (siehe auch Kap. 4) : $q_{1,2} = \frac{\varepsilon_{Hard} \cdot \varsigma_{Onboard}}{\varepsilon_{Hard} + \varsigma_{Onboard}} = 21.176 \frac{1}{h}$ Diese „heilende“ Onboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden (siehe Abschnitt 5.4.2, Diskussion der Vorzüge der hierarchischen Modellierung).
2	RFE/Verfügbarkeitskritischer Zustand • Im Zuge der FB wird D-b-W in die RFE überführt. • Damit Verfügbarkeitsverlust der D-b-W-Funktionalität • Zustand ist damit Top-Event B zuzuordnen. • Im Zustand ist das System sicher. • Aktivierung der „roten“ Warnlampe. (Zustand in Bild 5.6 violett hervorgehoben) • Abspeichern der Fehlermeldung im Diagnosespeicher • Startaufenthaltswahr-scheinlichkeit = 0	$q_{2,3}$	Es wird davon ausgegangen, daß der Fahrer das Fahrzeug nach Aufleuchten der roten Warnlampe durchschnittlich binnen 5 Minuten parkiert und eine Überführung in die Werkstatt durch den MB-Service in die Wege leitet. Die Übergangsrate entspricht Gl. 4-30 $q_{2,3} = 12 \frac{1}{h}$ Diese „heilende“ Offboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden (siehe Abschnitt 5.4.2, Diskussion der Vorzüge der hierarchischen Modellierung)
3	Verfügbarkeitskritischer Zustand • Abschleppkosten 500 DM • Reparaturkosten 1.500 DM für den Tausch des entsprechenden Sensors bzw. Sensormoduls • Dieser Zustand ist sowohl im Sinne der D-b-W-Funktion wie auch der Fahrfunktion verfügbar-keitskritisch, jedoch sicher. Somit wird er in Bild 5.6 farblich schwarz hervorgehoben. • Der Fehlerspeicher wird erst nach der Reparatur gelöscht. Gleiches gilt für die „rote“ Warnlampe. • Startaufenthaltswahr-scheinlichkeit = 0 • Zustand 3 ist keinem Top-Event zuzuordnen.	$q_{3,0}$	Fahrzeug wurde nach 5 Minuten parkiert und vom MB-Service innerhalb 1 Stunden in die Werkstatt überführt, wo es in 6 Stunden repariert und an den Kunden zurückgeführt wird. Die Übergangsrate bestimmt sich somit aus dem Kehrwert der Summe der MB-Service-Überführungs- und Reparaturzeit (siehe Gl. 4-31 und 4-32). $q_{3,0} = \frac{\nu_{MB-Service} \cdot \mu}{\nu_{MB-Service} + \mu} = 1/7 \frac{1}{h}$ Diese „heilende“ Offboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden.

Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
4	SF, die über Selbsttest bzw. SF-SIS-Modul erkannt werden können. • Vor FB sicherheitskritisch. • Damit ist Zustand 4 sicherheitskritisch und in Bild 5.6 farblich rot hervorgehoben • Startaufenthaltswahr-scheinlichkeit = 0	$q_{4,2}$	Die Übergangsrate bestimmt sich aus dem Kehrwert der Summe der mittleren Fehlererkennungszeit und –behandlungszeit (Gl. 4-25 bis 4-27und 4-28): $q_{4,2} = \frac{\varepsilon_{Soft} \cdot \varsigma_{Onboard}}{\varepsilon_{Soft} + \varsigma_{Onboard}} = 599\,\frac{1}{h}$ Diese „heilende“ Onboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden.
5	HF, die über HF-SIS-Modul erkannt werden können. • Vor FB sicherheitskritisch. • Damit ist Zustand 5 sicherheitskritisch und in Bild 5.6 farblich rot hervorgehoben) • Startaufenthaltswahr-scheinlichkeit = 0	$q_{5,6}$	Übergangsrate basiert auf der FE- und FB-Raten (siehe Gl. 4-24 und 4-28). Siehe hierzu $q_{5,6}$: $q_{5,6} = q_{1,2} = 21.176\,\frac{1}{h}$ Diese „heilende“ Onboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden.
6	Zustand degradierter Regelgüte • Im Zuge der FB wird D-b-W auf RG 2 bzw. 3 überführt. Zustand ist damit Top-Event A zuzuordnen. • Aktivierung der „gelben“ Warnlampe (Zustand in Bild 5.6 farblich gelb hervorgehoben). • Abspeichern von Fehlermeldung in Diagnosespeicher • Startaufenthaltswahr-scheinlichkeit = 0	$q_{6,7}$	Es wird davon ausgegangen, daß der Fahrer nach Aufleuchten der gelben Warnlampe durchschnittlich binnen 3 Stunden die Werkstatt aufsucht. Die Übergangsrate entspricht Gl. 4-29 $q_{6,7} = 1/3\,\frac{1}{h}$ Diese „heilende“ Offboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden.
7	Verfügbarkeitskritischer Zustand • Reparaturkosten 1.500 DM für den Tausch des entsprechenden Sensors bzw. Sensormoduls • Fzg. unverfügbar, jedoch sicher • Zustand in Bild 5.6 schwarz hervorgehoben • Der Fehlerspeicher wird erst nach der Reparatur gelöscht. Gleiches gilt für die „gelbe“ Warnlampe. • Startaufenthaltswahr-scheinlichkeit = 0 • Zustand ist nicht unmittelbar Top-Event B zuzuordnen.	$q_{7,0}$	Fahrzeug wird in der Werkstatt repariert und binnen 6 Stunden an den Kunden übergeben. Somit ergibt sich die Übergangsrate (siehe Gl. 4-32) aus: $q_{7,0} = \mu = 1/6\,\frac{1}{h}$ Diese „heilende“ Offboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden. **Anmerkung:** Dieser Zustand unterscheidet sich von Zustand 3 lediglich durch unterschiedliche Übergangsraten. Jedoch wird erst hiermit ermöglicht, die unterschiedlichen Instandsetzungskosten und die Zeitspanne bis das Fahrzeug wieder fahrtüchtig ist, zu berücksichtigen (siehe Gedächtnislosigkeit des Markov-Prozesses).

Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
8	Fehler in einem der drei Transputer (I/O, SWS, D-b-W) des Kanals 1 oder 2 der Rechner-HW. • Vor FB sicherheitskritisch. • Zustand 8 in Bild 5.6 farblich rot hervorgehoben • Startaufenthaltswahr-scheinlichkeit = 0	$q_{8,9}$	Die Zweikanaligkeit dieser Transputer ermöglicht ein 2v2-Voting mit anschließender Überführung des D-b-W in die RFE. Es wird von einer 100% Fehlererkennung und –behandlung ausgegangen.Unter Verwendung von Gl. 4-25 und 4-28 ergibt sich (siehe auch Kap. 4) : $q_{8,9} = q_{4,2} = 599\,\frac{1}{h}$ Diese „heilende“ Onboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht berücksichtigt werden.
	Weiterer Übergang aus Zustand 8	$q_{8,11}$	Exemplarisch sei hier davon ausgegangen, daß bis zur erfolgreichen Erkennung und Behandlung des Einfachfehlers im verbleibenden Kanal der Transputer-HW ein weiterer Fehler auftritt Dieser Fehler ist nicht mehr erkennbar, weswegen hier der Übergang in den sicherheitskritischen Zustand 11 erfolgt. Die gegenüber $q_{8,9}$ deutlich kleinere Übergangsrate spiegelt den Umstand wider, daß ein stochastisch unabhängiger Zweifachfehler sehr unwahrscheinlich ist. $q_{8,11} = \frac{q_{0,8}}{2} = 3 \cdot 10^{-6}\,\frac{1}{h}$
9	Verfügbarkeitskritischer Zustand • Im Zuge der FB wird D-b-W in die RFE überführt. • Damit Verfügbarkeitsverlust der D-b-W-Funktionalität, jedoch Sicherheit des Systems. Vergleiche auch Zustand 2. • Zustand ist damit Top-Event B zuzuordnen. • Aktivierung der „roten“ Warnlampe. (Zustand in Bild 5.6 violett hervorgehoben) • Abspeichern der Fehlermeldung im Diagnosespeicher • Startaufenthaltswahr-scheinlichkeit = 0	$q_{9,10}$	Es wird davon ausgegangen, daß der Fahrer das Fahrzeug nach Aufleuchten der roten Warnlampe durchschnittlich binnen 5 Minuten parkiert und eine Überführung in die Werkstatt durch den MB-Service in die Wege leitet. Die Übergangsrate entspricht Gl. 4-30 $q_{9,10} = q_{2,3} = 12\,\frac{1}{h}$ Diese „heilende“ Offboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden.

Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
10	Verfügbarkeitskritischer Zustand • Es wird davon ausgegangen, daß die Reparaturkosten für den Tausch der Transputer-HW 1.000 DM betragen. Abschleppkosten 500 DM. Bis auf die geringeren Reparaturkosten ist der Zustand identisch Zustand 3. • Startaufenthaltswahr-scheinlichkeit = 0	$q_{10,0}$	Die Übergangsrate bestimmt sich aus dem Kehrwert der Summe der MB-Service-Überführungs- und Reparaturzeit (siehe Gl. 4-31 und 4-32) $q_{10,0} = q_{3,0} = 1/7 \frac{1}{h}$ Diese „heilende“ Offboard Übergangsrate konnte in Abschnitt 5.2 bei der Fehlerbaumanalyse nicht eingesetzt werden (siehe Abschnitt 5.3., Diskussion der Vorzüge der MKA).
11	Sicherheitskritischer Zustand (Top-Event C) • Sämtliche Fehler, die über die SIS nicht erkannt werden können, führen zum Übergang in Zustand 11. Damit ist dieser Zustand bis zum Nachweis der Robustheit des D-b-W-Reglers gegen diese Fehlerphänomene als sicherheitskritisch anzusehen (vergleiche Top-Event C). Zustand ist in Bild 5.6 rot hervorgehoben. • Startaufenthalts-wahrscheinlichkeit = 0	-	Im Sinne der pessimistischen Analyse ist der Zustand als absorbierend anzusehen. Dies berücksichtigt den Umstand, daß aufgrund eines der nicht entdeckten Fehler die Gefahr der Verunfallung des Fahrzeugs besteht. Sollte sich der D-b-W-Regler als Robust gegen sämtliche in diesen Zustand einfließenden Fehler erweisen, besteht die Möglichkeit, den Zustand durch eine Fehlererkennung während einer turnusmäßigen Werkstattinspektionen zu verlassen. Diese optimistische Annahme hier mit Blick auf die Sicherheitsrelevanz des Systems vorerst nicht weiter betrachtet werden.

8.8 Anhang H: Modellierung der Markov-Kette des Minimal-Systems mittels des Tools MKV



- pi: Startwahrscheinlichkeit im jeweiligen Zustand
- p: Aufenthaltswahrscheinlichkeit im jeweiligen Zustand zum Zeitpunkt t = 300h
- pm: mittlere Aufenthaltswahrscheinlichkeit im jeweiligen Zustand.

Es ist zu erwähnen, daß nicht alle in die quantitative Zustandsraumanalyse einfließenden Zustandsübergangsraten grafisch in MKV wiedergegeben werden (siehe beispielsweise Übergangsrate vom Zustand 10 zum Zustand 0).

8.9 Anhang I: Auswirkungen der Fehlermöglichkeiten der jeweiligen FELB-Erweiterung

8.9.1 Anhang I1: Auswirkungen der Fehlermöglichkeiten des mit einer redundanten Raddrehzahlsensorik ausgestatteten D-b-W´s auf das Systemverhalten

Fehler in Komp.	Fehler-mode	FE-Maßn. und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Ein Kanal der Rd.-Sensorik	HF	HF-FE-Modul FE-R.: Gl. 4-24	FE kommt FL gleich	Gelbe Warnlampe, da mit verbleibender Sensorik weiterhin die volle D-b-W-Funktion aufrecht erhalten werden kann. FB-R.: Gl. 4-28	Der Einfachfehler wirkt sich lediglich auf die Fehlerwahrscheinlichkeit des Gesamtsystems aus. Bis zur FELB (6 Zyklen) wird davon ausgegangen, daß der Fehler sicherheitskritisch ist. Dieser transiente Sachverhalt kann in der FTA nur bedingt über die Modellierung temporärer Fehler berücksichtigt werden. **Top-Event: D** Im Rahmen der Detailanalyse via hierarchischer Modellierung (Abschnitt 5.3) wird die Reaktionszeit der FELB über einen „sicherheitsrelevanten“ Zwischenzustand modelliert, der nach der Fehlererkennungszeit (siehe Gl. 4-24) wieder verlassen wird. Der sicherheitsrelevante Zustand ist also nicht absorbierend. Nach der Onboard-FB Offboard-FB einleiten: • Gelbe Warnlampe aktivieren • Ablegen der Fehlermeldung im Diagnosespeicher • $\nu_{Fahrer\text{-}Gelb}$: Gl. 4-29 • Offboard-Reparaturrate gemäß Gl. 4-32
Zweiter Kanal der Vorder-Achs-Rd.-Sensorik (Mehr-fach-fehler-betr.)	HF	HF-FE-Modul FE-R.: Gl. 4-24	FE kommt FL gleich	D-b-W in RFE überführen FB-R.: Gl. 4-28	D-b-W in RFE überführen, da die Längsgeschwindigkeit nicht ausreichend über die Raddrehzahlsensorik der angetriebenen Hinterachse bestimmt werden kann. Fehler wirkt sich somit verfügbarkeitskritisch aus. **Top-Event: B** Bis zur FELB (6 Zyklen) auch sicherheitskritisch. Im Rahmen der Detailanalyse via hierarchischer Modellierung (Abschnitt 5.3) wird die Reaktionszeit der FELB über einen „sicherheitsrelevanten“ Zwischenzustand modelliert, der nach der Fehlererkennungszeit (siehe Gl. 4-24) wieder verlassen wird. Der sicherheitsrelevante Zustand ist also nicht absorbierend. Dieses Mehrfachfehlerszenario ist also identisch mit dem des Einfachfehlers innerhalb der Vorderachs-Rd.-Sensorik des Minimalsystems. Nach der Onboard-FB Offboard-FB einleiten: • Rote Warnlampe aktivieren • Ablegen der Fehlermeldung im Diagnosespeicher • $\nu_{Fahrer\text{-}Rot}$: Gl. 4-30 • MB-Service und Offboard-Reparaturrate gemäß Gl. 4-31 und 4-32

Fehler in Komp.	Fehler-mode	FE-Maßn. und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Zweiter Kanal der Hinter-Achs-Rd.-Sensorik (Mehr-fach-fehler-betr.)	HF	HF-FE-Modul FE-R.: Gl. 4-24	FE kommt FL gleich	Überführen auf RG2 FB-R.: Gl. 4-28	Fehler bewirkt die Degradation der Reglergüte, da Längsgeschwindigkeit über Vorderräder hinreichend genau bestimmt werden kann. **Top-Event: A** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF $a_{yv,h}$-Sensorik aus Anhang E des Minimal-Systems. Dieses Mehrfachfehlerszenario ist also identisch dem des Einfachfehlers innerhalb der Hinterachs-Rd.-Sensorik des Minimalsystems.
Ein Kanal der Vorder-Achs-Rd.-Sensorik	SF	FE gemäß Abschnitt 6.1.1 FE-R.: Gl. 4-26	FL nicht möglich	D-b-W in RFE überführen FB-R.: Gl. 4-28	Da der fehlerhafte Sensor nicht lokalisiert werden kann, ist D-b-W in RFE zu überführen. Fehler wirkt sich somit verfügbarkeitskritisch aus. **Top-Event: B** Die FB dieses Softfailures ist also identisch dem des HFs innerhalb der Vorderachs-Rd.-Sensorik des Minimalsystems bzw. dem zweiten HF der Vorderachssensorik der vorliegenden Tabelle. Weitere Kommentare zur FB bzw. hierarchischen Modellierung sind somit den entsprechenden Stellen zu entnehmen. Kommentar: Gegenüber dem Minimal-System kann der Softfailure erkannt und behandelt werden. Für eine zuverlässige Lokalisation bedarf es der Ausnutzung funktionaler Zusammenhänge, die im Rahmen der FELB-Erweiterung durch funktionale Redundanz diskutiert werden.
Ein Kanal der HA-Rd.-Sensorik	SF	FE gemäß Abschnitt 6.1.1 FE-R.: Gl. 4-26	FL nicht möglich	Degradation auf RG2 FB-R.: Gl. 4-28	Fehler bewirkt lediglich die Degradation der Reglergüte (siehe auch HF innerhalb der Hinterachs-Rd.-Sensorik des Minimal-Systems). **Top-Event: A**
Zweiter Kanal der VA- u. HA-Rd.-Sensorik (Mehr-fach-fehler-betr.)	SF	FE nicht mehr möglich	-	-	**Top-Event: C** In hierarchischer Modellierung Übergang in absorbierenden sicherheitskritischen Zustand. Dieses Mehrfachfehlerszenario ist also identisch mit dem des Einfachfehlers innerhalb der Rd.-Sensorik des Minimalsystems. Wie sich jedoch in der FTA bzw. hierarchischen Modellierung zeigen wird, ist dieser Zweifachfehler statistisch sehr unwahrscheinlich, weswegen er in der Pareto-Analyse keine wesentliche Rolle spielt.
Belie-biger Kanal der VA- u. HA-Rd.-Sensorik	TF	Nicht möglich	-	-	Siehe TF des abs. LRW-S. des Minimal-Systems (Anhang E) Es wird davon ausgegangen, daß die FE aufgrund der Kurzfristigkeit des Fehlerszenarios bedingt durch die Zählerstrategie nicht anspricht.

8.9.2 Anhang I2: Auswirkungen der Fehlermöglichkeiten des mit funktional redundanter Raddrehzahlsensorik ausgestatteten D-b-W´s auf das Systemverhalten

Fehler in Komp.	Fehler-mode	FE-Maßn. und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Abs. LRW-Sensor	HF	HF-FE-Modul FE-R.: Gl. 4-24	FE kommt FL gleich	• D-b-W in RFE überführen • Überwachung der vorderen Raddrehzahlen nicht mehr möglich FB-R.: Gl. 4-28	Bis auf den Einfluß des Fehlers auf die SIS der Raddrehzahlsensorik sei auf Anhang E verwiesen. Es ist jedoch zu betonen, daß die Auswirkung des Sensorfehlers auf die SIS des Raddrehzahlsensors nur formaler Natur ist, da die Erkennung des HF als 100%ig angenommen wird und somit unmittelbar auf RFE degradiert wird. **Top-Event: B** Nach der Onboard-FB Offboard-FB einleiten: • Rote Warnlampe aktivieren • Abschalten der SIS der Raddrehzahlsensorik • Ablegen der Fehlermeldung im Diagnosespeicher • $v_{Fahrer\text{-}Rot}$: Gl. 4-30 • MB-Service und Offboard-Reparaturrate gemäß Gl. 4-31 und 4-32
	SF	Selbstüberwachung FE-R.: Gl. 4-26	FE kommt FL gleich	• Siehe HF FB-R.: Gl. 4-28	Siehe HF, jedoch führt veränderte Fehlererkennungszeit aus sicherheitsrelevantem Zustand. **Top-Event: B**
	TF	Nicht möglich ⇒ Mißalarm	-	-	Siehe Anhang E: TF des Sensors. Darüberhinaus versagt die Fehlerüberwachung der Raddrehzahlsensorik (Mißalarm) bzw. kann unberechtigten Alarm auslösen (Fehlalarm). **Top-Event: C**
$a_{y\,v,h}$	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Degradation auf RG 3 FB-R.: Gl. 4-28	Fehler bewirkt die Degradation der Reglergüte. **Top-Event: A** Bzgl. der hierarchischen Modellierung etc. sei auf HF abs. LRW-Sensor verwiesen. Die schon aus Anhang E bekannte FB: • Längsgeschwindigkeit bei geringem Schlupf über: $v_x = \frac{v_{Rad_{vl}} + v_{Rad_{vr}}}{2} \cdot \cos\delta_{Rad}$ mit $v_{Rad_i} = \omega_{Rad_i} \cdot r_{dyn}$ gilt nachwievor, da die SIS der Rd.-Sensorik nicht auf das Beschleunigungssignal zurückgreift. Die Fehlerfreiheit der für die Bestimmung der Längsgeschwindigkeit relevanten Sensorinformationen kann also abgesichert werden. Nach der Onboard-FB Offboard-FB einleiten: • Gelbe Warnlampe aktivieren • Ablegen der Fehlermeldung im Diagnosespeicher • $v_{Fahrer\text{-}Gelb}$: Gl. 4-29 • Offboard-Reparaturrate gemäß Gl. 4-32

Fehler in Komp.	Fehler-mode	FE-Maßn. und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Einfach-Fehler der VA-Rd.-Sen-soren	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Degradation auf RG 2 FB-R.: Gl. 4-28	Längsgeschwindigkeit über das verbleibende korrekte Vorderrad und den funktionalen Zusammenhang (siehe Abschnitt 6.1.2) bei geringem Schlupf bestimmbar. Fehler bewirkt somit lediglich die Degradation der Reglergüte. **Top-Event: A** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF der Querbeschl.-Sensorik
Zwei-fach-Fehler der VA-Rd.-Sen-soren	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	D-b-W in RFE überführen FB-R.: Gl. 4-28	D-b-W in RFE überführen, da die Längs-geschwindigkeit nicht ausreichend über die Rd.-Sensorik der angetriebenen HA bestimmbar (Schlupf). Fehler wirkt sich somit verfügbarkeits-kritisch aus. **Top-Event: B** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF des abs. LRW-Sensors
Einfach- und Zwei-fach-fehler der HA-Rd.-Sen-soren	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Degradation auf RG 2 FB-R.: Gl. 4-28	Fehler bewirkt lediglich die Degradation der Reglergüte, da die Längsgeschwindigkeit über Vorderräder hinreichend genau bestimmt werden kann. **Top-Event: A** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF $a_{y\,v,h}$-Sensorik
Einfach-fehler der VA-Rd.-Sen-soren	SF	FE via funkt. Redundanz FE-R.: Gl. 4-26 Siehe jedoch Überwach-ungslücken aus Abschnitt 6.1.2	FL ebenfalls via funkt. Redundanz FL-R.: Gl. 4-26 Beachte Überwach-ungslücken (Abschnitt 6.1.2)	Überführen auf RG 2 FB-R.: Gl. 4-28	Längsgeschwindigkeit über das verbleibende korrekte Vorderrad und den funktionalen Zusammenhang (siehe Abschnitt 6.1.2) bei geringem Schlupf bestimmbar. Fehler bewirkt somit lediglich die Degradation der Reglergüte. **Top-Event: A** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF der Vorderachsraddrehzahlsensorik
Zwei-fach-Fehler der VA-Rd.-Sen-soren	SF	FE via funkt. Redundanz FE-R.: Gl. 4-26 Beachte Überwach-ungslücken (Abschnitt 6.1.2)	FL ebenfalls via funkt. Redundanz FL-R.: Gl. 4-26 Beachte Überwachu ngslücken (Abschnitt 6.1.2)	D-b-W in RFE überführen FB-R.: Gl. 4-28	D-b-W in RFE überführen, da die Längsgeschwindigkeit nicht ausreichend über die Raddrehzahlsensorik der angetriebenen Hinterachse bestimmt werden kann (Schlupf). Fehler wirkt sich somit verfügbarkeitskritisch aus. **Top-Event: B** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF des entsprechenden Sensors.

Fehler in Komp.	Fehler-mode	FE-Maßn. und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Einfach- und Zwei-fach-fehler der HA-Rd.-Sen-soren	SF	FE via funkt. Redundanz FE-R.: Gl. 4-26 Beachte Überwach-ungslücken (Abschnitt 6.1.2)	FL via funkt. Redundanz FL-R.: Gl. 4-26 Beachte Überwachu ngslücken (Abschnitt 6.1.2)	Überführen auf RG 2 FB-R.: Gl. 4-28	Längsgeschwindigkeit über die korrekte Vorderachssensorik und den funktionalen Zusammenhang (siehe Querbeschleunigungs-sensorik) bei geringem Schlupf bestimmbar. Fehler bewirkt somit lediglich die Degradation der Reglergüte. **Top-Event: A** Weitere Kommentare zur FB bzw. hierarchischen Modellierung: siehe HF der Hinterachsraddrehzahlsensorik
VA u. HA-Rd.-Sen-soren	TF und nicht erkenn-bare SF	Nicht möglich ⇒ Mißalarm	-	-	**Top-Event: C** In hierarchischer Modellierung Übergang in absorbierenden sicherheitskritischen Zustand. Siehe weiterhin TF des abs. LRW-S.
BLS u. Drossel-klappen-potentio-meter	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	D-b-W in RFE überführen FB-R.: Gl. 4-28	Rote Warnlampe, da Softfailures der Raddrehzahlsensorik nicht länger überwachbar. D-b-W in RFE überführen. Weitere Details zur Offboard-FB siehe HF $a_{y\,v,h}$-Sensorik **Top-Event: B**
Brems-Druck-sensor	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Im Minimal-System: gelbe Warnlampe FB-R.: Gl. 4-28	Solange der Schwimmwinkel-Schätzer korrekt funktioniert, wirkt sich die hier beschriebene Fehlfunktion nicht negativ auf das D-b-W-System aus. Siehe auch Anhang E **Top-Event: Qualitativ Top-D zugeordnet** Weitere Details zur Offboard-FB siehe HF $a_{y\,v,h}$-Sensorik
BLS u. Drossel-klappen-potentio-meter.	SF/TF	FE nicht möglich	-	-	Da nunmehr die SIS der Raddrehzahlsensorik nicht mehr funktionsfähig ist, besteht die Gefahr eines Mißalarms, aber auch Fehlalarms, hinsichtlich der Rd-Sensorik. Sicherheits-relevanter „schlafender“ Fehler **Top-Event: C**
Brems-Druck-sensor	SF/TF	FE nicht möglich	-	-	Mit Verweis auf obige Kommentare zu HF der Sensorik außerhalb der Betrachtungstiefe. **Top-Event: Qualitativ Top-D zugeordnet**

Vorfilter-Infor-mation (2v2-Voting)	CCF	Analog zum Minimal-System (Anhang E)	Analog zum Minimal-System (Anhang E)	Überführen in RFE	Vorfilter-Information kann aufgrund folgender Elementefehler ausfallen (SW-Fehler außerhalb Systemgrenze):
					• δ_{LRW}-Information von der T-Elster:
					  • T-Elster-HW (siehe unten: Transputer-HW); T-Elster-SW
					  • LRW-Sensorik-Fehler (siehe oben)
					• vx-Informationswegfall. Siehe Fehlermoden der Raddrehzahlsensorik.
					Ansonsten analog zum Minimal-System (Anhang E) **Top-Event: B u. C (die beiden Kanäle des Vorfilters entsprechen Gattern im Fehlerbaum)**

Fehler in Komp.	Fehler-mode	FE-Maßn. und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Modulare $\dot{\psi}$-Regler-Information (2v2 Voting)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Im Sinne eines CCF können hier neben SW-Fehlern folgende Fehlermoden zum Versagen eines der beiden Kanäle des Reglers führen. • Vorfilterausfall (Ursachen, siehe oben) • D-b-W-Transputer (Rechner des Reglers) • Sämtliche Sensoren, die bereits im Gatter SENSORIK des betreffenden Fehlerbaums für den Eintritt des Top-Events ursächlich sein können **Top-Event: B u. C (die beiden Kanäle des Reglers entsprechen Gattern im Fehlerbaum)** Wie Vorfilter nicht in hierarchischer Modellierung berücksichtigt. Anschließende Offboard-Fehlerbehandlung (siehe HF des abs. LRW-S)
SW-Schätzer-Information (2v2-Voting)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Analog zum Minimal-System. Siehe auch Anhang E. **Top-Event: A (die beiden Kanäle des SWS spiegeln sich als Gatter im Fehlerbaum wider)**
SIS-Information (einkanalig)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Mit Ausnahme der Raddrehzahlüberwachung basierend auf funktionaler Redundanz analog dem Minimal-System (siehe Anhang E)

8.9.3 Anhang I3: Auswirkungen der Fehlermöglichkeiten des mit analytisch redundanter Raddrehzahlsensorik ausgestatteten D-b-W´s auf das Systemverhalten

Fehler in Komp.	Fehler-mode	FE-Maßn. Und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Abs. LRW-Sensor	HF	HF-FE-Modul FE-R.: Gl. 4-24	FE kommt FL gleich	D-b-W in RFE überführen Überwachung der Raddrehzahlen durch analytische Redundanz nicht mehr möglich FB-R.: Gl. 4-28	Bis auf Einfluß des Fehlers auf die SIS der Rd-Sensorik sei auf Anhang E verwiesen. Es ist jedoch zu betonen, daß die Auswirkung des Sensorfehlers auf die SIS des Rd-Sensors nur formaler Natur ist, da die Erkennung des HF als 100%ig angenommen wird und somit unmittelbar auf RFE degradiert wird. **Top-Event: B** Nach der Onboard-FB Offboard-FB einleiten: • Rote Warnlampe aktivieren • Abschalten der SIS der Raddrehzahlsensorik • Ablegen der Fehlermeldung im Diagnosespeicher • $\nu_{Fahrer\text{-}Rot}$: Gl. 4-30 • MB-Service und Offboard-Reparaturrate gemäß Gl. 4-31 und 4-32
	SF	Selbstüber-wachung FE-R.: Gl. 4-26	FE kommt FL gleich	• Siehe HF FB-R.: Gl. 4-28	Siehe HF, jedoch führt eine veränderte Fehler-erkennungszeit aus sicherheitsrelevantem Zustand. **Top-Event: B**
	TF	Nicht möglich ⇒ Mißalarm	-	-	Siehe Anhang E: TF des Sensors. Darüber-hinaus versagt die Fehlerüberwachung der Rd-Sensorik (Mißalarm) bzw. kann einen unberechtigten Alarm auslösen (Fehlalarm). **Top-Event: C**
Gierraten-Sensor	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Überführen in RFE FB-R.: Gl. 4-28	Siehe HF des abs. LRW-S. Ausfall der analyt. Rd-Sensorüberwachung
	SF	Selbst-überwach-ung FE-R.: Gl. 4-25 Siehe jedoch Fahr-manöver-abhängig-keit	FE kommt FL gleich	Überführen in RFE FB-R.: Gl. 4-28	Analog Minimal-System (Siehe Anhang E) Sowie Ausfall der analyt. Rd-Sensorüber-wachung
	TF	Nicht möglich ⇒ Mißalarm	-	-	Siehe TF des abs. LRW-S.

Fehler in Komp.	Fehler-mode	FE-Maßnahme und FE-Rate	FL-Maßnahme und FL-Rate	FB-Maßnahme und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
$a_{y\,v,h}$	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Ausfall der analyt. Rd-Sensor-Überwach-ung Deshalb D-b-W in RFE überführen FB-R.: Gl. 4-28	Fehler wirkt sich verfügbarkeitskritisch aus. **Top-Event: B** Bzgl. der hierarchischen Modellierung etc. sei auf HF abs. LRW-Sensor verwiesen. Nach der Onboard-FB Offboard-FB einleiten: • Rote Warnlampe aktivieren • Ablegen der Fehlermeldung im Diagnosespeicher • $\nu_{Fahrer\text{-}Rot}$: Gl. 4-30 • MB-Service und Offboard-Reparaturrate gemäß Gl. 4-31 und 4-32
a_x	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Ausfall des SWS, damit Ausfall der analyt. Rd-Sensor-Überwach-ung Deshalb D-b-W in RFE überführen FB-R.: Gl. 4-28	Siehe HF Querbeschleunigungssensorik.
Einfach-Fehler der VA- u. HA-Rd.-Sen-soren	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Ausfall des SWS, damit Ausfall der analyt. Rd-Sensorüber-wachung Deshalb D-b-W in RFE überführen FB-R.: Gl. 4-28	Siehe HF Querbeschleunigungssensorik.
Zwei-fach-Fehler der VA- u. HA-Rd.-Sen-soren	HF	Fehler bedingt durch Ausfall des SWS bei Einfach-fehler nicht erkennbar.	-	-	**Top-Event: C**
Einfach-Fehler der VA- u. HA-Rd.-Sen-soren	SF	FE via analyt. Redundanz FEL-R.: Gl. 6-6	FE kommt FL gleich, siehe auch Abschnitt 6.1.3	Siehe einfache HF der Rd-Sensoren. FB-R.: Gl. 4-28	Siehe HF Querbeschleunigungssensorik.

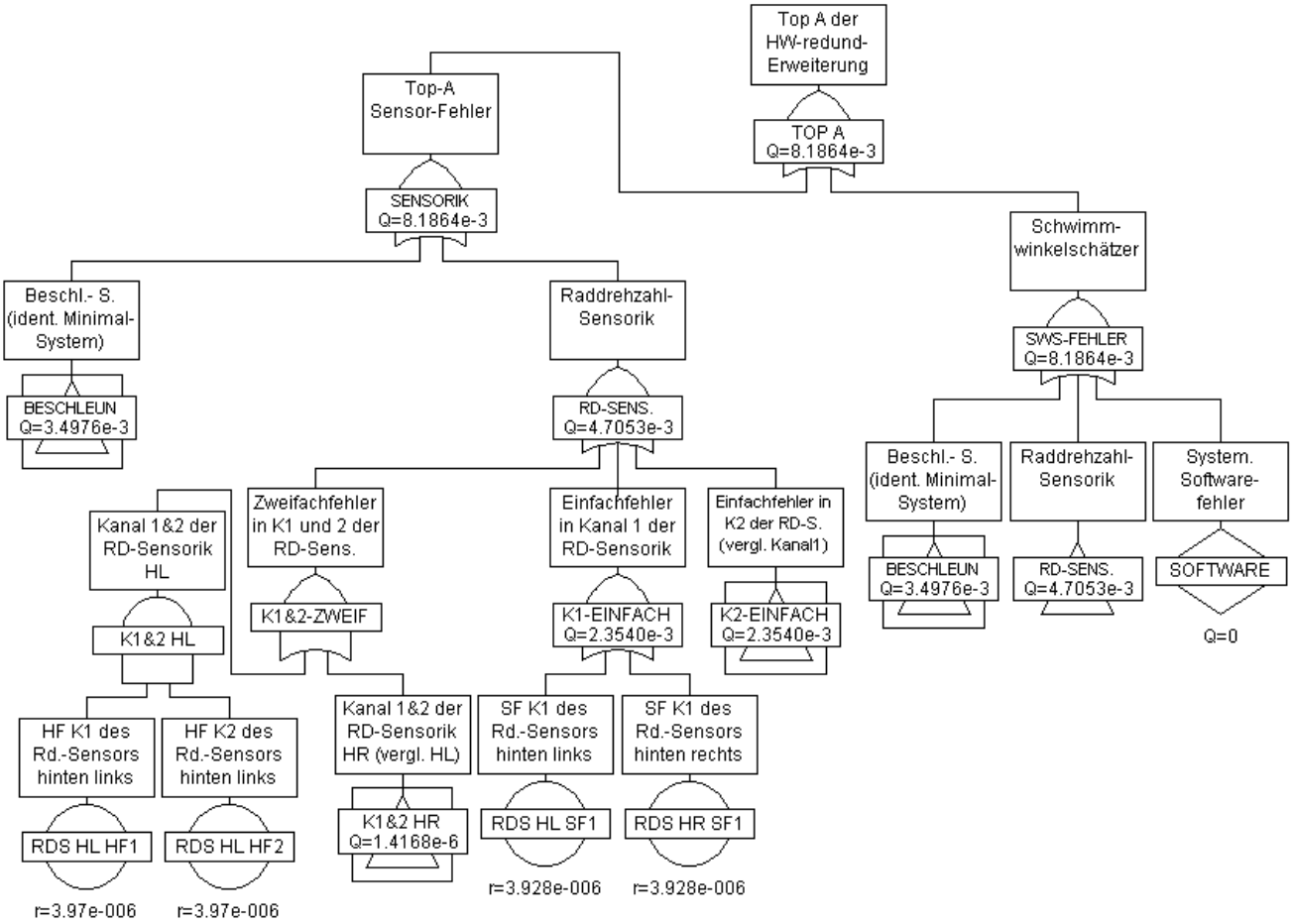
Fehler in Komp.	Fehler-mode	FE-Maßn. und FE-Rate	FL-Maßn. und FL-Rate	FB-Maßn. und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Zwei-fach-Fehler der VA- u. HA-Rd.-Sen-soren	SF	Siehe zweifache HF der Rd-Sensoren.	-	-	**Top-Event: C**
Vorder- u. Hinter-Achs-Rd.Sen-soren	TF	Nicht möglich ⇒ Mißalarm	-	-	**Top-Event: C** In hierarchischer Modellierung Übergang in absorbierenden sicherheitskritischen Zustand. Siehe weiterhin TF des abs. LRW-S.
Brems-Druck-sensor, Drossel-klappen-potentio-meter und Getriebe (Gang).	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Rote Warn-lampe, da Softfailures der Rd-Sensorik nicht länger überwach-bar. D-b-W in RFE überführen FB-R.: Gl. 4-28	**Top-Event: B** Weitere Details zur Offboard-FB siehe HF $a_{y\ v,h}$-Sensorik Anmerkung: der Fehler des Getriebes wird nur qualitativ mitmodelliert.
BLS	HF	Siehe HF des abs. LRW-S.	FE kommt FL gleich	Im Minimal-System: gelbe Warnlampe FB-R.: Gl. 4-28	Für die analytische Redundanz nicht erforderlich. **Top-Event: Qualitativ D zugeordnet (außerhalb Systemgrenze)**
Brems-Druck-sensor, Drossel-klappen-potentio-meter und Getriebe (Gang).	SF/TF	FE -System nicht möglich	-	-	Gefahr des Mißalarms, aber auch Fehlalarms, da nunmehr die SIS der Raddrehzahlsensorik nicht mehr funktionsfähig ist. Sicherheitsrelevanter „schlafender“ Fehler **Top-Event: C** Anmerkung: Der Fehler des Getriebes wird nur qualitativ mitmodelliert.
BLS	SF/TF	FE im Minimal-System nicht möglich	-	-	Mit Verweis auf obige Kommentare zu HF der Sensorik außerhalb der Betrachtungstiefe. **Top-Event: Qualitativ D zugeordnet (außerhalb Systemgrenze)**
Vorfilter-Infor-mation (2v2-Voting)	CCF	Analog zum Minimal-System	Analog zum Minimal-System	Analog zum Minimal-System	**Top-Event: B u. C** (die beiden Kanäle des Vorfilters entsprechen Gattern im Fehlerbaum, siehe Anhang K und L) Ansonsten weitestgehend analog Minimal-System Anhang E.

Fehler in Komp.	Fehler-mode	FE-Maßnahme und FE-Rate	FL-Maßnahme und FL-Rate	FB-Maßnahme und FB-Rate	Beteiligung an Top-Event und Auswirkung auf das System, Schadensschwere sowie Kommentare
Modulare ψ-Regler-Information (2v2-Voting)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler
SW-Schätzer-Information (2v2-Voting)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler bzw. Verlust der Überwachbarkeit der Rd-Sensorik.	Weitestgehend analog Minimal-System (Anhang E)
SIS-Information (einkanalig)	CCF	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Siehe Vorfilter-Fehler	Unter Berücksichtigung der zusätzlichen Sensorfehler (siehe Abschnitt 6.1.3 und aktuelle Tabelle) weitestgehend analog Minimal-System (Anhang E). **Top-Event: C (SIS-Gattern im Fehlerbaum)**

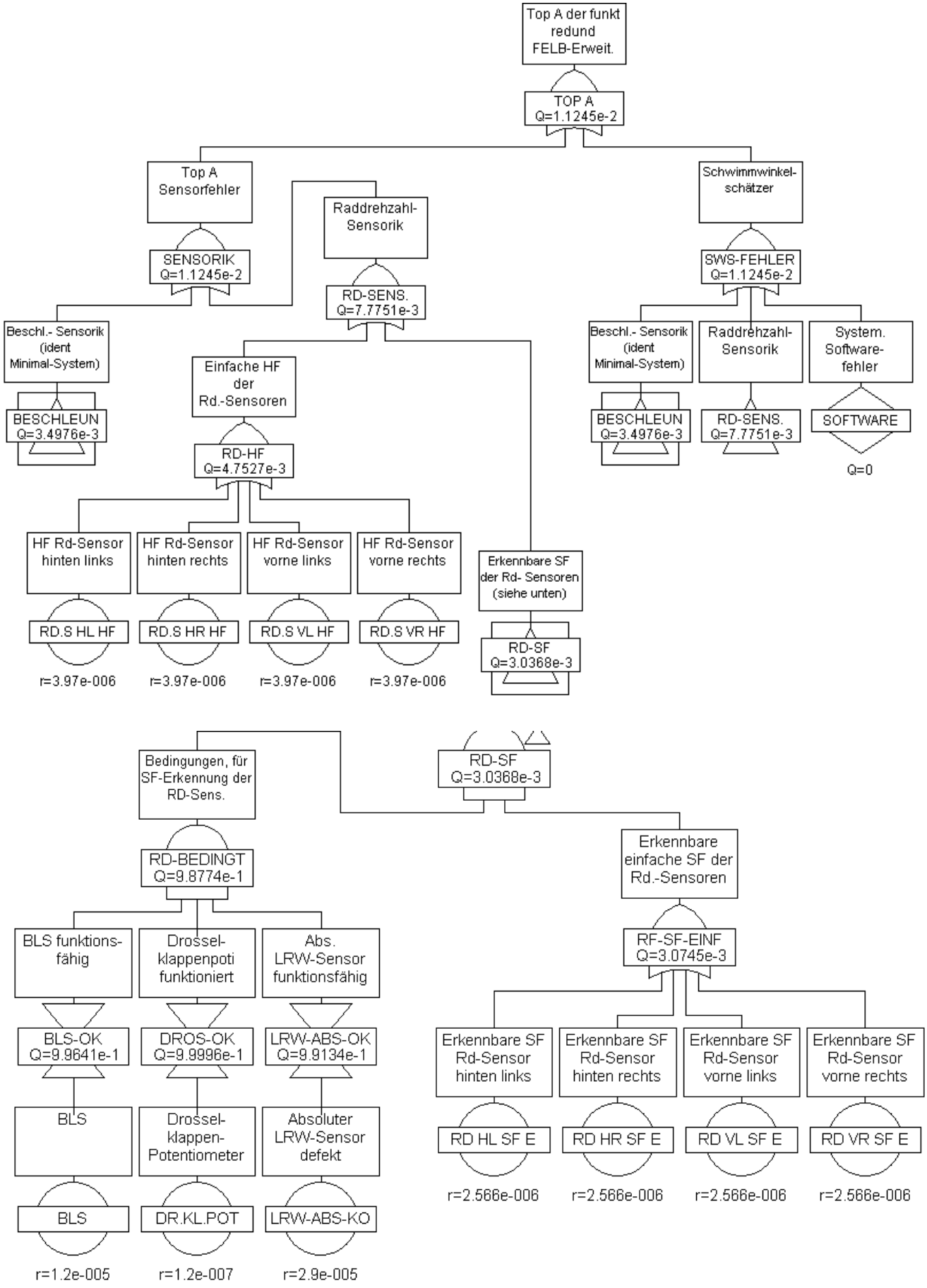
8.10 Anhang J: Fehlerbäume des Top-Events A der FELB-erweiterten D-b-W-Systeme

Anmerkung: Unter Top-Event A sind sämtliche Fehler zusammengefaßt, die zum Übergang des D-b-Ws von der höchsten Reglerstufe in die Reglerstufen 2 oder 3 führen (siehe Abschnitt 3.1.1.1).

8.10.1 Anhang J1: Fehlerbaum des Top-Events A des um eine redundante Raddrehzahlsensorik erweiterten Systems



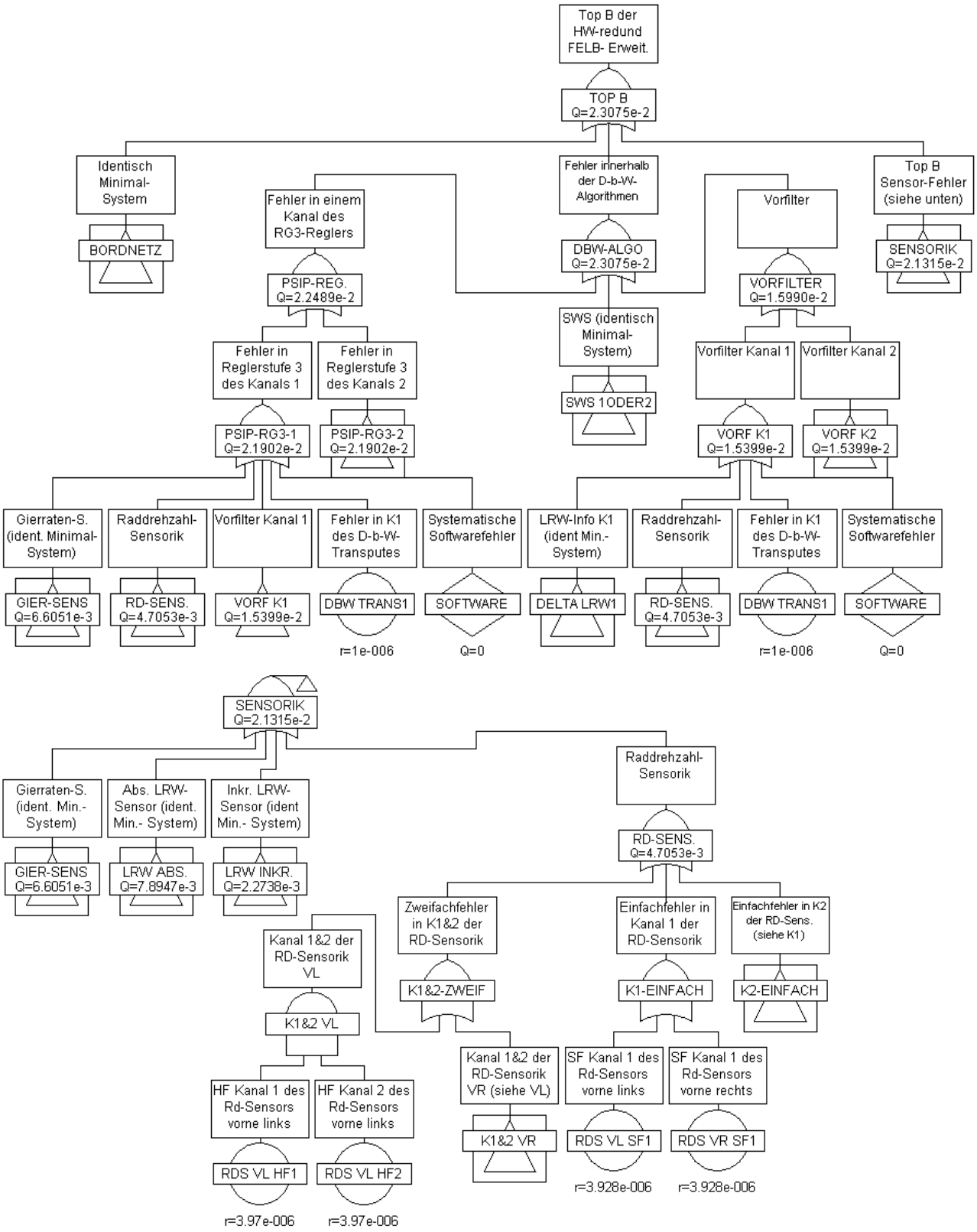
8.10.2 Anhang J2: Fehlerbaum des Top-Events A des um eine funktional redundante Raddrehzahlsensorik erweiterten Systems



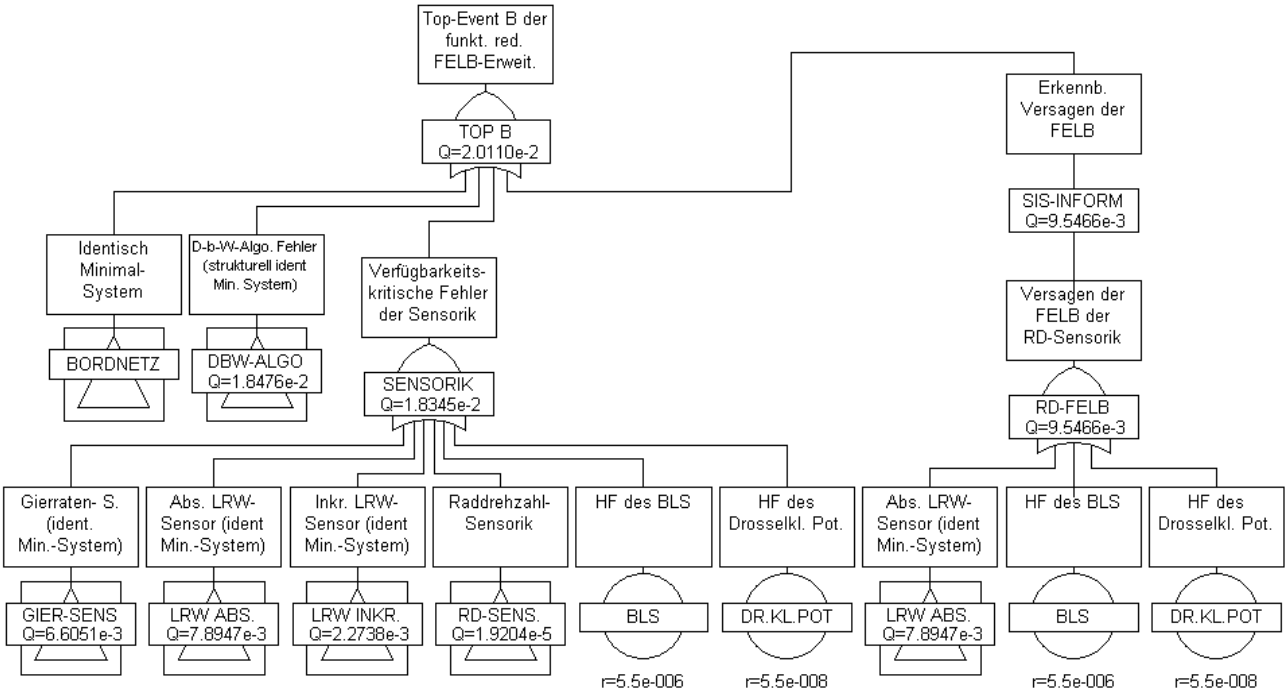
8.11 Anhang K: Fehlerbäume des Top-Events B der FELB-erweiterten D-b-W-Systeme

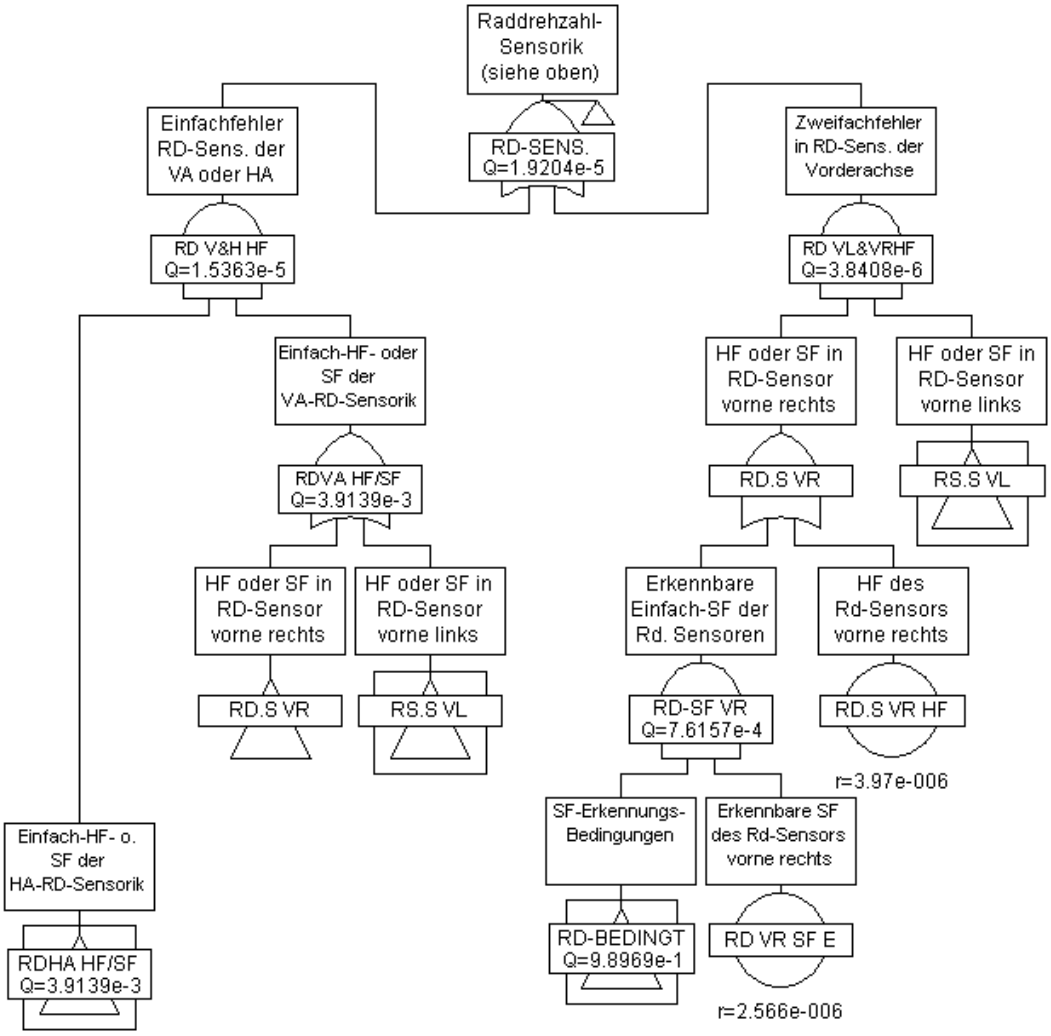
Anmerkung: Unter Top-Event B sind sämtliche Fehler zusammengefaßt, die zum Übergang des D-b-Ws in die Rückfallebene/Notlauf führen (siehe Abschnitt 3.1.1.2). Hierbei handelt es sich um die verfügbarkeitskritischen Fehler.

8.11.1 Anhang K1: Fehlerbaum des Top-Events B des um eine redundante Raddrehzahlsensorik erweiterten Systems

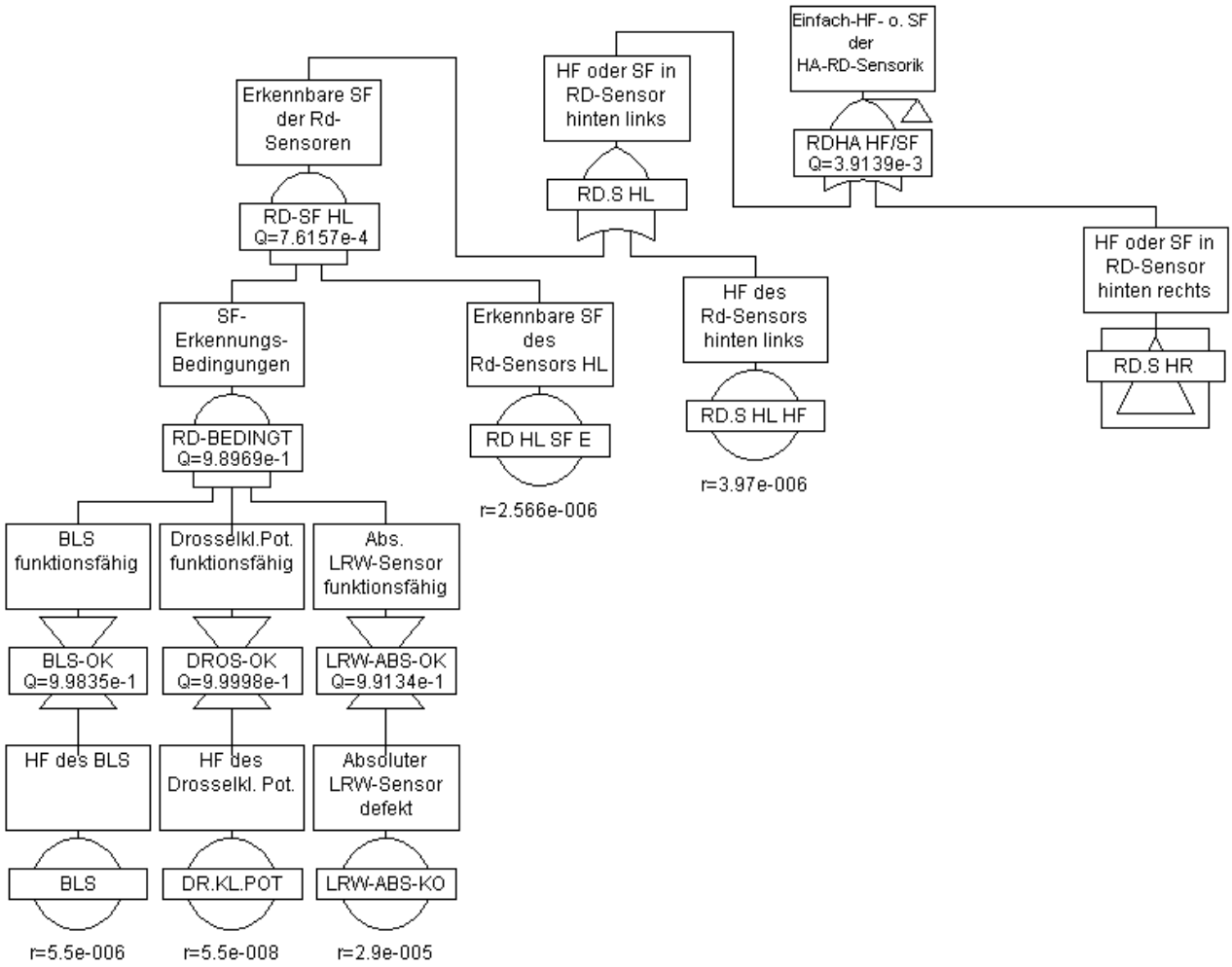


8.11.2 Anhang K2: Fehlerbaum des Top-Events B des um eine funktional redundante Raddrehzahlsensorik erweiterten Systems

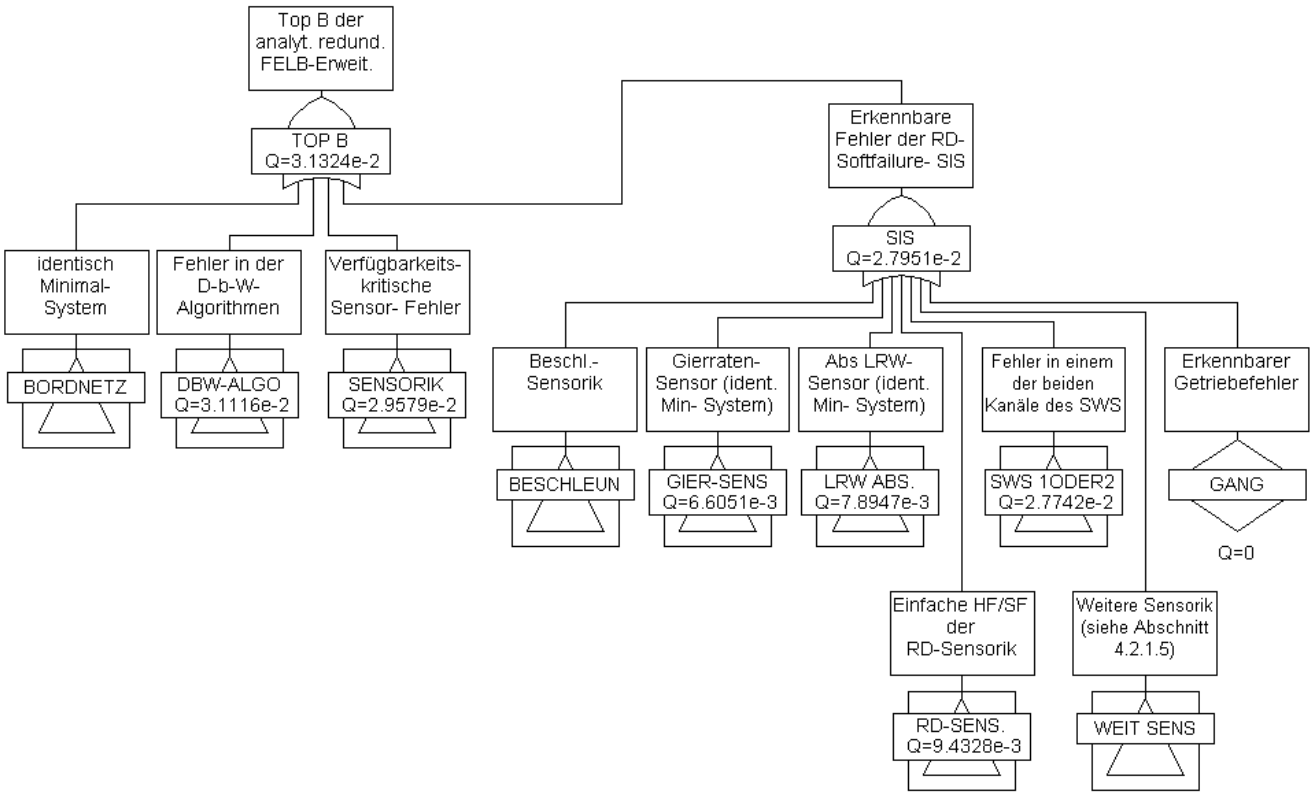


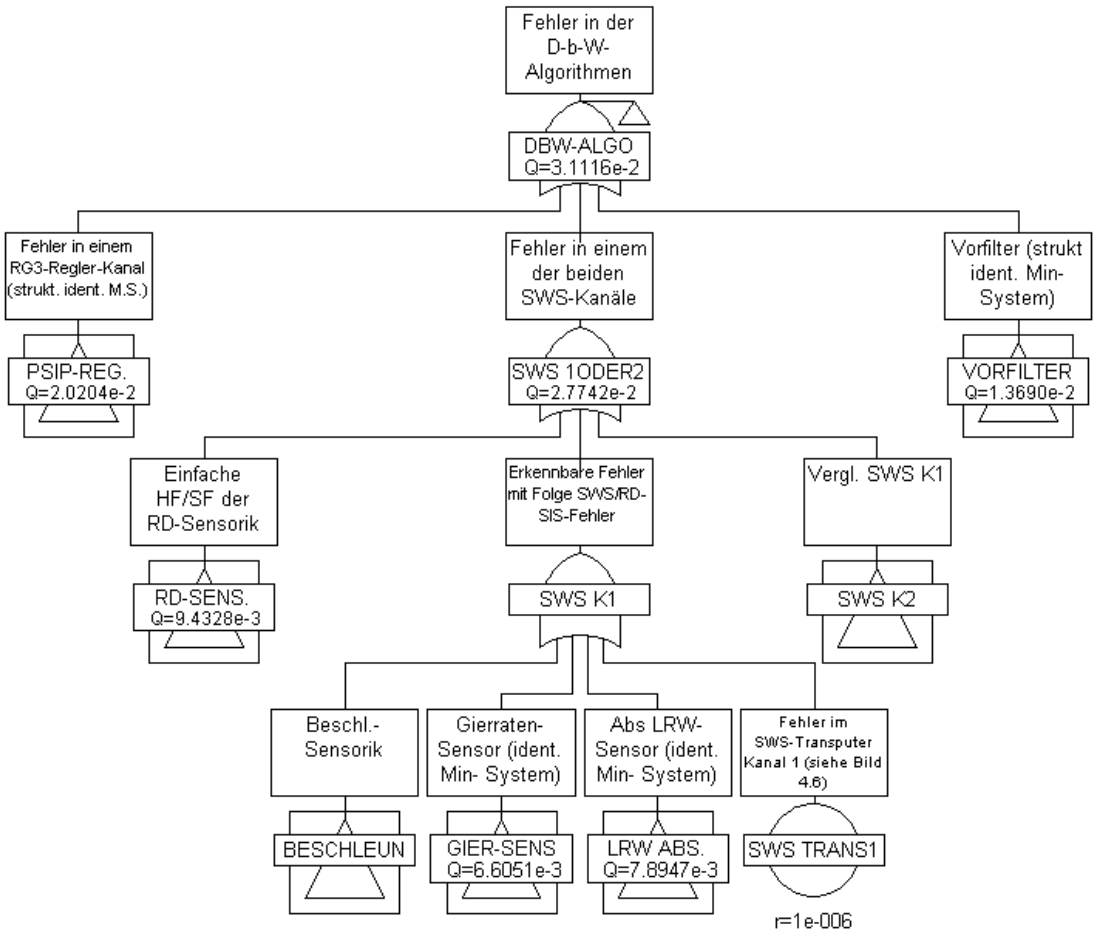


Fortsetzung des Fehlerbaums des Top-Events B des funktional erweiteren Systems

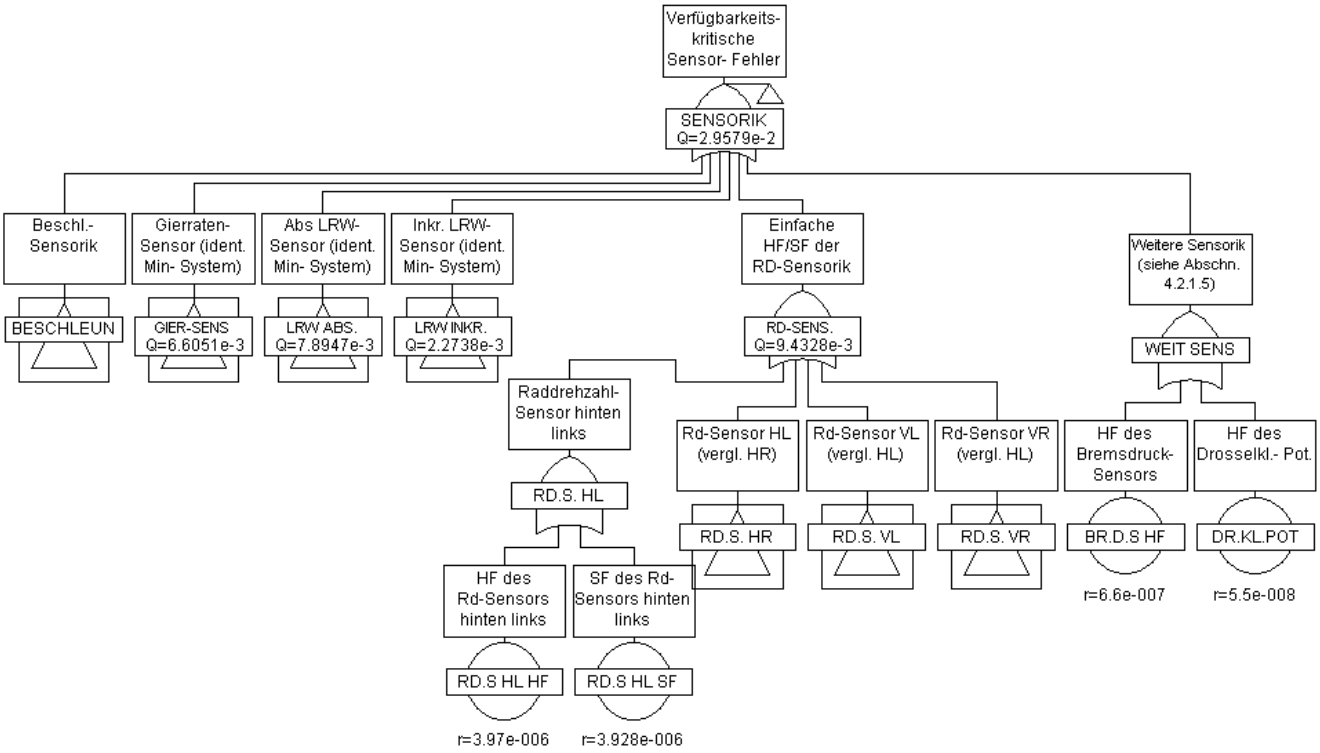


8.11.3 Anhang K3: Fehlerbaum des Top-Events B des um eine analytisch redundante Raddrehzahlsensorik erweiterten Systems





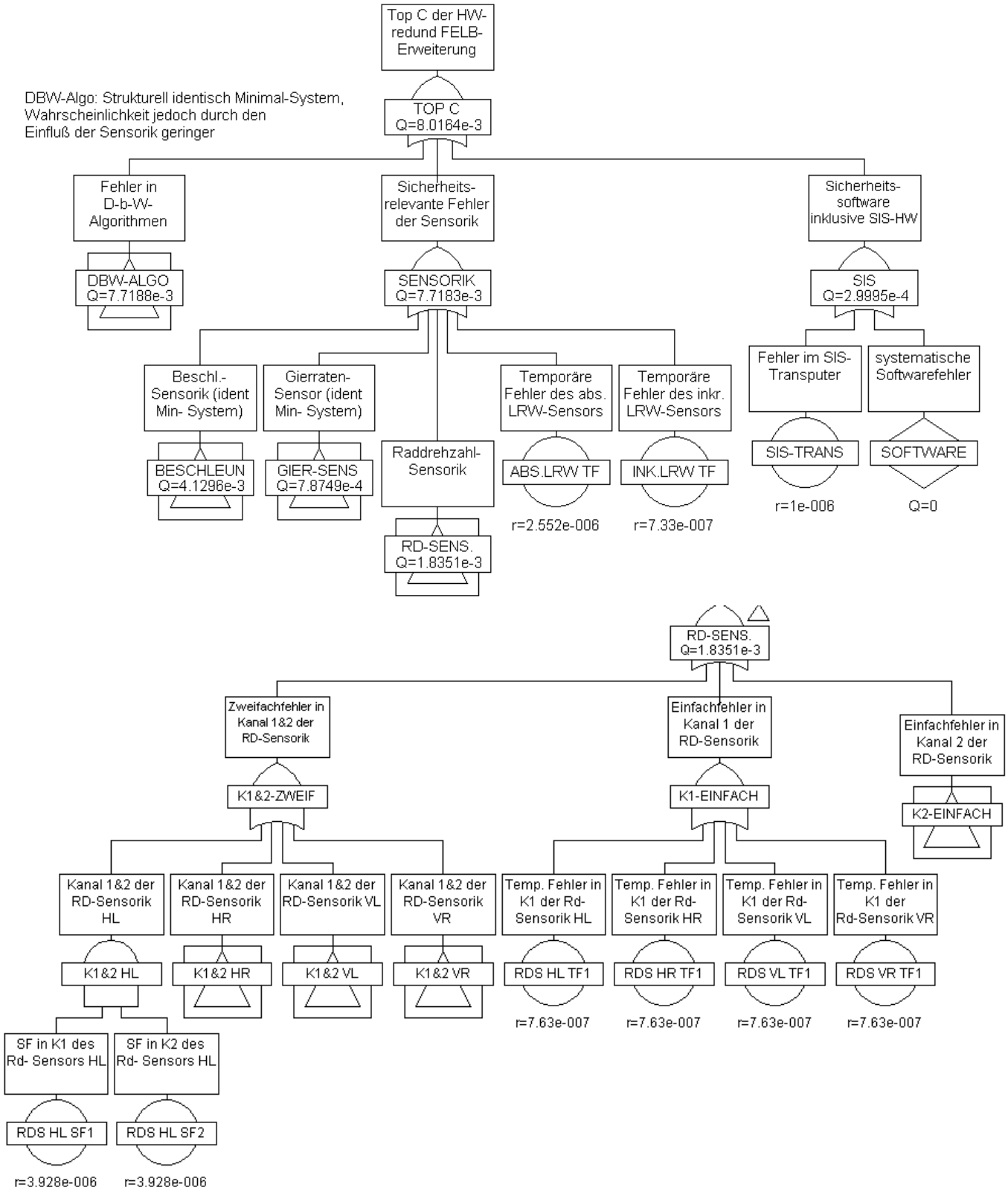
Fortsetzung des Fehlerbaums des Top-Events B des analytisch redundant erweiteren Systems



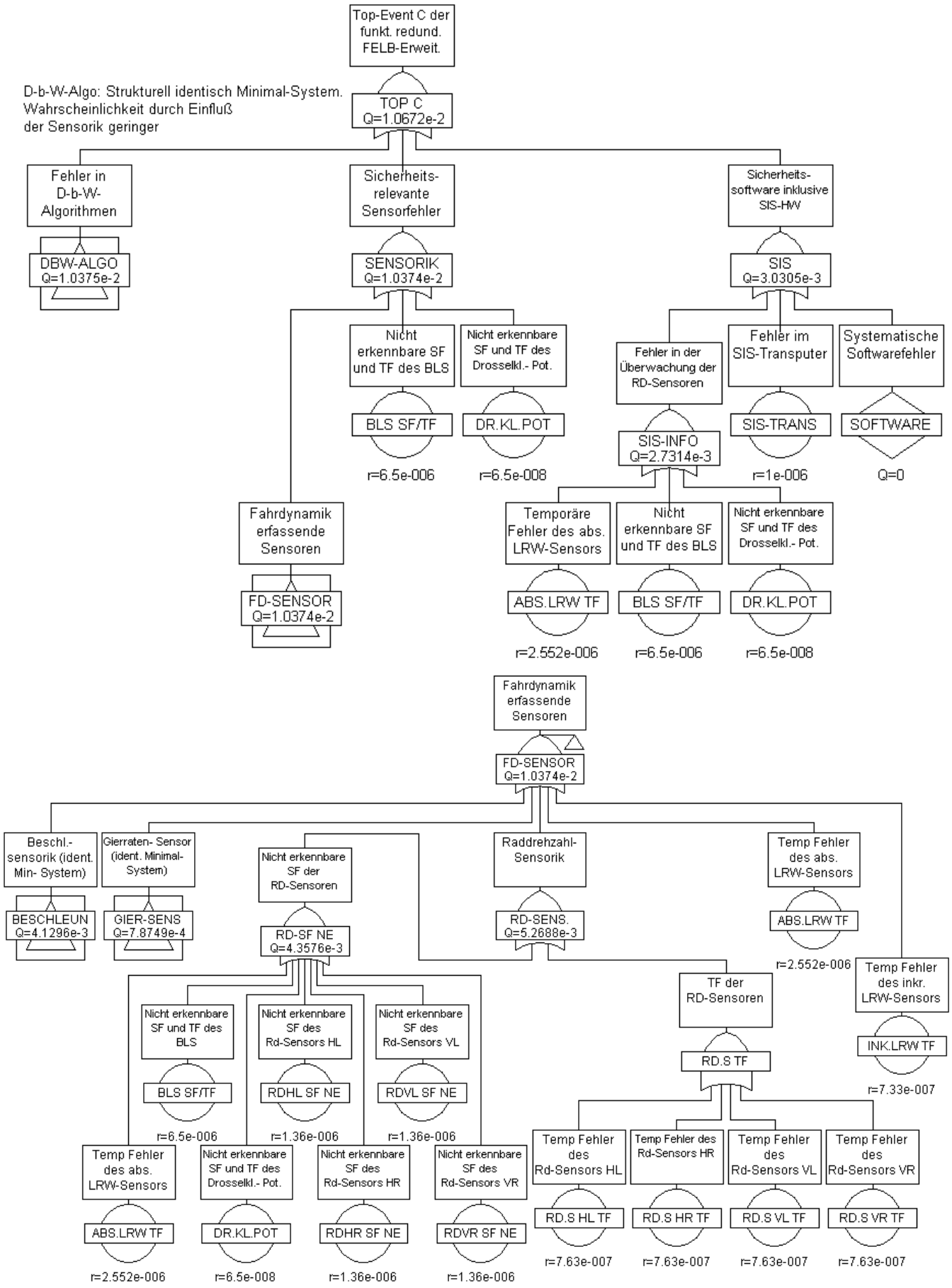
8.12 Anhang L: Fehlerbäume des Top-Events C der FELB-erweiterten D-b-W-Systeme

Anmerkung: Unter Top-Event C sind sämtliche sicherheitskritischen Fehler zusammengefaßt (siehe Abschnitt 3.1.1.3).

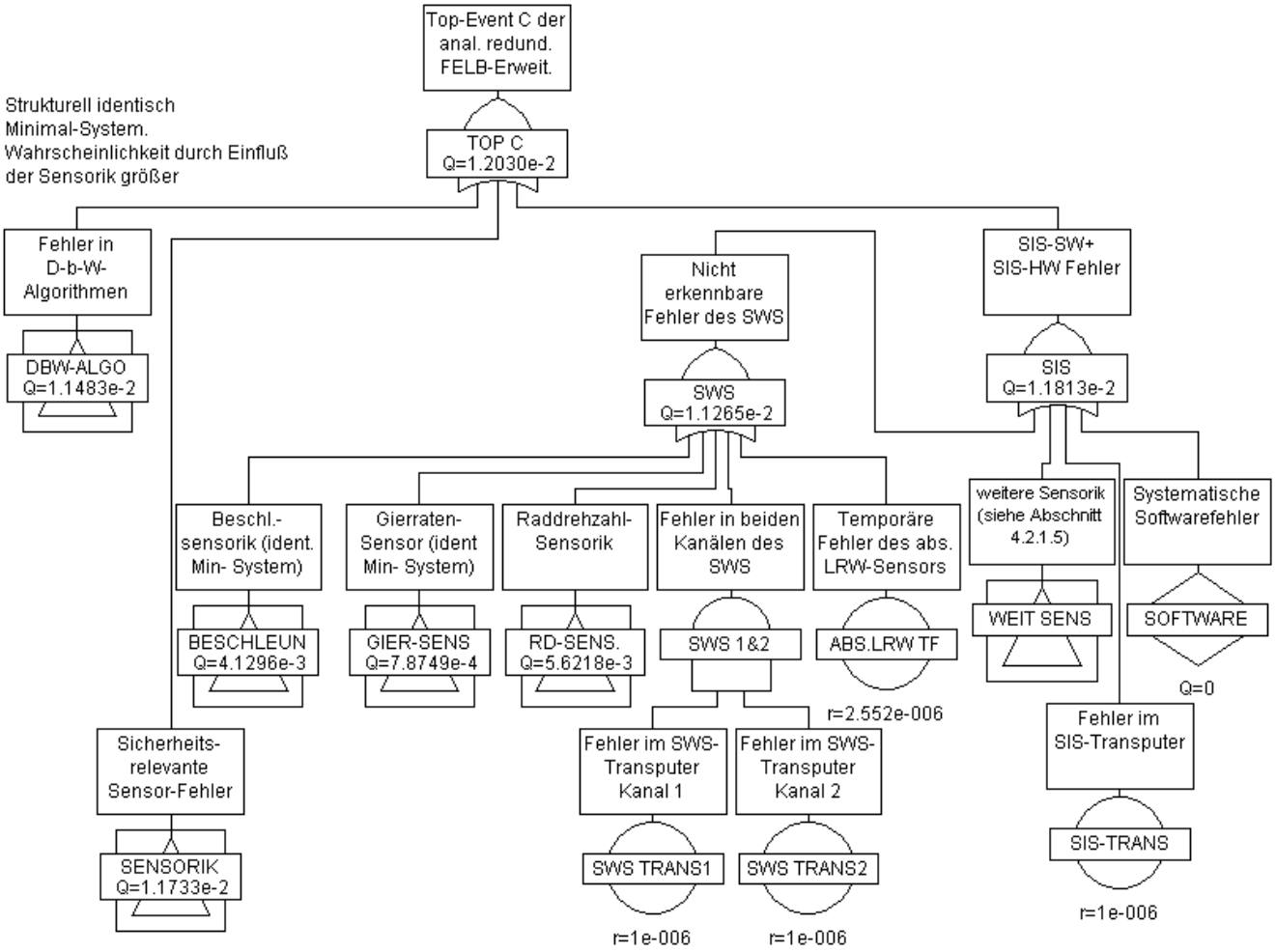
8.12.1 Anhang L1: Fehlerbaum des Top-Events C des um eine redundante Raddrehzahlsensorik erweiterten Systems



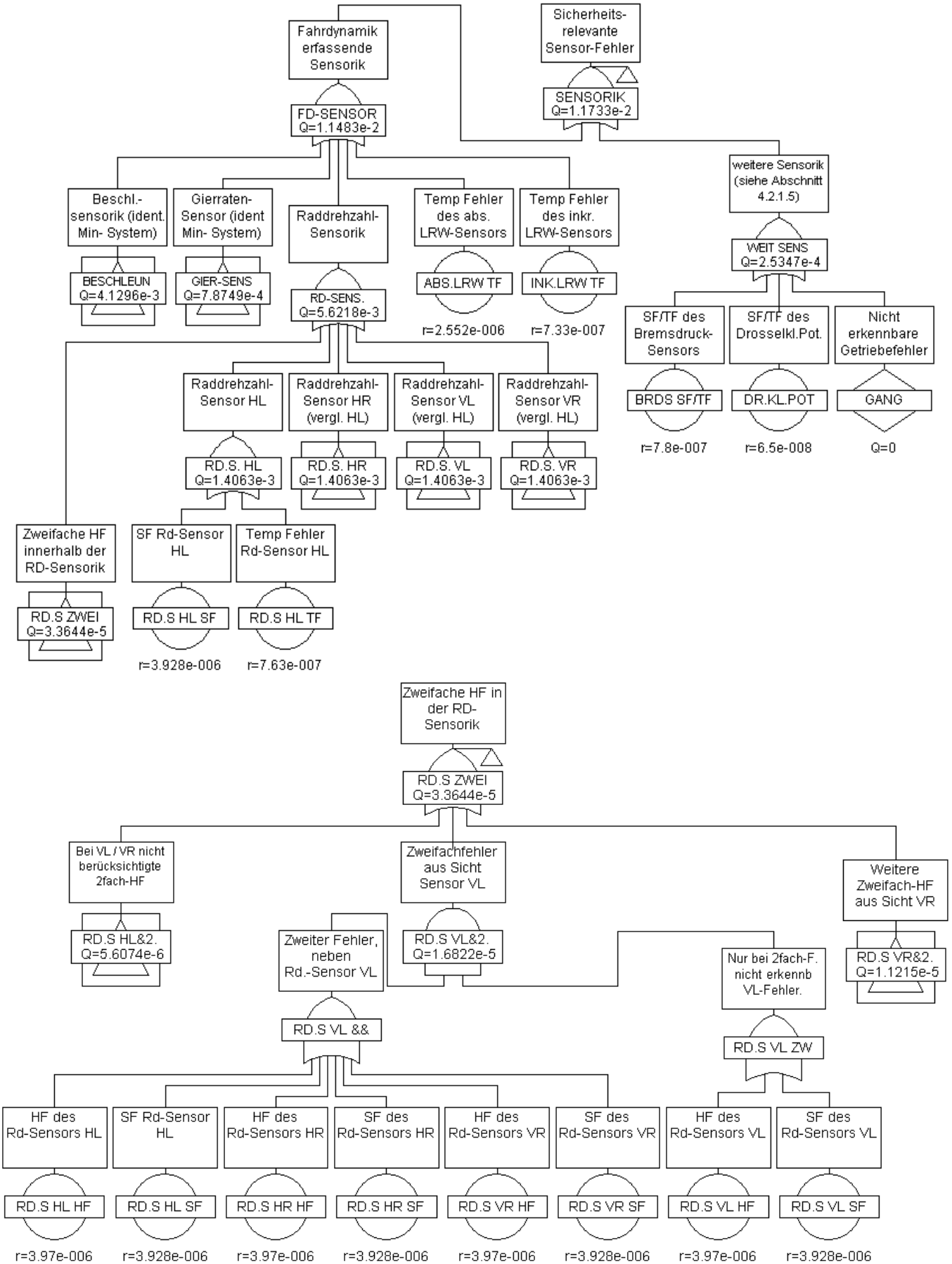
8.12.2 Anhang L2: Fehlerbaum des Top-Events C des um eine funktional redundante Raddrehzahlsensorik erweiterten Systems



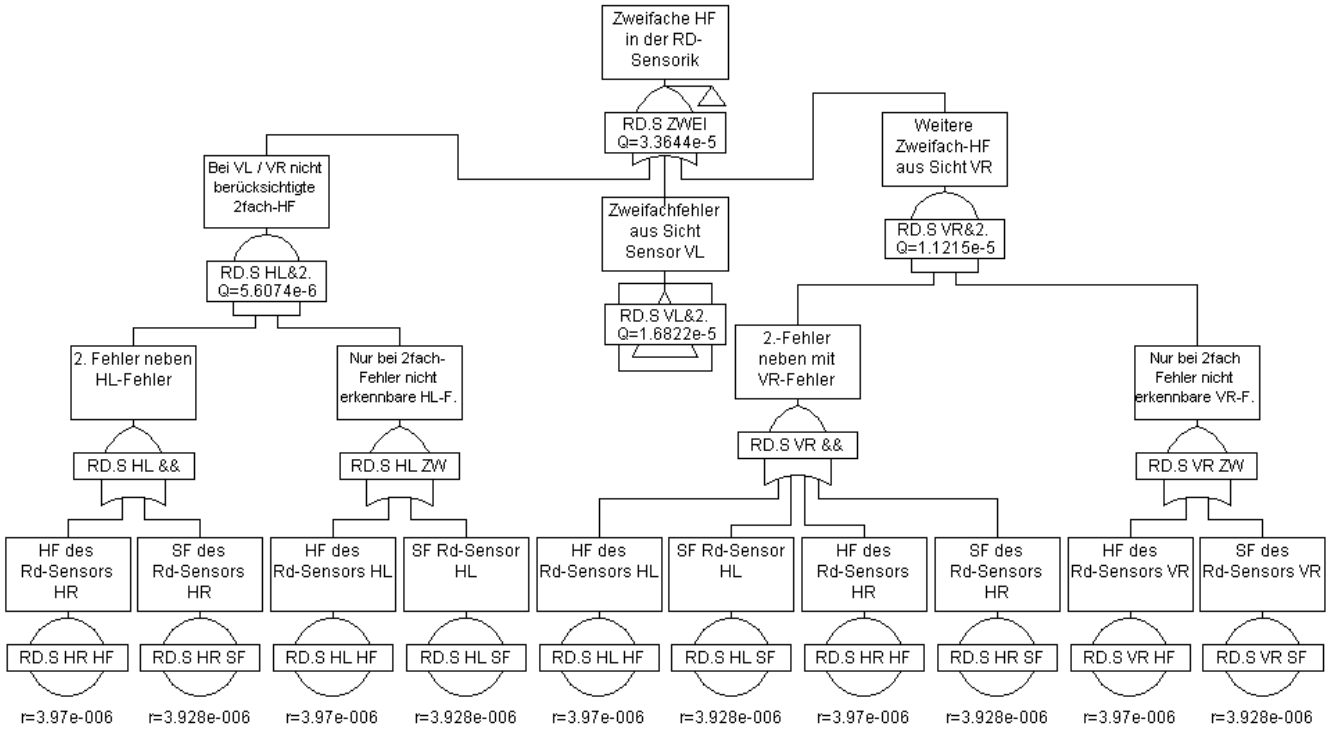
8.12.3 Anhang L3: Fehlerbaum des Top-Events C des um eine analytisch redundante Raddrehzahlsensorik erweiterten Systems



1. Fortsetzung des Fehlerbaums des Top-Events C des analytisch redundant erweiterten Systems



2. Fortsetzung des Fehlerbaums des Top-Events C des analytisch redundant erweiterten Systems



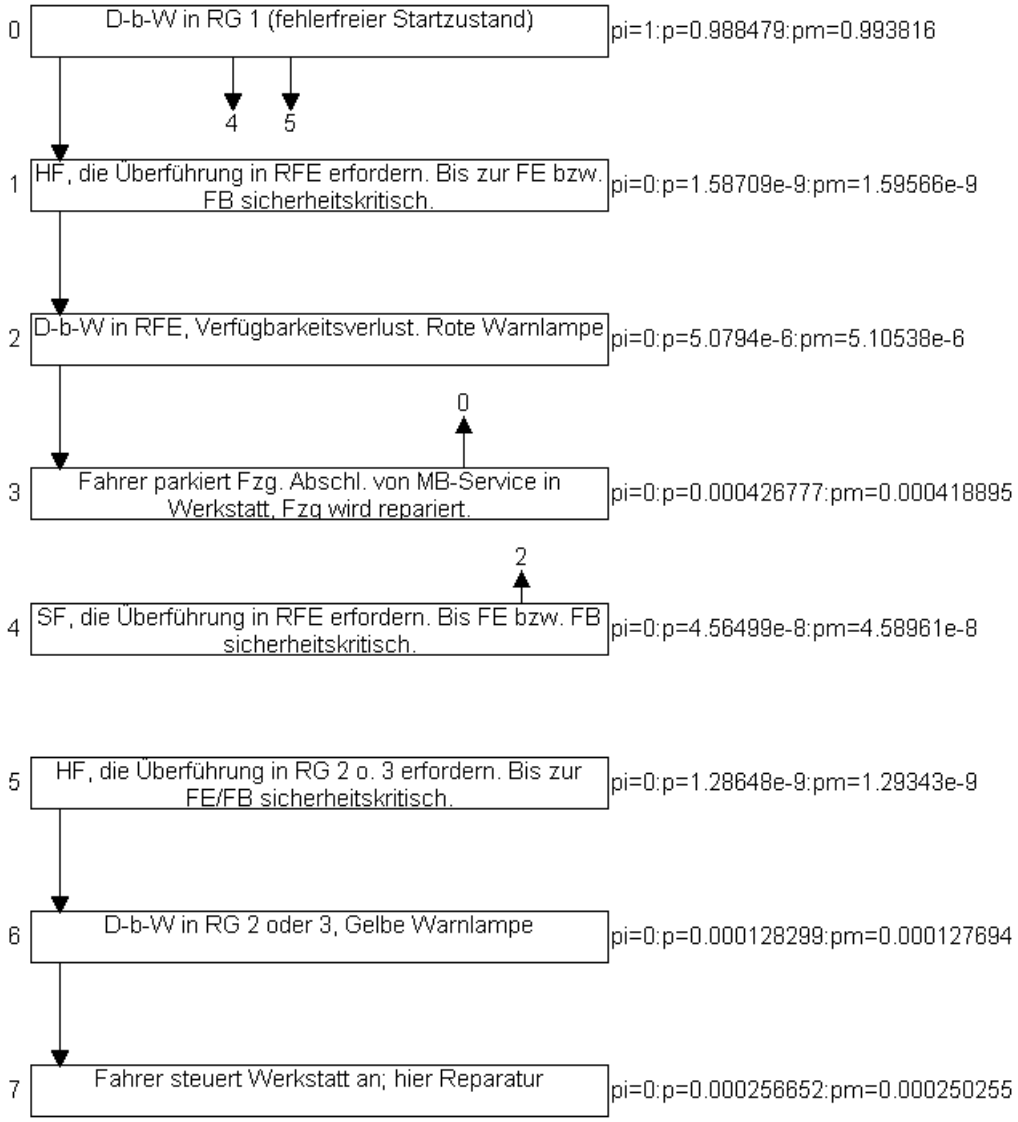
8.13 Anhang M: Änderungen der Zustände und Zustandsübergänge des mittels funktional redundanter FELB-Erweiterung modifizierten Systems

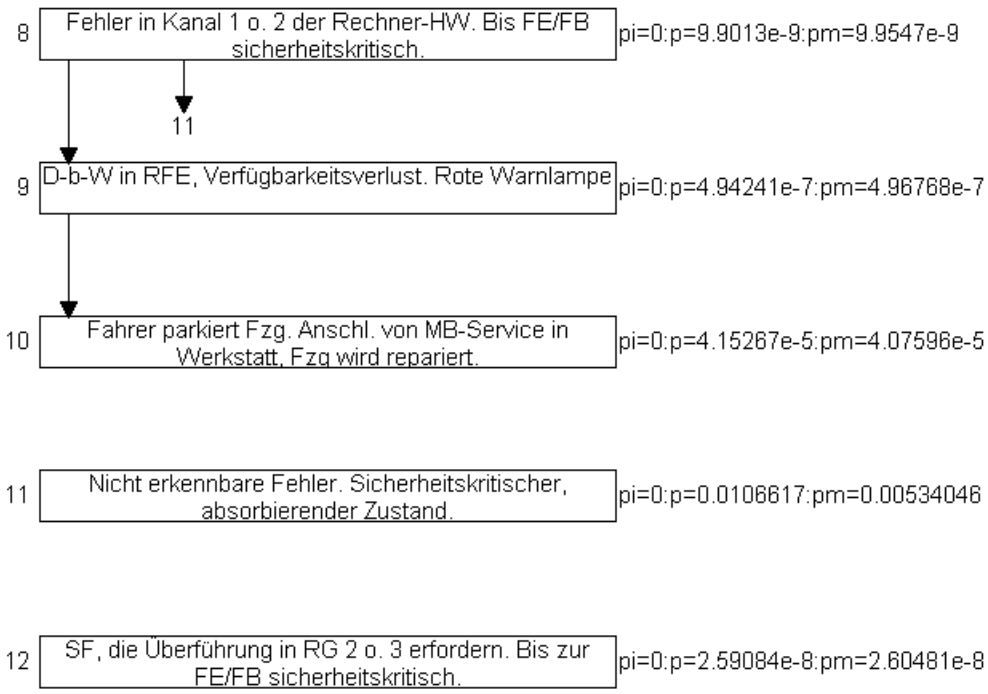
Um den Umfang der vorliegenden Arbeit zu minimieren, sollen an dieser Stelle nur die von der Zustandsraumdarstellung des Minimal-System (Anhang H) abweichenden Zustände und Übergänge aufgeführt werden.

Zu-stand	Beschreibung des Zustands	Über-gang (-srate)	Beschreibung des Übergangs
0	Siehe Zustand 0, Anhang H bzw. Bild 6.10	$q_{0,1}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • HF(abs. LRW-Sensor + inkr. LRW-Sensor + Gierratensensor) **Gegenüber $q_{0,1}$ des Minimal-Systems zusätzlich :** • HF BLS und DK-Poti **Dafür ohne Rd-Sensorik** $q_{0,1} = l_{Modul} = 34 \cdot 10^{-6} \frac{1}{h}$
		$q_{0,5}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • HF Längs- und Querbeschleunigungssensorik • HF Rd-Sensorik der Hinterachse **Gegenüber $q_{0,5}$ des Minimal-Systems zusätzlich :** • HF Rd-Sensorik der Vorderachse $q_{0,5} = \lambda_{Modul} = 27{,}56 \cdot 10^{-6} \frac{1}{h}$
		$q_{0,11}$	Fehlerrate, hervorgehend aus Fehlerbaum, fussend auf "Veroderung" folgender Eingangsgrößen (siehe Kap. 4): • TF (abs. LRW + inkr. LRW + Gier-S. + Längs- und Querbeschleunigungssensorik + Rd-Sensorik) • SF Gierraten-S. im nicht überwachbaren Fahrdynamikbereich. • SF Beschleunigungssensorik • Fehler in Transputer SIS • **Gegenüber dem Minimal-System zusätzlich nicht erkennbare Fehler des BLS + DK-Poti** • **Gegenüber dem Minimal-System nur noch SF der Rd-Sensorik im nicht überwachbaren Bereich** $q_{0,11} = \lambda_{Modul} = 35{,}76 \cdot 10^{-6} \frac{1}{h}$ Diese Übergangsrate entspricht der Summe der Gatter-Übergangsraten „Sensorik“ und SIS des Fehlerbaums des Top-Events C. Vergleiche Anhang L
		$q_{0,12}$	**Gegenüber dem Minimal-Systems zusätzlicher Zustands-übergang:** Fehler- bzw. Ausfallrate, die sich über einen Fehlerbaum mit der Veroderung aus folgenden Eingangsgrößen zusammensetzt (siehe auch Kap. 4) : • SF Rd-Sensorik im überwachbaren Bereich $q_{0,12} = \lambda_{Modul} = 10{,}27 \cdot 10^{-6} \frac{1}{h}$
12	**Gegenüber dem Minimal-System zusätzlicher Zustand** SF, die über die funkt. Redundanz erkannt werden (Pendant zu Zustand 4) • Vor FB sicherheitskritisch. • Zustand 12 in Bild 6.10 farblich rot hervorgehoben • Startaufenthaltswahr-scheinlichkeit = 0	$q_{12,6}$	**Gegenüber dem Minimal-Systems zusätzlicher Zustands-übergang:** Übergangsrate basiert auf der FE- und FB-Raten (siehe Gl. 4-26 und 4-28). Da der Übergang in Zustand 6 im Mittel nach Verstreichen der mittleren Fehlererkennungs und -behandlungszeit erfolgt, bestimmt sich die Übergangsrate aus dem Kehrwert der Summe beider Zeiten. Unter Verwendung von Gl. 4-25 und 4-28 ergibt sich (siehe auch Kap. 4) : $q_{12,6} = \frac{e_{Soft} \cdot V_{Onboard}}{e_{Soft} + V_{Onboard}} = 599 \frac{1}{h}$ Diese „heilende“ Onboard Übergangsrate konnte bei der Fehler-baumanalyse (Abschnitt 6.3) nicht berücksichtigt werden.

8.14 Anhang N: Modellierung der Markov-Kette des mittels funktionaler Redundanz erweiterten D-b-W-Systems

Wie beim Minimal-System erfolgt die Bestimmung der Aufenthaltswahrscheinlichkeiten in den Systemzuständen durch das Tool MKV.





Hierin entspricht:

- pi der Startwahrscheinlichkeit im jeweiligen Zustand
- p der zum Zeitpunkt t = 300 Stunden bestimmten Aufenthaltswahrscheinlichkeit im jeweiligen Zustand
- pm der mittleren Aufenthaltswahrscheinlichkeit im jeweiligen Zustand.

Es ist zu erwähnen, daß wie schon in Anhang H nicht alle in die quantitative Zustandsraumanalyse einfließenden Zustandsübergangsraten grafisch in MKV wiedergegeben werden (siehe beispielsweise Übergangsrate vom Zustand 10 zum Zustand 0).