

DIN EN 61025

ICS 29.020

Ersatz für
DIN IEC 61025:1993-12
Siehe jedoch Beginn der
Gültigkeit

**Fehlzustandsbaumanalyse (IEC 61025:2006);
Deutsche Fassung EN 61025:2007**

Fault tree analysis (FTA) (IEC 61025:2006);
German version EN 61025:2007

Analyse par arbre de panne (AAP) (CEI 61025:2006);
Version allemande EN 61025:2007

Gesamtumfang 50 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Beginn der Gültigkeit

Die von CENELEC am 2007-03-01 angenommene EN 61025 gilt als DIN-Norm ab 2007-08-01.

Daneben darf DIN IEC 61025:1993-12 noch bis 2010-03-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 61025:2004-01.

Für diese Norm ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (<http://www.dke.de>) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 56 „Dependability“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem auf der IEC-Website unter „<http://webstore.iec.ch>“ mit den Daten zu dieser Publikation angegebenen Datum (maintenance result date) unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Änderungen

Gegenüber DIN IEC 61025:1993-12 wurden folgende Änderungen vorgenommen:

- a) Der Titel der Norm wurde in „Fehlzustandsbaumanalyse“ geändert.
- b) Aufnahme „dynamischer Gatter“ und somit Behandlung von Störungen, die von der Reihenfolge der Ereignisse oder dem momentanen Zustand des betrachteten Systems abhängen. Hierzu sind beispielsweise vor einer Fehlzustandsbaumanalyse Untersuchungen nach dem Markoff-Verfahren notwendig.
- c) Die Norm wurde neu gegliedert und es wurden zusätzliche graphische Symbole mit aufgenommen.

Frühere Ausgaben

DIN IEC 61025: 1993-12

Deutsche Fassung

Fehlzustandsbaumanalyse
(IEC 61025:2006)

Fault tree analysis (FTA)
(IEC 61025:2006)

Analyse par arbre de panne (AAP)
(CEI 61025:2006)

Diese Europäische Norm wurde von CENELEC am 2007-03-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

© 2007 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61025:2007 D

Vorwort

Der Text des Schriftstücks 56/1142/FDIS, zukünftige 2. Ausgabe von IEC 61025, ausgearbeitet von dem IEC/TC 56 „Dependability“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2007-03-01 als EN 61025 angenommen.

Diese Europäische Norm ersetzt HD 617 S1:1992.

In Bezug auf HD 617 S1:1992 wurden im Wesentlichen folgende Änderungen vorgenommen:

- Detaillierte Erklärungen von Methoden der Fehlzustandsbaumanalyse wurden hinzugefügt;
- quantitative und Zuverlässigkeitsaspekte der Fehlzustandsbaumanalyse (FTA) wurden hinzugefügt;
- die Darstellung der Beziehung zu anderen Zuverlässigkeitstechniken wurde erweitert;
- Beispiele von Analysen und Methoden, die in dieser Norm erklärt werden, wurden hinzugefügt;
- derzeit gebräuchliche Formelzeichen wurden aktualisiert.

Abschnitt 7, der sich mit der Analyse befasst, wurde überarbeitet, um die herkömmliche logische Fehlzustandsbaumanalyse separat von der quantitativen Analyse zu behandeln, die schon seit einigen Jahren angewandt wird, um die Zuverlässigkeit von im Entwicklungsstadium befindlichen Produkten zu erhöhen.

Einige Inhalte, die bisher im Hauptteil dieser Norm enthalten waren, wurden in die Anhänge A und B verschoben.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2007-12-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2010-03-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61025:2006 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 60300-3-1 ANMERKUNG Harmonisiert als EN 60300-3-1:2004 (nicht modifiziert).

IEC 60812 ANMERKUNG Harmonisiert als EN 60812:2006 (nicht modifiziert).

IEC 61078 ANMERKUNG Harmonisiert als EN 61078:2006 (nicht modifiziert).

Inhalt

	Seite
Vorwort	2
Einleitung	5
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	6
4 Symbole	8
5 Allgemeines	9
5.1 Beschreibung und Aufbau eines Fehlzustandsbaums	9
5.2 Zielsetzung	10
5.3 Anwendungsgebiete	10
5.4 Kombinationen mit anderen Zuverlässigkeitsanalyseverfahren	11
6 Entwicklung und Beurteilung	13
6.1 Allgemeine Überlegungen	13
6.2 Notwendige Informationen über das System	15
6.3 Graphische Beschreibung des Fehlzustandsbaums und seiner Struktur	16
7 Entwicklung und Beurteilung des Fehlzustandsbaums	17
7.1 Allgemeines	17
7.2 Untersuchungsziel	17
7.3 Systemkenntnisse	17
7.4 Entwicklung des Fehlzustandsbaums	17
7.5 Konstruktion des Fehlzustandsbaums	18
7.6 Ausfallraten bei der Fehlzustandsbaumanalyse	34
8 Bezeichnungen und Benennungen in einem Fehlzustandsbaum	35
9 Bericht	36
Anhang A (informativ) Symbole	37
Anhang B (informativ) Verfahren zum disjunkten Zerlegen	44
B.1 Erfolgsorientierte Vorgehensweise	44
B.2 Ausfallorientierte Vorgehensweise	45
Literaturhinweise	47
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	48
 Bilder	
Bild 1 – Erläuterung der in einer Fehlzustandsbaumanalyse verwendeten Begriffe	8
Bild 2 – Darstellung einer Serienstruktur mit Hilfe eines Fehlzustandsbaums	20
Bild 3 – Fehlzustandsbaumdarstellung einer parallelen, aktiven Redundanz	21
Bild 4 – Beispiel eines Fehlzustandsbaums mit verschiedenartigen Gattern	23
Bild 5 – Darstellung von Ereignissen durch rechtwinklige Gatter	24

	Seite
Bild 6 – Beispiel für einen Fehlzustandsbaum mit einem wiederholten und einem verwiesenen Ereignis.....	25
Bild 7 – Behandlung gemeinsamer Ursache in rechtwinkliger Gatter-Darstellung.....	25
Bild 8 – Mittels Fehlzustandsbaumanalyse zu analysierende Brückenschaltung	29
Bild 9 – Darstellung der Brückenschaltung als Fehlzustandsbaum	30
Bild 10 – Brückensystem-FTA, Esary-Proschan, ohne disjunkt zu zerlegen	32
Bild 11 – Ausfallwahrscheinlichkeit des Brückensystems berechnet mit dem „seltene Ereignisse berücksichtigenden“ Näherungsverfahren	33
Bild 12 – Eintrittswahrscheinlichkeit des Hauptereignisses mit disjunktem Zerlegen	34
Bild A.1 – Beispiel eines P-UND-Gatters.....	43
Tabellen	
Tabelle A.1 – Häufig in Fehlzustandsbäumen benutzte Symbole und graphische Zeichen	37
Tabelle A.2 – Allgemeine Symbole für Ereignisse und Ereignisbeschreibung.....	40
Tabelle A.3 – Statische Gatter	41
Tabelle A.4 – Dynamische Gatter.....	42

Einleitung

Die Fehlzustandsbaumanalyse (en: Fault Tree Analysis, FTA) befasst sich mit dem Aufzeigen und dem Untersuchen von Bedingungen und Einflussgrößen, die zum Auftreten oder potentiell möglichen Auftreten eines festgelegten Hauptereignisses führen oder dazu beitragen können. Bei der Fehlzustandsbaumanalyse ist dieses Ereignis üblicherweise die Blockierung oder Beeinträchtigung der Leistungsfähigkeit des Systems, der Sicherheit oder anderer wichtiger betrieblicher Merkmale; bei der Erfolgsbaumanalyse dagegen wird das den Erfolg beschreibende Merkmal untersucht.

Die Fehlzustandsbaumanalyse wird oft zur Sicherheitsanalyse von Systemen (etwa Transportsysteme, Kraftwerke oder allgemein sonstige Systeme, bei denen die Betriebssicherheit beurteilt werden sollte) verwendet. Die Fehlzustandsbaumanalyse kann auch zur Analyse der Zuverlässigkeit und ihrer Elemente Funktionsfähigkeit, Verfügbarkeit und Instandhaltbarkeit verwendet werden.

In dieser Norm werden zwei Vorgehensweisen einer Fehlzustandsbaumanalyse behandelt. Die erste ist eine qualitative Vorgehensweise, bei der die Wahrscheinlichkeit des Eintretens der Ereignisse und der dazu beitragenden Faktoren – Eingangsereignisse – oder deren Ereignishäufigkeit nicht behandelt wird. Bei dieser Vorgehensweise werden Ereignisse/Fehlzustände eingehend untersucht, dies wird mit qualitativer oder herkömmlicher Fehlzustandsbaumanalyse bezeichnet. Diese Art der Analyse findet breite Anwendung in der Kernindustrie und in vielen anderen Fällen, bei denen die potentiellen Ursachen eines unerwünschten Ereignisses oder von Fehlzuständen gefragt sind, ohne Interesse für deren Eintrittswahrscheinlichkeit. Manchmal werden einige Ereignisse in einer herkömmlichen Fehlzustandsbaumanalyse quantitativ untersucht, aber solche Berechnungen sind losgelöst von umfassenden Zuverlässigkeitsbetrachtungen und demzufolge wird mittels der Fehlzustandsbaumanalyse auch nicht die umfassende Zuverlässigkeit berechnet. Die in der Industrie in breitem Maße angewendete zweite Vorgehensweise ist hauptsächlich quantitativer Art. Dabei wird mit einer detaillierten Fehlzustandsbaumanalyse ein ganzes Produkt, Prozess oder System modelliert und für die große Mehrheit der Grundereignisse, ob Fehlzustände oder Störungen, deren Eintrittswahrscheinlichkeit durch Analyse oder Versuch bestimmt. In diesen Fällen ist das Endergebnis die Eintrittswahrscheinlichkeit eines Hauptereignisses, die für die Wahrscheinlichkeit eines Ausfalls steht.

1 Anwendungsbereich

In dieser Internationalen Norm wird die Fehlzustandsbaumanalyse beschrieben und es werden folgende Anwendungshilfen gegeben:

- Erklärung der Grundlagen:
 - Beschreibung und Erklärung der zugehörigen mathematischen Modellbildung;
 - Erläuterung der Beziehungen zwischen Fehlzustandsbaumanalyse und anderen Zuverlässigkeitsanalyseverfahren;
- Beschreibung der Schritte und Maßnahmen bei der Durchführung einer Fehlzustandsbaumanalyse;
- Aufzeigen und Ermitteln zugehöriger Annahmen, Ereignisse und Ausfallarten;
- Benennung und Beschreibung von üblichen graphischen Symbolen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60050(191), *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 61165, *Application of Markov techniques*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe nach IEV 60050-191.

In der Methodik und bei der Anwendung des Fehlzustandsbaums werden viele Begriffe zur besseren Erklärung der Analyseabsicht oder des angedachten Verfahrens verwendet. Einige Begriffe werden auch als Synonyme für von verschiedenen Autoren analytisch korrekt beachtete Begriffe verwendet. In dieser Norm werden folgende zusätzliche Begriffe verwendet.

3.1

Ergebnis

Resultat einer Aktion oder sonstigen Eingabe; Folge einer Ursache

ANMERKUNG 1 Ein Ergebnis kann ein Ereignis oder ein Zustand sein. In einem Fehlzustandsbaum kann das Ergebnis einer Kombination von entsprechenden Eingangsereignissen, die durch ein Gatter dargestellt wird, entweder ein Zwischenereignis oder das Hauptereignis sein.

ANMERKUNG 2 Im Fehlzustandsbaum kann ein Ereignis auch eine Eingabe für ein Zwischenereignis sein, oder es kann das Hauptereignis sein.

3.2

Hauptereignis

Ergebnis der Kombinationen aller Eingangsereignisse

ANMERKUNG 1 Dies ist das interessierende Ereignis, von dem ausgehend der Fehlzustandsbaum entwickelt wird. Das Hauptereignis wird häufig auch mit Endereignis oder Hauptergebnis bezeichnet.

ANMERKUNG 2 Das Hauptereignis ist vorgegeben und Ausgangspunkt der Fehlzustandsbaumentwicklung. Es steht in der Hierarchie der Ereignisse an der Spitze.

3.3

Endereignis

Endergebnis der Kombinationen aller Eingaben, Zwischen- und Grundereignisse

ANMERKUNG Ergebnis von Eingangsereignissen oder Zuständen (siehe 3.2).

3.4

Hauptergebnis

Ergebnis, das durch das Konstruieren des Fehlzustandsbaums untersucht wird

ANMERKUNG Endergebnis der Kombinationen aller Eingaben, Zwischen- und Grundereignisse; es ist ein Ergebnis von Eingangsereignissen oder Zuständen (siehe 3.2).

3.5

Gatter

Symbol zur Herstellung symbolischer Verbindungen zwischen Ausgabeereignis und den entsprechenden Eingaben

ANMERKUNG Ein Gattersymbol beschreibt die Art der Beziehung, nach der Eingangsereignisse das Ausgabeereignis bewirken.

3.6

Schnittmenge

Gruppe von Ereignissen, die bei Eintritt aller Ereignisse das Hauptereignis verursachen

3.7

Minimalschnitt

kleinste Ereignismenge, die für den Eintritt des Hauptereignisses erforderlich ist

ANMERKUNG Das Ausbleiben irgendeines dieser Ereignisse würde den Eintritt des Hauptereignisses verhindern.

3.8**Ereignis**

Eintritt einer Bedingung oder einer Aktion

3.9**Grundereignis**

Ereignis oder Zustand, das oder der nicht weiter untersucht bzw. entwickelt werden kann

3.10**Primärerereignis**

Ereignis am Fuß des Fehlzustandsbaums

ANMERKUNG In dieser Norm kann Primärerereignis ein Grundereignis bedeuten, das nicht weiter untersucht werden muss, oder es kann ein Ereignis sein, welches an anderer Stelle untersucht wird (obwohl es aus Gruppen von Ereignissen und Gattern besteht), oder ein Ereignis, das überhaupt nicht weiter untersucht wird (nicht weiter untersuchtes Ereignis).

3.11**Zwischenereignis**

Ereignis, welches weder Hauptereignis noch Primärerereignis ist

ANMERKUNG Üblicherweise ist es das Ergebnis eines oder mehrerer Primärerereignisse oder anderer Zwischenereignisse.

3.12**nicht weiter untersuchtes Ereignis**

Ereignis ohne Eingangereignisse

ANMERKUNG Dieses wird aus verschiedenen möglichen Gründen in der aktuellen Analyse nicht untersucht, wie etwa Mangel an detaillierteren Informationen, oder es wird in einer anderen Analyse untersucht und dann in der aktuellen Analyse als nicht weiter untersucht vermerkt. Ein Beispiel nicht weiter untersuchter Gatter könnten im Handel erhältliche Einheiten sein.

3.13**singulärer Punktausfall (Ereignis)**

Ausfallereignis, das bei seinem Eintritt einen kompletten Systemausfall bewirken würde, das heißt ein Ereignis, welches durch sich alleine, unabhängig von anderen Ereignissen oder deren Kombinationen, das unerwünschte Hauptereignis (Ergebnis) bewirken würde

3.14**Ereignisse mit gemeinsamer Ursache**

unterschiedliche Ereignisse in einem System oder Fehlzustandsbaum, deren Eintritt durch dieselbe Ursache bewirkt wird

ANMERKUNG Ein Beispiel eines solchen Ereignisses könnte der Kurzschluss von Keramik Kondensatoren, verursacht durch das Biegen der gedruckten Leiterplatte, sein; dadurch, obwohl es sich um unterschiedliche Kondensatoren mit unterschiedlichen Funktionen handeln könnte, könnte deren Kurzschluss dieselbe Ursache haben – dasselbe Eingangereignis.

3.15**gemeinsame Ursache**

Ursache für den Eintritt mehrerer Ereignisse

ANMERKUNG In vorstehendem Beispiel könnte das Biegen der Leiterplatte selbst das Zwischenereignis sein, für das mehrere Ereignisse verantwortlich sein könnten, z. B. aus der Umwelt stammendes Schwingen und Schocken oder durch die Handhabung verursachtes Brechen der gedruckten Leiterplatte während des Fertigungsprozesses.

3.16**repliziertes oder wiederholtes Ereignis**

Ereignis, das Eingabe für mehr als ein Ereignis einer höheren Ebene ist

ANMERKUNG Dieses Ereignis kann durch eine gemeinsame Ursache oder Ausfallart eines Bauelementes bewirkt werden, das von mehr als einem Entwurfsteil benützt wird.

In Bild 1 sind einige der vorstehenden Definitionen bildlich dargestellt. In diesem Bild sind Ereignisse mit Anmerkungen und Beschreibungen zur besseren Erklärung der praktischen Anwendung von Fehlzustandsbäumen versehen. In Bild 1 sind die graphischen Erläuterungen von Schnittmengen und Minimalschnitten zur einfacheren graphischen Darstellung anderer zugehöriger Begriffe weggelassen. Die Symbole in Bild 1 und allen folgenden Bildern unterscheiden sich etwas von denjenigen in den Tabellen A.1, A.2, A.3 und A.4, da über den Gattersymbolen Textrahmen mit Beschreibungen der einzelnen Ereignisse gezeichnet sind.

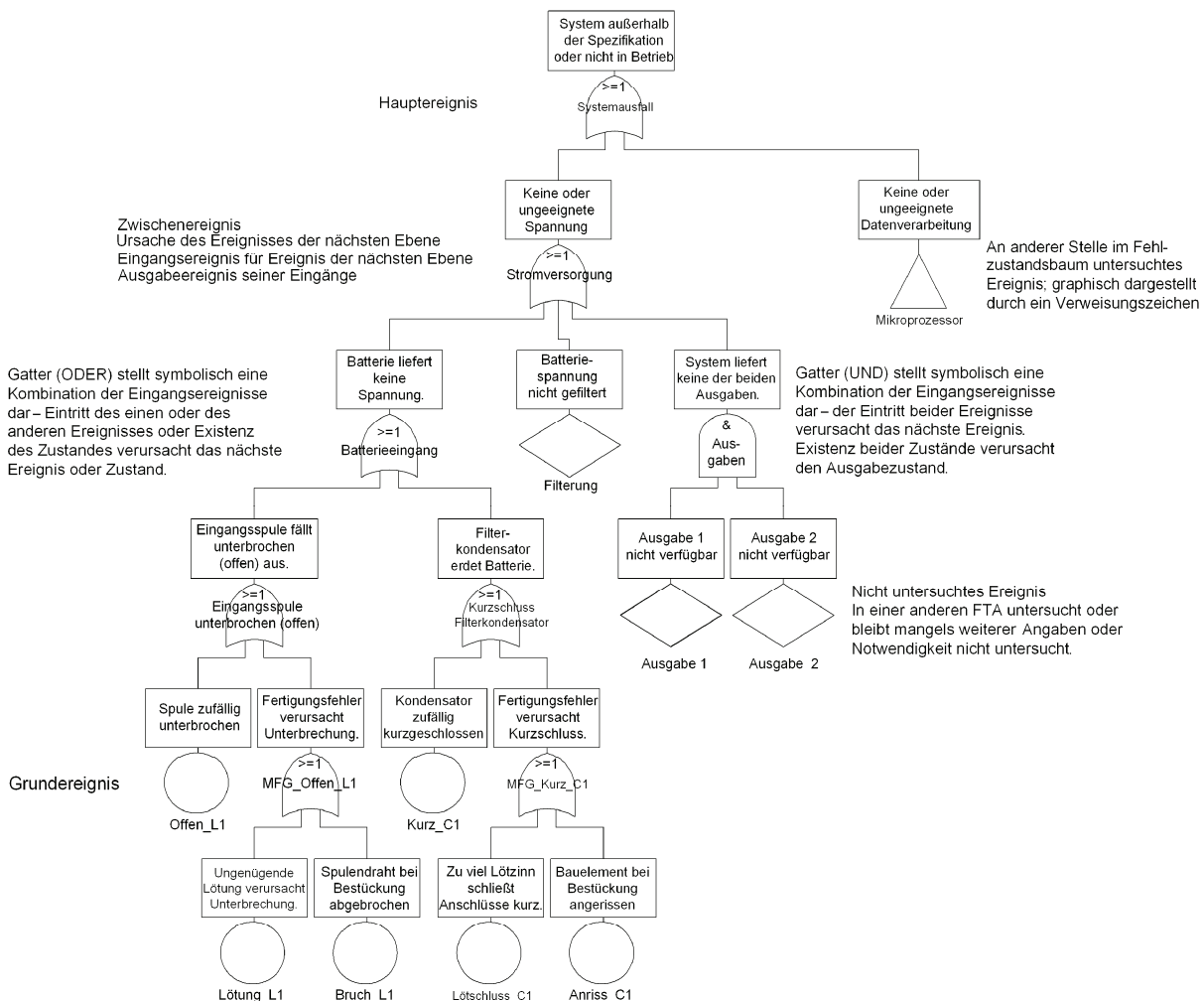


Bild 1 – Erläuterung der in einer Fehlzustandsbaumanalyse verwendeten Begriffe

ANMERKUNG Die Symbole in Bild 1 und in allen anderen Bildern können sich etwas von den in Anhang A gezeigten Symbolen unterscheiden. Der Grund hierfür sind die zur besseren Erläuterung der Beziehung der verschiedenen Ereignisse zusätzlich eingezeichneten Textrahmen.

4 Symbole

Die graphische Darstellung des Fehlzustandsbaums macht es erforderlich, dass graphische Zeichen bzw. Symbole, Bezeichnungen und Markierungen in einer durchgehend einheitlichen Weise verwendet werden. Die zur Beschreibung von Fehlzustandsbaumereignissen verwendeten Symbole können von den Gepflogenheiten der Anwender und, sofern verwendet, von Softwarepaketen abhängen. Allgemeine Anleitungen hierzu sind in Abschnitt 8 und im Anhang A enthalten.

Die in dieser Norm verwendeten Formelzeichen sind die üblichen genormten Zuverlässigkeitsformelzeichen wie etwa $F(t)$ oder einfach nur Wahrscheinlichkeit für das Eintreten eines Ereignisses F . Daher enthält diese Norm keine besondere Formelzeichenliste.

5 Allgemeines

5.1 Beschreibung und Aufbau eines Fehlzustandsbaums

Für die Analyse der Zuverlässigkeit gibt es verschiedene analytische Verfahren, die Fehlzustandsbaumanalyse ist eine davon. Ehe eine Fehlzustandsbaumanalyse in Angriff genommen wird, sollte der Analyst vorab Folgendes untersuchen: Sinn und Zweck jedes Verfahrens und dessen individuelle bzw. deren kombinierte Anwendbarkeit zur Beurteilung der Abfolge von Ereignissen oder Zuständen, die zu einem Ergebnis führen könnten, oder der daraus berechneten Zuverlässigkeit (Funktionsfähigkeit und Verfügbarkeit) eines gegebenen Systems oder Bauelements. Vor- und Nachteile der einzelnen Verfahren und deren Ergebnisse sollten abgewogen und es sollte beachtet werden, welche Daten für die Durchführung der Analyse ggf. erforderlich sind, wie komplex diese sein kann sowie andere in dieser Norm benannte Faktoren.

Ein Fehlzustandsbaum ist eine geordnete graphische Darstellung der Bedingungen und Faktoren, die den Eintritt eines unerwünschten Ergebnisses verursachen oder dazu beitragen; dieses wird mit Hauptereignis bezeichnet. Sollte das Ergebnis ein Erfolg sein, dann wird aus dem Fehlzustandsbaum ein Erfolgsbaum, bei dem die Eingangsereignisse zu dem Haupterfolgsergebnis beitragen. Die Darstellung eines Fehlzustandsbaums erfolgt in einer verständlichen, untersuchbaren und, falls notwendig, änderbaren Form zum Aufzeigen von:

- Faktoren mit Einfluss auf das untersuchte Hauptereignis, wie es in den meisten herkömmlichen Fehlzustandsbaumanalysen üblich ist;
- Faktoren, die die Zuverlässigkeit und Leistungseigenschaften des Systems beeinflussen für den Fall, dass das Fehlzustandsbaumanalyseverfahren zur Zuverlässigkeitsanalyse verwendet werden soll, um beispielsweise Konstruktionsschwächen, Umwelt- oder Betriebsbeanspruchungen, Bauelementeausfallarten, Fehlhandlungen des Bedienungspersonals, Softwarefehler zu erkennen;
- solchen Ereignissen, die mehr als ein Funktionsteil betreffen und die die Vorteile spezifischer Redundanzen unwirksam machen könnten oder die sich auf zwei oder mehr Teile eines Produkts auswirken, die ansonsten als betrieblich voneinander unabhängig angesehen würden (Ereignisse mit gemeinsamer Ursache).

Die Fehlzustandsbaumanalyse ist ein deduktives Analyseverfahren (von einer höheren Systemebene zu einer niedrigeren Systemebene) mit dem Ziel, die Kombination von Ursachen besonders hervorzuheben, die zum festgelegten Hauptereignis führen können. Abhängig vom Untersuchungsziel kann die Analyse qualitativer oder quantitativer Art sein.

Ein Fehlzustandsbaum kann auch als sein Komplement entwickelt werden, die Erfolgsbaumanalyse; dort ist das Hauptereignis ein Erfolg, und die Eingaben tragen zum Erfolg, dem erwünschten Ereignis, bei.

Falls die Wahrscheinlichkeit des Eintretens der Primärereignisse numerisch nicht geschätzt werden kann, kann man mittels einer qualitativen Fehlzustandsbaumanalyse Ursachen von potentiell unerwünschten Ergebnissen anhand individueller Primärereignisse untersuchen. Die Eintrittswahrscheinlichkeiten dieser Primärereignisse beschreibt man dann mit Worten wie „äußerst wahrscheinlich“, „sehr wahrscheinlich“, „durchschnittlich wahrscheinlich“, „kaum wahrscheinlich“ usw. Das Hauptziel einer qualitativen Fehlzustandsbaumanalyse ist die Ermittlung des Minimalschnitts, um zu erkennen, auf welche Weisen Grund- oder Primärereignisse zu dem Hauptereignis beitragen.

Sofern die Wahrscheinlichkeiten der Primärereignisse bekannt sind, kann man eine quantitative Fehlzustandsbaumanalyse durchführen. Mit dieser Analyseart können dann die Eintrittswahrscheinlichkeiten aller Zwischenereignisse und das Hauptereignis (Ergebnis) berechnet werden. Auch ist eine quantitative Fehlzustandsbaumanalyse bei der Zuverlässigkeitsanalyse eines Produkts oder Systems in der Entwicklungsphase sehr nützlich.

Die Fehlzustandsbaumanalyse kann zur Analyse von Systemen mit komplexen Wechselbeziehungen zwischen deren Subsystemen verwendet werden, wobei auch Wechselbeziehungen zwischen Hardware und Software berücksichtigt werden.

5.2 Zielsetzung

Eine Fehlzustandsbaumanalyse kann getrennt oder in Verbindung mit anderen Zuverlässigkeitsuntersuchungen durchgeführt werden. Zur Zielsetzung gehören:

- Aufzeigen von Ursachen und Kombinationen von Ursachen, die zum Hauptereignis führen;
- Beurteilen, ob eine bestimmte Zuverlässigkeitsmaßgröße eine festgelegte Forderung erfüllt;
- Aufzeigen potentieller Ausfallarten oder Einflussgrößen, welche am meisten zur Ausfallwahrscheinlichkeit oder Nichtverfügbarkeit eines instandsetzbaren Systems beitragen – hierdurch werden Wege zur Verbesserung der Systemzuverlässigkeit aufgezeigt;
- Analyse und Vergleich verschiedener Entwurfs-/Konstruktionsalternativen für eine bessere Systemzuverlässigkeit;
- Nachweis, dass in anderen Untersuchungen (wie etwa Markoff und FMEA) gemachte Annahmen weiterhin gelten;
- Aufzeigen solcher potentieller Ausfallarten, die ein Sicherheitsrisiko bewirken könnten, Berechnung der zugehörigen Eintrittswahrscheinlichkeiten und Beurteilung von Linderungsmöglichkeiten;
- Aufzeigen von gemeinsamen Ereignissen (beispielsweise der mittlere Zweig einer Brückenschaltung, siehe Bild 10);
- Suche nach einem Ereignis oder Kombinationen von Ereignissen, die am wahrscheinlichsten den Eintritt des Hauptereignisses bewirken können;
- Bewertung der Auswirkung eines eingetretenen Primäreignisses auf die Wahrscheinlichkeit des Hauptereignisses;
- Berechnung der einzelnen Ereigniswahrscheinlichkeiten;
- Berechnung der Verfügbarkeiten und Ausfallraten eines durch einen Fehlzustandsbaum dargestellten Systems oder dessen Teile, sofern ein stationärer Zustand vorausgesetzt werden kann und etwaige Reparaturen jeweils voneinander unabhängig sind (gleiche Einschränkung wie beim Erfolgspfad-diagramm/Zuverlässigkeitsblockdiagramm).

5.3 Anwendungsgebiete

Die Fehlzustandsbaumanalyse eignet sich besonders zur Untersuchung komplexer Systeme mit verschiedenen funktional zusammenhängenden oder abhängigen Subsystemen. Die Vorteile einer Fehlzustandsbaumanalyse sind besonders dann offenkundig, wenn die Systementwicklung das Ergebnis der Zusammenarbeit spezialisierter Entwicklungsgruppen ist und die einzelnen Fehlzustandsbäume miteinander verknüpft werden. Fehlzustandsbaumanalysen sind bei der Entwicklung von Kernkraftwerken, Transportsystemen, Telekommunikationssystemen, chemischen und anderen industriellen Prozessen, Eisenbahnsystemen, Unterhaltungselektronik, Medizinsystemen, Rechnersystemen usw. üblich. Fehlzustandsbaumanalyse ist ebenfalls von besonderem Nutzen bei Systemen, die aus Typ-verschiedenen Teilen (mechanische, elektronische und Software-Elemente) bestehen und die in gegenseitiger Wechselbeziehung stehen, die nicht in einfacher Weise mittels anderer Verfahren modelliert werden können. Ein Beispiel hierfür wäre eine Kombination von Ereignissen, bei der es entscheidend auf die Reihenfolge ihres Auftretens ankommt, wie etwa das Vorhandensein von schwingungsbedingter Ermüdung, die zu Rissen und so zum Ausfall von Bauelementen führt.

Das Werkzeug Fehlzustandsbaumanalyse kann vielfältig verwendet werden, beispielsweise:

- Ermittlung der passenden logischen Kombination von Ereignissen, die zum Hauptereignis führen, und möglicherweise deren Priorisierung;
- ein gerade in Entwicklung befindliches System untersuchen und mögliche Ursachen des unerwünschten Hauptereignisses absehen und verhindern oder diese entschärfen;
- ein System analysieren, seine Zuverlässigkeit berechnen, die Hauptbeiträger zur Ausfallwahrscheinlichkeit ermitteln und Entwurfsänderungen beurteilen;
- bei der Bewertung der Risiken und zugehöriger Wahrscheinlichkeiten assistieren.

Die Fehlzustandsbaumanalyse kann auf alle neuen oder modifizierten Produkte in allen Entwicklungsphasen als analytisches Werkzeug zur Ermittlung potentieller Entwurfs-/Konstruktionsprobleme angewendet werden,

einschließlich der frühen Entwicklungsphasen, in denen erst wenige Informationen zu den Konstruktionsdetails vorliegen. Solche frühen Arbeiten müssen dann auf Konstruktionsdetails ausgeweitet werden, sobald mehr Informationen über den Konstruktionsentwurf und seine Komponenten erhältlich werden. Mit der Fehlzustandsbaumanalyse können auch solche potentiellen Probleme behandelt werden, die aus der mechanischen Konstruktion herrühren, die sich aus der Umwelt- oder betrieblichen Beanspruchungen ergeben, auf Grund von Schwachstellen im Fertigungsprozess und Betriebs- und Instandhaltungsprozeduren.

5.4 Kombinationen mit anderen Zuverlässigkeitsanalyseverfahren

5.4.1 Kombination von Fehlzustandsbaumanalyse (FTA) und Fehlzustandsart- und -auswirkungsanalyse (FMEA)

Diese Analysekombination wird häufig in fachspezifischen Normen, insbesondere in Sicherheits- und Transportnormen empfohlen. Der Nutzen einer kombinierten Analyse ergibt sich aus Folgendem:

- Fehlzustandsbaumanalyse ist ein deduktives (von einer höheren zu einer niedrigeren Systemebene gehendes) und die Fehlzustandsart- und -auswirkungsanalyse^{N1)}, (en: Fault Mode and Effects Analysis, FMEA) ein induktives (von einer niedrigeren zu einer höheren Systemebene gehendes) Analyseverfahren. Eine Mischung deduktiver und induktiver Betrachtungen hilft dabei, die Vollständigkeit einer Analyse sicherzustellen.
- In Sicherheitsnormen wird häufig die Analyse eines einzelnen Ausfalls und in einigen Fällen auch von Mehrfachausfällen verlangt; erstere Forderung wird von der Fehlzustandsart- und -auswirkungsanalyse erfüllt. Die Fehlzustandsbaumanalyse kann sowohl einfache als auch mehrfache Ausfälle behandeln.
- Fehlzustandsart- und -auswirkungsanalyse ist ein brauchbares Verfahren für eine umfassende Ermittlung von Grundereignissen oder Gefährdungen, wogegen die Fehlzustandsbaumanalyse ein praktisches Verfahren für die Analyse der Ursachen unerwünschter Ereignisse ist.

Zusätzlich gibt es eine einfache Überprüfung der Folgerichtigkeit zwischen FMEA und FTA:

- Jeder in einer FMEA ermittelte einfache Ausfall, der zum Hauptereignis des Fehlzustandsbaums führt, muss als singulärer Punktausfall (in Form der Minimalschnitte) erscheinen;

ANMERKUNG Ein singulärer Punktausfall ist ein Ausfall, der bei seinem Eintritt einen kompletten Systemausfall bewirken würde.

- jeder in der FTA ermittelte einzelne Ausfallpunkt sollte auch als solcher in der FMEA erscheinen.

Der Wert dieser Überprüfung der Folgerichtigkeit erhöht sich noch, wenn die Analysen getrennt und unabhängig voneinander durchgeführt werden. Dies ist besonders bei Sicherheitsanalysen wichtig.

In der IEC-Norm IEC 60300-3-1 wird diese Methodik erklärt.

5.4.2 Kombination von FTA und Ereignisbaumanalyse (ETA)

Jedes Ereignis könnte man mit Hilfe eines Fehlzustandsbaums analysieren. In manchen Fällen kann dies jedoch aus verschiedenen Gründen nicht angebracht sein:

- Es ist manchmal einfacher, Ereignisabläufe zu erkunden als kausale Beziehungen aufzuzeigen;
- der sich ergebende Baum könnte sehr groß werden;
- häufig werden verschiedene Teile der Analyse von getrennt arbeitenden Teams behandelt.

Um die Untersuchung praktikabel zu gestalten, legt man häufig nicht das unerwünschte Hauptereignis als Erstes fest, sondern benennt potentiell unerwünschte Ereignisse an der Schnittstelle zwischen funktionalem und technischem Bereich.

Als anschauliches Beispiel soll das Hauptereignis „Verlust der Besatzung oder des Raumschiffes“ bei einem Weltraumflug betrachtet werden. Anstelle der Konstruktion eines großen Fehlzustandsbaums mit dem Spitzenereignis „Verlust der Besatzung oder des Raumschiffes“ kann man unerwünschte Zwischenereignisse wie „Ausfall der Zündung“ oder „Schubausfall“ als Hauptereignis festlegen und diese Ereignisse als getrennte

^{N1)} Nationale Fußnote: In DIN 25448:1990-05 als „Ausfalleffektanalyse“ bezeichnet.

Fehlzustandsbäume analysieren. Diese reduzierten Hauptereignisse würde man dann wiederum als Eingabe für einen Ereignisbaum verwenden und damit die betrieblichen Konsequenzen analysieren.

Diese Kombination von Ereignis- und Fehlzustandsbaumanalyse wird manchmal mit Ursache-Folgen-Analyse bezeichnet.

5.4.3 Kombination von Fehlzustandsbaum- und Markoffanalyse

Mit Fehlzustandsbaumanalysen, die lediglich eine Kombination statischer Ereignisse (Zeitabhängigkeit – zeitliche Abfolge der Zustandskombinationen wird weder beachtet noch modelliert – statische Gatter) vorsehen, werden üblicherweise Systeme beurteilt, bei denen die Reihenfolge der Ereignisse bedeutungslos ist. Jedoch ist es möglich, die Fehlzustandsbaumanalyse durch Einführung zusätzlicher Verknüpfungsglieder (Gatter) auszuweiten, hinter denen Markoff-Modelle stehen. Solche Gatter tragen den Namen „dynamische“ Gatter, wie zum Beispiel Prioritäts-UND-Gatter, Reihenfolge-Gatter und Ersatz-Gatter. Für solche Gatter muss man die Ausfallwahrscheinlichkeit zur Zeit t mittels eines geeigneten Markoff-Modells oder durch Simulation berechnen. Nach der entsprechenden Berechnung darf man das dynamische Gatter mit seinen Eingangswerten durch ein einziges Primäreignis ersetzen, für das die Eintrittswahrscheinlichkeit durch eine Markoffanalyse berechnet wurde. Einige im Handel erhältliche Softwarepakete erlauben die Modellierung dynamischer Gatter und ermöglichen die Berechnung der Eintrittswahrscheinlichkeit des hinter dem Gatter stehenden Ereignisses. Ein Beispiel eines dynamischen Prioritäts-UND-Gatters ist in Anhang A gezeigt.

Sowohl statische als auch dynamische Gatter eines Fehlzustandsbaums werden unter der Annahme verwendet, dass die individuellen Ereignisse voneinander unabhängig sind (es sei denn, diese sind als gemeinsam definiert). Besondere Sorgfalt muss jedoch der Unabhängigkeit der Ereignisse in dem Markoff-Modell und den Ereignissen im Fehlzustandsbaum gewidmet werden.

5.4.4 Kombination von Fehlzustandsbaumanalyse und binärem Entscheidungsdiagramm

Die Berechnung der Eintrittswahrscheinlichkeit des Hauptereignisses eines Fehlzustandsbaums mit vielen Schnittmengen bedarf der Wahrscheinlichkeitsberechnung aller Schnittmengenkombinationen. Auf Grund der großen Komplexität muss diese Berechnung häufig gestutzt werden. Man kann ein binäres Entscheidungsdiagramm (en: Binary Decision Diagram, BDD) rekursiv aus einem Fehlzustandsbaum konstruieren, das dann eine effiziente und exakte Berechnungsmethode eröffnet. Diese Methode ist in dem NASA-Handbuch „NASA Fault Tree Handbook with Aerospace Applications version 1.1“ [1]¹ gut erläutert.

Die BDD-Vorgehensweise ist dann angebracht, wenn die Stutzung der Schnittmengen-Wahrscheinlichkeitsberechnungen entweder zu einem nicht hinnehmbaren Genauigkeitsverlust führen würde oder für die FTA-Lösung übermäßig viel Zeit aufgewendet werden müsste. Dies ist besonders dann zu beachten, wenn in dem Modell viele sehr wahrscheinliche Ereignisse enthalten sind. Da die bei der BDD-Vorgehensweise generierten Schnittmengenpfade disjunkt zerlegt sind (siehe 7.5.5.4), können auf diese Weise Berechnungen zur Wirkbreite und Anfälligkeit effizient und exakt durchgeführt werden.

5.4.5 Kombination mit dem Zuverlässigkeitsblockdiagramm

Ein Zuverlässigkeitsblockdiagramm besteht aus Blöcken oder Modulen, die für eine Gruppe von Komponenten oder Ausfallarten stehen. Diese Gruppen werden üblicherweise entsprechend den Funktionsblockdiagrammen eines Produkts, Systems oder eines Prozesses gebildet. Diese Module besitzen entweder eine bestimmte Ausfallrate oder eine berechnete Überlebens- oder Ausfallwahrscheinlichkeit bei gegebener Verwendung oder bekanntem Betriebsprofil. Traditionell haben diese Blöcke eine Ausfallrate gleich der Summe der Ausfallraten ihrer einzelnen Bauelemente. Bei dieser Betrachtungsweise werden die Wechselbeziehungen der Bauelemente innerhalb eines Moduls nicht berücksichtigt.

Um die Genauigkeit der funktionalen Modellierung innerhalb eines Blockes (Software/Hardware, Wechselbeziehungen von mechanischen Teilen) zu erhöhen, kann man die Zuverlässigkeit gewisser Blöcke mit einem Fehlzustandsbaum modellieren. Die sich daraus ergebenden Informationen zur Eintrittswahrscheinlichkeit dieser Blöcke können dann mit dem betreffenden Block im Zuverlässigkeitsblockdiagramm verbunden werden. Auf diese Weise ergeben Zuverlässigkeitsblockdiagramme, die üblicherweise unabhängig voneinander ausfallende Bauelemente annehmen, eine realistischere Vorhersage.

¹ Zahlen in rechteckigen Klammern verweisen auf die Literaturhinweise.

6 Entwicklung und Beurteilung

6.1 Allgemeine Überlegungen

6.1.1 Überblick

Ein Fehlzustandsbaum ist eine geordnete graphische Darstellung der Bedingungen, die den Eintritt eines unerwünschten Ergebnisses verursachen oder dazu beitragen; dieses wird mit Hauptereignis bezeichnet. Die Darstellung eines Fehlzustandsbaums erfolgt in einer verständlichen, untersuchbaren und, falls notwendig, änderbaren Form zum Aufzeigen von:

- Faktoren, die die Zuverlässigkeit und Leistungsdaten des Systems beeinflussen. Zu diesen Faktoren gehören beispielsweise Konstruktionsschwächen, Umwelt- oder Betriebsbeanspruchungen, Bauelementausfallarten, Fehlhandlungen des Bedienungspersonals, Softwarefehler;
- Ereignissen mit gemeinsamer Ursache, die zum Ergebnis von mehreren Zwischenereignissen in einem Fehlzustandsbaum beitragen. Beispiele hierfür sind solche Ereignissen, die mehr als ein Funktionsteil betreffen und die die Vorteile spezifischer Redundanzen unwirksam machen könnten oder die sich auf zwei oder mehr Teile eines Produkts auswirken, die ansonsten als betrieblich voneinander unabhängig angesehen würden.

Die Fehlzustandsbaumanalyse ist ein deduktives Analyseverfahren (von einer höheren Systemebene zu einer niedrigen Systemebene) mit dem Ziel, die Kombination von Ursachen besonders hervorzuheben, die zum festgelegten Hauptereignis führen können. Abhängig vom Untersuchungsziel kann die Analyse qualitativer (Methode A) oder quantitativer (Methode B) Art sein.

Falls die Wahrscheinlichkeit des Eintretens der Hauptereignisse numerisch nicht geschätzt werden kann, kann man mittels einer qualitativen Fehlzustandsbaumanalyse (Methode A) Ursachen von potentiell unerwünschten Ergebnissen anhand individueller Hauptereignisse untersuchen. Die Eintrittswahrscheinlichkeiten dieser Primärereignisse beschreibt man dann mit Worten wie „äußerst wahrscheinlich“, „sehr wahrscheinlich“, „durchschnittlich wahrscheinlich“, „kaum wahrscheinlich“ usw., wie in 5.1 erläutert.

Sofern die Wahrscheinlichkeiten der Grundereignisse oder Primärereignisse bekannt sind, kann man eine quantitative Fehlzustandsbaumanalyse (Methode B) durchführen. Mit dieser Analyseart können dann die Eintrittswahrscheinlichkeiten aller Zwischenereignisse und das Hauptereignis (Ergebnis) berechnet werden.

6.1.2 Kombinationen von Ereignissen und Zuständen

Das Endergebnis eines Fehlzustandsbaums (Hauptereignis) kann selbst ein Fehlzustand oder ein Ereignis sein. Hier beschreibt der Fehlzustandsbaum einen Fehlzustand oder ein Ereignis, der oder das sich aus den beitragenden Ereignissen oder aus anderen Fehlzuständen ergibt. In der Fehlzustandsbaumanalyse können gewisse Kombinationen von Ereignissen entweder Zustände oder Ereignisse sein, wogegen die anderen dem Ergebnis entsprechen müssen. So können beispielsweise die Eingaben in ein ODER-Gatter, dessen Ausgabe entweder ein Zustand oder ein Ereignis ist, Zustände oder Ereignisse sein. Wenn das Ergebnis (Ausgabe) eines UND-Gatters ein Ereignis ist, müssen auch die Eingaben Ereignisse sein; sollte jedoch das Ergebnis (Ausgabe) ein Zustand sein, so müssen auch die Eingaben Zustände sein.

Ein Zustand kann durch die Wahrscheinlichkeit gekennzeichnet werden, dass er zur Zeit t besteht, wogegen ein Ereignis entweder durch die Ausfallrate oder Ausfallhäufigkeit oder durch die Eintrittswahrscheinlichkeit des Ereignisses zur Zeit t gekennzeichnet werden kann.

6.1.3 Untersuchung von Fehlzuständen die zu anderen Fehlzuständen oder Ereignissen führen

Traditionell wird ein Fehlzustandsbaum konstruiert, um Fehlzustände oder Ereignisse, die zu einem Ergebnis führen, zu untersuchen. Diese Vorgehensweise wird bereits seit langer Zeit in vielen Industriebereichen angewendet, mit besonderer Effizienz in der Kernindustrie. Auf diese Weise ist er ein leistungsfähiges und außerordentlich wertvolles Werkzeug zur Untersuchung potentieller Probleme, Ereignisse, Verbesserungen und anderer Präventivmaßnahmen, durch die ein unerwünschtes Ergebnis verhindert oder entschärft wird.