Methodische Grundlagen

3

Eine Fehlerbaumanalyse für komplexe Systeme stellt in der Praxis eine Herausforderung dar, deren Gelingen ein solides methodisches Vorgehen voraussetzt. Nach den theoretischen Grundlagen (Kap. 2) werden wir im Folgenden die wichtigsten Aspekte zum Analyseprozess erläutern. Schließlich ist ein gut strukturiertes methodisches Vorgehen das grundlegende Instrumentarium jedes Analysten, um eine FTA zum Ergebnis zu führen.

Wie bei fast jedem Analyseverfahren kommt der *Zielsetzung* und *Zweckdefinition* zu Beginn eine Hauptrolle zu. Viel zu oft starten FTAs ohne eine solide Vorbereitung und Klärung von Rahmenbedingungen, so dass während der Vertiefung viele Frage entstehen, die die Analysearbeit erschweren. Dementsprechend erläutern wir dies in Abschn. 3.1.

Den Rahmen der Analyse bilden die Funktionsumfänge und Teile des Systems, dessen klare Grenzen für eine FTA gezogen werden müssen. Dies setzt zu Beginn eine präzise Beschreibung der *Hauptereignisse* voraus sowie die korrekte Abbildung der Ursache-Wirkungszusammenhänge von Fehlzuständen. Neben dem technischen Verständnis des Systems sollte man sich dabei *bewusst* Beschränkungen auferlegen, so dass der richtige Detailgrad und die wesentlichen Fehlerursachen gefunden werden. Das prinzipielle Vorgehen zum Aufbau der FTA erläutert Abschn. 3.2 (die Details vertieft Kap. 4).

Ebenso essentiell für die FTA sind die grundlegenden Strukturierungsmöglichkeiten für den Fehlerbaum – sozusagen dessen „Makrostruktur" – die einem Analysten bekannt sein sollten. Dazu diskutiert Abschn. 3.3 gängige Muster, die in den meisten Literaturquellen zu wenig Erläuterung finden. Zur Strukturierung einer FTA für ein größeres System gehört insbesondere die Handhabung von mehrfach vorkommenden Teilen des Fehlerbaums. Die damit verbundene Problemstellung der Wiederverwendung und deren geeignete Modellierung beschreibt Abschn. 3.4.

© Springer-Verlag Berlin Heidelberg 2015

F. Edler, M. Soden, R. Hankammer, *Fehlerbaumanalyse in Theorie und Praxis*,
DOI 10.1007/978-3-662-48166-0_3

3.1 Vorbereitungen

Am Anfang einer FTA sollte die Zielsetzung und der Anwendungszweck festgelegt werden. Die Zielsetzung variiert dabei von rein qualitativen Fragestellungen (z. B. früh im Designprozess eines Systems) nach der möglichen Fehlerkombinatorik über Zuverlässigkeitsanalysen einzelnener Komponenten bis hin zum Vergleich von Architekturen hinsichtlich ihrer Fehlertoleranz bzw. den jeweiligen Restfehlerwahrscheinlichkeiten.

3.1.1 Klärung des methodischen Rahmens

Eine FTA steht immer im Kontext einer Systementwicklung oder Systemanalyse. Deshalb sollte vor Beginn der methodische Rahmen in Bezug auf weitere Aktivitäten geklärt werden. Vorab sollte man sich auch folgende Fragen stellen:

- Ist die FTA die richtige Methode, um zu den gewünschten Ergebnissen zu kommen? Zum Beispiel könnte für eine erste grobe Schätzung der Systemzuverlässigkeit eine Liste von Baugruppen und Diagnosegraden ausreichend sein (s. a. Abschn. 8.2.4)
- Was sind unter Umständen Techniken, die man ergänzend mit der FTA einsetzen kann, um effektiver oder besser ans Ziel zu gelangen (z. B. FMEDA[1], Markov-Modelle)?

Da in diese Fragestellung viele Faktoren mit hinein spielen, erläutert Kap. 8 und Kap. 10.

3.1.2 Informationsbeschaffung zum Untersuchungsgegenstand

Je nach Einsatzart und -zweck sollte man von der Zielsetzung ausgehend vorbereitende Schritte zur Beschaffung der zur Analyse notwendigen Unterlagen und Dokumente unternehmen. Ohne eine Systembeschreibung oder ein Referenzdokument wird jede weitere Diskussion und Modellierung schwierig bis fehlerhaft. Dabei bestimmt die Zielsetzung und der Anwendungskontext, welche Informationen bei der Analyse vorliegen sollten.

Zum Beispiel kann für eine quantitative Zuverlässigkeitsbetrachtung ein Schaltplan oder ein entsprechendes Hardwaredesigndokument ausreichend sein. Kommen Diagnosemaßnahmen hinzu, die in Software realisiert sind, empfiehlt sich die Hinzunahme des Softwaredesigns oder der Spezifikation, so dass eine verlässliche Abschätzung der Diagnosedeckungsgrade möglich ist. Weitere Informationsquellen können bereits vorhandene quantitative Analysen sein, aus denen geschätzte Fehlerraten und interne Diagnosemechanismen hervorgehen (z. B. FMEDA), Qualifizierungsberichte und Testreihen über Verhalten unter Stress (z. B. nach JEDEC/AEC-Q100[2]), Simulationsdaten, Schnittstellenbeschreibungen, Anforderungsdokumente externer Komponenten, Konstruktionsunterlagen der Mechanik, Wartungshandbücher etc.

[1] Failure Mode Effect and Diagnostic Analysis.
[2] s. a. https://www.jedec.org/

Bei komplexeren Systemen ist eine funktionale Beschreibung des Systems unerlässlich, aus der das Zusammenwirken einzelner Teilsysteme oder Komponenten hervorgeht. Ohne diese Information wird es für den Analysten schwierig, sich die nötigen Systemkenntnisse anzueignen. In der Regel findet man häufiger (physikalische und technische) Strukturbeschreibungen, so dass man das Verständnis der funktionalen Abhängigkeiten eventuell aus tiefer gehenden Anforderungsdokumenten gewinnen muss. Sollte Dokumentation dazu fehlen, lohnt es sich unter Umständen vorab die wichtigsten funktionalen Abhängigkeiten zu skizzieren und mit den Fachexperten abzustimmen (Beispiele für ein solches Vorgehen finden sich in Kap. 9). Von der Entwicklung einer FTA „ins Blaue“, z. B. durch unreflektierte Übernahme von Analyseergebnissen aus Vorgängerprojekten, raten wir eher ab.

Art und Reifegrad der Ausgangsdokumente hängen stark vom Anwendungskontext ab. Wird ein bestehendes System analysiert, sind in der Regel ausreichend reife Dokumente vorhanden, auf die sich die FTA stützen kann. Befindet man sich dagegen in einer frühen Designphase, sollten getroffene Annahmen dokumentiert werden, so dass diese zu einem späteren Zeitpunkt verifiziert und ggf. angepasst werden können.

Zum Beispiel haben angenommene Wartungsintervalle von Komponenten oder dynamische Aspekte der Software durch das Task-Management/Scheduling einen erheblichen Einfluss auf die Ausfallwahrscheinlichkeiten von Ereignissen (vgl. Abschn. 2.7). Ebenso können getroffene Annahmen über Topologie, Bauteileigenschaften, Steckverbindungen, Kabelwege, vorhandene Überwachungen in externen Komponenten, Informationen zu Wartung und Personal usw. für die Verlässlichkeit und Aussagekraft der Analyse von entscheidender Bedeutung sein.

3.1.3 Notationsregeln definieren

Weiterhin empfiehlt es sich, bereits zu Beginn einige Grundregeln festzulegen, wie im Fehlerbaum bestimmte Sachverhalte benannt werden. Ein wichtiger Bestandteil sind Notationskonventionen, durch die Bezug auf Systemelemente genommen wird. Ereignisse sollten generell Bezeichner aus Designdokumenten und Abkürzungen einheitlich verwenden und diese sollten bei Bedarf in ein Glossar übernommen werden. Zusätzlich bietet sich ein Namensschema für Ereignisse und Gatter an, um z. B. ähnliche Fehlerarten an verschiedenen Bauteilen leicht identifizieren zu können. Eine Vertiefung der Grundregeln zur korrekten Beschreibung und Tipps zu sprachlichen Formulierungen finden sich in Kap. 6.

3.1.4 Analyseplanung

An die Vorbereitungen sollte sich nachfolgend eine Planung für die Analyse anschließen, die unter Berücksichtigung aller Randbedingungen einen optimalen Rahmen zur Durchführung gewährleistet. Auch sollte man alle kritischen Ressourcen und Aktivitäten

identifizieren, die den Erfolg der FTA beeinflussen könnten. Hierzu zählen Experten für spezielle Sachverhalte genauso wie die Terminplanung im Projektkontext. Weiterführende Aspekte zu diesem Themenkomplex finden sich in den Kap. 7 und 8.

3.2 Ablauf der FTA-Erstellung

Die Analysemethode FTA umfasst grundsätzlich mehrere Phasen, die unabhängig vom gesetzten Ziel sind. Nach erfolgreicher Vorbereitung und Zielsetzung erfolgt der Ablauf der FTA in den folgenden Schritten (vgl. Abb. 3.1):

1. *Definieren der Hauptereignisse*. Je nach Zielsetzung sind dies Fehlzustände des Gesamtsystems, Fehlzustände einzelner Komponenten, Fehler von Baugruppen oder Funktionen. Oft gehören zu einer FTA *mehrere* Hauptereignisse, die dann jeweils in separaten Fehlerbäumen untersucht werden (aber sinnvollerweise auf Basis eines einheitlichen Datensatzes, vgl. Abschn. 7.3.2).
2. *Definition der Systemgrenzen und Eingrenzung der Funktionsumfänge*. Die Analyse sollte von vornherein festlegen, welche Teile des Systems berücksichtigt werden. Dazu zählt auch der Detaillierungsgrad auf dem die Analyse geführt wird, Betriebsparameter und für quantitative Analysen die betrachtete Lebensdauer des Systems.
3. *Modellierung des Fehlerbaums*. Ausgehend von den Hauptereignissen wird der Fehlerbaum entwickelt. Als deduktive Methode werden Ereignisse Schritt für Schritt auf Ursachen zurückgeführt. Dieser Vorgang sollte einer Systematik folgen, so dass das System korrekt abgebildet wird. Für quantitative Analysen werden die Basisereignisse in dieser Phase auch parametriert.
4. *Berechnung der Minimalschnitte und quantitativer Kennzahlen*. Dieser Schritt wird im Allgemeinen durch ein FTA-Werkzeug erledigt, das zur Modellierung verwendet wird und das die notwendigen Algorithmen implementiert. Der Analyst muss die für die Zielsetzung gewünschten Einstellungen und Parametrierungen vornehmen, so dass die Software die Eintretenswahrscheinlichkeiten, Ausfalldichten und/oder Importanzen in einer im Systemkontext adäquaten Weise berechnet.
5. *Auswertung*. Basierend auf den berechneten Minimalschnitten, Ausfallwahrscheinlichkeiten und Importanzen findet die Auswertung und Interpretation statt. Nach Bedarf werden weitere Iterationen durchlaufen, zum Beispiel falls Ergebnisse unplausibel sind oder Detaillierungen nötig werden. Am Ende steht die Erstellung eines Analyseberichts, der die wichtigsten Befunde zusammenfasst.

Wie aus Abb. 3.1 ersichtlich baut jeder Arbeitsschritt auf dem vorhergehenden auf. Deshalb sollte man Sorgfalt beim Voranschreiten walten lassen, um Folgefehler in der Analyse zu vermeiden. Beispielsweise muss die Motivation und Zielsetzung vom Analysten verstanden sein, bevor Hauptereignisse, Umfang und Detaillierung der FTA festgelegt werden. Das heißt, es gilt sich immer rückzuversichern, ob die bisher erstellten Arbeitsergebnisse schlüssig und plausibel sind (s. a. Kap. 8).

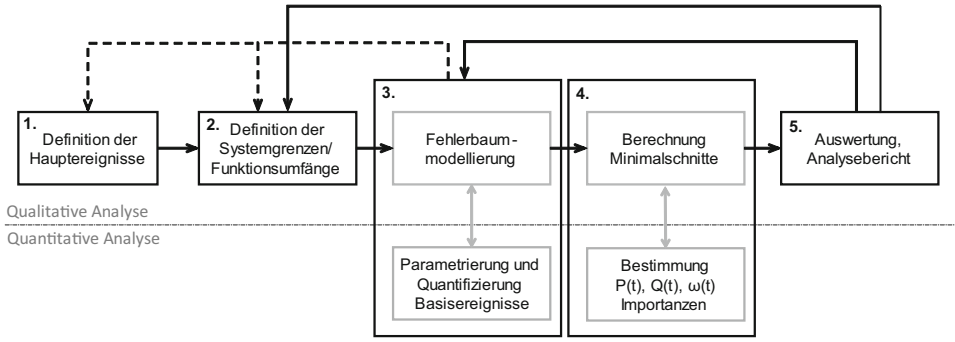

Abb. 3.1 Vorgehensmodell bei der FTA (vgl. auch [4])

Weiterhin möchten wir in diesem Kapitel die Herleitung und Definition der Hauptereignisse sowie wie die grundsätzliche Herangehensweise zur Strukturierung von Fehlerbäumen erläutern (Schritte 1 und 2). Diese makroskopische Sicht hilft erfahrungsgemäß, mögliche Fehlerquellen beim Einstieg in die Analyse zu eliminieren. Dem detaillierten Vorgehen bei der Modellbildung (Schritt 3) und der Auswertung (Schritt 4/5) widmen wir die eigenständigen Kap. 4 und Kap. 5.

3.2.1 Definition der Hauptereignisse

Die Identifikation und Beschreibung der Hauptereignisse bildet den Einstiegspunkt in die Analyse. Prinzipiell sollten die Hauptereignisse die Zielsetzung in Bezug auf einen Ausfall des zu analysierenden Systems widerspiegeln und so präzise wie möglich formuliert werden.

Abhängig vom Gesamtkontext beschreibt ein Hauptereignis einen kompletten Systemausfall, einen bestimmten Fehlzustand von Komponenten oder Fehler in Daten bzw. an Schnittstellen.

Bei einem Gesamtsystem, wie z. B. einem Fahrzeugantrieb, der Stromversorgung einer Industrieanlage etc. werden die Hauptereignisse für die FTA häufig direkt aus einer Gefahren- oder Risikoanalyse abgeleitet. Zugehörige Bezeichnungen, Normen sowie Methodik und Verfahren variieren dabei stark zwischen den verschiedenen Branchen. Wird eine FTA für eine sicherheitstechnisches Nachweisverfahren (z. B. bei der Produktzulassung) benötigt, ist es deshalb erforderlich, den branchenspezifischen Rahmen zu kennen (vgl. Kap. 8). Wird eine FTA für ein Teilsystem, eine Komponente oder eine funktionale Schnittstelle im Gesamtsystem benötigt, muss gewährleistet sein, dass die untersuchten Fehlzustände in den Kontext des Gesamtsystems passen. Dazu ist eine Abstimmung zwischen Systemintegrator und den Detailverantwortlichen erforderlich, was wir in Abschn. 8.5.1 vertiefen. Hauptereignisse können jedoch auch aus Einzelanalysen für das

jeweils betrachtete Systemelement abgeleitet werden. Hier gibt es eine Reihe von etablierten Methoden zur strukturierten Risikobestimmung (FMEA, HAZOP[3], ETA[4] etc.).

Eine präzise Beschreibung der Hauptereignisse folgt der Fragestellung nach dem *Wo* und dem *Was*. Ein einfaches und zielgerichtetes Vorgehen ist durch die Beantwortung der folgenden Fragen gewährleistet:

1. Wo manifestiert sich die Fehlfunktion? Die Lokalisierung des Fehlers im System sollte eingrenzen, an welcher Stelle der Fehler auftritt (z. B. Schnittstelle mit der Systemumgebung, Komponente, Signal, Daten).
2. Was genau ist fehlerhaft? Eine Umschreibung des Fehlzustandes sollte mindestens qualitativ beschreiben, was den Fehler charakterisiert (z. B. ein Datensignal ist verfälscht, ein Pegel zu hoch, etc).
3. Existieren messbare Kriterien für den Fehler? Wenn möglich sollte eine Bezifferung anhand von quantifizierbaren Größen stattfinden, wie zum Beispiel Grad eine Soll-/Ist-Wert-Abweichung in Prozent bzw. Absolutbetrag. Abweichungen von Sollgrößen können in verschiedenen Dimensionen auftreten:
   (a) Wertebereich, z. B. Absolutabweichung um 5 °C über Sollwert
   (b) Zeitbereich, z. B. Verzögerung eines Signals um mehr als 50 ms
   (c) Mischformen, z. B. Abweichung Zeit-Wert-Integral größer als 3500 Nms

Nicht immer können alle drei Fragen genau beantwortet werden, gerade wenn auf Systemebene eine Gefährdung analysiert wird. Dies zeigen im Folgenden einige Beispiele.

Beispiele für Hauptereignisse auf Systemebene, die nicht alle Kriterien beinhalten:

- Gasexplosion in der Anlage
- Bremsaktuator erzeugt unzulässiges Bremsmoment
- Ungewollte Beschleunigung von mehr als X m/s^2
- Verlust aller Kommunikationssysteme im Flugzeug
- Ausfall des Notkühlsystems des Reaktors

Meist erfolgt anschließend eine Suche nach mehreren möglichen Ursachen und Komponenten, die innerhalb der ersten Ebene des Fehlerbaums aufgespannt werden.

Hauptereignisse, für Fehler an Komponenten- oder Signalschnittstellen, beinhalten in der Regel mehr Details, hier einige Beispiele:

- CAN-Ausgangssignal T_OUT liefert unzulässige Abweichung vom Sollwert
- Ausgangssignal µC auf PIN 42 ist fälschlich auf HIGH

[3] Hazard and Operability Analysis.
[4] Event Tree Analysis.

- Datenpaket MSG enthält falsches Vorzeichen-Bit

Das folgende Beispiel ist einem realen Fall aus der Praxis entlehnt. Die Hauptereignisse waren etwa in dieser Art formuliert: „*Unerwünscht aktiv angesteuertes Momentensignal liegt an*." Selbst wenn der Systemkontext (z. B. als Funktionsblockdiagramm) bekannt ist, lässt diese Formulierung mehr Fragen offen, als sie beantwortet:

- *Wo* liegt das unerwünschte Signal an?
- *Ab welcher Grenze* (in Wert und/oder Zeit) ist der unerwünschte Signalwert kritisch?

Davon abgesehen finden sich weitere sprachliche Mängel. So impliziert das Konstrukt „aktiv angesteuert", dass es auch eine passive Ansteuerung geben könnte, was einen Widerspruch in sich darstellt. Das Wort „aktiv" ist in diesem Satz also überflüssig.

Hauptereignisse beschreiben also generell kritische Fehler an Ausgängen oder Schnittstellen zum übergeordneten System bzw. zur Systemumgebung. Der Fehlerbaum wird dann von den Ausgängen bzw. Schnittstellen Schritt für Schritt entlang von Wirk- und Signalpfaden (z. B. Schaltungsverläufe) und den jeweiligen funktionalen Abhängigkeiten folgend aufgebaut (s. a. Abschn. 3.3).

3.2.2 Systemgrenzen, Betriebsparameter und Auflösung

Die Definition des Betrachtungsumfangs bildet die weitere Vorbereitung der eigentlichen Analyse. Ausgehend von der Systembeschreibung sollten die Elemente und mögliche Fehlerursachen bestimmt werden, die im Fehlerbaum berücksichtigt bzw. ausgegrenzt werden.

3.2.2.1 Strukturelle Eingrenzung

In der Regel sind die Grenzen an Schnittstellen einer Komponente oder eines Teilsystems zu finden, wobei eine klare Aussage darüber getroffen werden sollte, ob die Schnittstelle Teil der Analyse ist oder nicht. Zum Beispiel sind bei Kommunikationsbussen neben dem eigentlichen physikalischen Konnektor (Stecker, Buchsen) des öfteren auch Treiberbausteine nötig. Ein ausführlicheres Beispiel zeigt Kap. 9.

3.2.2.2 Funktionale Eingrenzung

Neben der strukturellen Eingrenzung – oftmals entlang physikalischer oder technologischer Gegebenheiten – kann der Betrachtungsumfang auch an Funktionen festgemacht

werden. Dazu müssen dann alle Elemente eines Systems berücksichtigt werden, die zur Erbringung der betrachteten Funktionalität beitragen.

Zum Beispiel könnte bei einer Anlagensteuerung eines Druckbehälters die FTA-Analyse auf eine Überwachungsfunktion fokussieren, die im Fehlerfall eine Notabschaltung durchführt. Diese Analyse der *Sicherheitsfunktion* würde dann Teile der Anlagensteuerung bewusst aussparen.

Je nach Abstraktionsgrad reicht das Spektrum von Systemfunktionen hinunter zu einzelnen Softwarefunktionen. Dies kann dazu führen, dass man einen *Querschnitt* durchs System analysiert, der Teile von Software und Hardware umfasst (siehe auch Abschn. 4.6).

3.2.2.3 Faktoren des Einsatzprofils

Wichtige Festlegungen betreffen die zu betrachtende Betriebsdauer, üblicherweise als *mission time* oder *system life time* bezeichnet und die angenommenen Betriebsbedingungen des Systems. Aus diesen Vorgaben leiten sich in der Regel Stressparameter ab, die insbesondere bei quantitativen Analysen einen großen Einfluss haben. Eine wichtige Rolle spielt hier die Festlegung des zeitlichen Horizonts, da dieser Parameter neben einzelnen Fehlerraten in der Regel auch die Gesamtaussage zur Zuverlässigkeit und/oder Verfügbarkeit des Systems beeinflusst (vgl. Abschn. 2.7). Gegebenenfalls muss man anhand der angenommenen Vorgabe zur Betriebsdauer prüfen, ob alle Elemente eine ausreichende mittlere Lebenserwartung haben, oder ob es einen periodischen Austausch geben muss. Beispiel: Bauteile wie Relais oder Schalter haben eine begrenzte Lebensdauer, abhängig von der Anzahl der Schaltvorgänge.

3.2.2.4 Angestrebter und möglicher Detaillierungsgrad der FTA

Ein weiterer Faktor für die Analyse stellt der Detaillierungsgrad dar, der die Auflösung und den Gesamtumfang des Fehlerbaums bestimmt. Dadurch legt man fest, an welcher Stelle Ereignisse als nicht weiter zerlegbar angesehen und folglich durch Primärereignisse dargestellt werden. Dies kann abhängig vom Anwendungskontext zu unterschiedlich detaillierten Fehlerbäumen führen. Wird zum Beispiel eine FTA begleitend zu frühen Entwicklungsphasen durchgeführt, können einzelne Zweige nicht weiter verfeinert werden als im vorläufigen Designentwurf beschrieben. Die Schaltungsbestückung und andere Layoutmerkmale können dabei verständlicherweise noch nicht einbezogen werden. Stellt die Zielsetzung der Analyse hingegen eine Verifikation der Zuverlässigkeit dar, wird man nicht umhin kommen, Fehler einzelner Bauteile mit zu berücksichtigen. Dazu ist ggf. eine Anknüpfung an andere Analysen sinnvoll, wie z. B. die FMEDA (s. a. Kap. 10).

3.2.2.5 Ein- und Ausgrenzung möglicher Fehlerursachenklassen

Bei der Definition des Betrachtungsumfangs kann ein weiterer begrenzender Faktor die Auswahl bzw. Begrenzung auf bestimmte Klassen von Fehlerursachen sein. Als Fehlerursachenklassen lassen sich eine Zahl von systematischen und zufälligen Fehlern unterscheiden:

- Externe Störeinflüsse (z. B. elektromagnetische Interferenzen)
- Überlastung durch Betrieb außerhalb des Missions- bzw. Stressprofils (z. B. Überhitzung)
- Dimensionierungs- und Auslegungsfehler (z. B. Wahl von Bauteilen mit zu geringer Lebenserwartung)
- Werkstofffehler (z. B. Zinnwhisker)
- Fertigungsfehler (z. B. kalte Lötstellen)
- Verschleiß (z. B. Getriebeabrieb)
- Menschliches Versagen (z. B. Unterlassen von vorgeschriebenen Notreaktionen)
- Design- und Umsetzungsfehler (z. B. Programmierfehler)
- Zufällige Fehler (z. B. Bitfehler in Speicherbausteinen oder bei Signalübertragung, spontane Hardwarefehler)

Diese Liste hat keinen Anspruch auf Vollständigkeit, sollte aber als Ausgangspunkt für eine Beschränkung der zu entwickelnden FTA hinsichtlich bestimmter Ursachenklassen dienen. Dabei orientiert sich die Beschränkung an den Rahmenbedingungen, unter denen die FTA erstellt wird (s. a. Abschn. 8.2).

Sicherlich ist es intuitiv, z. B. bei einer quantitativen FTA zur Bestimmung der durchschnittlichen Ausfallwahrscheinlichkeit eines Systems nicht alle systematischen Fehler wie Programmierfehler oder Werkstofffehler mit einzubeziehen. Andererseits ist es zum Beispiel bei einer empfangenen Nachricht über einen Kommunikationsbus unerheblich, ob diese ein falsches Datum durch einen Programmierfehler oder durch einen zufälligen Fehler beinhaltet. Hier müsste man allerdings spätestens bei der Quantifizierung Annahmen treffen, um diesem Ereignis eine Eintretenswahrscheinlichkeit zuzuordnen und letztlich dort den Ausschluss von Fehlerursachenklassen treffen.

3.2.2.6 Systemvarianten und ihre Behandlung

Stellt ein Systemdiagramm verschiedene Varianten oder gar eine Plattform in unterschiedlichen Konfigurationen dar, muss man zu Beginn der Analyse festlegen, welche Ausbaustufe(n) berücksichtigt wird bzw. werden. Dabei können kleinere Variationspunkte unter Umständen in einem Fehlerbaum abgehandelt werden, zum Beispiel in dem man mit Hausereignissen verschiedene Zweige an- oder abschaltet. Sobald sich Systemvarianten in mehreren Merkmalen soweit unterscheiden, dass sie zu unterschiedlichen Analysen führen, sollte man von einer gemeinsamen Betrachtung absehen. Andernfalls erhöht sich die Komplexität unverhältnismäßig.

Abbildung 3.2 zeigt ein Beispiel für eine FTA, die zwei Varianten umfasst. Angenommen ein Automobilhersteller entwickelt ein Motorsteuergerät für eine Plattform, in der je nach Ausbaustufe ein Adaptive Cruise Control (ACC) enthalten ist oder nicht. Da Steuersignale vom ACC die Geschwindigkeit am Motorsteuergerät

http://www.springer.com/978-3-662-48165-3

Fehlerbaumanalyse in Theorie und Praxis
Grundlagen und Anwendung der Methode

Edler, F.; Soden, M.; Hankammer, R.

2015, XVIII, 290 S. 105 Abb., 9 Abb. in Farbe.,
Hardcover
ISBN: 978-3-662-48165-3