

	DIN IEC 62502 (VDE 0050-3)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 29.020 Einsprüche bis 2008-10-31 Entwurf Verfahren zur Analyse der Zuverlässigkeit – Ereignisbaumanalyse (IEC 56/1259/CD:2008) Analysis techniques for dependability – Event Tree Analysis (IEC 56/1259/CD:2008) Anwendungswarnvermerk Dieser Norm-Entwurf mit Erscheinungsdatum 2008-08-04 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 79 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Das internationale Dokument IEC 56/1259/CD:2008 „Analysis techniques for dependability – Event Tree Analysis“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine autorisierte deutsche Übersetzung.

Das internationale Dokument wurde vom TC 56 „Dependability“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
–	IEC 60050(191):1990 + A1:1999 + A2:2002	IEV Teil 191:2005	–
EN 60300-3-1:2004	IEC 60300-3-1:2003	DIN EN 60300-3-1:2005-05	–
–	IEC 60300-3-9:1995 ^{N1)}	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60300-3-1:2005-05, *Zuverlässigkeitsmanagement – Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik (IEC 60300-3-1:2003); Deutsche Fassung EN 60300-3-1:2004*

IEV Teil 191, *Internationales Elektrotechnisches Wörterbuch – Teil 191: Zuverlässigkeit und Dienstgüte*

^{N1)} Nationale Fußnote: IEC 60300-3-9 wird derzeit überarbeitet und befindet sich noch im Entwurfsstadium. Hierzu ist als aktueller deutscher Entwurf E DIN IEC 60300-3-9 (VDE 0050-1):2007-05 verfügbar.

Verfahren zur Analyse der Zuverlässigkeit – Ereignisbaumanalyse

Inhalt

	Seite
Einleitung.....	6
1 Anwendungsbereich	6
2 Normative Verweisungen.....	7
3 Begriffe.....	7
4 Symbole und Abkürzungen.....	8
5 Allgemeine Beschreibung	9
6 Vorteile und Einschränkungen einer Ereignisbaumanalyse	10
6.1 Vorteile	10
6.2 Einschränkungen	11
7 Beziehungen zu anderen Analyseverfahren.....	11
7.1 Kombination von Ereignisbaum- und Fehlzustandsbaumanalyse.....	11
7.2 Analyse der Schutzebenen (Layer of Protection Analysis – LOPA)	12
7.3 Verbindung mit anderen Verfahren.....	13
8 Erstellen von Ereignisbäumen	13
8.1 Allgemeines	13
8.2 Schritte in der Ereignisbaumanalyse	13
9 Auswertung	18
9.1 Einleitende Bemerkungen.....	18
9.2 Qualitative Analyse – Handhabung von Abhängigkeiten.....	18
9.3 Quantitative Analyse	21
10 Dokumentation.....	24
Anhang A (informativ) Graphische Darstellung.....	25
Anhang B (informativ) Beispiele.....	26
B.1 Anlageninterner Brand (Kernkraftwerk)	26
B.1.1 Einleitung	26
B.1.2 Auswahlverfahren	26
B.1.3 Quantitative Analyse	27
B.1.4 Resultat	28
B.2 Ereignisbaumanalyse für einen Bahnübergang.....	28
B.2.1 Symbole und Bezeichnungen	28
B.2.2 Zielsetzung.....	28
B.2.3 Systemdefinition.....	29
B.2.4 Gefährdungsidentifikation	30
B.2.5 Ereignisbaumanalyse.....	30
B.2.6 Quantitative Analyse	31
B.2.7 Ergebnisanalyse und Festlegung der notwendigen Maßnahmen	33

	Seite
B.2.8 Schlussfolgerung	33
B.3 Verbindung mit der Fehlzustandsbaumanalyse und Boole'sche Vereinfachungen	33
Literaturhinweise	39
Bild 1 – Prozess des Aufstellens eines Ereignisbaumes	10
Bild 2 – Grundlegende graphische Darstellung eines Ereignisbaums	18
Bild 3 – Funktionale Abhängigkeiten in Ereignisbäumen	19
Bild 4 – Modellierung struktureller oder physikalischer Abhängigkeiten	20
Bild 5 – Reihenfolge der Ereignisse	21
Bild 6 – Verbindung mit Fehlzustandsbäumen	23
Bild A.1 – Häufig verwendete graphische Darstellung für Ereignisbäume	25
Bild B.1 – Ereignisbaum eines typischen Brandereignisses in einem Dieseldieselmotorgebäude	27
Bild B.2 – Schema einer Bahnübergangsanlage (BÜ-Anlage)	29
Bild B.3 – Ereignisbaumanalyse einer Bahnübergangsanlage	31
Bild B.4 – Einfaches Beispiel	34
Bild B.5 – Fehlzustandsbaum für System 1	35
Bild B.6 – Fehlzustandsbaum für System 2	35
Bild B.7 – Veränderter Ereignisbaum	36
Bild B.8 – Ereignisbaum mit „gruppierten Ausfällen“	38
Tabelle 1 – Abkürzungen	8
Tabelle 2 – Formelzeichen	9
Tabelle A.1 – Graphische Elemente	25
Tabelle B.1 – In diesem Anhang verwendete Symbole	28
Tabelle B.2 – Systemüberblick	29
Tabelle B.3 – Risikoreduktionsparameter für die Unfälle aus Bild B.3	32

Einleitung

Diese internationale Norm definiert die grundlegenden Verfahrensprinzipien und -prozeduren der Ereignisbaumanalyse.

Die IEC 60300-3-1 führt die Ereignisbaumanalyse als geeignete Methode für generelle Zuverlässigkeits- als auch Risiko- und Sicherheitsanalysen explizit auf. Eine kurze Darstellung der Ereignisbaumanalyse findet sich auch in der IEC 60300-3-9.

Die grundlegenden Prinzipien dieser Methodik sind seit der Konzeption dieses Verfahrens in den 1960'er Jahren unverändert geblieben. Die Ereignisbaumanalyse wurde erstmals 1975 in der Nuklearindustrie in einer Studie der amerikanischen kerntechnischen Genehmigungsbehörde (U.S. Nuclear Regulatory Commission), dem so genannten WASH-1400-Bericht, erfolgreich angewendet.

Im Laufe der folgenden Jahre gewann die Ereignisbaumanalyse weit verbreitete Akzeptanz als eine ausgereifte Methodik für Zuverlässigkeit- und Risikoanalysen und findet Anwendung in so verschiedenen Industriezweigen wie der Luftfahrtindustrie, Nuklearanlagen, Autoindustrie, chemischen Industrie, Hochseeproduktion von Öl und Gas sowie der Verteidigungsindustrie und der Verkehrstechnik.

Im Gegensatz zu einigen anderen Zuverlässigkeitsverfahren wie dem Markoff-Verfahren fußt die Ereignisbaumanalyse auf relativ elementaren mathematischen Prinzipien. Wie jedoch die IEC 60300-3-1 erwähnt, erfordert die korrekte Durchführung einer Ereignisbaumanalyse ein hohes Expertenwissen bezüglich der Anwendung dieses Verfahrens. Dies ist zum Teil darin begründet, dass die korrekte Behandlung von abhängigen Ereignissen besondere Sorgfalt erfordert. Darüber hinaus kann die enge Verbindung zwischen der Fehlzustandsbaumanalyse (zum Teil auch als Fehlerbaumanalyse bezeichnet) und der qualitativen und quantitativen Analyse von Ereignisbäumen genutzt werden.

Diese Norm hat zum Ziel, die konsolidierten grundlegenden Prinzipien der Ereignisbaumanalyse zu definieren und die gegenwärtige Nutzung des Verfahrens als Hilfsmittel zur Bewertung von Zuverlässigkeits- und Risiko-bezogenen Analysen darzustellen.

1 Anwendungsbereich

Diese internationale Norm definiert die konsolidierten grundlegenden Prinzipien der Ereignisbaumanalyse. Sie gibt Leitlinien sowohl für die Modellierung der Konsequenzen des Startereignisses als auch für die qualitative und quantitative Analyse dieser Konsequenzen im Rahmen von Zuverlässigkeits- und Risiko-bezogenen Maßzahlen.

Folglich behandelt diese internationale Norm folgende Themen bezüglich Ereignisbäumen:

- a) Definition der essentiellen Begriffe und Beschreibung der Symbolbenutzung und Arten der graphischen Darstellungen;
- b) Spezifizierung der Verfahrensschritte für die Aufstellung eines Ereignisbaums;
- c) Ausarbeitung der Annahmen, Einschränkungen und Vorteile des Durchführens der Analyse;
- d) Ermittlung der Beziehungen zu anderen Zuverlässigkeits- und Risiko-bezogenen Verfahren sowie Erläuterung geeigneter Anwendungsgebiete;
- e) Bereitstellung von Leitlinien für die qualitativen und quantitativen Aspekte der Auswertung;
- f) Auflistung praktischer Beispiele.

Diese internationale Norm kann in allen Industriezweigen angewendet werden, in denen Zuverlässigkeits- und Risiko-bezogene Maßzahlen für die Konsequenzen eines Startereignisses bewertet werden müssen.

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):1990, *International Electrotechnical Vocabulary (IEV), Chapter 191: Dependability and quality of service*

IEC 60300-3-1:2003, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability: Guide on methodology*

IEC 60300-3-9:1995, *Dependability Management – Part 3-9: Application guide – Risk assessment of technological systems*

3 Begriffe

Für die Anwendung dieses Dokumentes gelten die Begriffe nach IEC 60050(191). Folgende zusätzliche Begriffe werden in dieser Norm verwendet:

3.1

Knoten

Punkt in der graphischen Darstellung der Ereignisbaumanalyse, durch den zwei oder mehrere mögliche Ergebnisse für den schadensmindernden Faktor dargestellt werden

ANMERKUNG Das Hauptereignis des entsprechenden Fehlzustandsbaums kann direkt mit einem Knoten verbunden werden.

3.2

Gemeinsame Ursache

Ursache für das Auftreten mehrerer Ereignisse

ANMERKUNG Siehe IEC 61025. Dies bezeichnet eine Ursache, die verantwortlich für mehrere Ereignisse ist, die unter Umständen unabhängig sein können, so z. B. natürliche Gefahren, Fehler technischer Einrichtungen, biologische Infektionen oder menschliche Handlungen.

3.3

Ereignis

Auftreten einer Bedingung oder einer Aktion

ANMERKUNG Siehe IEC 61025.

3.4

Überschrift

Auflistung der schadensmindernden Faktoren in der Zeile über der Darstellung des Ereignisbaums

3.5

Startereignis

Ereignis, das den Startpunkt des Ereignisbaums und der Folge von Ereignissen markiert, die zu den verschiedenen möglichen Ergebnissen führen können

3.6

Schadensmindernder Faktor

System, Funktion oder anderweitiger Faktor, der die Konsequenzen des Startereignisses mindert

ANMERKUNG Viele Industriebereiche verwenden spezifische, äquivalente Bezeichnungen, so z. B. Verteidigungslinie, Schutzlinie, Schutzsystem, Sicherheitsbarriere, Sicherungslinie, Risikoreduktionsfaktor, etc.

3.7

Ergebnis

Mögliches Resultat einer Folge von Ereignissen nach Beachtung aller Reaktionen der relevanten schadensmindernden Faktoren, wobei ein Fortführen des Ereignisbaumes nicht weiter erforderlich ist

3.8

Reihenfolge

Kette von Ereignissen, die ausgehend vom Startereignis durch nachfolgende Ereignisse zu einem speziellen Ergebnis führen

ANMERKUNG Siehe IEC 60050(191).

3.9

Hauptereignis

Ergebnis, das durch das Konstruieren des Fehlzustandsbaums untersucht wird

ANMERKUNG Jeweils unter diesem interessierenden Ereignis auf der obersten Ereignisebene wird der entsprechende Fehlerbaum aufgestellt. Siehe IEC 61025.

4 Symbole und Abkürzungen

Die graphische Darstellung eines Ereignisbaumes erfordert eine konsistente Verwendung von Symbolen, Identifikatoren und Bezeichnungen. Da die Beschreibung eines Ereignisbaumes je nach den Präferenzen des Nutzers variiert, findet sich eine Aufstellung der gebräuchlichsten graphischen Darstellungen in Anhang A.

Die folgenden Abkürzungen aus Tabelle 1 werden in dieser Norm verwendet:

Tabelle 1 – Abkürzungen

Abkürzung	
CCA	Analyse der gemeinsamen Ursachen (en: Common Cause Analysis)
ETA	Ereignisbaumanalyse (en: Event Tree Analysis)
FMEA	Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (en: Failure Mode and Effects Analysis)
FTA	Fehlzustandsbaumanalyse (en: Fault Tree Analysis)
LESF	Die Kombination der Zuverlässigkeitstechnik „large event trees (LE)“ verbunden mit „small fault trees (SF)“
LOPA	Analyse der Schutzebenen (en: Layer of Protection Analysis)
SELF	Die Kombination der Zuverlässigkeitstechnik „small event trees (SE)“ verbunden mit „large fault trees (SF)“

Die folgenden Formelzeichen aus Tabelle 2 werden in dieser Norm verwendet:

Tabelle 2 – Formelzeichen

Formelzeichen	
A	Kursive Großbuchstaben bezeichnen den Fall, dass das Ereignis A eingetreten ist.
$\bar{A}$	Kursive Großbuchstaben mit Querbalken bezeichnen den Fall, dass das Ereignis A nicht eingetreten ist.
$O_{I_E, A, B}$	Mit diesem Symbol wird das Ergebnis gekennzeichnet, das eintritt, falls alle im Index aufgelisteten Ereignisse (durch Kommata getrennte kursive Großbuchstaben) eingetreten sind.
$\alpha, \dots, \delta$	Kleingeschriebene griechische Buchstaben bezeichnen spezielle Ergebnisse des Ereignisbaumes.
„+“	Dieses Symbol bezeichnet ein logisches „ODER“.
„*“	Dieses Symbol bezeichnet ein logisches „UND“.
$P(I_E \cdot A \cdot \bar{B} \cdot \bar{C})$	Wahrscheinlichkeit, dass das Ereignis I_E eingetreten ist UND Ereignis A eingetreten ist UND Ereignis B nicht eingetreten ist UND Ereignis C nicht eingetreten ist.
λ_δ	Rate (siehe [16]) des Eintretens des Ergebnisses δ

5 Allgemeine Beschreibung

Die Ereignisbaumanalyse (ETA) ist eine induktive logische Technik, um ein System in Bezug auf Zuverlässigkeit (siehe IEC 60050(191) und Risiko-bezogene Maßzahlen zu modellieren; außerdem können die verschiedenen möglichen Ergebnisse eines gegebenen Startereignisses identifiziert und deren Häufigkeit bewertet werden.

Ausgehend vom Startereignis beschäftigt sich die Ereignisbaumanalyse mit der Frage „Was geschieht falls...“ und stellt in Folge dessen eine Art Baum mit den verschiedenen möglichen Ergebnissen dar. Daher ist es entscheidend, dass eine umfassende Liste der Startereignisse aufgestellt wird; somit kann sichergestellt werden, dass der Ereignisbaum alle wichtigen Ereignisfolgen des betrachteten Systems korrekt darstellt. Mithilfe dieser Vorwärtslogik kann die Ereignisbaumanalyse als Methode bezeichnet werden, die die schadensmindernden Faktoren, die einem Startereignis folgen, darstellt; hierbei können leicht weitere schadensmindernde Faktoren berücksichtigt werden.

Aus qualitativer Sicht erleichtert die Ereignisbaumanalyse die Identifizierung aller möglichen Unfallszenarien – durch die baumähnliche Struktur mit Erfolgs- bzw. Fehlerzweigen – und möglicher Design- bzw. Prozedurschwächen. Der Erfolgszweig modelliert den Zustand, unter dem der schadensmindernde Faktor wie beabsichtigt aktiv ist. Wie bei anderen Zuverlässigkeitstechniken ist folgendes besonders zu beachten: bei der Modellierung von Abhängigkeiten sind die Wahrscheinlichkeiten, die zur Quantifizierung des Ereignisbaumes verwendet werden, durch die Ereignisabfolge bedingt, die vor dem jeweiligen Ereignis eingetreten ist. Abschnitt 9 beschäftigt sich sowohl mit den qualitativen Aspekten der Analyse als auch mit den quantitativen Regeln für die Berechnungen, die für die Abschätzung der (dimensionslosen) Wahrscheinlichkeiten oder Häufigkeiten ($[1/h]$) jedes möglichen Ergebnisses durchgeführt werden. Themen, die die Quantifizierung von Softwarefehlern und die Quantifizierung menschlicher Faktoren betreffen, sind nicht Bestandteil der vorliegenden Norm, da diese von anderen IEC-Publikationen abgedeckt werden, z. B. IEC/PAS 62508 und IEC 62429.

Die Vorteile der Ereignisbaumanalyse als Zuverlässigkeits- und Risiko-bezogene Technik als auch deren Einschränkungen werden in Abschnitt 6 dargelegt. Als ein Beispiel einer Einschränkung sollte der Ausschluss von Modellen für die zeitabhängige Abfolge von Ereignissen erwähnt werden. Diese Einschränkung hatte die

Entwicklung eng verwandter Methoden wie der dynamischen Ereignisbaumanalyse zur Folge, die die Modellierung zeitabhängiger Abfolgen erleichtert. Diese dynamische Ereignisbaumanalyse wird in dieser Norm nicht weiter detailliert, jedoch finden sich Referenzen in den Literaturhinweisen für weitergehende Informationen.

Die Ereignisbaumanalyse ist eng verwandt mit der Fehlzustandsbaumanalyse, indem mit Hilfe des Hauptereignisses des Fehlzustandsbaumes die bedingte Wahrscheinlichkeit für den jeweiligen Knoten des Ereignisbaums geliefert wird. Dies wird in Abschnitt 7 weiter ausgeführt, in dem auch der Zusammenhang zwischen der Ereignisbaumanalyse und anderen Analysetechniken wie der Ursachen- und Folgenanalyse und der Analyse der Schutzebenen (en: Layer of Protection Analysis – LOPA) behandelt wird. Die Ursachen- und Folgenanalyse vereint die Ursachenanalyse und die Folgenanalyse und benutzt somit sowohl den deduktiven als auch den induktiven Ansatz. LOPA wurde als spezielle Adaption der Ereignisbaumanalyse seitens der Prozessindustrie entwickelt.

Da die ersten Schritte und ein wohldurchdachter Ansatz entscheidend für den Erfolg sind, beschreibt Abschnitt 8 das Aufstellen eines Ereignisbaumes, beginnend mit einer präzisen Systemdefinition. Darüber hinaus beschäftigt sich Abschnitt 8 mit den verschiedenen Aspekten des Systems (technisch, betrieblich, menschlich und funktional) sowie mit dem Detailgrad der Analyse. Ebenso ist die Frage von Bedeutung, auf welche Weise die Liste der relevanten Startereignisse aufgestellt werden kann.

Bild 1 stellt die Hauptschritte bei der Durchführung einer Ereignisbaumanalyse dar. Obwohl der Prozess auf den ersten Blick geradlinig erscheint, so muss der Analyst stets bedenken, dass die Konstruktion eines Ereignisbaumes in besonderem Maße ein iterativer Prozess ist.

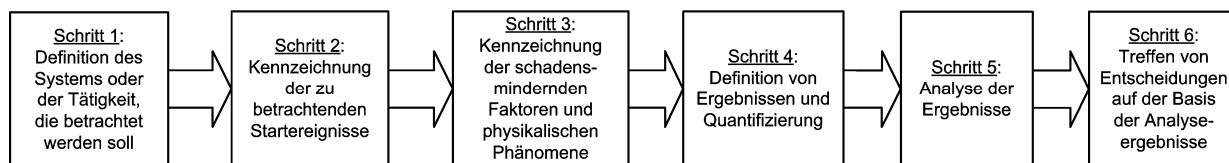


Bild 1 – Prozess des Aufstellens eines Ereignisbaumes

In Abschnitt 10 wird die für die Analyse und deren Resultate notwendige Dokumentation kurz dargelegt.

Anhang A stellt die gebräuchlichsten graphischen Darstellungen eines Ereignisbaumes zusammen. Anhang B stellt Beispiele zur Verfügung, die die Anwendung der Ereignisbaumanalyse in zahlreichen Industriefeldern verdeutlicht und gibt Hilfestellung bei der Durchführung von Ereignisbaumanalysen. Anhang C enthält Literaturhinweise.

6 Vorteile und Einschränkungen einer Ereignisbaumanalyse

6.1 Vorteile

Eine Ereignisbaumanalyse weist die folgenden Vorteile auf:

- sie ist auf alle Arten technischer Systeme anwendbar;
- sie ermöglicht die Visualisierung der Ereignisketten, die aus einem einleitenden Ereignis folgen;
- sie ermöglicht die Einschätzung von mehrfachen gleichzeitigen Systemstörungen (Zustände, die dazu führen, dass eine erforderliche Funktion nicht ausgeführt wird, z. B. Defekt eines Überwachungssystems) oder von Ausfällen (Beendigung der Fähigkeit, eine erforderliche Funktion auszuführen, z. B. das Ereignis eines Ventils, das offen bleibt), sowie andere abhängige Ereignisse;
- sie ist sowohl bei Ausfällen als auch bei erfolgreichen Funktionen anwendbar;
- sie identifiziert Endereignisse, die auf andere Weise nicht erkannt werden;
- sie identifiziert mögliche Einzelausfälle, Bereiche von Systemschwachstellen und mit geringen Mitteln umsetzbare Gegenmaßnahmen. Dies ermöglicht einen optimierten Einsatz von Ressourcen und eine verbesserte Kontrolle des Risikos durch verbesserte Verfahren und Sicherheitsfunktionen;

- g) sie erlaubt die Identifizierung und Nachweisbarkeit von Fehlerausbreitungspfaden eines Systems;
- h) sie ermöglicht die Aufspaltung großer und komplexer Systeme in kleinere handlichere Teile durch Clusterbildung von kleineren Funktionseinheiten oder Subsystemen.

Die Stärke der Ereignisbaumanalyse – verglichen mit vielen anderen Zuverlässigkeits- und Risiko-bezogenen Verfahren – ist die Fähigkeit, die Reihenfolge und die Wechselwirkung der verschiedenen schadensmindernden Faktoren zu modellieren, die nach dem Eintreten des Startereignisses folgen. So werden das System und seine Wechselwirkungen mit allen schadensmindernden Faktoren in einem Schadensfall-Szenario für den Analytiker im Hinblick auf weitere Risikoauswertungen erkennbar.

6.2 Einschränkungen

Eine Ereignisbaumanalyse beinhaltet die folgenden Einschränkungen:

- a) die Startereignisse werden nicht durch die Analyse selbst aufgedeckt; es ist eher die analytische Aufgabe der Personen, die bei der Methode mit einbezogen werden, eine komplette Liste der Startereignisse aufzustellen;
- b) es ist die Aufgabe der Personen, die in den Prozess einbezogen wurden, eine komplette Liste der möglichen Betriebsszenarios aufzustellen;
- c) subtile Systemabhängigkeiten könnten übersehen werden und zu übermäßig optimistischen Schätzungen der Zuverlässigkeit und Risiko-bezogenen Maßnahmen führen;
- d) wenn ein System zu lange Zeit in einem bestimmten Zustand ist, kann es zu einem Ausfallzustand kommen, der schwierig in einem Ereignisbaum zu modellieren ist;
- e) die Methode benötigt praktische Erfahrungen des Analytikers und vorausgehende Systemuntersuchungen, z. B. um die bedingten Wahrscheinlichkeiten und die abhängigen Ereignisse korrekt zu behandeln;
- f) die Ereignisbaumanalyse ist nicht für die direkte Behandlung abhängiger Ausfälle, insbesondere gemeinsam verursachter Ausfälle, in der quantitativen Analyse geeignet. Dieser Aspekt sollte durch eine Fehlzustandsbaumanalyse abgedeckt werden, die dann mit der Ereignisbaumanalyse verknüpft werden kann;
- g) obwohl mehrfache Reihenfolgen von Ereignissen, die zum Systemfehler führen, identifiziert werden können, können die Schadensumfänge, die mit bestimmten Pfaden verbunden sind, möglicherweise nicht ohne zusätzliche Analyse unterscheidbar sein; dieser Notwendigkeit muss man sich bewusst sein.

7 Beziehungen zu anderen Analyseverfahren

7.1 Kombination von Ereignisbaum- und Fehlzustandsbaumanalyse

In der Praxis wird die Ereignisbaumanalyse nicht als allein stehende Analyse durchgeführt; vielmehr entwickelt sie ihren größten Nutzen, wenn sie zusammen mit einer Fehlzustandsbaumanalyse eingesetzt wird, siehe [13]. In diesem Fall können zum Beispiel Fehler mit gemeinsamer Ursache berücksichtigt werden, womit die Kombination von Ereignisbaum- und Fehlzustandsbaumanalyse viele der Unzulänglichkeiten der Ereignisbaumanalyse überwindet. Somit schafft die Kombination von Ereignisbaum- und Fehlzustandsbaumanalyse einen sinnvollen Ausgleich und wird somit zu einem wirkungsvollen Analyseverfahren für Zuverlässigkeits- und Risikoanalysen.

Diese Verbindung von Ereignisbaum- und Fehlzustandsbaumanalyse ist sehr verbreitet; so kann z. B. die Fehlzustandsbaumanalyse für die Berechnung der Eintrittsrates des Startereignisses einer Ereignisbaumanalyse eingesetzt werden. Zu vermerken ist ebenfalls, dass die bedingten Wahrscheinlichkeiten der Ereignisse in einer Reihenfolge von Ereignissen häufig mit einer Fehlzustandsbaumanalyse berechnet werden.

Grundsätzlich kann von jedem Startereignis aus eine Ereignisbaumanalyse erfolgen. In manchen Fällen kann dies aus folgenden Gründen jedoch nicht zweckmäßig sein:

- a) der resultierende Baum würde sehr komplex werden;
- b) in manchen Fällen ist die Analyse kausaler Beziehungen leichter zu vollziehen als die strikte Reihenfolge von Ereignissen;

- c) oft sind getrennte Arbeitsgruppen mit der betrieblichen (z. B. Ablaufregeln) und technischen Analyse betraut. Ausgehend vom Startereignis ist die Schnittstelle zwischen betrieblichem und technischem Bereich zu Beginn der Analyse nicht immer eindeutig.

Aufgrund des Punktes c) werden für praktische Abläufe zuerst die möglichen Ereignisse an der Schnittstelle zwischen betrieblichem und technischem Bereich definiert. Speziell in Sicherheitsanwendungen ist dies das Standardvorgehen, zumal normalerweise Einzelfehler per Design ausgeschlossen werden, z. B. durch fehler-sicheres Design; in diesen Fällen wird somit sichergestellt, dass normalerweise ein Ereignisbaum nicht direkt (ohne weitere schadensmindernde Faktoren) zu schwerwiegenden Ergebnissen durch einen Einzelfehler führt.

Es kann zwischen zwei Ansätzen gewählt werden, um Ereignisbäume und Fehlzustandsbäume zu verbinden. Ein Ansatz ist der so genannte LESF (Large ET – Small FT) Ansatz. Für den Fall, dass der Ereignisbaum unverhältnismäßig groß werden würde, kann der SELF (Small ET – Large FT) Ansatz verwendet werden.

Beim LESF Ansatz tauchen alle Systemzustände, die das untersuchte System unterstützen (Hilfssystem), explizit in den Ereignisbäumen auf. Die Hauptereignisse der Fehlzustandsbäume unterliegen Randbedingungen, die davon ausgehen, dass das Hilfssystem in einem der Ereignisreihenfolge entsprechenden Zustand ist. Für jeden Satz an Randbedingungen des jeweiligen Systems müssen getrennte Fehlzustandsbäume angewendet werden. Diese getrennten Fehlzustandsbäume können aus einem einzelnen Fehlzustandsbaum gewonnen werden, der das Hilfssystem umfasst und bedingt ist durch das mit dieser Ereignisreihenfolge verbundene Hilfssystem – bevor es mit einer speziellen Reihenfolge verknüpft wird. Dieser Ansatz liefert LESF, der explizit die bestehenden Abhängigkeiten darstellt. Da LESF mit kleineren Fehlzustandsbäumen auftritt, stellen diese Ereignisbäume geringere Anforderungen an die Rechnerkapazitäten und Entwicklungsstand der Rechnerprogramme. Die Komplexität dieser Fehlzustandsbäume nimmt jedoch mit der Anzahl der Hilfssysteme und der Zustände der im Baum deutlich dargestellten Hilfssysteme rasant zu. Des Weiteren ist der Quantifizierungsprozess mühsam und unterliegt der Gefahr von Auslassungen, da Rechnerprogramme für die automatische Quantifizierung noch nicht ausreichend vorhanden sind. Eine weitere Überlegung ist, dass der LESF-Ansatz nicht ausdrücklich festlegt, welche spezifischen Kombinationen von Fehlern der Hilfssysteme zu einem Systemversagen führen – auch als Versagen des Hauptsystems bezeichnet. Ein vereinfachtes Beispiel solch eines großen Ereignisbaums ist in Anhang B.1 angeführt; siehe [26] für weitere Details.

Beim SELF-Ansatz wird zuerst ein Ereignisbaum erstellt, der die Funktionen als Überschriften enthält. Anschließend wird dieser Ereignisbaum zu Ereignisbäumen erweitert, die den Zustand der Hauptsysteme als Überschriften enthalten. Die Fehlzustandsbäume der Hauptsysteme werden bis auf geeignete Grenzen zu den Hilfssystemen entwickelt. Die Fehlzustandsbäume der Hilfssysteme können getrennt aufgestellt werden und zu einem späteren Zeitpunkt in die Modelle der Hauptsysteme integriert werden. Mit diesem Ansatz werden Ereignisbäume erstellt, die knapp und präzise sind und die einen umfassenden Blick auf die Unfallreihenfolge ermöglichen. Zudem können die kleinen Ereignisbäume leichter mit den vorhandenen Rechnerprogrammen modelliert werden. Jedoch sind Abhängigkeiten und die entsprechende Bedeutung der Hilfssysteme nicht deutlich dargestellt. Ein theoretisches Beispiel eines solchen kleinen Ereignisbaums ist in Anhang B.3 angeführt; siehe [4] für weitere Details.

Die Kombination von Ereignisbaum- und Fehlzustandsbaumanalyse wird mitunter als Ursachen- und Folgenanalyse bezeichnet; siehe [29].

7.2 Analyse der Schutzebenen (Layer of Protection Analysis – LOPA)

Die Analyse der Schutzebenen (LOPA) ist eine speziell standardisierte Form der Ereignisbaumanalyse, die als vereinfachte Form für eine Risikoanalyse für eine spezielle Anwendung genutzt wird. LOPA ist als Arbeitsblatt ähnlich der FMEA aufgebaut: die Startereignisse sind in Reihen angeordnet und die verschiedenen Schutzebenen, die die standardisierten schadensmindernden Faktoren darstellen, in Spalten. Daher kann jede Ereignisreihenfolge einer LOPA auch als Ereignisbaumanalyse behandelt werden. Zum Zwecke einer Risikoanalyse werden auch Schwere- oder Schadensmaßzahlen in das Arbeitsblatt integriert.

Aus diesem Grund kann LOPA als eine Ereignisbaumanalyse mit einer eingeschränkten Menge an schadensmindernden Faktoren angesehen werden, die dem jeweiligen Anwendungsumfeld angepasst sind. LOPA wird vorwiegend in der Prozessindustrie angewendet. Weitere Details über LOPA finden sich in [1] und [5].

7.3 Verbindung mit anderen Verfahren

Die Ereignisbaumanalyse kann mit jedem anderen Verfahren kombiniert werden, das die Ableitung einer Wahrscheinlichkeit für Erfolg oder Ausfall eines entsprechenden schadensmindernden Faktors unterstützt. Beispiele hierfür ist das Markoff-Verfahren oder das Zuverlässigkeitsblockdiagramm (Reliability Block Diagram – RBD), siehe [14]. In diesen Fällen dienen die anderen Verfahren jedoch ausschließlich als Ergänzung zur Ereignisbaumanalyse.

Im Falle nichttrivialer und zeitlicher Abhängigkeiten des Systemverhaltens (siehe 9.3.2) bietet sich das Markoff-Verfahren an – unter Beachtung dessen anderer spezifischer Beschränkungen. Weitere Details finden sich in [15].

Ein weiteres eng verwandtes Verfahren zur Analyse der Zuverlässigkeit ist das Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA), siehe [12], die eine formale, systematische Prozedur zur Systemanalyse ist, um die möglichen Fehlermodi, deren Ursachen und Auswirkungen auf das Systemverhalten zu identifizieren. Allgemein erleichtert es die FMEA, die Schwere möglicher Ausfälle zu ermitteln und festzustellen, ob das Systemdesign schadensmindernde Faktoren beinhaltet, die die Fehlerwahrscheinlichkeit reduzieren. Dies kann als erster Schritt bei der Erstellung eines Ereignisbaumes dienen, indem kritische Fehler eines Systems als mögliche Startereignisse identifiziert werden.

Das Markoff-Verfahren, Zuverlässigkeitsblockdiagramm und FMEA sind in den IEC-Veröffentlichungen [15], [12] und [14] genormt.

8 Erstellen von Ereignisbäumen

8.1 Allgemeines

Die Ereignisse, welche die Ereignisreihenfolgen darstellen, sind üblicherweise wie folgt charakterisiert:

- a) Funktionen: Die Erfüllung (oder die Nichterfüllung) von Funktionen als schadensmindernde Faktoren;
- b) Systeme: Das Eingreifen (oder Nichteingreifen) der Systeme als schadensmindernde Faktoren, die für eine Schadensminderung bei einem Schadensfall sorgen sollen;
- c) Phänomene: Das Eintreten oder Nichteintreten physikalischer Phänomene.

Üblicherweise werden die Funktionen, die als Folge eines einleitenden Ereignisses erforderlich sind, zuerst identifiziert und anschließend die Systeme (schadensmindernde Faktoren), die diese Funktionen wahrnehmen können: Die physikalischen Phänomene beschreiben die Entwicklung, die innerhalb und außerhalb des betrachteten Systems stattfinden kann (z. B. Druck- und Temperaturtransienten, Brand, Containment-dispersionen).

Der Anwendungsbereich und der Zweck der Ereignisbaumanalyse sollten eindeutig definiert sein, bevor die ausführlichen Schritte, die in 8.2 beschrieben sind, begonnen werden.

8.2 Schritte in der Ereignisbaumanalyse

Das Verfahren für die Erstellung einer Ereignisbaumanalyse (siehe Bild 1) besteht aus den folgenden sechs Schritten:

Schritt 1: Definition des Systems oder der Tätigkeit, die betrachtet werden sollen (siehe 8.2.1):

Eindeutige Spezifikation und Definition der Grenzen des Systems oder der Tätigkeit, für die die Ereignisbaumanalysen durchgeführt werden sollen;

Schritt 2: Kennzeichnung der zu betrachtenden Startereignisse (siehe 8.2.2):

Durchführung eines Screenings, um die zu betrachtenden Ereignisse oder Kategorien von Ereignissen zu identifizieren, die in der Analyse behandelt werden sollen. Kategorien umfassen beispielsweise Zusammenstöße, Brände, Explosionen, Freisetzung giftiger Stoffe, etc.;

Schritt 3: Kennzeichnung der schadensmindernden Faktoren und physikalischen Phänomene (siehe 8.2.3):

Identifizierung der verschiedenen schadensmindernden Faktoren, die die Weiterentwicklung des einleitenden Ereignisses im Hinblick auf seine Ergebnisse beeinflussen können. Diese schadensmindernden Faktoren umfassen sowohl technische Systeme als auch menschliche Handlungen. Außerdem sind die physikalischen Phänomene oder anderweitige Ereignisse, wie Zündung oder meteorologische Bedingungen, zu identifizieren, die das Startereignis beeinflussen. Der Ereignisbaum wird so erstellt, dass alle schadensmindernden Faktoren und physikalischen Phänomene berücksichtigt werden (siehe 7.1);

Schritt 4: Definition von Ergebnissen und Quantifizierung (siehe 8.2.4):

Für jedes Startereignis sind die verschiedenen Ergebnisse (z. B. Schadens-Szenarien) festzulegen, die auftreten können; zudem ist eine aktuelle quantitative Analyse auf der Grundlage des aufgestellten Ereignisbaumes durchzuführen;

Schritt 5: Analyse der Ergebnisse (siehe 8.2.5):

Die verschiedenen Ergebnisse werden dann im Hinblick auf ihre Auswirkungen und ihren Einfluss auf die Analyseergebnisse analysiert;

Schritt 6: Treffen von Entscheidungen auf der Basis der Analyseergebnisse (siehe 8.2.6):

Die qualitativen und quantitativen Ergebnisse der Analyse werden dann in notwendige Maßnahmen umgesetzt.

8.2.1 Definition des Systems oder der Tätigkeit, die betrachtet werden sollen

Eine Ereignisbaumanalyse konzentriert sich auf Wege, bei denen sich ein Startereignis aufgrund von Ausfällen verschiedener schadensmindernder Faktoren bis zu Schadensfällen weiterentwickeln kann. Eine sorgfältige Identifizierung und eine Untersuchung der schadensmindernden Faktoren ist daher ein wichtiger erster Schritt in der Bewertung der Wirksamkeit eines schadensmindernden Faktors.

In der Praxis arbeiten Systeme kaum isoliert. Die meisten werden an andere Systeme angeschlossen oder stehen in Wechselwirkung mit ihnen. Durch eine klare Festlegung der Grenzen, insbesondere zu Hilfsystemen wie elektrischer Energie und Druckluft, können Analytiker vermeiden, dass Schlüsselemente eines Systems an Schnittstellen übersehen werden oder dass ein System dadurch nicht entsprechend berücksichtigt wird, dass andere Einrichtungen mit in die Analyse einbezogen werden.

Konzeptionell können Ereignisbaumanalysen alle Ereignisse und Bedingungen umfassen, die zu Startereignissen beitragen können oder die gewisse Schutzniveaus gegen entsprechende Schadensfälle bilden können. Jedoch ist es nicht praktisch, alle möglichen Beiträge in die Studie einzuschließen. Viele Analysen definieren analytische Grenzen, die

- a) den Tiefgang der Analysenergebnisse begrenzen (z. B. kann der Analytiker entscheiden, nicht alle elektrischen Verteilersystemprobleme im Detail zu analysieren, wenn ein Navigationssystem untersucht wird);
- b) ausdrücklich bestimmte Arten von Ereignissen oder Bedingungen von der Analyse ausschließen, wie z. B. Sabotage.

Der Anfangszustand eines Systems, einschließlich der entsprechenden Einrichtungen, die als nicht in Betrieb befindlich angenommen werden, beeinflusst die Kombinationen der Ereignisse, die notwendig sind, um daraus folgende Probleme zu produzieren. Wenn z. B. eine Schutzverriegelung routinemäßig außer Betrieb genommen wird, muss der Ereignisbaum entsprechend angepasst werden, um die geänderten Szenarien im Hinblick auf ein möglicherweise erhöhtes Risiko zu betrachten.

8.2.2 Kennzeichnung der zu betrachtenden Startereignisse

Dieser Schritt umfasst üblicherweise die Anwendung umfassender Verfahren zur Identifizierung von Gefährdungen wie „Was geschieht, falls...“, vorläufige Auswertungen oder vorläufige Gefährdungsanalysen, um systematisch alle Aktivitäten innerhalb des Anwendungsbereichs der entsprechenden Studie auszuwerten,

z. B. die Betrachtung der Betriebserfahrung im Bereich des jeweiligen Industriebereichs. Dieser Schritt hilft, die Gefährdungen und die möglichen Startereignisse zu identifizieren, die sich aus diesen Gefährdungen ergeben. Diese Identifizierungsmethoden betrachten umfassend den gesamten Betrieb innerhalb des Anwendungsbereichs der Studie und versuchen, die vollständige Breite möglicher einleitender Ereignisse und die Breite der Resultate zu identifizieren, die mit solchen Ereignissen verbunden sind. Das Ergebnis dieser Identifizierungsprozesse ist üblicherweise eine umfangreiche Liste der möglichen Ereignisse und der erwarteten Auswirkungen.

Es sollte dann das allgemeine Ziel sein, das gesamte Spektrum von Ereignissen, die innerhalb des Anwendungsbereichs der Analyse auftreten können, zu identifizieren. Nachdem dies durchgeführt wurde, wenden die Analytiker Screening-Kriterien an, um die wichtigsten Ereignisse zu identifizieren, die mit den Ereignisbäumen analysiert werden. Grundsätzlich gibt es zwei Optionen für das Aussortieren von Startereignissen, nämlich den Ausschluss aufgrund eher unwahrscheinlicher physikalischer Eigenschaften (z. B. spezifische Werte für Druck, Temperatur oder für Brandlasten werden nicht überschritten) oder wegen der niedrigen Frequenzen für die einleitenden Ereignisse, die üblicherweise in einer konservativen Weise abgeschätzt werden. Dieser Schritt hilft, jene Ereignisse zu identifizieren, die weiter analysiert werden müssen, um die komplizierten Wechselwirkungen der Systeme zu verstehen. Im Rahmen dieser Analyse muss man die Möglichkeit jeder möglichen Wechselwirkung zwischen den einleitenden Ereignissen und den schadensmindernden Faktoren überprüfen, z. B. ob die Umwelt, beeinträchtigt durch das Startereignis, z. B. Verlust der gesamten Energieversorgung nach einem Erdbeben, umgekehrt die Wirksamkeit der schadensmindernden Faktoren nachteilig beeinflussen kann.

Nachdem die Anfangsliste von Ereignissen festgelegt und die Aussortierung erfolgt ist, umfasst die resultierende Liste der Startereignisse diejenigen, die mit Ereignisbäumen analysiert werden. Dies sind die Ereignisse, die von erfahrenen Experten als komplex genug identifiziert werden, die eine zusätzliche Analyse der Wechselwirkungen verschiedener Systeme und Personalhandlungen erfordern. Diese führen zu verschiedenen Ergebnissen, ausgehend von einem Startereignis.

Wenn es viele Ereignisse gibt, die mit den Ereignisbäumen analysiert werden, sollten die Startereignisse in verschiedene Kategorien, wie Zusammenstöße, Brände, Explosionen, Freisetzung giftiger Stoffe, etc. gruppiert werden. In einigen Fällen ist eine solche Kategorisierung von Ereignissen möglicherweise nicht anwendbar. Wenn z. B. das Ziel der Studie ist, nur die Ergebnisse zu identifizieren, die mit Bränden verbunden sind, dann sollte die Screening-Analyse, die im vorhergehenden Schritt durchgeführt wird, alle Ereignisse aussortiert haben, die nicht mit Bränden zusammenhängen, so dass dieser letzte Schritt der Kategorisierung der Ereignisse nicht notwendig ist.

Startereignisse, die in derselben Kategorie gruppiert werden, erfordern üblicherweise das Eingreifen der gleichen schadensmindernden Faktoren und führen zu ähnlichen Ergebnissen.

8.2.3 Kennzeichnung der schadensmindernden Faktoren und physikalischen Phänomene

Sobald ein Startereignis definiert ist, müssen alle schadensmindernden Faktoren, die angefordert werden, um die Ergebnisse oder die möglichen Schadensfälle abzuschwächen, entsprechend ihrer Zeit des Eingreifens definiert werden und organisiert werden. Sie bestehen aus technischen Komponenten wie Meldeeinrichtungen, Verriegelungen, automatischen Ventilen und aus administrativen und personellen Systemen wie Feuerwehr, Notfallschutz und menschliche Wahrnehmung durch Sichtprüfung, Tastsinn, Ton oder Geruch.

Diese Funktionen werden in Form von Überschriften im Funktionsergebnisbaum strukturiert. Für jede Funktion muss ein Satz möglicher Erfolge und Ausfälle identifiziert und quantifiziert werden. Jeder Satz von Erfolgen beziehungsweise Ausfällen, verknüpft mit einem schadensmindernden Faktor, führt zu einer Verzweigung des Ereignisbaums, die nicht notwendigerweise auf einen Knoten mit zwei Verzweigungen eingeschränkt ist.

Die physikalischen Phänomene, manchmal als phänomenologische Ereignisse bezeichnet, können auch das Ergebnis eines Startereignisses beeinflussen. Wenn z. B. eine brennbare Flüssigkeit freigesetzt wird, kann es technische Sicherheitseinrichtungen geben, die das Leck isolieren. Wenn jedoch das Leck nicht isoliert ist, wird das endgültige Ergebnis der Freisetzung durch verschiedene physikalische Reaktionen, wie sofortige Zündung, verzögerte Zündung oder Dispersionseigenschaften beeinflusst. Diese physikalische Reaktion wird auch als Knoten in den Ereignisbäumen modelliert.

In einer Systemanalyse, die mehrfache Ereignisbäume für mehrfache Startereignisse erfordert, kann der Aufwand des Zeichnens dieser Ereignisbäume vereinfacht werden, indem man sie entsprechend den schadensmindernden Faktoren kategorisiert. Dieses erlaubt, dass die gleiche Ereignisbaumlogik (d. h. schadensmindernden Faktoren mit dem gleichen Ausfall oder Erfolg) für verschiedene zu betrachtenden Ereignisse wiederholt wird. Oder, wenn die schadensmindernden Faktoren in einer identischen Weise auf verschiedene Ereignisse reagieren, können die Frequenzen der einzelnen Ereignisse normalerweise summiert werden, um zu einer repräsentativen Frequenz für alle Ereignisse dieses Typs zu kommen. Weitere Einzelheiten über die quantitative Analyse sind in 9.3 beschrieben.

8.2.4 Definition von Ergebnissen und Quantifizierung

Wie oben ausgeführt, ist eine der Stärken des Ereignisbaumanalyseverfahrens seine Fähigkeit, die zeitlichen Aspekte und die Wechselwirkung der verschiedenen Systeme zu modellieren, die auf das Startereignis reagieren. Um diese Wechselwirkungen adäquat zu berücksichtigen, muss der Analytiker

- a) die logische Weiterentwicklung des Startereignisses durch die verschiedenen schadensmindernden Faktoren zu möglichen Ergebnissen/Schadensfall-Szenarien festlegen;
- b) die Abhängigkeiten unter den schadensmindernden Faktoren feststellen;
- c) das bedingte Ansprechverhalten eines Systems, unter der Voraussetzung bestimmen, dass die vorherigen Systeme angesprochen haben;
- d) den Ereignisbaum aufstellen, um das oben Genannte einzubeziehen.

Sicher führen nicht alle Startereignisse (z. B. Systemfehler) zu katastrophalen Ergebnissen. Entsprechend wird nicht jeder schadensmindernde Faktor oder jede Verriegelung angefordert, auf jedes auftretende Ereignis zu reagieren. Es gibt eine logische Weiterentwicklung zu einer Unfallreihenfolge von dem Zeitpunkt an, wenn das einleitende Ereignis auftritt. Während die Unfallreihenfolge voranschreitet und schwerwiegender wird, reagieren Systeme auf unterschiedliche Weisen. Das Verstehen der Weiterentwicklung und der zeitlichen Regelung des Systems und des physikalischen Ansprechverhaltens ist wesentlich für das Aufstellen einer korrekten Logik des Ereignisbaums. Wenn z. B. ein Brand durch Selbstentzündung in einem Abfallbehälter entsteht, würde die erste Reaktion sein, dass das Personal den Brand mit Handlöschern löscht, wenn Personal anwesend wäre und wenn Löscher vorhanden wären. Das vollständige Brandschutzsystem und das Ansprechverhalten der Feuerwehr würden nicht angefordert, es sei denn der Schweregrad des Unfalles erhöht sich.

Die meisten Systeme sind an andere Maschinen und Prozesse angeschlossen oder stehen in Wechselwirkung mit ihnen. Diese Wechselwirkungen oder Abhängigkeiten beeinflussen (vermindern) das Schutzniveau, das durch redundante Systeme bereit gestellt wird, die bestimmte Einrichtungen gemeinsam nutzen. Im Beispiel eines Öltankers mit redundanten Lenk- und Antriebssystemen sind die Ausfälle jedes Systems möglicherweise nicht unabhängig voneinander, wenn die Lenksysteme ein gemeinsames Hydraulikflüssigkeitsversorgungssystem teilen.

Ereignisbäume beziehen bedingte Wahrscheinlichkeiten mit ein. Das heißt, die Wahrscheinlichkeit eines spezifischen Ansprechverhaltens (z. B. Erfolg oder Ausfall) für einen schadensmindernden Faktor ist abhängig von dem spezifischen Ansprechverhalten der schadensmindernden Faktoren, die diesem vorausgehen.

Der empfohlene Ereignisbaum-Aufbauprozess besteht aus den folgenden Schritten:

- a) Setzen des Startereignisses zuerst auf die linke Seite des Baums;
- b) Setzen der schadensmindernden Faktoren und der physikalischen Phänomene quer oberhalb des Baums, z. B. in der chronologischen Reihenfolge, in der sie die Unfallweiterentwicklung beeinflussen;
- c) Festlegung von Erfolg (normalerweise angezeigt im oberen Zweig der Verzweigung) und Ausfall (im unteren Zweig der Verzweigung) für jeden schadensmindernden Faktor an jedem Zweig; betrachtet werden müssen zudem
 - i) einige Knoten können mehr als zwei Ergebnisse haben und werden mit der passenden Zahl von Zweigen dargestellt;
 - ii) einige Knoten haben nur ein Ergebnis, das heißt, es gibt es eine direkte Linie zu dem schadensmindernden Faktor. Dies tritt auf, wenn die bedingte Wahrscheinlichkeit 1,0 ist; der schadensmindernde Faktor beeinflusst das Ergebnis nicht aufgrund eines vorhergehenden Erfolgs oder Ausfalls eines anderen schadensmindernden Faktors.

Diese Schritte werden ausführlicher in Anhang A in allgemeiner Form veranschaulicht und spezifischer in den Bildern B.1 und B.3 mit Beispielen aus den Bereichen der Bahnsysteme und der Kraftwerke ausgeführt.

8.2.5 Analyse der Ergebnisse

Die Ergebnisse der Ereignisbaumanalyse werden durch den Endpunkt jedes Ereignisbaumzweiges bestimmt. Jedes Ergebnis kann sowohl qualitativ als auch quantitativ ausgewertet werden. Im ersten Fall identifiziert das Ergebnis die verschiedenen Ereignisreihenfolgen im Hinblick auf das Eintreten des untersuchten einleitenden Ereignisses. Die quantitative Auswertung stellt bessere Einblicke hinsichtlich der relativen Bedeutung der schadensmindernden Faktoren zur Verfügung, weil das Ergebnis in diesem Fall durch eine Frequenz dargestellt wird. Für die Quantifizierung der Ereignisbaumanalyse sind ausreichende und genügend zuverlässige Daten für das Eintreten des Ereignisses erforderlich.

Es ist manchmal vorteilhaft, die möglichen Ergebnisse in verschiedene Kategorien entsprechend des Schadenstyps (Verlust an Menschenleben, Sachschaden, Umweltschädigung oder Ausmaß eines Schadens) aufzuspalten. Die Zahl der Ergebnisse des Ereignisbaums wird durch Definition der Arten der zu analysierenden Ergebnisse festgelegt wie z. B.

- a) Ausfall- oder Schadenzustände des Systems,
- b) Zerstörung des Systems,
- c) Schweregrad der Umweltauswirkung oder
- d) Verlust von Menschenleben.

Für praktische Auswertung der mehrfachen Ergebnisse, die untersucht werden sollen, ist es nützlich, die vergleichbaren Ergebnisse einzustufen und zu gruppieren, um die Ergebnisse zu vereinfachen.

8.2.6 Treffen von Entscheidungen auf der Basis der Analyseergebnisse

Die Ergebnisse der Ereignisbaumanalyse können verwendet werden, um eine Basis für das Treffen von Entscheidungen zu formulieren, die zur Vorauswahl der unter Sicherheitsgesichtspunkten optimalen Lösungen zur Verbesserung der Zuverlässigkeit beitragen und die das Risiko auf einer begründeten technischen und organisatorischen Basis verringern. Die Korrekturmaßnahmen können Änderungen am technischen System, an betrieblichen Abläufen, Instandhaltungsverfahren, etc. umfassen.

Insbesondere basieren die Entscheidungen auf dem Nutzen der durchgeführten Analyse, der wie folgt zusammengefasst werden kann:

- a) Fähigkeit, Risikotoleranz oder -akzeptanz zu bewerten: Sind die Ergebnisse, die den zugehörigen Schaden aufgrund der relevanten Risikoannehmbarkeitskriterien berücksichtigen, akzeptabel?
- b) Mögliche Verbesserungen: Identifiziert werden Bereiche von Risiko-reduzierenden Faktoren und relevanten Änderungen an der untersuchten Systemarchitektur, um die Annehmbarkeitskriterien zu erfüllen.
- c) Empfehlungen für Verbesserungen: Entwickelt werden spezifische Vorschläge für die Verbesserung des zukünftigen Betriebsverhaltens, einschließlich einer der folgenden Maßnahmen:
 - i) Änderungen an den Einrichtungen
 - ii) Verfahrensänderungen
 - iii) Änderungen auf administrativer Ebene wie geplante Wartungsaufgaben, Personaltraining, etc.
- d) Rechtfertigung für die Zuteilung von Geldmitteln: Abschätzung, wie die Implementierung kostenintensiver oder umstrittener Verbesserungsvorschläge das Betriebsverhalten beeinflusst.

Da das analysierte System im Laufe seiner Lebenszeit Änderungen unterworfen sein kann, sollte die Ereignisbaumanalyse während der Lebenszeit des Systems aktuell gehalten werden, um sie für den Entscheidungsprozess nutzen zu können. Dieser Prozess der regelmäßigen periodischen Aktualisierung existiert bereits in einigen Industrien und wird als „lebende Ereignisbaumanalyse“ bezeichnet.

9 Auswertung

9.1 Einleitende Bemerkungen

Bevor mit einer quantitativen Analyse der Häufigkeit oder Wahrscheinlichkeit von Ergebnissen der verschiedenen Ereignisreihenfolgen begonnen werden kann, müssen die qualitativen Gesichtspunkte des Ereignisbaummodells sorgfältig analysiert werden. Darunter fallen die Abhängigkeiten der Ereignisse einschließlich des Startereignisses und der Hauptereignisse als auch die Zwischen- oder Basisereignisse der verbundenen Fehlzustandsbäume.

Um die Schilderung der grundlegenden Prinzipien der Auswertung zu erleichtern, wird in Bild 2 die grundlegende graphische Darstellung eines Ereignisbaumes vorgestellt.

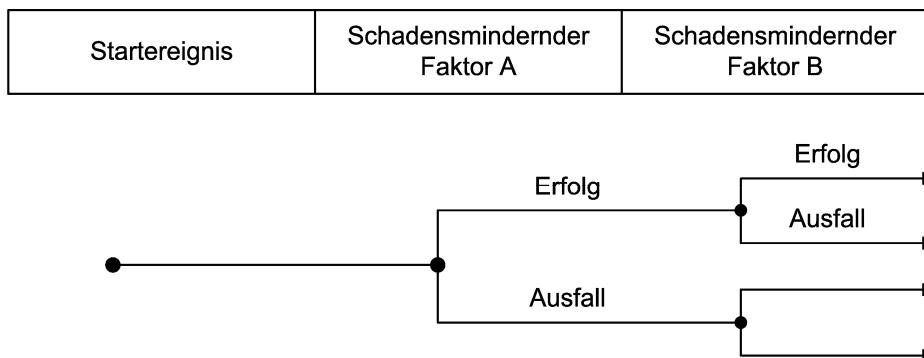


Bild 2 – Grundlegende graphische Darstellung eines Ereignisbaums

9.2 Qualitative Analyse – Handhabung von Abhängigkeiten

9.2.1 Allgemeines

Die Zielsetzung der qualitativen Analyse kann wie folgt zusammengefasst werden:

- Verständnisgewinn über die Faktoren, die die Abhängigkeit zwischen den Funktionen oder den Komponenten des Systems bestimmen;
- Aufdeckung der wichtigen möglichen und abhängigen Fehlerereignisse;
- Erleichterung für die korrekte quantitative Analyse des Ereignisbaums und Herstellung einer einwandfreien Verbindung mit den Fehlzustandsbäumen.

Die qualitative Analyse und speziell die Abhängigkeitsanalyse wird in einem separaten Abschnitt behandelt. Dies geschieht, um die besondere Bedeutung des Themas hervorzuheben, nicht hingegen, um zu zeigen, dass sie getrennt von der Ereignisreihenfolgen- oder Systemanalyse durchgeführt werden sollte.

Es gibt zwei bedeutende Arten von Abhängigkeiten, nämlich

- Funktionale Abhängigkeiten (siehe 9.2.2) und
- Strukturelle oder physikalische Abhängigkeiten (siehe 9.2.3).

So können z. B. Abhängigkeiten funktional sein, wenn der Ausfall eines schadensmindernden Faktors dazu führt, dass das Einschreiten eines funktionierenden schadensmindernden Faktors unmöglich gemacht wird. Dies ist z. B. der Fall, falls die schadensmindernden Faktoren einige gemeinsame Komponenten besitzen, so dass eine Fehlfunktion solch einer Komponente beide schadensmindernde Faktoren außer Betrieb setzt. Weitere Details zu dieser Unterscheidung finden sich in [33].

Aus Gründen der Übersichtlichkeit werden die folgenden Ereignisbäume auf Systemebene durchgeführt, nachdem sie den Zwischenschritt als funktionaler Ereignisbaum durchlaufen haben.

9.2.2 Funktionale Abhängigkeiten

Die Reihenfolge der Darstellung der verschiedenen schadensmindernden Faktoren im Ereignisbaum wird nicht nur durch den Zeitpunkt ihres Eingreifens als mögliche schadensmindernde Faktoren bestimmt, sondern auch durch ihre logische Ordnung. Es muss beachtet werden, ob der erfolgreiche Einsatz eines schadensmindernden Faktors unabhängig vom erfolgreichen Einsatz eines anderen schadensmindernden Faktors ist. Dies könnte zum Beispiel der Fall sein, falls

- ein schadensmindernder Faktor als Hilffssystem für einen anderen dient, oder
- Änderungen in den Umgebungsparametern dergestalt auftreten, dass der Erfolg oder Ausfall eines anderen schadensmindernden Faktors beeinflusst wird.

So ist z. B. in Bild 2 ein Ereignisbaum dargestellt, bei dem die aufeinander folgenden Fehler des Systems A und B zu den gezeigten Ergebnissen führen. In diesem Beispiel wird das System A durch das System B unterstützt.

Nach einer Umordnung der Systeme A und B im Ereignisbaum (siehe Bild 3) benötigt der Zweig, der einem Fehler des Systems B folgt, keine weitere Aufteilung in zwei Zweige für System A, da ein Fehler des Systems B einen Funktionsausfall des Systems A zur Folge hat. Somit wird ein so genanntes „Abschneiden“ des Ereignisbaumes ermöglicht. Da dies vornehmlich von Rechnerprogrammen durchgeführt wird, besteht der Hauptbeitrag des Analysten darin, die verschiedenen Abhängigkeiten des Modells zu durchdenken.

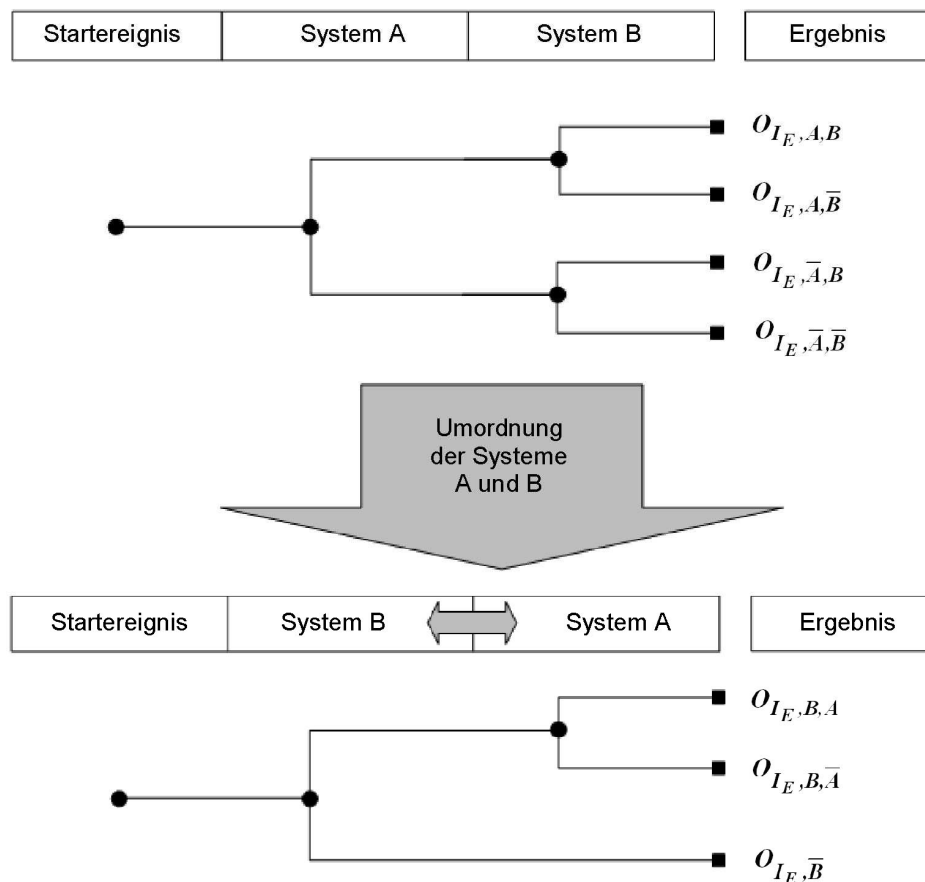


Bild 3 – Funktionale Abhängigkeiten in Ereignisbäumen

Vor Beginn des Umordnungsprozesses muss beachtet werden, dass die Darstellung eines Ereignisbaums unter Umständen nur eine spezielle zeitliche Reihenfolge der Fehler des Systems modelliert. Folglich modelliert der Ereignisbaum nicht den kompletten Satz an möglichen zeitlichen Reihenfolgen nach einem Startereignis. Dem muss Rechnung getragen werden, sobald die Hilfsmittel der Verbindung mit Fehlzu-standsbäumen oder Boole'schen Methoden Anwendung finden (siehe 9.3.2 und Anhang B.3).

9.2.3 Strukturelle oder physikalische Abhängigkeiten

Strukturelle oder physikalische Abhängigkeiten haben im Allgemeinen Ausfälle mit gemeinsamer Ursache zur Folge. Diese wiederum verursachen im Allgemeinen mehrere Ereignisse (siehe Abschnitt 3). Beispiele für Fehler mit gemeinsamen Ursachen sind solche, die durch Ereignisse wie Feuer, Erdbeben, Stürme, Ausfälle technischer Systeme (z. B. schwerwiegender Stromausfall oder Explosion – sowohl intern als auch extern verursacht) oder menschliche Handlungen (menschliche Fehlhandlungen oder Gewaltakte) hervorgerufen werden.

Daher wird eine Analyse der gemeinsamen Ursachen durchgeführt, um die Anfälligkeit der verschiedenen schadensmindernden Faktoren für Ausfälle auf Grund von externen oder internen Umgebungsbedingungen, Systemen oder Funktionen zu bestimmen.

So muss die Frage geklärt werden, ob das Auftreten des Startereignisses (z. B. eines Erdbebens) die bedingte Wahrscheinlichkeit des Auftretens aller Hauptereignisse der unterlegten Fehlzustandsbäume beeinflusst (siehe 9.3.2).

Ein weiterer Schritt der qualitativen Analyse ist die Identifizierung gemeinsamer Systeme oder Funktionen, die die verschiedenen schadensmindernden Faktoren beeinflussen. Dies ist z. B. bei einem Ereignisbaum der Fall, bei dem ein Ausfall des Systems A, gefolgt von einem Ausfall des Systems B, zu einem unerwünschten Ergebnis führt. Falls das System A darauf angewiesen ist, dass Teile des Systems B einwandfrei funktionieren, so kann der „gemeinsame Anteil“ extrahiert werden und folgende drei Systeme untersucht werden: System A, System B* (System B ohne den gemeinsamen Anteil) und System C, das den gemeinsamen Anteil repräsentiert, der von System A und System B verwendet wird. Dieses Szenario ist in Bild 4 dargestellt.

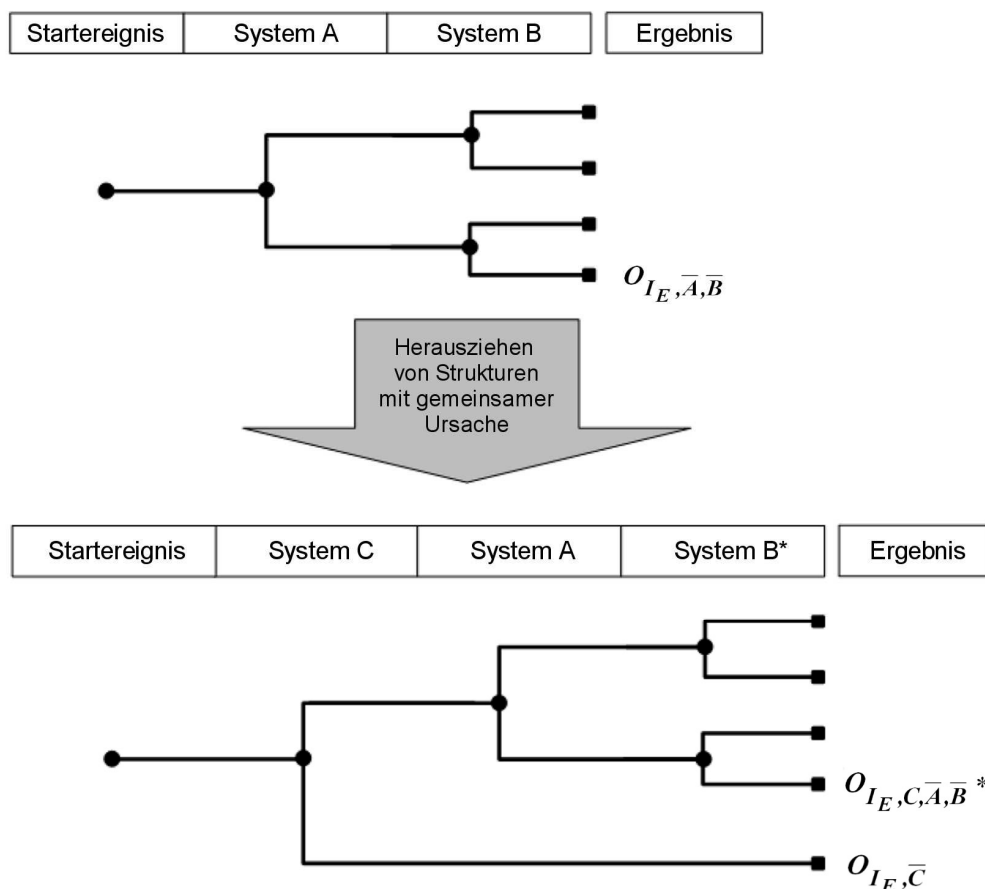


Bild 4 – Modellierung struktureller oder physikalischer Abhängigkeiten

In den meisten Fällen sind die Abhängigkeiten jedoch weit umfangreicher als in der Abbildung dargestellt.

So können z. B. die Fehler, die bei Instandhaltungsmaßnahmen auftreten, die durch Mitglieder desselben Instandhaltungsteam durchgeführt werden, nicht wie oben dargestellt in einfacher Weise modelliert werden. In Fällen mehrfacher Kombinationen abhängiger Systeme und deren Komponenten kann man die so genannte Verbindung mit Fehlzustandsbäumen verwenden, die in 9.3.2 detailliert beschrieben ist.

9.3 Quantitative Analyse

9.3.1 Unabhängige Ereignisabfolge

Für den Fall, dass alle bedingten Wahrscheinlichkeiten für den Erfolg oder Ausfall der schadensmindernden Faktoren unabhängig voneinander sind, ist die quantitative Analyse einfach.

Hierzu betrachte man einen Ereignisbaum mit drei schadensmindernden Faktoren – System A, B und C. Bild 5 stellt eine spezielle Reihenfolge im resultierenden Ereignisbaum dar, bei der System A intakt ist, während System B und System C ausgefallen sind. Im folgenden Absatz werden die grundlegenden Prinzipien erläutert, wie die Häufigkeit oder Wahrscheinlichkeit eines Ergebnisses dieser speziellen Reihenfolge δ berechnet wird. Praktische Beispiele sind in Anhang B in Bild B.1 und Bild B.3 angeführt.

In Übereinstimmung mit anderen Normen für Zuverlässigkeitstechniken wie der IEC 61165 behandelt die vorliegende Norm die verschiedenen Konzepte für Häufigkeit und Wahrscheinlichkeit in folgender Form:

Unter dem Begriff „Häufigkeit λ “ wird die Anzahl der Ereignisse pro Zeiteinheit verstanden; der Begriff „Wahrscheinlichkeit eines Ereignisses A, $P(A)$ “ hingegen bezeichnet eine reelle Zahl im abgeschlossenen Intervall $[0,1]$, die einem Ereignis zugeschrieben wird. Weitere Details finden sich in ISO 3534-1.

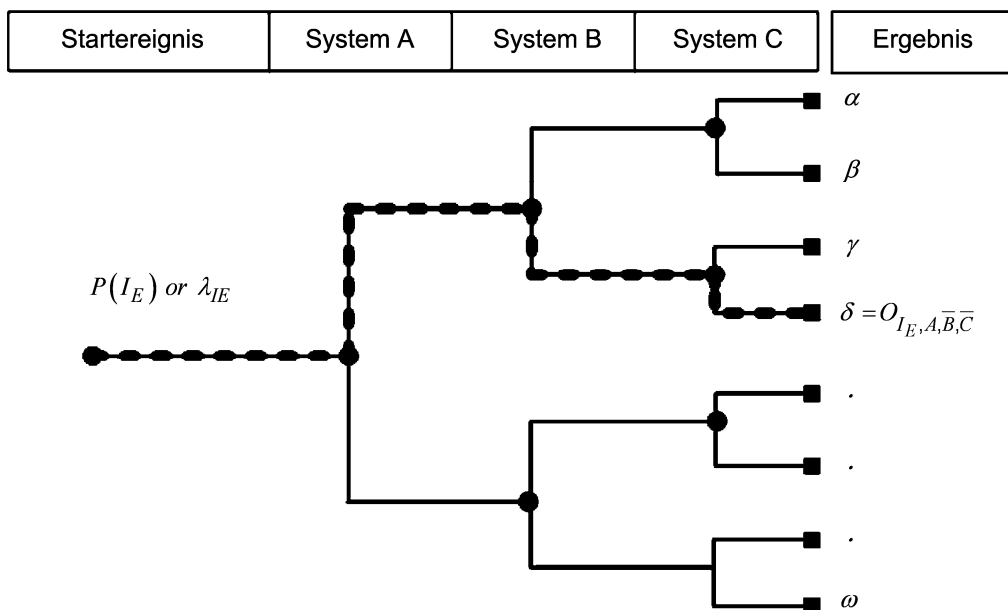


Bild 5 – Reihenfolge der Ereignisse

Zusammen mit den Definitionen in Tabelle 2 kann das Theorem der bedingten Wahrscheinlichkeit genutzt werden, um Gleichung (1) für die Wahrscheinlichkeit $P(\delta)$ dieser speziellen Reihenfolge δ aufzustellen.

$$\begin{aligned} P(\delta) &= P(I_E \cdot A \cdot \bar{B} \cdot \bar{C}) \\ &= P(I_E) \cdot P(A | I_E) \cdot P(\bar{B} | I_E \cdot A) \cdot P(\bar{C} | I_E \cdot A \cdot \bar{B}) \end{aligned} \quad (1)$$

mit

- a) $P(I_E)$ als der Wahrscheinlichkeit des Eintretens des Starterereignisses I_E und
- b) $P(A | I_E)$ als der bedingten Wahrscheinlichkeit für den Erfolg des Systems A, falls das Starterereignis I_E eingetreten ist.

Falls die Erfolge oder Ausfälle eines Systems von den anderen Systemen unabhängig sind, kann Gleichung (1) wie folgt vereinfacht werden, wobei mit $P(I_E)$ die Wahrscheinlichkeit des Eintretens des Starterereignisses bezeichnet wird:

$$P(\delta) = P(I_E) \cdot P(A | I_E) \cdot P(\bar{B} | I_E) \cdot P(\bar{C} | I_E) \quad (2)$$

Falls das Hauptaugenmerk auf dem Konzept der Häufigkeit liegt, kann dieses mathematische Modell auch dazu genutzt werden, die Häufigkeit λ_δ der Reihenfolge δ in Gleichung (3) mit Hilfe der Häufigkeit λ_{I_E} des Starterereignisses zu berechnen.

$$\lambda_\delta = \lambda_{I_E} \cdot P(A | I_E) \cdot P(\bar{B} | I_E) \cdot P(\bar{C} | I_E) \quad (3)$$

Gleichung (3) wird in den Beispielen im Anhang B in den Kapiteln B.1.3, B.2.5 und B.2.6 verwendet.

Nach Durchführung dieser Auswertung für alle möglichen Reihenfolgen $\alpha, \beta, \gamma, \delta, \dots, \omega$ erhält man eine vollständige quantitative Bewertung der Ergebnisse des Starterereignisses.

Falls die Werte für die Häufigkeit des Eintretens des Starterereignisses mit großer Unsicherheit behaftet sind, sollte man sich nicht allein auf die quantitative Bewertung verlassen, sondern Sensitivitätsanalysen durchführen, um die kritischsten Reihenfolgen herauszufinden.

9.3.2 Verbindung mit Fehlzustandsbäumen und Boole'sche Vereinfachungen

Wie in 7.1 und 9.2.3 dargelegt, können Fehlzustandsbäume dazu verwendet werden, die bedingte Wahrscheinlichkeit von Ausfällen der schadensmindernden Faktoren zu berechnen.

Bild 6 stellt einen Ereignisbaum mit den beiden schadensmindernden Faktoren System A und System B dar. Die Wahrscheinlichkeiten eines Ausfalls der Systeme A und B werden mit F_A und F_B bezeichnet. Diese Werte werden durch angehängte Fehlzustandsbäume berechnet, welche in der Darstellung nur durch ihre Hauptereignisse als Ergebnisse von UND- und ODER-Gattern, (siehe [13]) dargestellt sind.

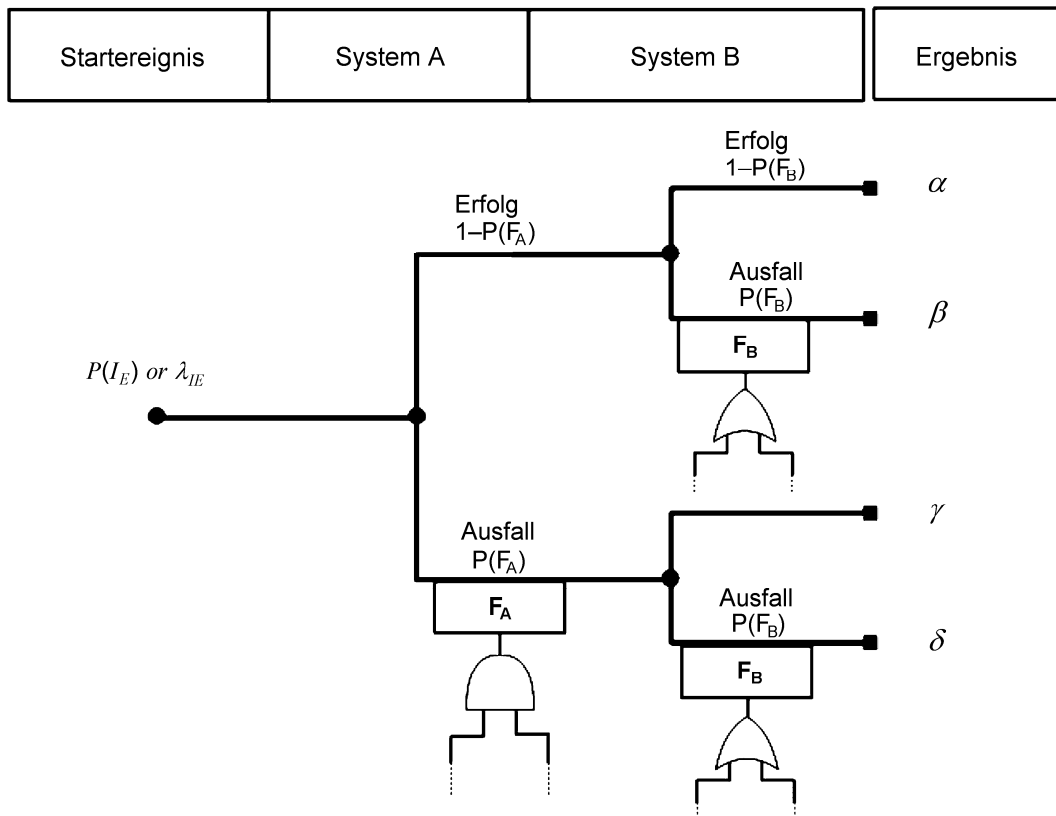


Bild 6 – Verbindung mit Fehlzustandsbäumen

Die Wahrscheinlichkeiten der entsprechenden Hauptereignisse F_A und F_B werden als bedingte Wahrscheinlichkeiten $P(F_A)$ und $P(F_B)$ für die Ausfälle des jeweiligen Systems A und Systems B verwendet. Die bedingten Wahrscheinlichkeiten für den Erfolg der Systeme ergeben sich dann zu $1 - P(F_A)$ und $1 - P(F_B)$.

Falls die schadensmindernden Faktoren durch Ereignisse mit gemeinsamer Ursache beeinträchtigt werden, kann mit Hilfe der Boole'schen Algebra der Ereignisbaum reduziert werden und diese Ereignisse identifiziert werden.

Die Ergebnisse jeder Reihenfolge im Ereignisbaum kann durch ein logisches UND-Gatter ermittelt werden, wodurch die Hauptereignisse miteinander verbunden werden, die mit dem jeweiligen Erfolg oder Ausfall eines schadensmindernden Faktors verknüpft sind. Die hierzu notwendige Boole'sche Vereinfachung und Analyse der Minimalschnitte wird gemäß [14] durchgeführt.

Anhang B.3 stellt ein detailliertes Beispiel für die Boole'sche Vereinfachung eines speziellen Ereignisbaumes dar.

Besondere Sorgfalt ist anzuwenden, falls eine dimensionslose Wahrscheinlichkeit mit einer Häufigkeit der Einheit [1/h] zusammengebracht wird. Wie oben angeführt, kann das Startereignis entweder mit einer dimensionslosen Wahrscheinlichkeit für das Auftreten $P(I_E)$ oder mit einer Häufigkeit λ_{IE} [1/h] beschrieben werden.

Ursprünglich liefert das Hauptereignis eines Fehlzustandsbaums, der mit dem jeweiligen schadensmindernden Faktor verbunden ist, eine Wahrscheinlichkeit eines speziellen Zustandes (z. B. Erfolg oder Ausfall) dieses schadensmindernden Faktors. Die mit der Fehlzustandsbaumanalyse ermittelten Wahrscheinlichkeiten können mit der Auftretenswahrscheinlichkeit oder Häufigkeit des Startereignisses verbunden werden (siehe 9.3.1). Für den Fall, dass das Eintreten des Hauptereignisses als Fehlerrate oder Häufigkeit gegeben ist, können diese Maßzahlen für das Eintreten des Hauptereignisses nicht ohne Weiteres mit der Auftretenshäufigkeit des Startereignisses (siehe 9.3.1) verbunden werden. Folglich muss auf andere Analysemethoden wie das Markoff-Verfahren zurückgegriffen werden (siehe [15]). Falls nicht-triviale Wiederherstellungs- oder Reparaturstrategien für die verschiedenen schadensmindernden Faktoren einbezogen sind, kann die

temporale Logik des Markoff-Verfahrens ein realistischeres Modell ermöglichen. Eine detailliertere Analyse der verschiedenen Betriebsmodi eines Systems und damit zusammenhängender Zuverlässigkeitsmaßzahlen finden sich in [17].

Die grundlegenden Regeln für die Quantifizierung eignen sich relativ gut für die Implementation durch einen Rechner. Hierfür existieren viele Softwarepakete, um die qualitative und quantitative Analyse eines Ereignisbaumes zu erleichtern. Jedoch kann entsprechend der IEC-Regularien kein spezielles Softwarepaket empfohlen werden.

Praktische Anwendungsbeispiele der theoretischen Ausführungen dieses Kapitels finden sich in Anhang B.

Neben den eher theoretischen Gesichtspunkten des Umordnens, Extrahierens und der Boole'schen Verfahren beim Fehlzustandsbaum ist es von besonderer Wichtigkeit, klare Vorgaben für die Zielsetzung und die Anforderungen an die Analyse festzulegen. Eine umfassendere Darstellung zur Erstellung eines prägnanten Verfahrens für eine Ereignisbaumanalyse ist in [3] veröffentlicht.

10 Dokumentation

Die Dokumentation einer Ereignisbaumanalyse sollte einige der unten aufgeführten Punkte enthalten. Zusätzliche und ergänzende Informationen können zum Zwecke der verbesserten Klarheit vor allem bei komplexen Systemen zur Verfügung gestellt werden. Entscheidend ist, dass die durchgeführten Schritte umfassend in der Dokumentation enthalten sind.

Die Kapitelangaben in eckigen Klammern verweisen im Folgenden auf beispielhafte Umsetzung im Anhang B.2.

- a) Zielsetzung und Umfang der Analyse [B.2.2], [B.2.4]
- b) Systembeschreibung [B.2.3]:
 - i) Beschreibung des Designs;
 - ii) Betrieb des Systems;
 - iii) Detaillierte Definition der Systemgrenzen.
- c) Annahmen [B.2.3], [B.2.4]:
 - i) Annahmen über das Systemdesign;
 - ii) Annahmen über Betrieb, Instandhaltung, Prüfung und Inspektion;
 - iii) Annahmen über Zuverlässigkeits- und Verfügbarkeitsmodellierung.
- d) Ereignisbaumanalyse [B.2.5], [B.2.6]:
 - i) Begründung und Quellen für die Liste der Startereignisse;
 - ii) Analyse einschließlich der graphischen Darstellung;
 - iii) Benutze Datenquellen.
- e) Ergebnisse, Schlussfolgerungen und Empfehlungen [B.2.7].

Weitere allgemeine Leitlinien für die Dokumentation finden sich in IEC 60300-3-1.