Kapitel 3
Methodik zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen

Bernd Bertsche unter Mitarbeit von Jochen Gäng

Im Folgenden soll eine Methodik zur Zuverlässigkeitsbewertung mechatronischer Systeme vorgestellt werden, die in frühen Entwicklungsphasen anwendbar ist. Eine wichtige Anforderung an diese Methodik ist die Verknüpfung an mechatronischen Entwicklungsmethoden, um so die Entwicklungstätigkeiten sowie die Konzeptauswahlentscheidungen zu unterstützen. Dies erlaubt dann das zuverlässigste Konzept auszuwählen. Dadurch können Kosten und Zeit gespart werden, da

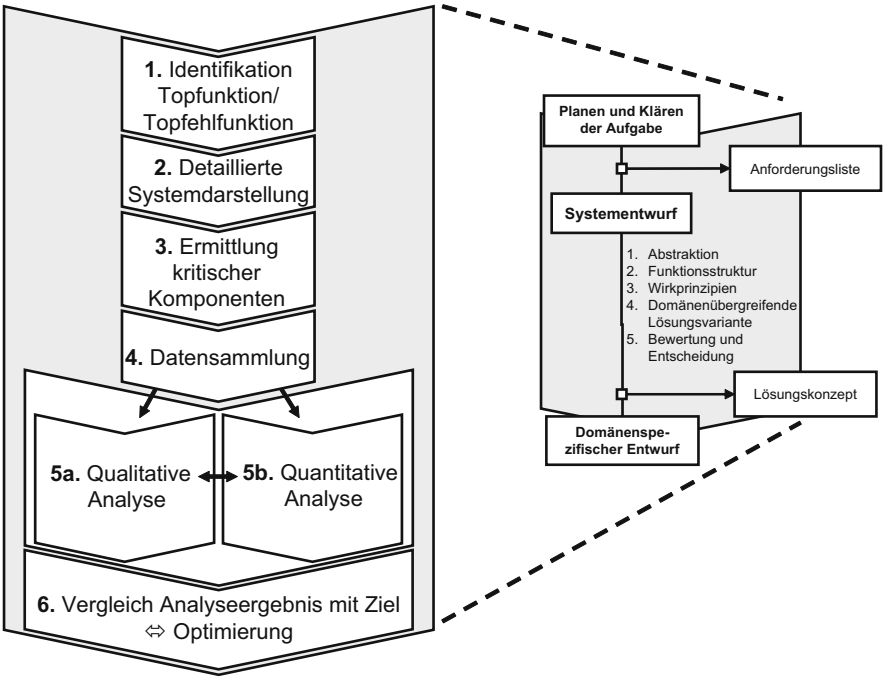

Abb. 3.1 Methodik zur Zuverlässigkeitsbewertung in frühen Entwicklungsphasen [3.46, 3.19]

B. Bertsche et al., *Zuverlässigkeit mechatronischer Systeme*,

die Auswahl eines unzuverlässigen Konzepts im Nachhinein viele aufwändige Änderungen bis zu einer Neukonzeption mit sich bringen kann.

Für die Auswahl der Entwicklungsmethode bietet sich das V-Modell aus der Richtlinie VDI 2206 [3.44] an (siehe Kap. 2.2). Mit dem Schwerpunkt der frühen Entwicklungsphasen muss besonders die erste Phase des V-Modells, der Systementwurf, näher betrachtet werden.

Anhand des Systementwurfes ist eine Vorgehensweise entstanden, die insgesamt sechs Schritte umfasst (Abb. 3.1). Diese sind im Laufe der Förderzeit der Forschergruppe nach und nach erweitert worden. Im Folgenden werden die einzelnen Schritte detailliert beschrieben und erklärt.

3.1 Identifikation Topfunktion/Topfehlfunktion

Im ersten Teilschritt der Methodik zur Zuverlässigkeitsbewertung werden so genannte Topfunktionen und Topfehlfunktionen bestimmt. Hierbei stellen die Topfunktionen die Art von Funktionen dar, welche eine hohe Abstraktionsebene besitzen. Nach [3.2] sind Topfunktionen zur Erfüllung der Produktziele für das Gesamtsystem unerlässlich. Die Topfunktionen werden weiter untergliedert in Teilsystemfunktionen und Subsystemfunktionen bis hin zu Bauteilfunktionen (Abb. 3.2). Wie zu sehen ist, können Topfunktionen aus mehreren Teilsystemfunktionen bestehen.

Die Vorgehensweise zur Erlangung der Topfunktionen ähnelt dabei der Vorgehensweise bei der FMEA. Im Gegensatz zur FMEA werden für die Zuverlässigkeitsbewertung mechatronischer Systeme jedoch nichtfunktionale Betrachtungen, wie z. B. Garantie oder Reparaturfreundlichkeit nicht mit aufgenommen.

Zur Verdeutlichung des Aufstellens von Topfunktionen bzw. Topfehlfunktionen wird als einfaches Beispiel ein Telefon verwendet. Für dieses System sind die Topfunktionen wie folgt festgelegt:

- Ferngespräch aufbauen
- Sprachkommunikation ermöglichen.

Um nun an die Topfehlfunktionen zu gelangen, werden die Topfunktionen im einfachsten Fall negiert. Es ist aber auch möglich, dass einer Topfunktion mehrere Topfehlfunktionen zugeordnet werden. Bei dem Telefon sind die Topfehlfunktionen:

- Aufbau eines Ferngesprächs nicht möglich
- Sprachkommunikation nicht möglich
- Sprachkommunikation nur eingeschränkt möglich.

Die aufgestellten Topfunktionen bzw. die Topfehlfunktionen besitzen aus Kundensicht verschiedene Wertigkeiten. An dieser Stelle wird das in Kap. 2.8 bereits schon erwähnte Klassierungsverfahren nach [3.10] eingesetzt. Beispielsweise ist eine Funktion, die nur eingeschränkt nutzbar ist, für den Kunden nicht so gravie-

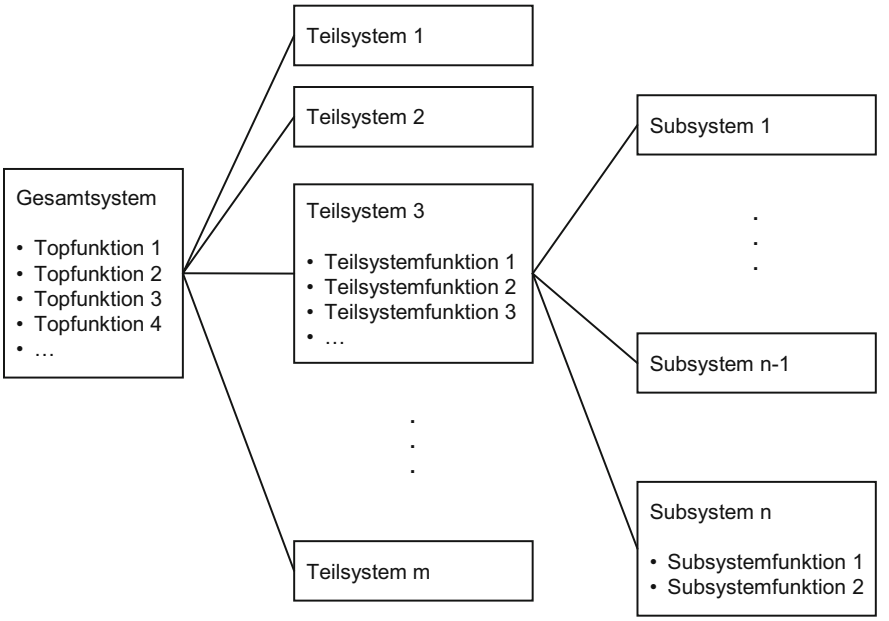

Abb. 3.2 Hierarchische Aufteilung der Funktionen des Systems

rend wie eine Funktion, die gar nicht zur Verfügung steht. Diesen Schweregraden und dadurch auch den Funktionen bzw. den Fehlfunktionen werden in einem weiteren Schritt Zuverlässigkeitsziele zugeordnet. Dadurch wird ermöglicht, dass die Zuverlässigkeitsbewertung mit den vorgegebenen Zuverlässigkeitszielen verglichen werden kann. Wie die einzelnen Zuverlässigkeitszielwerte ermittelt werden, ist in Kap. 2.8 erklärt.

3.2 Detaillierte Systemdarstellung

Im zweiten Schritt soll ausgehend von den Topfunktionen bzw. Topfehlfunktionen eine Methode verwendet werden, die Informationen wie beispielsweise aus dem Lastenheft oder allgemein von einem prinzipiellen Aufbau aufnehmen kann und damit eine funktionale Beschreibung ermöglicht. Informationen können nach [3.45] in unterschiedlicher Form vorliegen.

- Verbale Beschreibung,
- Blockbild/Graph,
- Prinzipskizzen,
- Prinzipschaltplan,
- Materielle Muster.

Die Quellen der Informationsgewinnung für frühe Entwicklungsphasen sind nach [3.31]

- Erfahrung,
- Bekannte Produkte,
- Vorentwicklung,
- Kataloge,
- Normen,
- Anforderungslisten.

Wird exemplarisch der Bereich Mechanik herausgegriffen, kann hier die Informationslage mit Hilfe einer Prinzipskizze und einer verbalen Beschreibung untersucht werden. Die Prinzipskizzen zeigen sowohl Hauptelemente des zu entwickelnden Produkts als auch eine grobe Baugruppenanordnung. Mittels der verbalen Beschreibung wird zusätzlich der funktionale Aufbau analysiert. Letzteres tritt auch stets bei der Anwendung der gesamten Informationsarten über alle Domänen hinweg auf. Deshalb ist es sinnvoll Methoden anzuwenden, welche funktionale Gesichtspunkte in den Vordergrund stellen. Hier können z. B. so genannte Anwendungsfälle (englisch: Use Case) verwendet werden. Der generelle Aufbau einer Anwendungsfall-Schablone ist in Abb. 3.3 zu sehen. Im Folgenden werden die einzelnen Punkte detailliert beschrieben.

1. Eintrag eines kurzen und sinnvollen Namens des Anwendungsfalls
2. Beschreibung des Ziels
3. Angabe von Bedingungen, welche erfüllt sein müssen, bevor der Anwendungsfall aufgerufen wird. Hierbei können mehrere Bedingungen möglich sein. Diese werden dann durchnummeriert.
4. Die Angabe des erwarteten Ergebnisses, das nach einem erfolgreichen Durchlaufen des Anwendungsfalls erwartet wird.
5. Die Angabe des erwarteten Ergebnisses, das nach einem fehlerhaften Durchlaufen des Anwendungsfalls erwartet wird.
6. Aufzählung von beteiligten Personen und Systemen, z. B. Nutzer, Maschinen, Softwarekomponenten.
7. Beschreibung des Hauptablaufs, welcher als Schrittfolge hin zum Ziel des Anwendungsfalls definiert ist.
8. Erweiterungen der Schrittfolgen aus Punkt 7.
9. Bestimmung des Ereignisses, das die Schrittfolge bestimmt.
10. Bezeichnung der einzelnen Schritte.
11. Neben dem Hauptablauf kann es noch alternative Schrittfolgen geben, welche ebenso zum Ziel des Anwendungsfalls führen.

Ein Vorteil der Verwendung der Anwendungsfälle ist, dass sie Teil der Unified Modeling Language (UML) sind. UML stellt eine standardisierte und weit verbreitete Modellierungssprache für Software dar. Durch die grafische Notation und die verschiedenen Werkzeuge kann UML sowohl von Software-Experten als auch von Ingenieuren verstanden werden. Dadurch kann UML als eine Schnittstelle zwischen den Domänen dienen.

Anwendungsfall < Nr >	**< Anwendungsfall Name > *1***	
Ziel	***2***	
Vorbedingung	***3***	
Nachbedingung Erfolg	***4***	
Nachbedingung Fehlschlag	***5***	
Akteure	***6***	
Beschreibung ***7***	Schritt	Aktion
	Ereignis	***9***
	1.1	***10***
	1.2	***10***
	…	
Erweiterung ***8***	Schritt	Aktion
	Ereignis	***9***
	1.1.1	***10***
	1.2.1	***10***
Alternativen	***11***	

Abb. 3.3 Anwendungsfall-Schablone in Anlehnung an [3.24]

Mittels der Beschreibung der funktionalen Ablauffolge in den Anwendungsfällen besteht die Möglichkeit Informationen über das System, explizit über mögliche zu verbauende Komponenten, zu erfahren. Wird beispielsweise in einem der formulierten Anwendungsfälle die Abfrage einer Geschwindigkeitsinformation beschrieben, so kann daraus gefolgert werden, dass in dem betrachteten System ein Sensor verbaut werden muss, der eine Geschwindigkeitsinformation liefert. Werden nun alle Anwendungsfälle systematisch nach solchen Informationen durchsucht, so lässt sich mit den gewonnenen Erkenntnissen ein erstes physikalisches Modell aufbauen, in dem die aus den Anwendungsfällen identifizierten mechanischen und elektro-mechanischen Komponenten enthalten sind. Diese sind

aber nicht vollständig, da alle Komponenten eines Systems nur durch eine funktionale Ablauffolge nicht identifiziert werden können. In einer ersten Abstraktion kann in dem aufgestellten physikalischen Modell die Steuerung, welche aus Elektronik und Software besteht, als Informationsverarbeitung betrachtet werden. Im Laufe des Entwicklungsprozesses muss festgelegt werden, welcher Teil davon in Software und welcher in Elektronik umgesetzt werden soll. Weiterführende Informationen zu dem sogenannten Hardware/Software-Codesign sind in Kap. 8.1.3 zu finden.

Als Basis für weitere Zuverlässigkeitsanalysen wird nun ein Modell benötigt, welches Strukturen und das Verhalten des mechatronischen Systems beschreiben kann. Da mechatronische Systeme im Allgemeinen über Software verfügen, kann kein Modell verwendet werden, welches auf physikalischen Eigenschaften basiert. Geeigneter ist ein Modell, welches das System funktional betrachtet sowie in der Lage ist, funktionale und systematische Fehler zu untersuchen. Auch die in dem Buch thematisierten frühen Entwicklungsphasen können durch diese funktionale Betrachtungsweise einfacher dargestellt werden.

3.2.1 Qualitative Verhaltensmodelle

Ein Modell lässt sich nach [3.7, 3.44] durch die drei konstituierenden Merkmale Abbildung, Verkürzung und Pragmatik definieren. Durch den Einsatz von Modellen während der Entwicklung entstehen gemäß der Richtlinie VDI 2206 zur Entwicklung mechatronischer Systeme [3.44] Zeit- und Kostenvorteile, da das Verhalten eines mechatronischen Systems bereits vor der Erstellung eines Prototyps überprüft werden kann. Indem ein Modell vom Original abstrahiert, wird die Komplexität reduziert und komplexe Systeme werden damit besser beherrschbar.

Man unterscheidet verschiedene Arten von Modellen, welche sich nach Einsatzzweck (Zuverlässigkeitsanalyse, Funktionsprüfung, …), Gegenstand der Modellbildung (Zuverlässigkeit, Verhalten, …) und verwendeter Darstellungsformen (Modelica, SystemC, CAD, …) untergliedern lassen. In der Mechatronik beschreiben Anforderungs- und Verhaltensmodelle bereits frühzeitig die geforderten Funktionen des Gesamtsystems.

Wie in [3.44] erläutert, erfordert die Modellbildung eine realitätsnahe Beschreibung des Systems. Auf Basis eines solchen Modells kann eine Modellanalyse Eigenschaften und Verhalten des mechatronischen Systems ermitteln. Zur Bestimmung der Zuverlässigkeit ist dabei insbesondere von Interesse, welche Fehler im System vorhanden sein können und wie sich diese auf das Verhalten des Gesamtsystems, bis hin zu einem möglichen Systemversagen, auswirken können.

Um den Entwickler beim Entwurf und der frühzeitigen Analyse funktionaler Zusammenhänge im mechatronischen System zu unterstützen, müssen folgende Anforderungen an die Modellbildung und -analyse erfüllt sein:

- Ganzheitliche Beschreibung und Analyse hybrider Systeme: Das Verhalten der Komponenten aus den unterschiedlichen Domänen (Mechanik, Elektronik, Software) muss in einer geeigneten Modellierungssprache zusammen mit

menschlichen Bedieneingriffen beschrieben werden können. Es sind hybride Verhaltensweisen abzubilden, die sich sowohl aus zeit-/wertekontinuierlichen als auch zeit-/wertediskreten Vorgängen zusammensetzen. Ein ganzheitliches Modell muss alle Komponenten integrieren, sodass eine domänenübergreifende Analyse des Systemverhaltens ermöglicht wird.

- Modellierung unvollständiger und unpräziser Informationen: Oftmals, zumeist in frühen Entwicklungsphasen sind Komponenten oder das Verhalten einzelner Komponenten des Systems nur teilweise festgelegt. Dies führt zu unvollständigen Informationen über das Systemverhalten. Weiter können Informationen zwar vorliegen, jedoch noch unscharf bzw. unpräzise sein. Ein Beispiel hierfür ist die Angabe, dass „Wasser aufzuheizen ist, bis es heiß ist“, ohne dass konkret Temperatur und Zeitdauer angegeben sind.
- Durchgängigkeit im Produktentstehungsprozess: Einmal erstellte Modelle müssen im Rahmen der weiteren Entwicklung wiederverwendet werden können, um so eine erhöhte Effizienz zu erreichen. Beispielsweise müssen Modelle eine schrittweise Verfeinerung bis hin zum Übergang in den detaillierten Entwurf bzw. die Implementierung ermöglichen.

Je nach Domäne unterscheiden sich die verbreiteten Modellierungssprachen und -werkzeuge, welche jeweils auf die speziellen Erfordernisse einer Domäne eingehen. In der Regelungstechnik sind beispielsweise Blockdarstellungen und Differenzialgleichungen üblich. Da jedoch die programmierbare Logik eines Systems, die sich aus Software und Elektronik zusammensetzt, immer in Bezug zu der technischen Umgebung definiert ist, genügt eine isolierte Modellierung einzelner Domänen nicht. Als Lösung für dieses Problem wurde von den Autoren der Ansatz einer qualitativen Modellierungssprache gewählt. Es wird nachfolgend eine kurze Einführung in qualitative Modellierungssprachen sowie in die eigens entwickelte Methode der Situationsbasierten Qualitativen Modellbildung und Analyse (SQMA) gegeben.

3.2.2 Qualitative Modellierungssprachen

Qualitative Modellierungssprachen stellen nach [3.40] vereinfachte Modelle realer Systeme dar, welche das grundlegende Systemverhalten beschreiben und dabei Details des Systems vernachlässigen. Das Qualitative Reasoning ist ein Teilbereich der Künstlichen Intelligenz, welches versucht menschliche Denkweisen und kontinuierliche Größen wie Zeit und Raum anzunähern. Dadurch ist es möglich, auch hybride, diskret-kontinuierliche Systeme zu beschreiben.

Wichtige Ansätze zur qualitativen Modellbildung sind diejenigen von Brown [3.8], Forbus [3.15] und Kuipers [3.28]. Letzterer wird häufig in der Literatur zitiert. Er verwendet Intervalle, um physikalische Größen zu repräsentieren sowie qualitative Constraints (z. B. Addition, Multiplikation, Negation), um das Verhalten auf Grundlage der Intervalle zu modellieren.

Ein Vergleich der eigens für die Automatisierungstechnik entwickelten SQMA-Methode in [3.40] mit anderen qualitativen Modellierungssprachen hat gezeigt, dass SQMA sehr gut für die Modellierung komplexer technischer Prozesse und deren Analyse geeignet ist. Während die qualitative Modellbildung programmierbarer mechatronischer Systeme in Kap. 7.4 ausführlich erläutert wird, sollen hier zunächst die Grundzüge der SQMA-Methode in einer kurzen Übersicht vorgestellt werden.

3.2.3 Die Situationsbasierte Qualitative Modellbildung und Analyse (SQMA)

Für den Einsatz qualitativer systemtheoretischer Modelle in der Automatisierungstechnik wurde am Institut für Automatisierungs- und Softwaretechnik der Universität Stuttgart seit den 1990-er Jahren die Situationsbasierte Qualitative Modellbildung und Analyse (SQMA) entwickelt (vgl. [3.16, 3.30]). Ausgehend davon wurde SQMA in [3.35] um die Möglichkeit zur Online-Prozessüberwachung auf sicherheitskritische Zustände erweitert. Zusätzliche Ergänzungen wurden im Rahmen der Forschergruppe „Systemzuverlässigkeit mechatronischer Systeme“ vorgenommen. Diese umfassen unter anderem unscharfe Intervallgrenzen [3.40] und die ganzheitliche Analyse komplexer softwarebasierter Prozessautomatisierungssysteme hinsichtlich Sicherheit [3.4] und Zuverlässigkeit [3.48].

Folgende Konzepte zeichnen die SQMA-Methode aus:

1. SQMA-Modelle weisen eine hierarchische Struktur auf. Komplexe Systeme können somit schrittweise zerlegt werden, bis ein Modell aus verschiedenen Hierarchieebenen entsteht.
2. SQMA-Modelle setzen sich aus einzelnen SQMA-Komponenten mit eindeutig definierten Schnittstellen zusammen, die untereinander verknüpft sind. Einzelne Komponenten können mehrfach in verschiedenen Modellen verwendet werden.
3. Wie bei den anderen oben genannten qualitativen Ansätzen werden Modellgrößen in SQMA mit Hilfe von Intervallen beschrieben.
4. Das Verhalten einer SQMA-Komponente wird durch qualitative Regeln festgelegt.
5. Für Komponenten und das Gesamtsystem werden Situationen sowie Übergänge (Transitionen) rechnergestützt ermittelt.

Um ein SQMA-Modell zu erstellen und am Rechner zu analysieren, muss zunächst für jede SQMA-Komponente eine Textdatei erstellt werden, welche die Modellbeschreibung enthält. In zusätzlichen Dateien werden daraufhin die Komponenten für ein bestimmtes System festgelegt und miteinander verknüpft. Zuletzt wird die Systemumgebung definiert, falls das System Schnittstellen mit der Umgebung besitzt.

Darüber hinaus besteht die Möglichkeit, SQMA-Modelle grafisch darzustellen sowie die Übergänge zwischen Situationen am Bildschirm zu visualisieren. Abbildung 3.4 zeigt einen beispielhaften Ausschnitt aus der grafischen Struktur des SQMA-Modells einer Wandler-Überbrückungskupplung. Neben der Wandler-Überbückungskupplung (ts_Kupplung), welche über ein Ventil angesteuert wird (ts_Ventil), sind Sensoren (z. B. ts_BeschlSensor) sowie die programmierbare Steuerung (sw_ClutchCtrl) dargestellt. Die Schnittstellen zum menschlichen Bediener wurden für eine erste Analyse vernachlässigt.

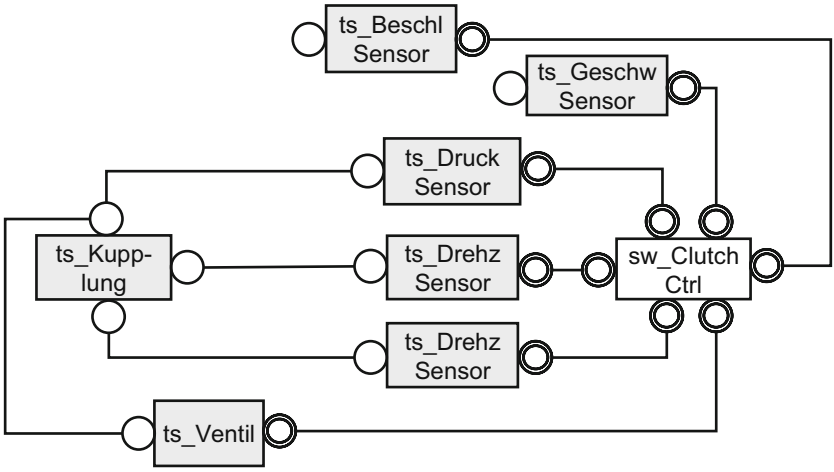

Abb. 3.4 SQMA-Modell

3.3 Ermittlung kritischer Komponenten

Ein System kann, wie bereits in Kap. 2.3 zu finden ist, aufgrund mehrerer Ursachen ausfallen. Hierbei gibt es Komponenten im System, die mit einer größeren Wahrscheinlichkeit ausfallen und dadurch je nach Eintritt sowie nach Anordnung in der Zuverlässigkeitsstruktur ein größeres Risiko, d. h. das Produkt der Schadensschwere und der Eintrittswahrscheinlichkeit, als die anderen Komponenten darstellen. Die Komponenten mit einem hohen Risiko haben einen hohen negativen Einfluss auf die Zuverlässigkeit, sind daher kritisch anzusehen und sollten nie ausfallen. Bezogen auf die Zuverlässigkeitsarbeit bedeutet dies, dass Komponenten mit einem höheren Risiko im Gegensatz zu denen mit einem geringeren Risiko stärker betrachtet werden müssen. Hierfür bieten sich Analysearten an, welche die Einstufung der Komponenten in Kritikalitätsklassen vornehmen. Beispielsweise kann hier die ABC-Analyse genannt werden.

Auch für die Zuverlässigkeitsbewertung mechatronischer Systeme wird eine globale Risikobestimmung, aber nicht nur auf Komponentenebene, sondern auf

Funktionsebene durchgeführt. Ausgehend von dem Modell des Systems erfolgt die Risikoabschätzung. Hierzu werden zunächst die globalen Fehlerauswirkungen ermittelt. Unter einer globalen Auswirkung wird nach [3.29] ein physikalischer Effekt verstanden, welcher zu einem Fehlverhalten des Gesamtsystems führt. Dies bemerkt der Benutzer durch einen Verlust an Komfort oder gar durch den vollständigen Ausfall der zugehörigen Funktion.

Für die Risikoabschätzung werden die durch die SQMA aufgestellten Situationen und Zustände verwendet, um aufzuzeigen, welche Komponenten bzw. welche kombinierten Situationen kritisch für das Gesamtsystem anzusehen sind. Diese Vorgehensweise verfeinert die generischen Vorgaben der Norm IEC 61508 hinsichtlich einer risikobasierten Bewertung für sicherheitsbezogene Systeme und erlaubt eine Übertragung auf den Bereich der Zuverlässigkeitsanalyse.

Zur Auswahl der zutreffenden Kritikalitätsklassen, wird ein Risikograph gemäß [3.10] verwendet. Hierbei betrachtete Kriterien sind das Schadensmaß, die Aufenthaltsdauer von Personen im Gefahrenbereich, die Möglichkeit zur Gefahrenabwendung sowie die Auftretenswahrscheinlichkeit. Wurde eine Kritikalität festgelegt, wird die globale Auswirkung daraufhin in die einzelnen Komponenten zurück verfolgt (vgl. auch Kap. 7.2.1.2).

3.4 Datensammlung

Neben dem Aufzeigen von Schwachstellen und Fehlerzusammenhängen sind für die quantitative Zuverlässigkeitsbewertung vor allem entsprechende Informationen in Form von Lebensdauerdaten erforderlich. Hierzu gibt es nach IEEE 1413 [3.23] mehrere Möglichkeiten, um an diese zu gelangen.

- Gesichertes Wissen aus firmeneigenen oder allgemeinen Datenbanken.
- Gesichertes Wissen aus physikalischen Vorhersagen.
- Empirisch bzw. experimentell ermittelte Ergebnisse aus Tests oder Feldeinsätzen
- Wissen aus nichtdokumentierten Quellen.

Gemäß Kap. 2.3 basieren Fehler in der Mechanik bzw. der Elektronik, welche zu Ausfällen führen können, im Gegensatz zur Software nicht nur auf inhärenten Fehlern, sondern auch auf physikalischen Begebenheiten. Dementsprechend unterscheidet sich das Vorgehen der Datensammlung. Das heißt, nicht alle aufgezählten Möglichkeiten aus obiger Aufzählung zur Erlangung von Informationen in Form von Lebensdauerdaten können für die Software verwendet werden [3.18].

Eine Herausforderung der Datensammlung in frühen Entwicklungsphasen ist, dass die für die Bestimmung genauer Zuverlässigkeitswerte benötigten Randbedingungen, wie beispielsweise Temperatur oder Belastung, häufig fehlen. Deshalb fokussiert sich dieser Abschnitt auf den Umgang mit unsicheren Informationen bzw. auf

die Frage, wie Informationen ermittelt werden können. Zu Beginn ist es wichtig, Begrifflichkeiten zu klären. Oftmals ist von Unsicherheit, Unschärfe und Ungenauigkeit die Rede. Im Folgenden werden die Begriffe definiert.

- Unsicherheit:
  Nach [3.42] kennzeichnet Unsicherheit im generischen Sinne eine Situation, in der es unmöglich ist, die Merkmale und Prozesse eines gegebenen Sachverhalts exakt zu beschreiben. Bei der Wissensrepräsentation tritt Unsicherheit immer dann in Erscheinung, wenn das Wissen mit der gegebenen Modellsprache über bestimmte Aspekte eines Sachverhalts nicht adäquat formuliert werden kann. Dadurch kann es vorkommen, dass die gegebenen Informationen nicht korrekt sind.
- Unschärfe:
  Die klassische Logik wird durch zwei abgegrenzte Zustände ausgezeichnet. Diese werden typischerweise als wahr oder falsch bezeichnet. Oftmals sind diese beiden Aussagen nicht ausreichend. Hier ist es sinnvoll, unscharfe Logik, wie beispielsweise die Fuzzy-Logik, einzusetzen. Hierbei werden Zugehörigkeitsfunktionen beschrieben, die Elementen einer Grundmenge eine reelle Zahl zwischen 0 bis 1 zuordnet. Dadurch wird ermöglicht, dass Elemente auch nur mit einer bestimmten Zugehörigkeit einem Zustand angehören.
- Ungenauigkeit/Impräzision:
  Ungenauigkeit und Impräzision sind Synonyme und bedeuten die Abweichungen einer Repräsentationsform von der Form der dargestellten Realität. Ein Modell zum Beispiel ist ungenau, wenn – bei überwiegender Übereinstimmung mit der Realität – einige Parameter nicht mit den realen Eigenschaften korrelieren. Zahlenwerte sind ungenau, wenn keine ein-eindeutige Beziehung zum Korrelat besteht [3.42].

Im Folgenden werden verschiedene Ansätze vorgestellt, mit denen es möglich ist, trotz Unsicherheiten, Unschärfe oder auch Ungenauigkeit der Informationen Zuverlässigkeitsdaten zu erstellen. Hierbei muss vor allem auf die wichtigste Randbedingung, die Datensituation, geachtet werden.

Zur Darstellung der ganzen Randbedingungen bietet es sich an, einen Programmablaufplan zu verwenden. Dieser repräsentiert eine grafische Darstellung des Ablaufs von Operationen in einem System (Abb. 3.5). Je nach Datensituation soll durch den Programmablaufplan eine passende Analyseart aufgezeigt werden. Insgesamt stehen 5 verschiedene Analysearten zur Verfügung:

1. Die Verwendung von Versuchsdaten
2. Nutzung von Netzstrukturen
3. Nutzung von quantitativem Expertenwissen
4. Nutzung von qualitativem Expertenwissen
5. Verwendung von Ausfallratenkatalogen.

In den nächsten Abschnitten wird auf die einzelnen Punkte eingegangen.

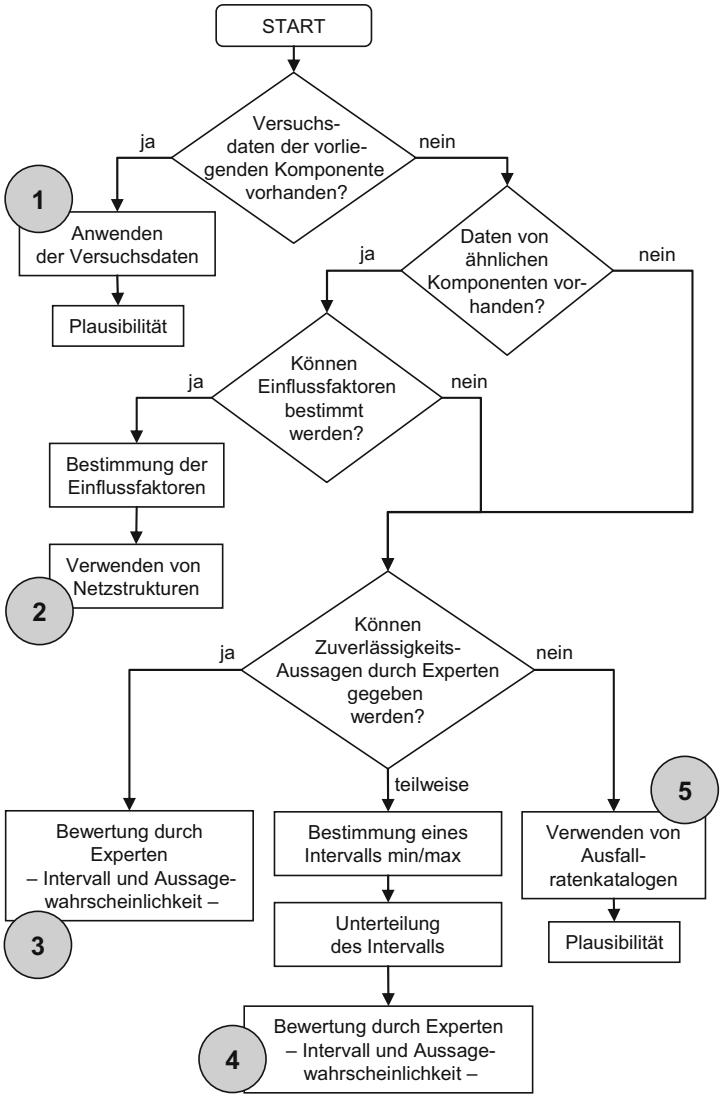

Abb. 3.5 Programmablaufplan für den Umgang mit unsicheren Daten

3.4.1 Verwendung von Versuchsdaten

Bei der Verwendung von Versuchsdaten muss angemerkt werden, dass die Qualität und auch der Umfang der Daten sehr stark variieren kann. Versuchs- bzw. Testbedingungen, welche genau auf das neue System abgestimmt sind, existieren zumeist in den frühen Entwicklungsphasen nicht. Zwar kann die betrachtete Kom-

ponente bereits im Einsatz gewesen und getestet worden sein, jedoch meistens in einem anderen System. Bei der Übernahme der Daten für das neue System können sich Randbedingungen ändern, so dass der Zuverlässigkeitswert von dem bekannten abweichen kann.

Die Berechnung der Zuverlässigkeitswerte funktioniert genauso wie es für alle Komponenten bzw. Systeme bekannt ist: mit Hilfe einer Verteilung. Für die in diesem Abschnitt exemplarisch betrachtete Domäne Mechanik bietet sich an, die Weibull-Verteilung zu verwenden, da es mit dieser möglich ist, verschiedene Ausfallarten abzubilden. Diese umfassen Frühausfälle, Zufallsausfälle sowie Verschleiß- und Ermüdungsausfälle. Allgemein kann bei der Auswertung der Daten zwischen einer zweiparametrigen und einer dreiparametrigen Weibullverteilung unterschieden werden. Der Unterschied liegt darin, dass bei der dreiparametrigen Weibullverteilung die ausfallfreie Zeit t_0 berücksichtigt wird. Diese Zeit symbolisiert, bis zu welchem Zeitpunkt kein Ausfall der Komponente auftritt. Im Gegensatz dazu sind in der zweiparametrigen Weibullfunktion nur der Formparameter b sowie die charakteristische Lebensdauer T integriert. Ausfälle treten hier bereits schon gleich zu Beginn auf.

Die Vorgehensweise zur Ermittlung der zuverlässigkeitstechnischen Kenngrößen ist bei den angesprochenen Verteilungsarten identisch. Zuerst werden die Daten nach der Ausfallzeit aufsteigend geordnet und anschließend einem Rang zugewiesen, welcher abhängig von der Anzahl der Prüflinge ist. Dieses nun ermittelte Zahlenpaar wird in ein Diagramm übertragen. Häufig kommt es auch vor, dass neben den Ausfallzeiten weitere Informationen von nicht ausgefallenen Komponenten vorliegen. Auch diese können in die Auswertung mit einfließen. Zur Vertiefung dieses Themengebietes sowie des Themas Vertrauensbereiche, welches vor allem bei einer geringen Anzahl von Tests relevant ist, wird auf weiterführende Literatur wie [3.2] oder [3.5] verwiesen.

Eine weitere Möglichkeit zur Erlangung von Zuverlässigkeitswerten liegt darin, dass aus einer firmeninternen Datenbank die Informationen entnommen werden. Häufig sind viele Werte hinterlegt, zudem sind auch die Belastungen, Werkstoffe sowie die Randbedingungen bekannt. Dadurch wird ermöglicht, dass die verwendeten Informationen eine höhere Plausibilität als die aus unbekannten Quellen aufweisen.

Ein essentieller Punkt dieses Abschnitts ist die Überprüfung der Plausibilität der Informationen bzw. Daten sowie die Ähnlichkeit der Produkte. Eine Ähnlichkeit liegt vor, wenn die Produkte bezüglich des Verhältnisses aus Belastung und Belastbarkeit, der Einsatzbedingungen (z. B. Lastkollektive oder Temperatur) und der Gestalt ähnlich sind, wohingegen für die Plausibilitätsprüfung eine Übereinstimmung der Größenordnung der Daten von Vorgänger- und aktuellem Produkt vorliegen muss. Da durch die Verwendung von ähnlichen, aber nicht immer hundertprozentig identischen Komponenten sowie deren Randbedingungen ausgegangen wird, müssen diese Punkte näher betrachtet werden. Beispielsweise sind die Änderungen bei Vorgängerprodukten in der Mechanik zumeist nicht allzu groß, da es sich in aller Regel um Änderungskonstruktionen bzw. Anpassungskonstruktionen handelt. Dadurch ist die Gestalt zumeist ähnlich. Komplette Neuentwicklungen,

bei denen gar keine Ähnlichkeit mehr vorliegt, sind bei der Mechanik eher die Ausnahme. Anders kann dies bei Betrachtung von anderen Komponenten, die keinen direkten Bezug aufweisen, aussehen. Hier können die Grundfunktionen ähnlich sein, aber der Einbauraum und der Einsatzzweck können sich unterscheiden. Darüber hinaus muss auch noch auf unterschiedliche Einflüsse geachtet werden, um die Plausibilität sicherzustellen. Beispielsweise können hier die auf die Komponenten einwirkenden Belastungen, die Belastbarkeit der Komponente oder das Temperaturkollektiv genannt werden. Bei Abweichungen von Belastung und Belastbarkeit treten sehr unterschiedliche Zuverlässigkeitswerte auf. Deshalb ist es sinnvoll, dass diese Einflüsse schon in dieser Phase abgeschätzt werden können sowie von den bereits vorliegenden Komponenten die Einflussfaktoren bekannt sind.

3.4.2 Nutzung von Netzstrukturen

Zuverlässigkeitsdaten müssen nicht immer direkt von der zu untersuchenden Komponente vorliegen. Es besteht auch die Möglichkeit, die Zuverlässigkeitsdaten von Komponenten, die bereits getestet wurden, welche aber nicht zwingend identisch, sondern nur ähnlich zu der untersuchten sind, zu nutzen. Sinnvoll ist es aber hierbei, dass Informationen über die Einflussfaktoren wie beispielsweise die Temperatur oder die Lastzustände vorliegen. Falls diese bekannt sind, können Netzstrukturen verwendet werden. Besonders sinnvoll ist es, wenn die Strukturen automatisch aus den vorliegenden Daten lernen können. Hier sind vor allem Neuronale Netze und Bayes'sche Netze zu nennen.

Da bereits in Kap. 2.9 die Verwendung von Netzstrukturen thematisiert wurde, wird für weiterführende Informationen auf dieses Kapitel verwiesen.

3.4.3 Nutzung von quantitativem Expertenwissen

Neben der Nutzung von Informationen aus Datenbanken ist es auch möglich, Wissen aus nichtdokumentierten Quellen zu erlangen. Stichwort hierbei ist das Expertenwissen. Jedoch kann die Situation vorkommen, dass die befragten Experten sich nicht in der Lage befinden, immer quantitative Aussagen bzw. Einschätzungen über die Zuverlässigkeit von Komponenten zu treffen. Oftmals liegt die Tatsache darin begründet, dass sich die Experten durch später überprüfbare schlechte oder falsche Angaben anfechtbar machen. Somit wollen viele ihr Wissen nicht immer offen preisgeben.

Eine weitere Herausforderung besteht im Aufnehmen des Expertenwissens, da die Informationen, die zwischen Personen ausgetauscht werden, nach [3.36] nicht immer korrekt ausgetauscht werden. Insgesamt gibt es vier verschiedene Schritte des Informationsaustausches. Zuerst muss der Experte die Frage des Interviewers verstehen. Anschließend muss er sich an die relevanten Informationen erinnern,

um die Fragen beantworten zu können. Diese Informationen werden dann beurteilt und bewertet. Als letzter Schritt werden die Informationen sowie die Bewertungen dem Interviewer mitgeteilt. Die nächste Herausforderung liegt darin, dass die Information vom Interviewer korrekt aufgenommen wird. Nach [3.36] kann es vorkommen, dass sich der Experte teilweise mit zu vielen Informationen auseinandersetzen muss, um die Fragen beantworten zu können. Dies kann dazu führen, dass die Antworten des Experten ungenau werden, da der Experte Vereinfachungen und Annahmen trifft.

Tabelle 3.1 Schwierigkeitsklassen für Expertenwissen [3.26]

Ziel der Frage	Schwierigkeitsgrad
erster und letzter Ausfall	1
Maxima und Mittelwerte	2
Wahrscheinlichkeiten	3
Verteilungsparameter	4

Für einen Experten gestaltet es sich zumeist schwierig, genaue Verteilungsparameter anzugeben. Viel einfacher für ihn ist es beispielsweise einen Bereich des Ausfallzeitpunktes einer Komponente anzugeben. In Tabelle 3.1 sind diese unterschiedlichen Schwierigkeitsklassen der Information angegeben. Hierbei symbolisiert eine hohe Ziffer einen hohen Schwierigkeitsgrad.

Falls die Experten keine quantitativen Angaben zur Zuverlässigkeit geben können oder wollen, muss eine weitere Art der Informationsgewinnung von Experten in Betracht gezogen werden. Diese sind in den folgenden Abschnitten zu finden.

3.4.4 Nutzung von qualitativem Expertenwissen

Liegen anstatt Zuverlässigkeitsdaten nur Informationen über das Verhandensein der einzelnen Komponenten eines Systems vor, jedoch keine Zuverlässigkeitsdaten, so kann auf unterschiedliche Art und Weise trotzdem eine Zuverlässigkeitsaussage bestimmt werden. Zum einen ist es möglich, durch Experten eine qualitative Aussage dahingehend zu erhalten, dass die einzelnen Komponenten des Systems nach ihrer Ausfallwahrscheinlichkeit sortiert werden. Dadurch werden die „Haupttreiber“ ermittelt, welche die Zuverlässigkeit bzw. die Unzuverlässigkeit des Systems maßgeblich bestimmen.

Die andere Möglichkeit besteht darin, dass die Komponenten des Systems einzeln betrachtet werden. Das Ziel ist es, qualitative Aussagen zu quantifizieren. Dieses Vorgehen wird in mehrere Punkte unterteilt:

1. Es werden unterschiedliche Datenquellen verwendet, um ein Minimum und ein Maximum des Zuverlässigkeitswertes der Komponente zu bestimmen. Diese Datenquellen können firmeninterne Daten, sowie Herstellerangaben sein oder

aus Ausfallratenkatalogen stammen. Alternativ kann in diesem Punkt auch das Minimum und das Maximum von den Experten genannt werden. Dies würde dem ersten Punkt aus Tabelle 3.1 entsprechen. Beide Möglichkeiten können auch miteinander kombiniert werden. Die gefundenen Informationen aus den Datenquellen können durch Experten weiter eingeschränkt werden. In allen Fällen muss aber überprüft werden, ob die Werte plausibel sind.

2. Der Bereich des Minimums und des Maximums wird nun in einem nächsten Schritt weiter unterteilt. Hierbei sollen gleichgroße Intervalle entstehen. Die Anzahl der Intervalle kann von den Experten gewählt werden. Empfehlenswert ist eine Einteilung in mindestens drei Intervalle.
3. Der Experte wird nun gefragt, in welchem Intervall und mit welcher Aussagewahrscheinlichkeit er diese Komponente abschätzt. Mehrfachnennungen sind möglich, jedoch soll die Summe der Aussagewahrscheinlichkeit immer 100% betragen. Dadurch wird eine Verteilung erzeugt, mit der dann die Ausfallrate eingegrenzt werden kann.

Das folgende Beispiel soll diese Herangehensweise aufzeigen:
Die Zuverlässigkeit eines Tasters soll untersucht werden. Durch die Verwendung von unterschiedlichen Datenquellen und anschließender Plausibilitätsprüfung werden von den Experten eine minimale Ausfallrate von $\lambda = 400$ FIT und eine maximale Ausfallrate von $\lambda = 580$ FIT festgelegt. Nach der weiteren Unterteilung des bestimmten Intervalls stehen den Experten in dem vorliegenden Beispiel für ihre Schätzung insgesamt sechs gleichgroße Intervalle zur Verfügung. In Tabelle 3.2 sind diese Intervalle sowie die unterschiedlichen Aussagen der Experten zu finden.

Tabelle 3.2 Expertenaussage über die Zuverlässigkeit eines Tasters

	λ = [400 FIT, 430 FIT)	λ = [430 FIT, 460 FIT)	λ = [460 FIT, 490 FIT)	λ = [490 FIT, 520 FIT)	λ = [520 FIT, 550 FIT)	λ = [550 FIT, 580 FIT)
Experte 1	0,1	0,8	0,1			
Experte 2				0,7	0,3	
Experte 3			1,0			
Experte 4	0,1	0,2	0,3	0,2	0,1	0,1
Experte 5		0,1	0,8	0,1		
Experte 6		0,25	0,25	0,25	0,25	
Experte 7			0,25	0,5	0,25	

Durch diese Expertenaussagen kann in einem abschließenden Schritt die Ausfallrate als Verteilung angegeben werden.

3.4.5 Verwendung von quantitativem und qualitativem Expertenwissen

Wird ein System betrachtet, dessen Komponenten durch die Experten aus Zuverlässigkeitssicht nicht vollständig quantitativ erfasst werden können, besteht die Möglichkeit zusätzlich qualitatives Expertenwissen zu nutzen. Die bereits bestimmten quantitativen Zuverlässigkeitswerte werden hierfür genommen und der Größe nach sortiert. Dabei bietet es sich an, dass die „unzuverlässigste“ Komponente ganz oben steht. Komponenten, welche noch keinen Zuverlässigkeitswert zugewiesen bekommen haben, sollten auf eine separate Liste gesetzt werden. Nun werden diese Komponenten durch einen Gruppenentscheid der Experten in die existierende Liste der quantifizierten Komponenten einsortiert. Abbildung 3.6 soll dies aufzeigen.

Wie bei den kombinierten Daten zu sehen ist, liegt beispielsweise Komponente 4 nach dem Ermessen der Experten in ihrem Zuverlässigkeitswert zwischen Komponente 3 und Komponente 7. Der Komponente 3 und Komponente 7 ist ein Zuverlässigkeitswert hinterlegt, so dass für Komponente 4 ein Bereich angegeben werden kann, der zwischen diesen beiden liegt. In dem vorliegenden Fall besitzt die Komponente 4 also eine Ausfallrate im Bereich von $1120\ \text{FIT} < \lambda < 1200\ \text{FIT}$.

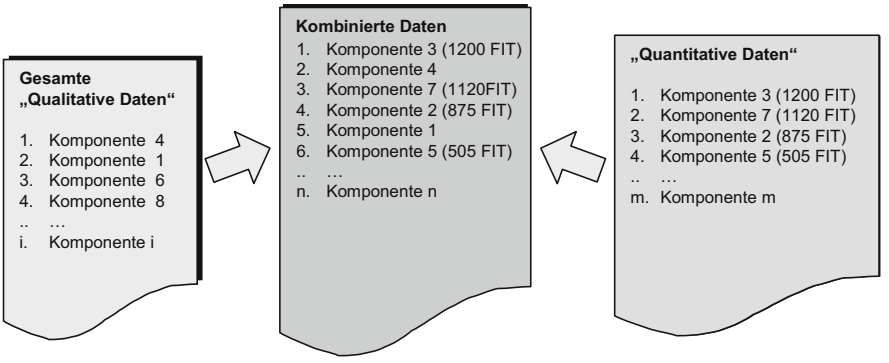

Abb. 3.6 Zusammenführen von qualitativen und quantitativen Expertenwissen

3.4.6 Verwendung von Ausfallratenkatalogen

Die geschichtliche Entwicklung von Ausfallratenkatalogen reicht bis zum zweiten Weltkrieg zurück. Während dieser Kriegszeit kam es zu vielen Fehlern durch neu eingesetzte Waffentechnologien. Zudem war das Auftreten der Fehler nicht prognostizierbar. Aus diesem Grunde wurden in den USA in der Zeit zwischen 1945 und 1950 verschiedene Navy-, Army- und Air Force-Studien betrieben, die sich

insbesondere mit den Themen Geräteinstandhaltung, Instandhaltungskosten und Zuverlässigkeit elektronischer Komponenten beschäftigten.

Das steigende Zuverlässigkeitsbewusstsein in den USA über den Militärbereich hinaus führte nach [3.11] in den frühen 50er Jahren des vergangenen Jahrhunderts zur Einsetzung der „IEEE Transactions on Reliability“, die sich ebenfalls mit der Zuverlässigkeit elektronischer Komponenten befasste. Im Jahre 1957 veröffentlichte AGREE (Advisory Group on the Reliability of Electronic Equipment) einen Bericht, der umgehend zu einer Militärspezifikation (MIL-SPEC) über die Zuverlässigkeit elektronischer Komponenten des US-Militärs führte. Diese Entwicklung gab auch den Ausschlag für die Schaffung eines Ausfallratenkataloges, mit dessen Hilfe die Ausfallraten elektronischer Komponenten in militärisch verwendeten Komponenten und Systemen abgeschätzt werden sollten. Das dort vorgestellte Militärhandbuch ist das als Grundlage aller Ausfallratenkataloge geltende MIL-HDBK-217. Dieses beinhaltet Daten über die Zuverlässigkeit einzelner Komponenten und Bauteile sowie Verfahren, mit denen die Systemzuverlässigkeit aus der Zuverlässigkeit der verbauten Komponenten und Bauteile ermittelt werden können.

3.4.6.1 Übersicht und Inhalt der Ausfallratenkataloge

Heutzutage gibt es viele verschiedene Ausfallratenkataloge mit unterschiedlichen Schwerpunkten, so dass jeder Katalog zumeist einen begrenzten Umfang an Komponenten abbildet. Dementsprechend gibt es auch keinen „Standard-Ausfallratenkatalog“, der allumfassend eingesetzt werden kann. Die Ausfallratenkataloge können trotz der Unterschiede in den Einsatzgebieten in zwei Kategorien eingeteilt werden:

- Branchenübergreifend relevante Ausfallratenkataloge
- Branchenspezifische Ausfallratenkataloge.

Die branchenübergreifend relevanten Ausfallratenkataloge umfassen Komponenten aus dem Maschinenbau und der Elektrotechnik. Bekannte Ausfallratenkataloge für diese Kategorie sind in Tabelle 3.3 zu finden.

Im Gegensatz zu den branchenübergreifenden Ausfallratenkataloge aus Tabelle 3.3 entstammen die Daten der branchenspezifischen Ausfallratenkataloge aus Datenbanken von sicherheitskritischen Branchen. Beispiele hierfür sind die Verfahrenstechnik, Offshore-Anwendungen sowie Kernkraftwerkstechnik. Die Anzahl der erhältlichen Ausfallratenkataloge dieser Kategorie ist sehr groß, aber nach [3.21] ist die Implementierung in Zuverlässigkeitsprognosen recht selten.

Werden Ausfallraten anhand der Ausfallratenkataloge bestimmt, gibt es noch eine weitere Unterscheidung. Sie können je nach ihrem Aufbau in zwei Gruppen eingeteilt werden:

- Ausfallratenkataloge mit Berechnungsmodellen zur Bestimmung der Ausfallrate
- Ausfallratenkataloge als reine Ausfalldatensammlung.

Tabelle 3.3 Übersicht branchenübergreifender Ausfallratenkataloge

Titel des Katalogs	Datenquelle/ Art der Daten	Veröffentlicht von (Jahr)	Bemerkungen
China GJB/z 299B	Elektronische Komponenten	Chinesisches Militär	Basiert auf einer älteren Version von MIL-HDBK-217
EPRD-97 (Electronics Parts Reliability Data)	Elektronische Komponenten	Reliability Analysis Center, USA (1997)	Datenbank aus Felddaten
IEC TR 62380	Elektronische Komponenten	IEC, Schweiz (2004)	Nachfolger von RDF 2000 und RDF 95
MIL-HDBK-217F	Elektronische Komponenten	US Department of Defense, USA (1995)	Standardwerk
NPRD-95 (Non-electronic Parts Reliability Data)	Nicht-elektronische Komponenten	Reliability Analysis Center, USA (1995)	Datenbank aus Felddaten
NSWC-98 (Naval Surface Warfare Center)	Mechanische Komponenten	NSWC, USA (1998)	Mathematische Modelle und Methoden
Telcordia SR-332	Elektronische Komponenten	AT&T Bell Labs, USA	Identisch zu Bellcore TR-332

Ausfallratenkataloge mit Berechnungsmodellen zur Bestimmung der Ausfallrate (z. B. MIL-HDBK-217F) beschreiben eine Vorgehensweise zur Bestimmung der Ausfallrate abhängig von den Betriebs- und Einsatzbedingungen einer Komponente. Hierzu wird eine vorgegebene oder zu ermittelnde Basisausfallrate mit den anhand der Berechnungsmodelle bestimmten Faktoren multiplikativ verrechnet. Üblicherweise kann die laut Ausfallratenkatalog tatsächliche Ausfallrate λ_p gemäß IEEE 1413 [3.23] als Funktion einer Basisausfallrate λ_G und einer Reihe von Einflussfaktoren π_i beschrieben werden:

$$\lambda_p = f(\lambda_G, \pi_i) \tag{3.1}$$

Im Gegensatz hierzu muss bei den Ausfallratenkatalogen, die als reine Ausfalldatensammlung aufgebaut sind (z. B. NPRD), die Ausfallrate nicht erst berechnet, sondern direkt aus den Tabellen abgelesen werden.

3.4.6.2 Vor- und Nachteile von Ausfallratenkatalogen

In [3.21] werden verschiedene Ausfallratenkataloge miteinander verglichen. Hauptaugenmerk liegt auf den Unterschieden der Ausfallraten, wenn ein und dieselbe Komponente betrachtet wird. Als Anschauungsobjekte werden hierbei verschiedene elektronische Komponenten verwendet. Auffällig ist, dass es immense Differenzen zwischen den einzelnen Ausfallraten gibt. Beispiele für die Streuung der Ausfallraten zwischen den einzelnen Katalogen sind in [3.1] veröffentlicht. So liegen die Daten nach [3.1] für einen Wechselstrommotor zwischen $\lambda = 0{,}15$ FIT und $\lambda = 556$ FIT, was einer Abweichung um den Faktor 3700 entspricht. Dies

zeigt, dass eine zuverlässige Datensammlung ein wichtiger Faktor ist. Ohne zuverlässige und konsistente Daten, deren Herkunft und Einsatzbedingungen über die gesamte Lebensdauer bekannt sind, werden die Berechnungen verfälscht. Deshalb sollten in den Ausfallratenkatalogen immer umfassende und vielfältige Daten mit einer genauen Aufschlüsselung der im Betrieb herrschenden Belastungen und Einsatzbedingungen enthalten sein.

Des Weiteren zeigt sich, dass insbesondere die Arbeit mit gedruckten Ausfallratenkatalogen einen enormen zeitlichen Arbeitsaufwand erfordert, da die dort beinhalteten Berechnungsmodelle oftmals von einer Vielzahl von Faktoren abhängen. Dadurch wird die korrekte Eingabe und Bedienung erschwert. In dieser Hinsicht bietet das Ermitteln der Zuverlässigkeitswerte mit Hilfe von softwarebasierten Lösungen, welche einige der Ausfallratenkataloge anbieten, eine enorme Erleichterung: Hier wird der Anwender gezielt durch das jeweilige Berechnungsmodul geführt und die jeweils nötigen Eingaben über Dialoge angefordert.

3.5 Qualitative und quantitative Analyse

Wie in Kap. 2.1 dargestellt, wird bei den Zuverlässigkeitsbewertungen zwischen qualitativen und quantitativen Analysen unterschieden. Auch bei der vorliegenden Zuverlässigkeitsbewertung für mechatronische Systeme werden diese beiden Analysearten betrachtet. In Abhängigkeit der zur Verfügung stehenden Informationen entscheidet sich, welche Analyseart genutzt werden kann.

Bei der qualitativen Analyse kommen vorwiegend die FMEA und die FTA zum Einsatz. Für weiterführende Informationen für diese beiden Analysen wird auf Kap. 2.1.1 bzw. auf [3.2] verwiesen. Als ein interessanter Aspekt ist anzusehen, dass mit Hilfe von SQMA Fehlerzusammenhänge herausgelesen werden können. Zudem lassen sich auch System- und Funktionsstrukturen erstellen. Diese mögliche Automatisierung reduziert den Arbeitsaufwand bei der Erstellung deutlich.

Neben der qualitativen Analyse kann bei der Methodik zur Zuverlässigkeitsbewertung mechatronischer Systeme auch eine quantitative Analyse durchgeführt werden. Dafür muss aber gewährleistet sein, dass die verwendeten Komponenten identifiziert und für diese jeweils ein Zuverlässigkeitswert vorliegt.

Als Herausforderung ist die Bewertung der Software zu sehen. In der Literatur sind zwar zahlreiche Modelle bekannt, die mittels verschiedener Softwaremaße, wie z. B. der Anzahl der Codezeilen, die Software-Zuverlässigkeit beschreiben. Jedoch existiert nach [3.37] und [3.41] kein Modell, welches für alle Einsatzbereiche verwendbar ist. Basierend auf Regressionsmethoden werden die verschiedenen Modelle durch vorhandene Datensätze aufgestellt. Die teilweise großen Unterschiede zwischen den Ergebnissen deuten darauf hin, dass kein allgemein gültiges und normiertes Software-Zuverlässigkeitsmodell existiert. Dies wird auch in [3.14] bestätigt. Eine Herausforderung besteht darin, dass schon in frühen Entwicklungsphasen Informationen über die Software-Zuverlässigkeit benötigt werden, um eine quantitative Aussage treffen zu können. Dies ist aber

nicht immer möglich. Aus diesem Grund wird eine Vorgehensweise benötigt, durch die, neben einer quantitativen Bestimmung der Zuverlässigkeit, eine Auswahl des zuverlässigsten Lösungskonzepts mit Hilfe eines relativen Vergleichs vorgenommen werden kann.

Die im Weiteren verwendete Vorgehensweise ermöglicht es, trotz des Fehlens eines allgemein gültigen Software-Zuverlässigkeitsmodells, einen relativen Vergleich zwischen verschiedenen Lösungskonzepten vorzunehmen. Der Ansatz basiert auf der Verwendung eines unbekannten Parameters. Prinzipiell ist zwar die Anwendung dieses unbekannten Parameters (hier: α) nicht auf die Software beschränkt, jedoch ist die Anwendung hier am sinnvollsten.

In der Regel ist für ein Gesamtsystem ein Zuverlässigkeitsziel vorgegeben (siehe Kap. 3.1). Es wird nun ein Grenzwert α_{zul} für den unbekannten Parameter α angegeben, bei dem das vorgegebene Zuverlässigkeitsziel gerade noch erreicht wird. Dieser Grenzwert kann als „Entwicklungsspielraum“ definiert werden. Dadurch können zwar für mechatronische Systeme keine absoluten Zuverlässigkeitswerte bestimmt werden, aber ein relativer Vergleich ist über diesen Ansatz möglich. In Kap. 7.2.2 sind noch weitere Ansätze zu finden, mit denen es möglich ist, unter bestimmten Randbedingungen die Zuverlässigkeit des mechatronischen Systems absolut zu bestimmen.

Anhand eines abstrakten Beispiels soll das Vorgehen des relativen Vergleiches erklärt werden. Das zu betrachtende mechatronische System besteht aus den Domänen Mechanik, Elektronik und Software. In den einzelnen Domänen tritt jeweils nur eine Ausfallart auf. Zudem wird angenommen, dass die Ausfallzeitpunkte der insgesamt drei Ausfallarten unabhängig sind sowie jeweils einer Exponentialverteilung folgen. Die letzte Annahme ist, dass die Domänen in Reihe verknüpft sind. Daraus folgt für das Gesamtsystem eine Ausfallrate von

$$\lambda_{System} = \lambda_{Mechanik} + \lambda_{Elektronik} + \lambda_{Software} \tag{3.2}$$

Als Entwicklungsziel sei

$$\lambda_{System} \leq \lambda_{Ziel} \tag{3.3}$$

vorgegeben. Um dieses Ziel zu erreichen, ist die Formel umzustellen nach

$$\lambda_{Software} \leq \lambda_{System} - \lambda_{Mechanik} - \lambda_{Elektronik} = \lambda_{zulässig\ Software}\ . \tag{3.4}$$

Hierbei kann $\lambda_{zulässig\ Software}$ als diejenige Ausfallrate der Software interpretiert werden, bei dem das Zuverlässigkeitsziel des gesamten mechatronischen Systems gerade noch erreicht wird.

Diese aufgezeigte Berechnungsmethode wird entsprechend Abb. 3.7 für drei zu vergleichende Lösungsvarianten A, B und C durchgeführt. Als Ergebnis werden zulässige Software-Ausfallraten ausgegeben, bei denen das Zuverlässigkeitsziel für das Gesamtsystem gerade erreicht wird. Diese Ergebnisse werden miteinander verglichen, wobei eine größere Softwareausfallrate einen größeren Entwicklungsspielraum darstellt.

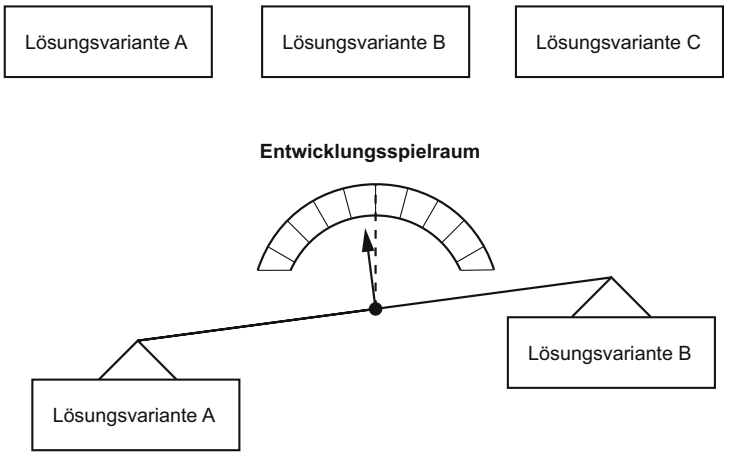

Abb. 3.7 Auswahl einer Lösungsvariante aufgrund des Entwicklungsspielraums [3.27]

Zwar kann durch dieses Vorgehen die zuverlässigste Lösungsvariante eines mechatronischen Systems quantitativ ermittelt werden, jedoch sollten Annahmen für das Ausfallverhalten von Software getroffen werden. Hierbei sollte der Ausfallzeitpunkt funktional unabhängig und durch eine Exponentialverteilung beschrieben sein. Daraus und unter der Verwendung des Entwicklungsspielraums α sowie der Einflussgrößen E folgt für eine beliebige Software-Komponente die Gleichung

$$\lambda_i = \alpha \cdot E_i \tag{3.5}$$

Der Faktor α beschreibt einen Zusammenhang zwischen den Einflussgrößen, die in frühen Entwicklungsphasen bestimmbar sind, und deren Ausfallraten λ.

Implizite Softwarezuverlässigkeit

Die Auswahl an Größen, die Einfluss auf die Software haben, ist sehr vielfältig. Dies kann von der Programmkomplexität, der Defektdichte oder der Programmiersprache bis hin zu weichen Einflussgrößen wie der Teamzusammensetzung oder Arbeitsbedingungen reichen. Hierbei beschreibt die Defektdichte, welche nach [3.32] ein wichtiges Maß zur Bestimmung der Software-Zuverlässigkeit darstellt, das Verhältnis zwischen der Anzahl der Fehler und einer definierten Größe der Anzahl der Codezeilen. Aus obigen Gründen wird die Defektdichte für die Zuverlässigkeitsbestimmung weiter untersucht.

Der hier vorgestellte Ansatz soll aber nicht auf Informationen aus Test und Betrieb zurückgreifen, sondern auf das in den Unternehmen häufig nicht oder nur unzureichend dokumentierte Wissen von Experten. Diese Experten können oft-

mals auf langjährige Erfahrung zurückgreifen. In [3.14] wird vorgeschlagen die oben beschriebene Defektdichte über ein Bayes'sches Netz zu bestimmen. Das Wissen der Experten kann durch diesen Ansatz formalisiert werden. Weiterführende Informationen über Bayes'sche Netze sind in Kap. 2.9 zu finden.

Um den Repräsentanten für die Zuverlässigkeitsbewertung, die Defektdichte, quantitativ zu bestimmen, werden von den Experten noch verschiedene Informationen zum Füllen des Bayes'schen Netzes benötigt. Konkret wird in [3.14] eine Möglichkeit zum Aufstellen eines Bayes'sches Netzes vorgestellt. In diesem Beispiel müssen die in frühen Phasen abschätzbaren Einflussfaktoren wie Komplexität des Problems, Entwicklungs- sowie Testaufwand bestimmt werden (Abb. 3.8). Als Ausgangsknoten erhält man die Defektdichte. Jedem Knoten wird ein diskreter Wertebereich zugewiesen. Beispielsweise kann der Wertebereich des Knotens „Komplexität des Problems" zwischen sehr niedrig und sehr hoch liegen. Der gegenseitige Einfluss der Knoten wird in Form von Tabellen angegeben. Die Werte in diesen Tabellen basieren auf dem Expertenwissen der jeweiligen Anwender.

Neben der Defektdichte müssen noch weitere Einflussgrößen zur Erlangung der Zuverlässigkeit betrachtet werden. So spielt die unterschiedliche Nutzungszeit *op* (operational profile) der Softwarekomponente eine große Rolle. Es wird angenommen, dass zwei Softwarekomponenten betrachtet werden. Die eine besitzt eine Defektdichte von 30 Fehler pro 1000 Codezeilen, wird aber sehr selten aufgerufen, wohingegen die andere Softwarekomponente eine geringere Defektdichte von 5 Fehler pro 1000 Codezeilen aufweist, jedoch permanent im Einsatz ist. Hier-

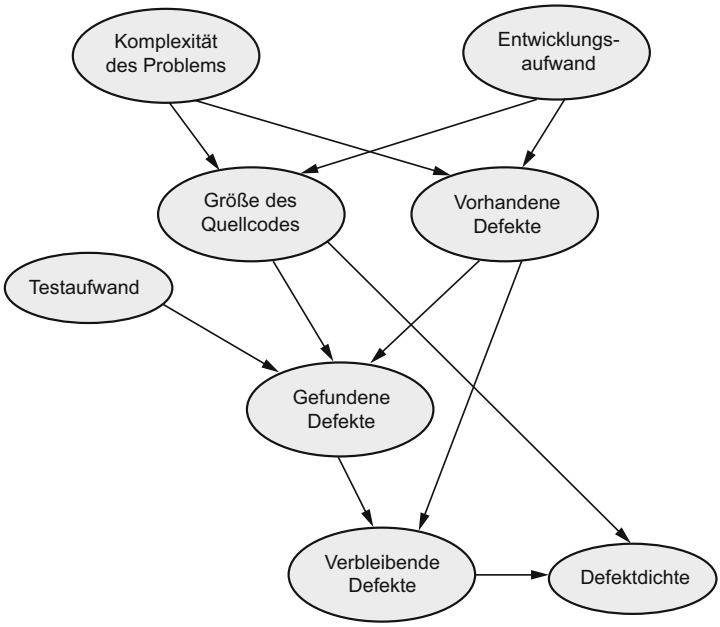

Abb. 3.8 Beispiel für ein Bayes'sches Netz zur Ermittlung der Defektdichte [3.14]

durch wird ersichtlich, dass nicht nur die Defektdichte *dd* die Zuverlässigkeit bestimmt. Die nun verwendete Gleichung lautet dann

$$\lambda_i = \alpha \cdot dd_i \cdot op_i \tag{3.6}$$

Der Faktor op_i wird wie auch die Defektdichte dd_i durch die Experten bestimmt. Bis auf den Faktor α können alle weiteren Größen bestimmt werden. Somit stellt α bei der Bestimmung der Zuverlässigkeit verschiedener Lösungsvarianten den letzten verbleibenden Freiheitsgrad dar. Dieser kann als Vergleichsmaßstab für den Entwicklungsspielraum verwendet werden. Zu berücksichtigen ist, dass α für alle Softwarekomponenten als konstant angenommen wird. Dies ist zulässig, da zunächst davon ausgegangen wird, dass sich alle Softwarekomponenten beim Auftreten eines Fehlers identisch verhalten. Falls diese Annahmen nicht ausreichen, können weitere komponentenspezifische Einflussgrößen integriert werden. Eine Ausweitung auf ein mehrdimensionales α ist jedoch nicht ohne weiteres möglich.

Die einzelnen Komponenten aller Domänen müssen nun in eine Zuverlässigkeitsstruktur angeordnet werden. Hierfür wird die Fehlerbaumanalyse genutzt. Pro Schweregrad wird jeweils ein Fehlerbaum erstellt.

Berechnung

Bei der Befragung der Experten kann es vorkommen, dass diese nicht nur exakte Zahlenwerte nennen können, sondern auch unscharfe Daten bzw. Verteilungen angeben werden. Diese können dann mit Hilfe der Monte-Carlo-Methode behandelt werden. Hierbei handelt es sich um ein Verfahren aus der Stochastik, bei dem sehr häufig durchgeführte Zufallsexperimente die Grundlage darstellen. Mit den Ergebnissen wird versucht, analytisch nicht oder nur aufwändig lösbare Probleme mit Hilfe von Simulationen numerisch zu lösen.

3.6 Vergleich des Analyseergebnisses mit dem Zuverlässigkeitsziel

Im letzten Schritt werden die vorliegenden Ergebnisse mit den gesetzten Zielen verglichen. Ist die Abweichung von Soll- und Ist-Wert akzeptabel, so muss keine weitere Zuverlässigkeitsoptimierung durchgeführt werden. Falls nun aber Soll- und Istwert weit auseinander liegen, ist eine Optimierung notwendig. Dazu werden alle kritischen Komponenten aus den Domänen herausgegriffen und ihre Eigenschaften, z. B. deren Größe, Material oder logische Zusammenhänge, überarbeitet. In einem nächsten Schritt werden diese verbesserten Komponenten integriert und eine weitere Zuverlässigkeitsanalyse durchgeführt. Dieser Vorgang wird so lange wiederholt, bis das gewünschte Ziel erreicht wird.