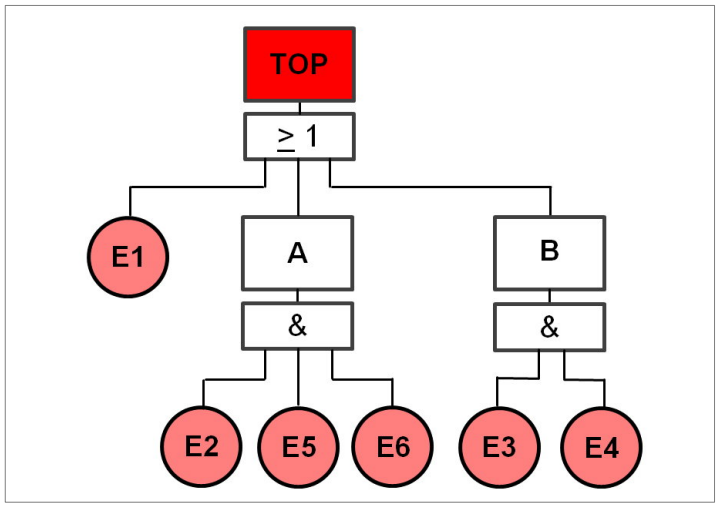
Fehlerbaumanalyse



Englische Bezeichnungen)

Fault Tree Analysis (FTA)

Kurzdefinition

Die Fehlerbaumanalyse ist eine deduktive Methode zur Analyse wichtiger unerwünschter Ereignisse (TOP-Ereignisse). In einem Top-Down-Verfahren wird ausgehend vom betrachteten TOP-Ereignis eine Baumstruktur entwickelt, in der das Zusammenwirken potentieller Ursachen für das unerwünschte Ereignis mit Hilfe von logischen Verknüpfungen dargestellt wird. Die Fehlerbaumanalyse kann den Entwicklungsprozess, die Festlegung einer geeigneten Systemarchitektur oder die Ableitung von Design-Anforderungen aktiv unterstützen. Die quantitative Auswertung erlaubt die Berechnung konkreter Zuverlässigkeitskenngrößen, wie z.B. die Wahrscheinlichkeit für das Auftreten eines Ausfalls.

Einsatz-möglichkeiten

- Untersuchungsobjekte können Produkte, Systeme, Prozesse, Dienstleistungen oder Software sein.
- Analyse zentraler Risiken, die bedeutende Auswirkungen (Gefahren für Gesundheit und Leben, wirtschaftlicher Schaden usw.) mit sich bringen können. Beispiele dafür sind: Produktentwicklung in der Automobilindustrie, Planung von Industrieanalagen, vorbeugender Brandschutz, Sicherheitsprüfung kerntechnischer Anlagen
- Präventives Identifizieren möglicher Ausfallursachen in der Entwicklungsphase mit dem Ziel, das Auftreten dieser Ausfälle im Endprodukt zu vermeiden

- Analyse der Ursachenketten für aufgetretene Fehler (z.B. Ausfall einer Produktionsanlage), um so den Fehler in Zukunft zu vermeiden
- Sind die Ausfallwahrscheinlichkeiten von Komponenten oder Sub-Systemen bekannt, können Systemzuverlässigkeit und das Ausfallverhalten des Gesamtsystems quantitativ analysiert werden.

Vorteile

+ Die Fehlerbaumanalyse erlaubt es, kritische Komponenten oder Sub-Systeme zu identifizieren und bedeutende Risiken zu reduzieren.
+ Es können komplexe Systeme mit vielen Schnittstellen und Wechselwirkungen analysiert werden.
+ Eine Fehlerbaumanalyse schafft ein tiefes Verständnis des Systemverhaltens.
+ Das Wissen über Ursachenketten ermöglicht es, Design-Anforderungen zur Vermeidung von Ausfällen abzuleiten.

Nachteile / Risiken / Grenzen

– Eine detaillierte Ausarbeitung ist zeitaufwendig.
– Für jedes TOP-Ereignis muss ein eigener Fehlerbaum erstellt und ausgewertet werden.
– Die klassische Fehlerbaumanalyse ist ein statisches Modell, so dass zeitlich versetzte Ausfälle nicht analysiert werden können.
– Eine quantitative Analyse ist oft nicht möglich, da konkrete Zuverlässigkeitswerte von Komponenten nicht bekannt sind und erst durch aufwendige Testreihen ermittelt werden können.

Voraussetzungen

- **Die Syntax des Fehlerbaums muss festgelegt werden:** Für die logische Verknüpfung von Ereignissen im Fehlerbaum gibt es unterschiedliche Symbol-Systeme. Vor Start muss die verwendete Notation ausgewählt werden. In dieser Beschreibung wird eine mit der DIN 25424-1:1981-09 konforme Notation gewählt (s. Tabelle 1).
- **Die Managementunterstützung muss gewährleistet sein:** Das Management muss dafür sorgen, dass die Teammitglieder für die Aufgabe zur Verfügung stehen und es muss Änderungen am System oder Prozess basierend auf den Ergebnissen der Methode freigeben.
- **Das Zusammenwirken der Komponenten im System muss vorher genau bekannt sein**: Wenn Systemzuverlässigkeit und Ausfallverhalten bestimmt und richtig beschrieben werden sollen, muss das gesamte System vollständig dokumentiert sein.

Qualifikation

Die Methode benötigt einen Moderator, der die Gruppenarbeit leitet und das Team durch die einzelnen Schritte der Fehlerbaumanalyse führt. Der Moderator muss mit der Methode vertraut sein und bereits Erfahrungen mit ihrer Anwendung gesammelt haben. Zusätzlich benötigt er entsprechende Moderationserfahrung. Für die manuelle Analyse ohne Software-Einsatz sind fundierte Kenntnisse der Booleschen Algebra erforderlich.

Jedes Teammitglied trägt mit der Kompetenz seines Fachbereichs bei. Die Teammitglieder benötigen darüber hinaus keine weiteren Qualifikationen.

Benötigte Informationen

- Alle bereits verfügbaren Dokumente zum System, Prozess oder der Dienstleistung (Lastenheft, Konstruktionszeichnungen, Flussdiagramme usw.)
- Falls eine FMEA durchgeführt wurde, muss die FMEA-Tabelle zur Unterstützung der Schritte 2 und 3 zur Verfügung stehen.
- Ausfalldaten der Komponenten bzw. Sub-Systeme, wenn der Fehlerbaum auch quantitativ ausgewertet werden soll

Ergebnisse

- Dokumentation systematischer Fehlerzusammenhänge in der Visualisierung als Fehlerbaum bzw. Fehlerbäume
- Liste aller möglichen Fehlerkombinationen, die zu einem unerwünschten Ereignis führen (sog. "Cut Sets")
- Liste aller minimalen Ausfallkombinationen, die zum TOP-Ereignis führen ("Minimal Cut Sets")
- Identifizierte Systemschwachstellen zur gezielten Optimierung
- Bei quantitativer Auswertung: Gesamtwahrscheinlichkeit für das Eintreten des unerwünschten Ereignisses und Zuverlässigkeitskenngrößen hinsichtlich Verfügbarkeit und Sicherheit

Benötigte Hilfsmittel

- Beamer und ggfs. Tafel oder Whiteboard zur gemeinsamen Entwicklung des Fehlerbaums
- Erstellung und Auswertung eines Fehlerbaums können schon bei relativ kleinen Systemen aufwendig werden. Die Fehlerbaumanalyse wird dann softwaregestützt durchgeführt. Hierfür ist kommerzielle Software erforderlich.

Durchführung

Produkte, Systeme, Software, Prozesse oder auch Dienstleistungen können mit Hilfe der Fehlerbaumanalyse untersucht werden. Der Ablauf ist bei allen Anwendungsfällen identisch. Zur besseren Lesbarkeit beschreiben die folgenden Schritte die Fehlerbaumanalyse eines technischen Systems, stellvertretend für alle anderen Untersuchungsobjekte. Die Analyse der Ausfallwahrscheinlichkeit wird hier nicht beschrieben.

Aus Gründen der einfacheren Lesbarkeit wird im Folgenden nur die grammatikalisch männliche Form (Teilnehmer, Moderator) verwendet. Es sind dabei aber stets Personen jeden Geschlechts gemeint.

Teamzusammensetzung

Besetzen Sie das Team mit erfahrenen Fachleuten aus den Bereichen, die mit dem System in Berührung kommen. Neben Entwicklung, Qualität oder Produktion können das der Kundendienst oder sogar Vertreter des Kunden sein. Berücksichtigen Sie bei der Auswahl, dass Ausfälle nicht nur durch Komponentenversagen, sondern auch durch Bedienfehler verursacht werden können.

Für die Moderation der Teamarbeit können Sie die Methode "Moderation von Arbeitsgruppen" einsetzen.

Schritt 1: Analysieren Sie Ihr System!

Definieren Sie den Umfang des zu untersuchenden Systems und beschreiben Sie es. Am besten geeignet ist dafür die Form eines Blockdiagramms. Sie können mit einer Black-Box beginnen und diese dann schrittweise von oben nach unten in feinere Teilsysteme zerlegen (Bild 1).

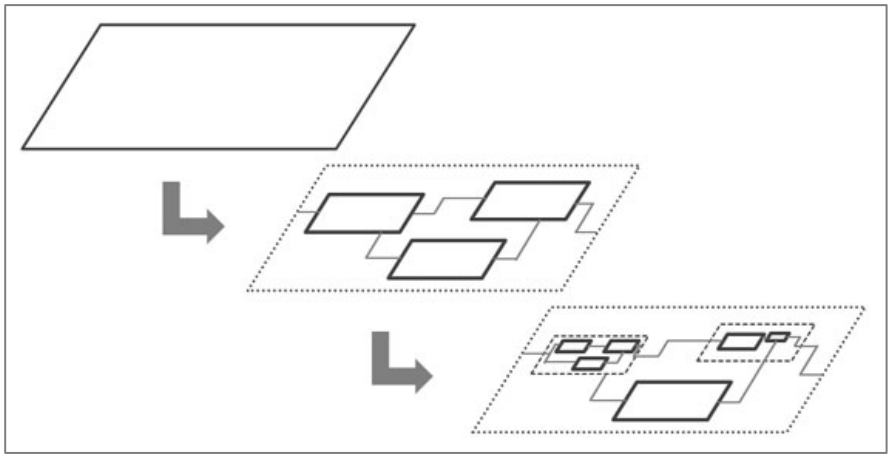


Bild 1: Schrittweise Verfeinerung des Systems top-down in immer kleinere Teilsysteme

Die Teilsysteme stehen über Eingangs- und Ausgangsströme miteinander in Beziehung. Diese Schnittstellen müssen mit ihren Toleranzen identifiziert werden. Dies können Signale (elektrisch, optisch…), Materialflüsse (Gas, Flüssigkeit…) oder Energie (Heizung, Kühlung…) sein. Ermitteln Sie die Umgebungsbedingungen sowohl des Gesamtsystems als auch der einzelnen Sub-Systeme (Temperatur, Druck, Feuchtigkeit…).

Sie erhalten so ein Systemblockdiagramm bzw. Funktionsblockdiagramm, bei denen die einzelnen Sub-Systeme und Komponenten miteinander in Beziehung stehen und die Organisation und das Verhalten des Gesamtsystems verdeutlichen. Um die Fehlerbaumanalyse effizient und wirtschaftlich zu gestalten gilt es bei der Erstellung des Blockdiagramms unbedingt auf zwei Aspekte zu achten:

1. Selektion der wesentlichen Elemente – Systemgrenzen

Identifizieren Sie die wesentlichen Elemente des Systems. Dies sind kritische Teilsysteme, die hohe Anforderungen zu erfüllen haben, bekanntermaßen risikobehaftet sind oder neue Technologien beinhalten, über die keine Erfahrungswerte vorliegen. Die Auswahl der relevanten Sub-Systeme kann z.B. durch eine Nutzwertanalyse oder Portfolio-Analyse erleichtert werden. Fokussieren Sie die Fehlerbaumanalyse auf diese Elemente.

2. Granularität des Blockdiagramms – Systemtiefe

Wählen Sie eine passende Auflösung der Sub-Systeme und Komponenten. Eine zu grobe Aufschlüsselung geht auf Kosten der Gründlichkeit, eine zu feine Aufschlüsselung erhöht den Aufwand enorm und liefert nicht unbedingt bessere Ergebnisse. Die Wahl der Granularität ist abhängig vom Ziel der Fehlerbaumanalyse: Um eine erste Systemabschätzung zu erhalten, genügt eine grobe Aufschlüsselung. Für die Analyse eines konkreten Designs ist eine feinere Auflösung bis in einzelne Komponenten sinnvoll.

Schritt 2: Definieren Sie die unerwünschten Ereignisse!

Die Definition und die Anzahl der unerwünschten Ereignisse legen maßgeblich den Umfang der Analyse fest, denn jedes TOP-Ereignis wird in einem separaten Fehlerbaum untersucht. TOP-Ereignisse können Fehlzustände des Gesamtsystems oder von Teilsystemen sein. Legen Sie die Ausfallkriterien genau fest. Dazu gehört auch die Beschreibung der zu betrachtenden Betriebsphase (z.B. "Absturz des Flugzeugs in der Flugphase nach Erreichen der Reiseflughöhe").

Die Selektion der TOP-Ereignisse kann beispielsweise durch genaue Systemkenntnis, aus Untersuchung von Unfällen oder Vergleich mit Ausfällen von ähnlichen Systemen geschehen. Oft werden dazu Methoden wie die FMEA oder Hazard and Operability Studies (HAZOP) eingesetzt (Crawly, F. u. Tyler, B.: HAZOP: Guide to Best Practice, 2015).

Schritt 1 und Schritt 2 können vertauscht oder auch iterativ ablaufen, denn es kann sinnvoll sein, Systemgrenzen und Systemtiefe nach genauer Beschreibung des TOP-Ereignisses anzupassen.

Schritt 3: Erstellen Sie den Fehlerbaum!

Bilden Sie nun den Ablauf der Ereignisse lückenlos ab, die zum Eintreten des unerwünschten Ereignisses führen, indem Sie den Fehlerbaum Ebene für Ebene konstruieren. Stellen Sie für jedes Ereignis in der jeweiligen Ebene die Frage: "Wie kann es dazu kommen (Ursache), dass dieses Ereignis (Wirkung) eintritt?". Für diesen Schritt ist ein gutes Verständnis des Ursache-Wirkungs-Gefüges im betrachteten System nötig. Eine gute Moderation stellt sicher, dass alle potentiellen Ursachen im Team diskutiert werden.

Unterscheiden Sie zwischen drei Ausfallsarten:

1. Primärausfall

Dies ist das Versagen einer Komponente oder eines Sub-Systems, das nicht weiter analysiert wird (z.B. "Glühfaden einer Signallampe durchgebrannt"; "Sicherheitsventil schadhaft", wobei die Komponenten des Ventils nicht weiter untersucht werden sollen). Ziel ist es, den Fehlerbaum so weit zu entwickeln, dass nur noch Primärausfälle übrig bleiben.

2. Kommandierter Ausfall

Dieses Versagen entsteht durch ein unzulässiges oder fehlendes Eingangssignal oder durch den Ausfall einer Hilfsquelle (z.B. versehentliches Ausschalten einer Signallampe).

3. Sekundärer Ausfall

Dies ist ein Folgeausfall, der aus unzulässigen Einsatzbedingungen einer Komponente resultiert (z.B. Betrieb der Signallampe ungeschützt im Regen).

Symbole zur Darstellung der logischen Verknüpfungen

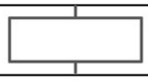
Symbol	Bezeichnung	Bedeutung
	Kommentar	Das Rechteck enthält Beschreibungen von Ein- und Ausgängen von Verknüpfungen.
	Standardeingang	Das Symbol steht für ein primäres Versagen. Es enthält keine weiteren Fehlerbedingungen.
	ODER-Verknüpfung	Das Ereignis A tritt ein, wenn mindestens ein Eingang wahr ist. Die Verknüpfung kann beliebig viele Eingänge haben.
	UND-Verknüpfung	Das Ereignis A tritt nur ein, wenn alle Eingänge wahr werden. Die Verknüpfung kann beliebig viele Eingänge haben.
	NICHT-Verknüpfung	Das Symbol negiert: Das Ereignis A tritt ein, wenn E nicht eintritt und umgekehrt.
	Transfereingang	Mit diesem Symbol wird der Fehlerbaum abgebrochen und an anderer Stelle fortgesetzt.
	Transferausgang	

Tabelle 1: Standardsymbole zur Erstellung eines Fehlerbaums

Verwenden Sie bei der Konstruktion des Fehlerbaums die in Tabelle 1 dargestellten Standardsymbole. Weitere Sondersymbole sind z.B. in der DIN 25424-1:1981-09 "Fehlerbaumanalyse; Methode und Bildzeichen" beschrieben. Diese logischen Verknüpfungen werden auch "Gatter" genannt.

Einfaches Beispiel Dampfkessel

Betrachten wir als Beispiel eine vereinfachte Dampfkesselanlage (z.B. Elektrodampfkessel) bestehend aus einem Dampfkessel, in dem mit Hilfe von Elektroheizstäben Wasser bis zu einem maximalen Druck (P_{max}) verdampft wird, einer Steuereinheit, die bei Erreichen des maximalen Drucks die Energiezufuhr entsprechend verringert und einem Sicherheitsventil, das bei Drücken oberhalb des maximalen Werts öffnet.

Als TOP-Ereignis wählen wir die Explosion des Dampfkessels. Dieses Ereignis stellt die Startebene des Fehlerbaums dar (Bild 2). Identifizieren Sie nun alle Ursachen, die alleine oder in Kombination unmittelbar zum Eintreten des TOP-Ereignisses führen. Eine mögliche Ursache ist ein Defekt am Dampfkessel. Dies entspricht einem primären Versagen der Komponente "Dampfkessel", das nicht weiter aufgeschlüsselt wird. Der Fehlerbaum endet an dieser Stelle mit einem Standardeingang (s. Bild 2).

Eine weitere Ursache für das TOP-Ereignis kann in unzulässigen Einsatzbedingungen bestehen, entsprechend einem sekundären Ausfall. Verbinden Sie diese beiden möglichen Ursachen in dieser Ebene logisch mit dem TOP-Ereignis, hier mit einer ODER-Verknüpfung (s. Bild 2).

Top-down die Ausfall-Logik verfolgen

Der sekundäre Ausfall wird nun weiter analysiert. Er ist die Folge eines Betriebs bei Umgebungsbedingungen außerhalb der Spezifikation oder von Dampfdrücken oberhalb des zulässigen maximalen Werts, beides sind sekundäre Ausfälle. Diese werden wiederum mit einer ODER-Verknüpfung mit dem darüber liegenden Zwischenereignis logisch verbunden. Die Ursache "unzulässige Umgebungsbedingungen" wird an anderer Stelle (nicht hier im Beispiel ausgeführt) weiter analysiert. Die Ergebnisse finden an dieser Stelle Eingang in den Fehlerbaum, was durch das Symbol "Transfereingang" dargestellt wird. Solche Transfergatter ermöglichen es, den Fehlerbaum in übersichtliche Teilbäume zu strukturieren.

Schritt für Schritt analysieren, bis nur noch Standardeingänge vorhanden sind

Das Ereignis "Ausfall durch Druck > P_{max}" wird weiter untersucht. Ursachen sind hier eine "überhöhte Energiezufuhr" und das Nichtöffnen des Sicherheitsventils. Die logische Verbindung mit dem darüber liegenden Ereignis ist hier eine UND-Verknüpfung, da beide Ereignisse gleichzeitig auftreten müssen. Das Zwischenereignis "überhöhte Energiezufuhr" wird an anderer Stelle weiter untersucht (Transfereingang). Das Zwischenereignis "Sicherheitsventil öffnet nicht" wird entweder durch einen Defekt am Ventil verursacht oder durch eine falsche Ventileinstellung. Beide Ereignisse werden als Eingänge einer ODER-Verknüpfung mit dem darüber liegenden Ausgang verbunden. Sie werden nicht weiter untersucht und daher als Standardeingang (primärer Ausfall) dargestellt (Bild 2).

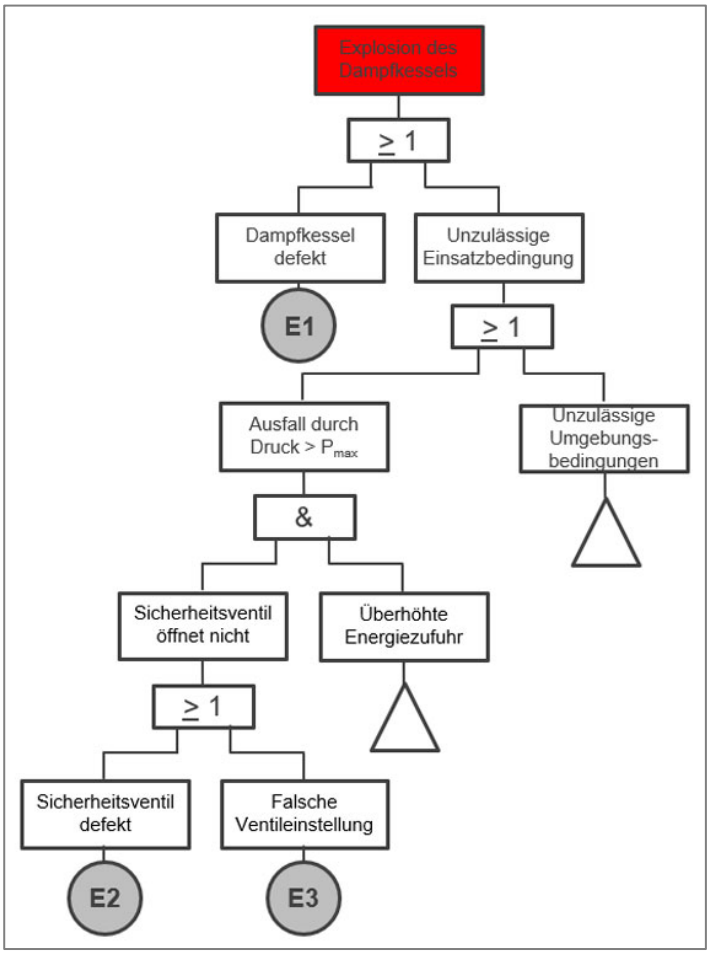


Bild 2: vereinfachtes Beispiel eines Fehlerbaumes

Führen Sie die Fehlerbaumaufstellung so lange weiter, bis nur noch Standardeingänge vorhanden sind. Dann ist der Fehlerbaum komplett und kann analysiert werden.

Schritt 4: Bestimmen Sie die möglichen Ausfallkombinationen!

Untersuchen Sie nun die Fehlertoleranz des Systems, indem Sie die Struktur des Fehlerbaums analysieren. Die Art und Weise der Verknüpfungen im Fehlerbaum gibt Aufschluss über die Bedeutung einzelner Ereignisse. Die Ausfallkombinationen (Gruppen von primären Ereignissen), unter denen das TOP-Ereignis wahr wird, werden "Schnitte" oder auch "Cut Sets" genannt.

Vom intuitiven Fehlerbaum zur berechenbaren Matrix

Ein Algorithmus zum Auffinden der Schnitte wird an einem neutralen Beispiel-Fehlerbaum (Bild 3) beschrieben. Zur Darstellung der Schnitte ist eine Matrixform geeignet. Erstellen Sie für jede Ebene des Fehlerbaums eine Matrix bestehend aus den Primär- und Zwischenereignissen dieser Ebene. Die Start-Matrix enthält das TOP-Ereignis. Ersetzen Sie dieses Ereignis mit den Eingängen des darunterliegenden Gatters der Ebene 1. Dies ist ein ODER-Gatter, daher werden so viele Zeilen hinzugefügt wie das Gatter Eingänge besitzt, hier zwei. E1 als Primärereignis bleibt bei der Weiterentwicklung der Matrix in der Zeile stehen und stellt bereits eine "Ausfallkombination" dar.

Umformungen mit Boolescher Algebra

Die folgenden Schritte folgen streng den Gesetzen der Booleschen Algebra. Sie sind hier nur in wenigen Schritten beispielhaft aufgeführt. Bei umfangreicheren Analysen ist hierfür der Einsatz einer geeigneten Software dringend zu empfehlen.

Das Zwischenereignis A wird nun durch die Eingänge des UND-Gatters in Ebene 2 ersetzt und zwar in einer Zeile (UND-Verknüpfung). B und C bilden eine weitere Ausfallkombination, allerdings stellen sie keine Primärereignisse dar und müssen weiter entwickelt werden. Beide werden durch die Eingänge der jeweiligen ODER-Gatter in Ebene 3 ersetzt, wobei alle gegenseitigen Kombinationen gebildet werden. Es entsteht so eine neue Ausfallkombination E2 und E3, die aus Primärereignissen besteht und als weiterer Schnitt in der Matrix stehen bleibt. Die Zwischenereignisse D und E werden im nächsten Schritt durch die Eingänge der UND-Gatter ersetzt.

Die Matrix enthält nun ausschließlich Primärereignisse. Die fünf Zeilen enthalten alle Schnitte, die das TOP-Ereignis auslösen. Die Ausfallkombination E3, E4, E3 der Zeile vier kann durch die Kombination E3, E4 ersetzt werden, da ein einmaliges Auftreten von E3 genügt, um das TOP Ereignis auszulösen (Idempotenzgesetz der Booleschen Algebra).

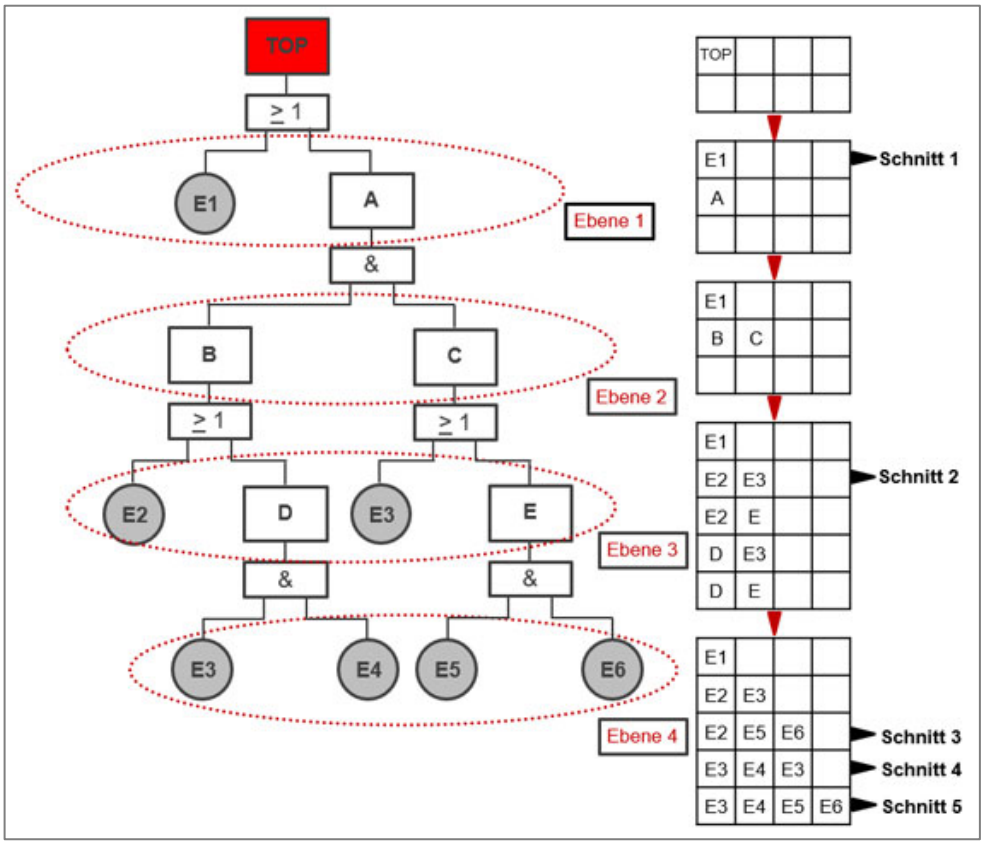


Bild 3: vereinfachtes Beispiel eines Fehlerbaumes mit fünf Ausfallkombinationen (Schnitten, Cut Sets)

Was braucht es minimal zur Katastrophe?

Interessant sind nun diejenigen Kombinationen, die direkt zum TOP-Ereignis führen und keine weiteren Ausfallkombinationen mehr enthalten. Diese sogenannten Minimalschnitte (Minimal Cut Sets) enthalten keine redundanten Elemente mehr: Treten alle Ereignisse eines Minimalschnitts ein, so tritt auch das TOP-Ereignis ein, tritt auch nur ein Ereignis nicht ein, so tritt auch das TOP-Ereignis nicht ein. Die Kombination E3, E4 (Schnitt 4) ist in Schnitt 5 enthalten, Schnitt 5 ist daher kein Minimalschnitt (Absorptionsgesetz der Booleschen Algebra). Der Fehlerbaum enthält also vier Minimalschnitte, die übersichtlich in einem sogenannten äquivalenten Minimalschnittbaum dargestellt werden (Bild 4). Das TOP-Ereignis ist dabei durch ein ODER-Gatter mit allen Minimalschnitten logisch verknüpft.

Die Anzahl der primären Ereignisse eines Minimalschnittes wird Ordnung genannt. Je weniger Primärereignisse nötig sind um das TOP Ereignis auszulösen, desto wahrscheinlicher ist in der Regel das Auftreten des Minimalschnitts.

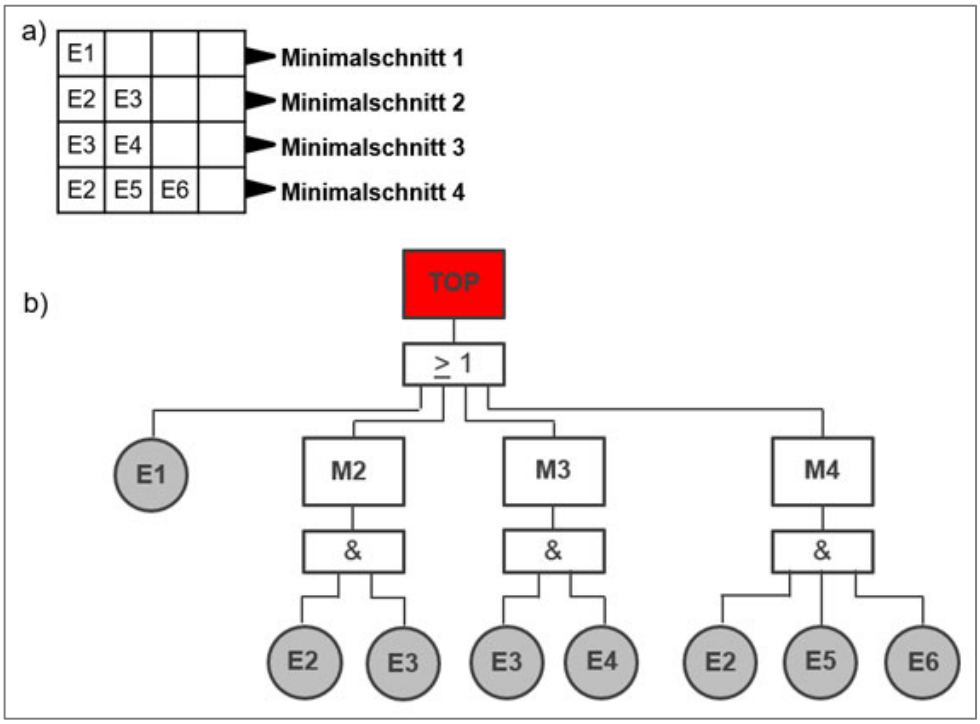


Bild 4: Minimalschnitte (a) und äquivalenter Fehlerbaum (b)

Legen Sie daher besonderes Augenmerk auf Minimalschnitte erster Ordnung. Hier reicht bereits das Eintreten eines einzigen primären Ereignisses (hier Ereignis E1), um das TOP-Ereignis auszulösen (Single Point Failure). Diese Ausfallmöglichkeiten haben die höchste Priorität bei der Maßnahmenplanung zur Fehlervermeidung, d.h. diese Ereignisse sollten selbst unter extremen Bedingungen zuverlässig verhindert werden.

Minimalschnitte sind nicht voneinander unabhängig, denn bestimmte primäre Ereignisse können in mehreren Minimalschnitten vorhanden sein. Suchen Sie Primärausfälle, die in mehreren Minimalschnitten auftreten. Hier sind das E2 und E3. Diese Ausfälle haben die zweithöchste Priorität bei der Maßnahmenplanung.

In der Praxis sind Fehlerbäume sehr schnell so umfangreich, dass das Auffinden der Minimalschnitte nur noch mit Unterstützung von Software sinnvoll möglich ist.

Tipps für die Praxis

- Strukturieren Sie komplexe Fehlerbäume mit Hilfe von Teilbäumen, die durch Transfergatter an den Hauptbaum angeknüpft werden. Dies fördert die Lesbarkeit des Fehlerbaums.
- TOP-Ereignisse auf Systemebene können oft nicht quantitativ beschrieben werden (z.B. Gasexplosion in einer Chemieanlage). Anders ist dies bei TOP-Ereignissen an Teilsystemen: Stellen Sie sich hier folgende Fragen: Wo tritt der Fehler auf? Was genau ist fehlerhaft? Existieren messbare Kriterien für den Fehler? (z.B. "Stromstärke im LED-Kreis 50% über zulässigem Maximalwert"). Mit einer quantitativen Formulierung gewährleisten Sie einen effizienten Ablauf der Analyse.

Varianten

Fehlerbaumanalyse mit quantitativer Auswertung

Sind die Zuverlässigkeits- oder Ausfallzahlen für die Komponenten bekannt, so kann aus den Eintrittswahrscheinlichkeiten der Einzelereignisse das Ausfallverhalten des Gesamtsystems errechnet werden (Edler, F.; Soden, M. u. Hankammer, R.: Fehlerbaumanalyse in Theorie und Praxis: Grundlagen und Anwendung der Methode, 2015).

Fachartikel (Anleitungen und Anwendungsbsp.)

Mit FMEA auf der sicheren Seite – ein Praxisbeispiel

Methode –Ausgabe 11/2017 – von Dr. Christine Knorr

Funktionale Sicherheit – Herausforderung bei Entwicklungsprojekten

Fachbeitrag – Ausgabe 07/2010 – von Dr. Pierre Metz

Herkunft

Mit Beginn der 1960er Jahre wurden Techniken zur systematischen Analyse sicherheitskritischer Systeme entwickelt. Dazu gehören neben der Hazard and Operability Analysis (HAZOP) und der FMEA auch die Fehlerbaumanalyse. H. Watson und A. Mearns haben 1961 in den Bell Laboratorien diese Methode entwickelt, um das Abschusskontrollsystems für die von Boeing hergestellte Interkontinentalrakete vom Typ LGM-30 Minuteman zu analysieren (Wikipedia (engl.): Fault Tree Analysis). In den 1970er und 1980er Jahren wurde die Fehlerbaumanalyse unter anderem in der Luft- und Raumfahrt und bei der Planung von Kernkraftwerken eingesetzt. Mittlerweile findet die Fehlerbaumanalyse in der Automobilbranche und in vielen weiteren Branchen Anwendung. In Deutschland ist die Fehlerbaumanalyse in der DIN 25424-1:1981-09 "Fehlerbaumanalyse; Methode und Bildzeichen" behandelt (Teil 1: Methode und Bildzeichen, Teil 2: Handrechenverfahren zur Auswertung eines Fehlerbaumes).

Ergänzende Methoden

- Moderation von Arbeitsgruppen – zur Gestaltung der Teamarbeit
- Brainstorming – zur gemeinsamen, strukturierten Suche nach Ausfallursachen
- FMEA – zur systematischen Untersuchung von Fehlerfolgen. FMEA und FTA ergänzen sich gegenseitig
- Nutzwert-Analyse – zur Selektion kritischer Teilsysteme
- Portfoliotechnik – zur Selektion kritischer Teilsysteme
- Risikoidentifikation – zur Identifikation von TOP-Ereignissen
- Risikoanalyse – zur Analyse von TOP-Ereignissen und ihren Ursachen
- Ishikawa-Diagramm – zur Identifikation von Ursachen
- Gegenwartsbaum – ähnliche Methode zur Ursachenanalyse aus der Theory of Constraints

Autor: Dr. Christine Knorr

erstellt am: 08.04.2018

Hier geht es zur Online-Version:

www.projektmagazin.de/methoden/fehlerbaumanalyse

Die Online-Version auf unserer Website bietet zusätzlich:

- ergänzende Kommentare unserer Leser
- vollständige Liste aller Publikationen des Projekt Magazins zur Methode
- weitere Service-Informationen zu Software, Bücher, Dienstleistungen, Seminare und Events