Zuverlässigkeit

3. Teil

Prof. Erika Hausenblas

Montanuniversität Leoben, Österreich

7. Oktober 2014

Inhalt

Ein Überblick

Fehlerbaumanalyse - ein Überblick

- Definition des zu untersuchenden Systems oder Prozesses
- Konstruktion des Fehlerbaums
- Qualitative und Quantitative Analyse
- Dokumentation der Ergebnisse

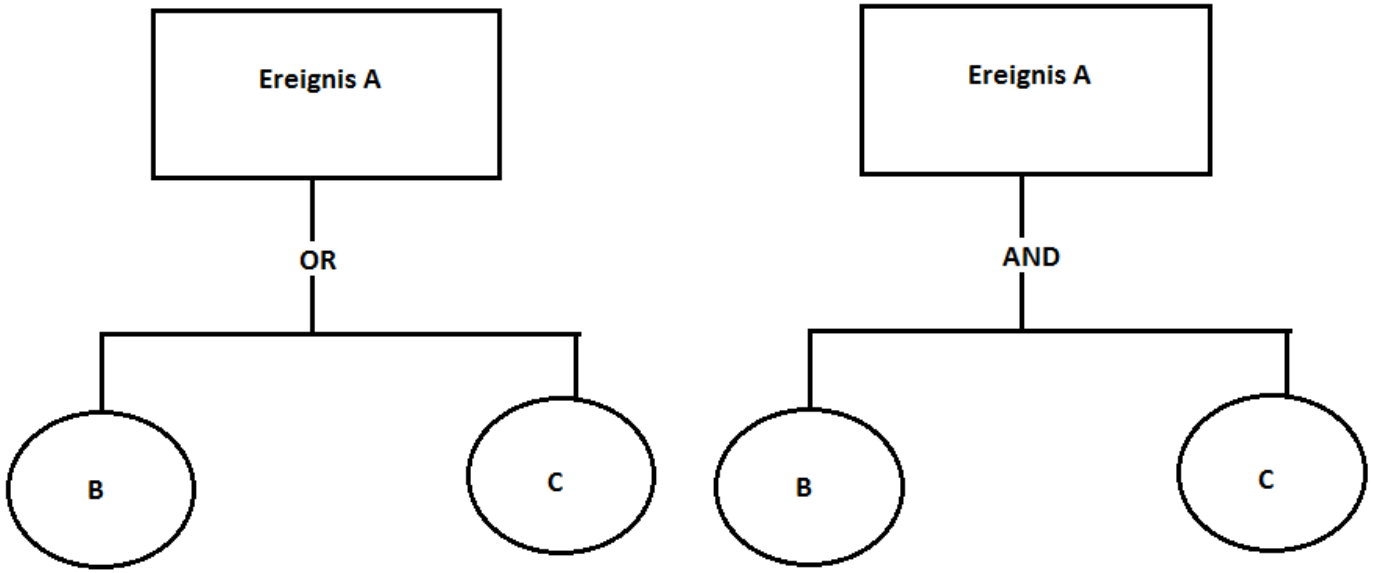
Systemdefinition

- physikalische Randbedingungen
- Granularitätsstufe der Basis Ereignisse
- Anfangskonfiguration des Systems
- weitere Annahmen
- anfängliche Betriebsbedingungen
- unerlaubte Ereignisse

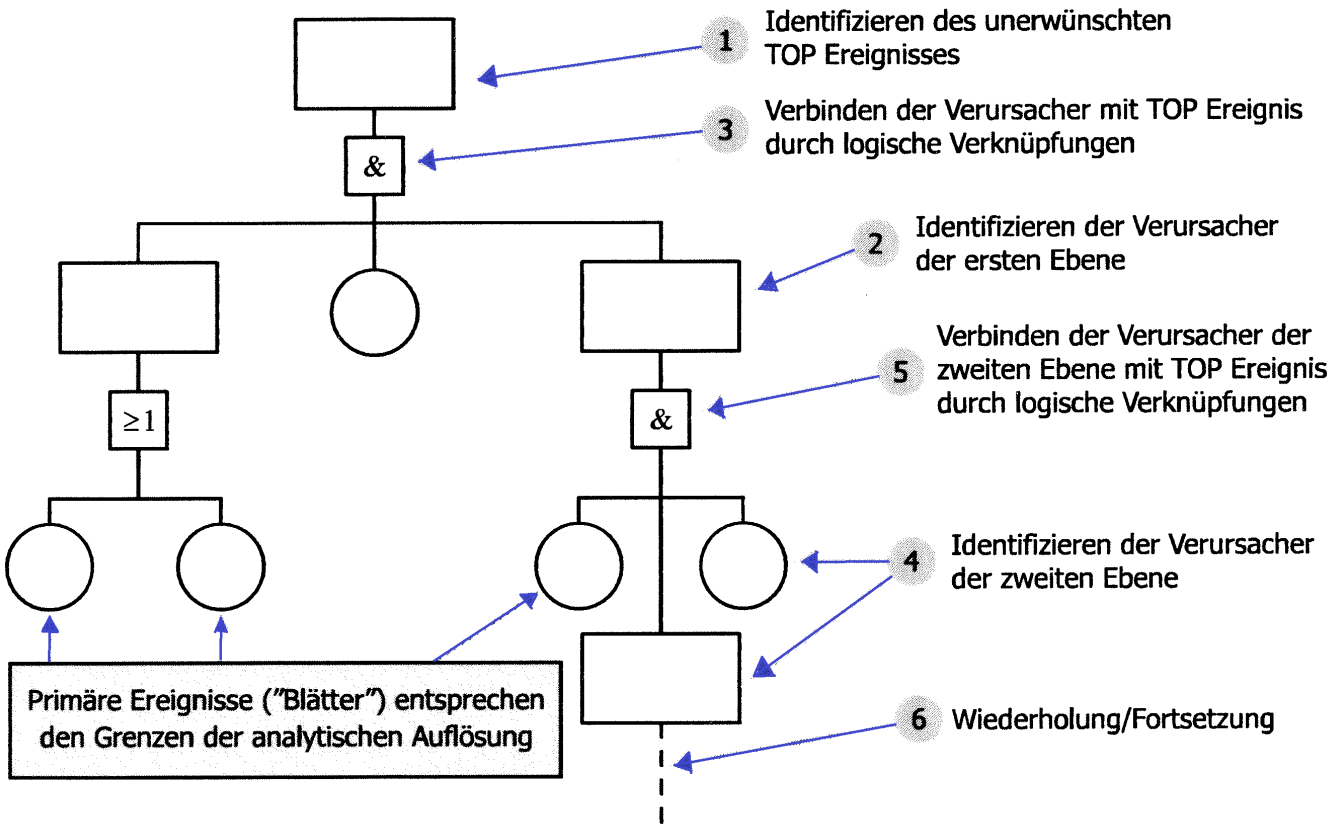
Die grafische Darstellung von Fehlerbäumen ist standardisiert. Sie ist angelehnt an die Diagramme für boolesche Schaltnetze (amerikanische Norm). Speziell für Software wurde die Software-Fehlerbaum-Analyse (Software Fault Tree Analysis, SFTA) entwickelt (Leveson, 1995; Lyu, 1996).

Konstruktion eines Fehlerbaumes

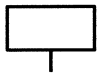
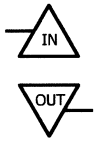
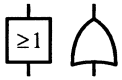
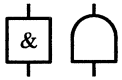
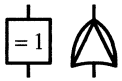
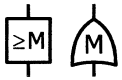
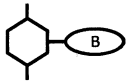
Bausteine:



Konstruktion eines Fehlerbaumes



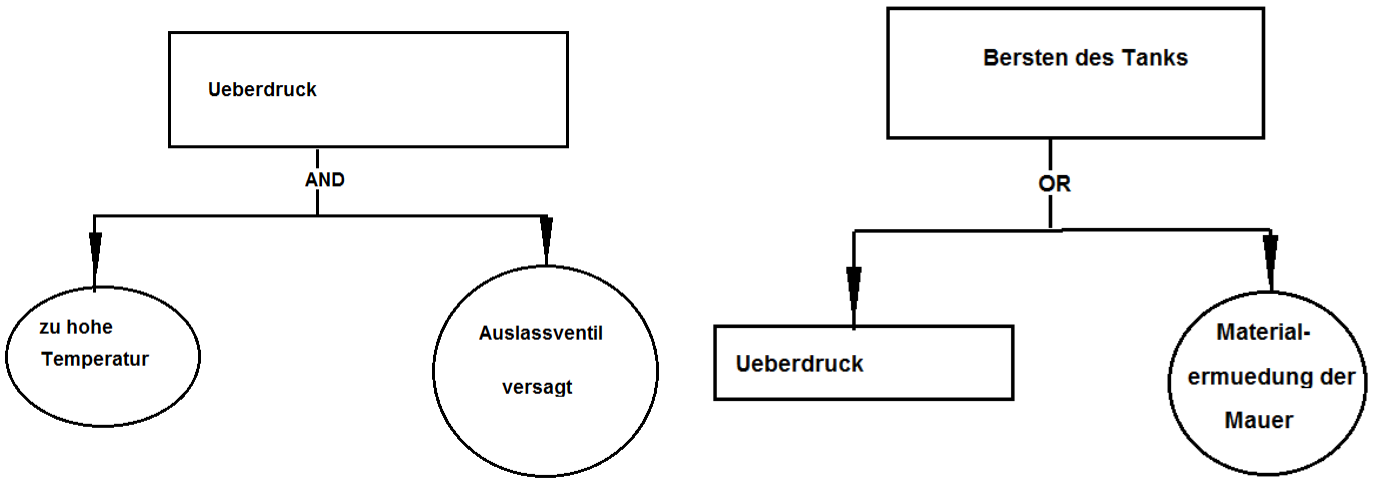
Graphische Symbole

Symbol(e)	Name	Bedeutung
	Top/Zwischen-ereignis	Ein Ereignis, das aus der Interaktion mehrerer Ereignisse durch eine logische Verknüpfung resultiert, u.a. das *unerwünschten Ereignis* (Top Event) und die *Zwischenereignisse* (Intermediate Events).
	Primäres Ereignis	Ein *Primäres Ereignis* (PE) repräsentiert den Ausfall einer Komponente oder einen Bedien-Fehler. Es wird nicht weiter aufgegliedert und stellt somit die feinste Auflösung des Fehlerbaums dar.
	Unentwickeltes Ereignis	Mit der Raute werden fehlerhafte Ereignisse symbolisiert, die nicht weiter aufgegliedert werden, da keine näheren Details bekannt sind oder die weitere Verfeinerung des Fehlerbaums nicht erwünscht ist.
	Transfer Symbole	Das Dreick wird benutzt, um (Teil-)Bäume zu verbinden. Das IN-Symbol signalisiert den Input von einem anderen Baum (in der Regel auf einer neuen Seite). Und das OUT-Symbol erscheint an der Position des Top Event und bedeutet, dass diese Stelle den Input für einen anderen Baum liefert.
	ODER-Verknüpfung	Bei der ODER-Verknüpfung tritt das Ausgangsereignis ein, sobald mindestens ein Eingangsereignis eingetreten ist. Die ODER-Verknüpfung kann beliebig viele Eingänge haben.
	UND-Verknüpfung	Der Ausgang der UND-Verknüpfung ist genau dann wahr, wenn alle seine Eingänge wahr sind. Die Anzahl der Eingänge ist beliebig.
	X-ODER-Verknüpfung	Die X-ODER-Verknüpfung ist wahr, wenn genau einer der Eingänge wahr ist. Die Anzahl der Eingänge ist beliebig.
	X-ODER-Verknüpfung	Die M-VON-N-Verknüpfung ist wahr, wenn mindestens M der N Eingänge wahr sind. Die Anzahl der Eingänge ist beliebig.
	Bedingte Verknüpfung	Das Ausgangsereignis der bedingten Verknüpfung tritt ein, wenn das Eingangsereignis eintritt und die Bedingung B erfüllt ist.

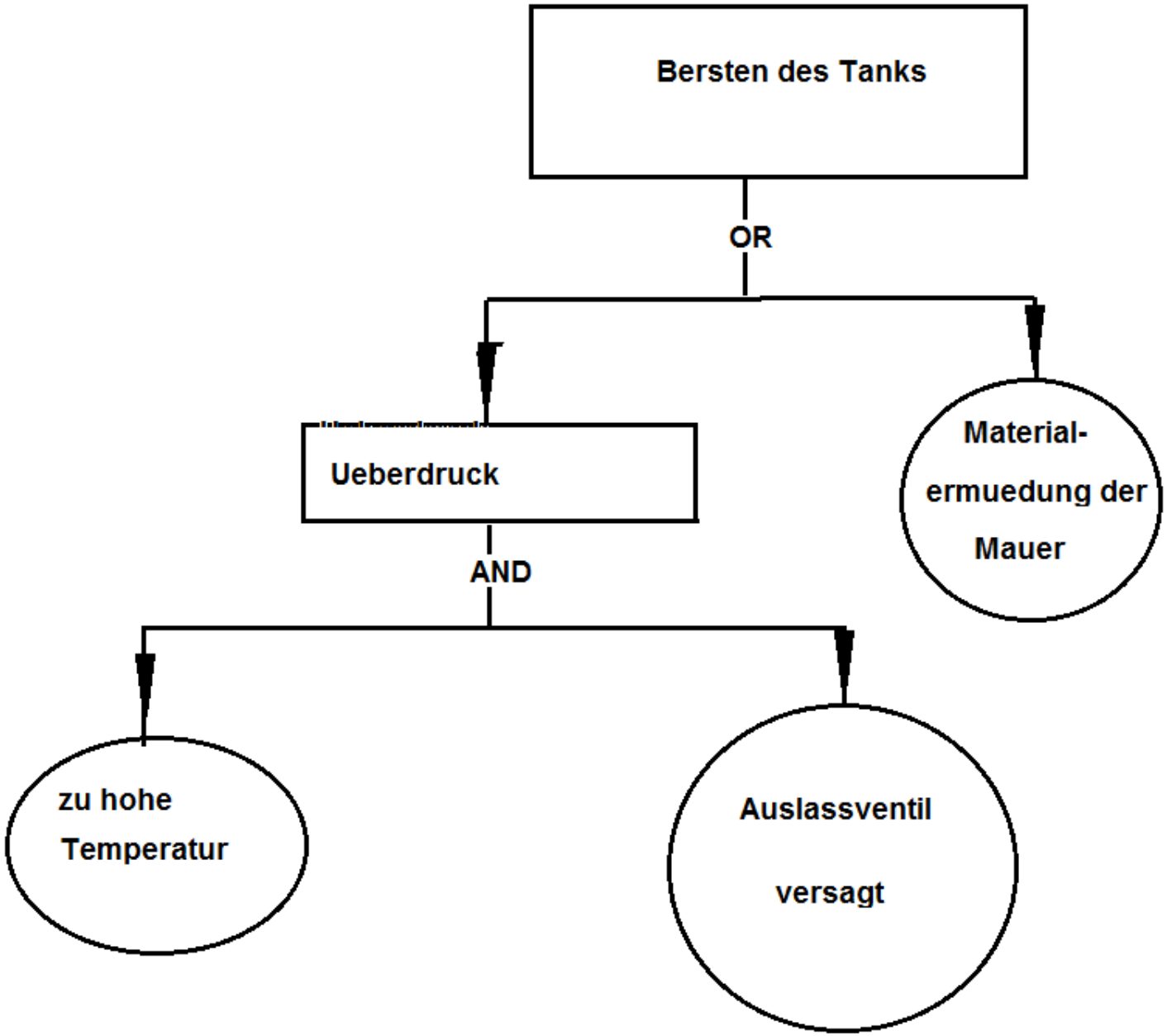
Beispiel 1.

Ein Wassertank kann durch Überdruck oder durch Materialermüdung der Mauer bersten. Materialermüdung ist in diesem Fall ein Basisereignis. Basisereignisse sind Ereignisse, über die man bereits genaue Kenntnisse und vor allem statistische Daten hat, und für die man nicht noch noch tiefer liegenden Ursachen suchen muss. Überdruck ensteht wenn einerseits das Ablassventil nicht funktioniert und andererseits der Kessel überhitzt wird.

Beispiel 1.


Ueberdruck
AND
zu hohe Temperatur
Auslassventil versagt
Bersten des Tanks
OR
Ueberdruck
Material-ermuedung der Mauer

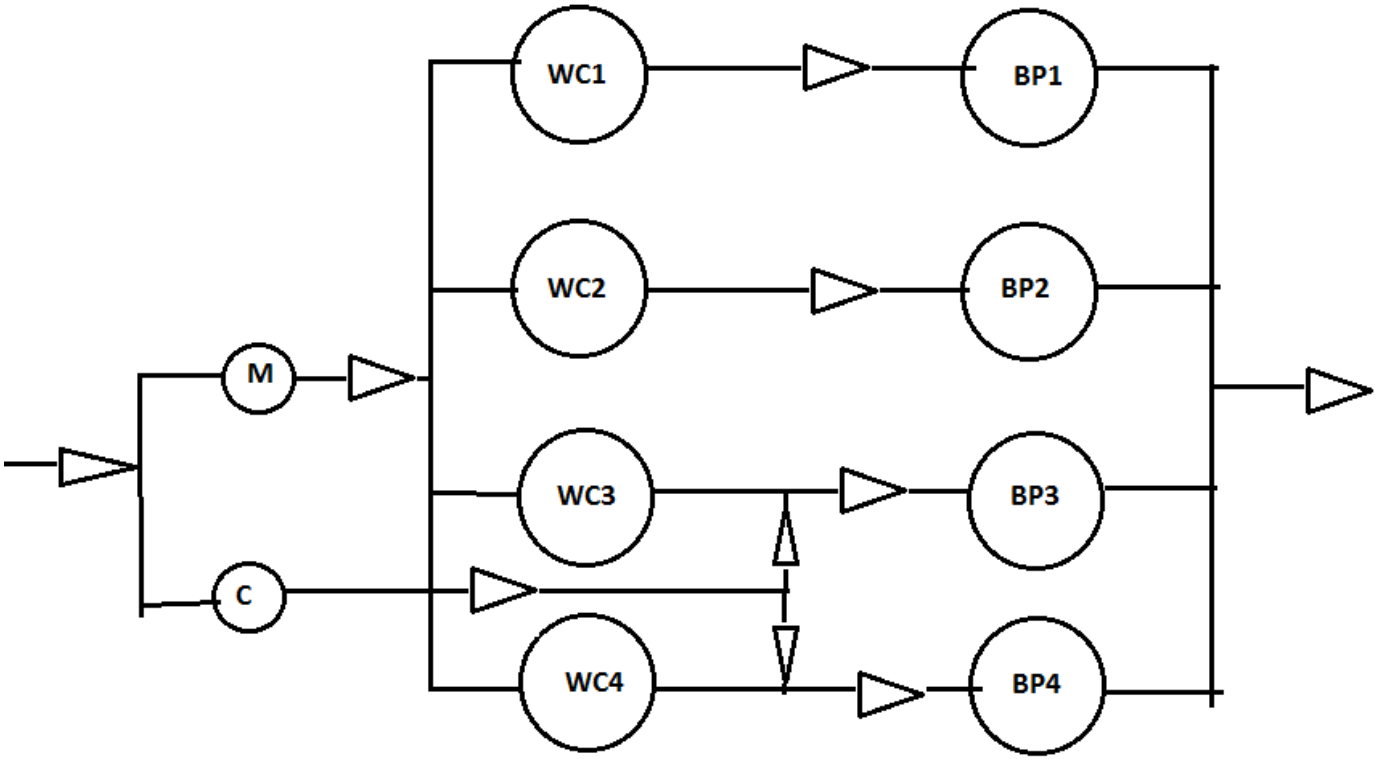
Beispiel 1.


Bersten des Tanks
OR
Ueberdruck
Material-
ermuedung der
Mauer
AND
zu hohe
Temperatur
Auslassventil
versagt

Beispiel 2. - Bremsen

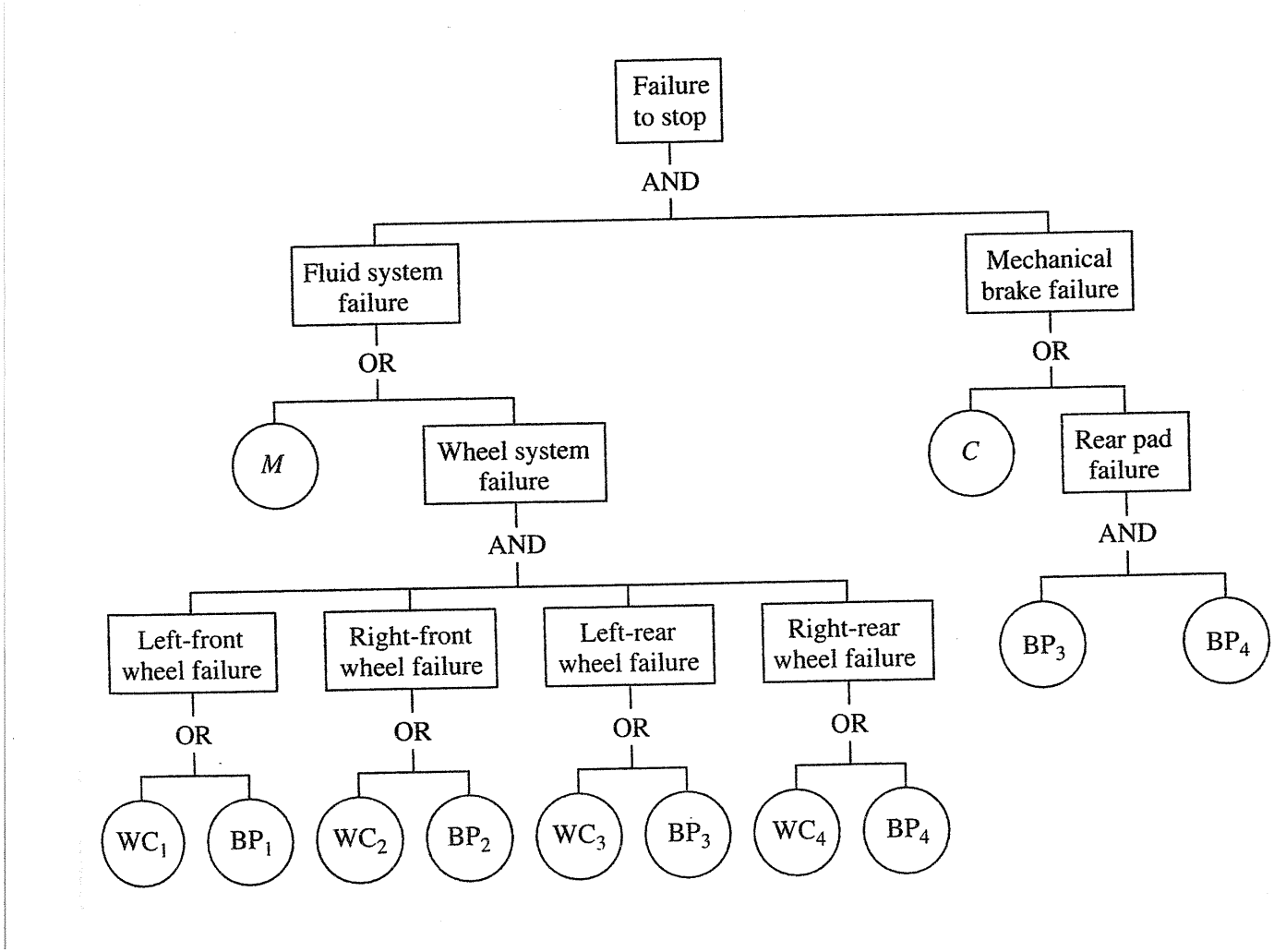
Das Bremssystem in einem Auto besteht aus einem hydraulischen System (Bremspedal) und aus einem mechanischen System (Handbremse). Beide Untersysteme müssen ausfallen, damit das Bremssystem versagt. Das hydraulische System fällt aus sobald der Hauptbremszylinder ausfällt (Ereignis M), einer der Blockierkraftregler am Rad ausfällt (Ereignisse $WC_1, \ldots, WC_4$), oder der Bremsbelag fällt aus (Ereignisse $BP_1, \ldots, BP_4$). Das mechanische Bremssystem fällt aus falls das Kabelsystem ausfällt (Ereignis C), oder bei beiden Hinterradbremsen der Bremsbelag ausfällt.

Beispiel von oben



Beispiel 2. - Bremsen

Zeichnen Sie den Fehlerbaumanalyse des obigen Beispiels



Ein weiteres Beispiel

Ein Sachverhalt und die dazugehörige Fehlerbaumanalyse.

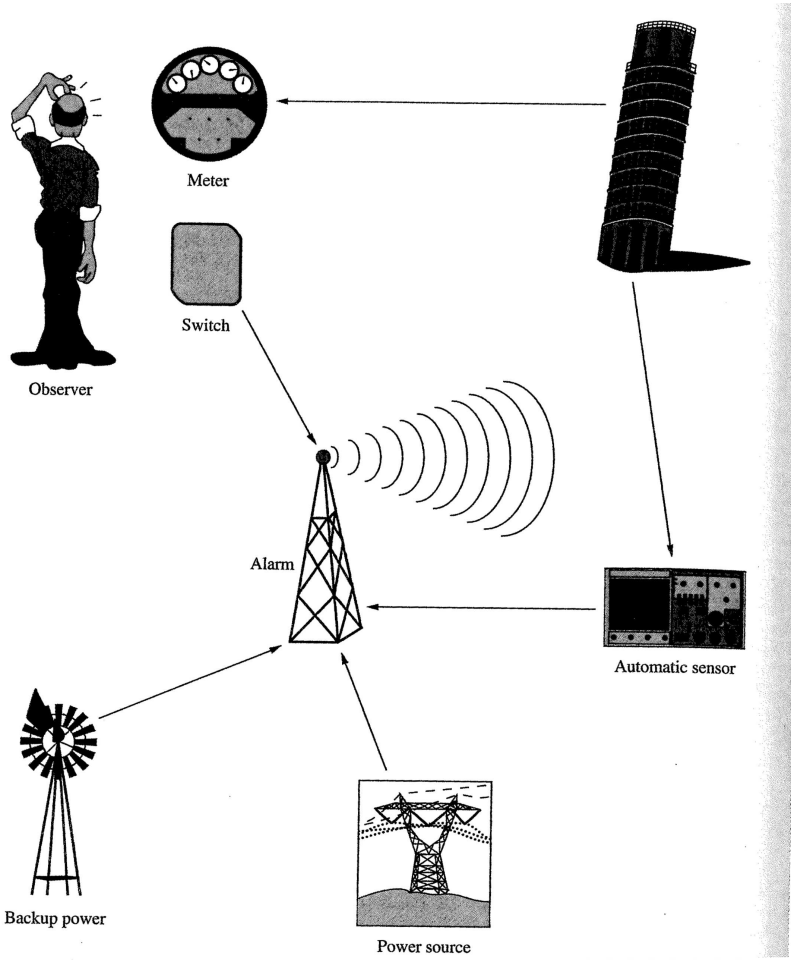
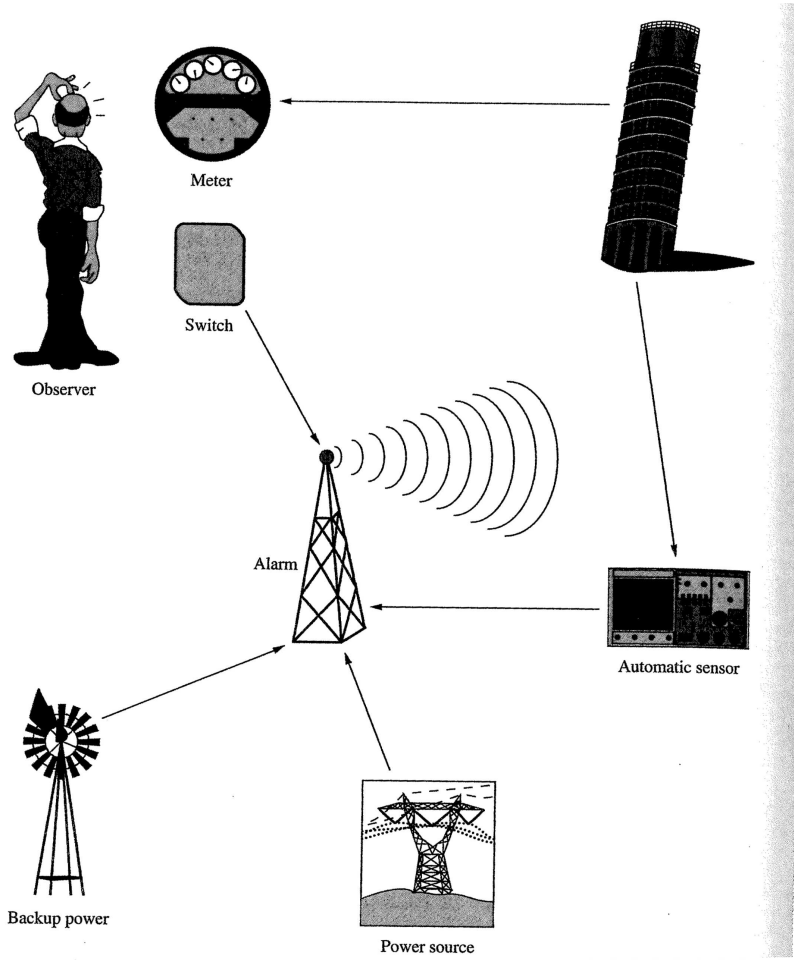


Abbildung :

Ein weiteres Beispiel

Ein Sachverhalt und die dazugehörige Fehlerbaumanalyse.



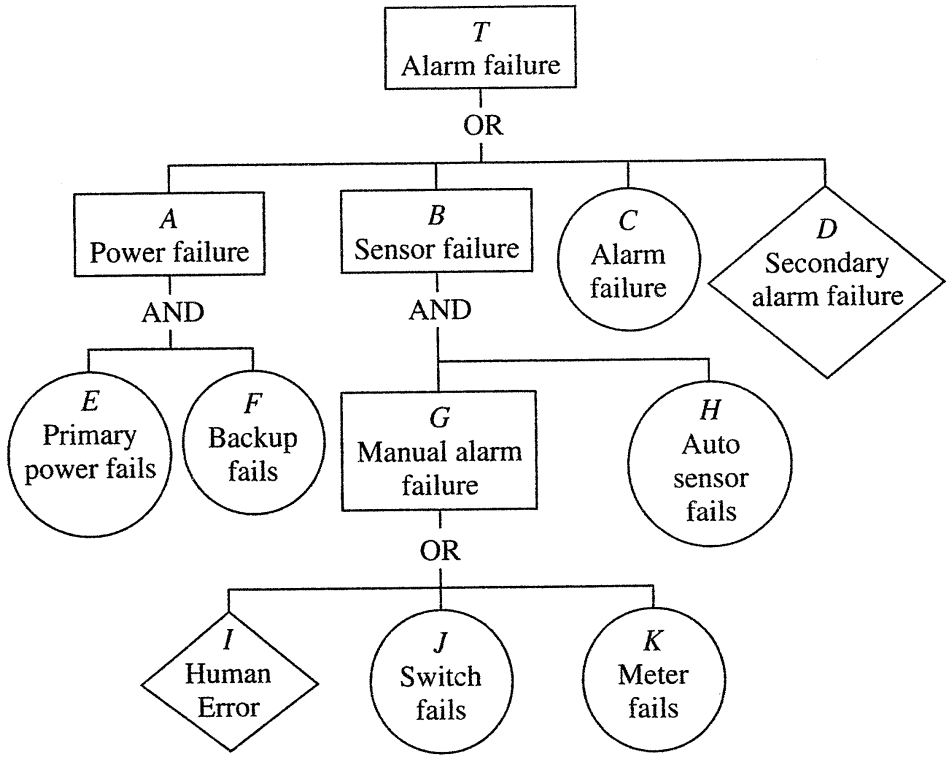


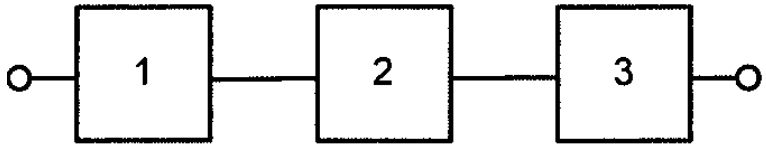
Abbildung :

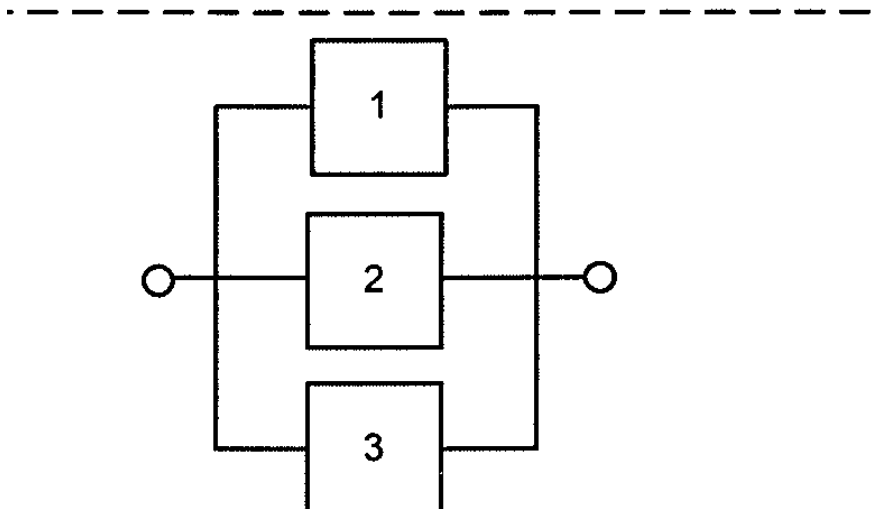
Reliability Blockdiagramme

- Während in der FTA eine Redundanz lediglich als UND-Verknüpfung dargestellt wird, erscheint im Reliability Blockdiagrammen (RBD) dies durch die parallele Anordnung markanter.
- Unterschied zwischen *ODER/UND*-Pfad ist hier also grafisch stärker hervorgehoben.
- Weniger *Elemente* werden benötigt; dadurch ist ein guter Einstieg zur Darstellung der Zusammenhänge möglich.
- Jedes Gate stellt eine entsprechende Zwischenebene oder eine Art Gruppe dar. Hierdurch ist von oben nach unten ein immer höherer Detaillierungsgrad gegeben.
- hierarchische Baumstruktur.

Reliability Blockdiagrammen

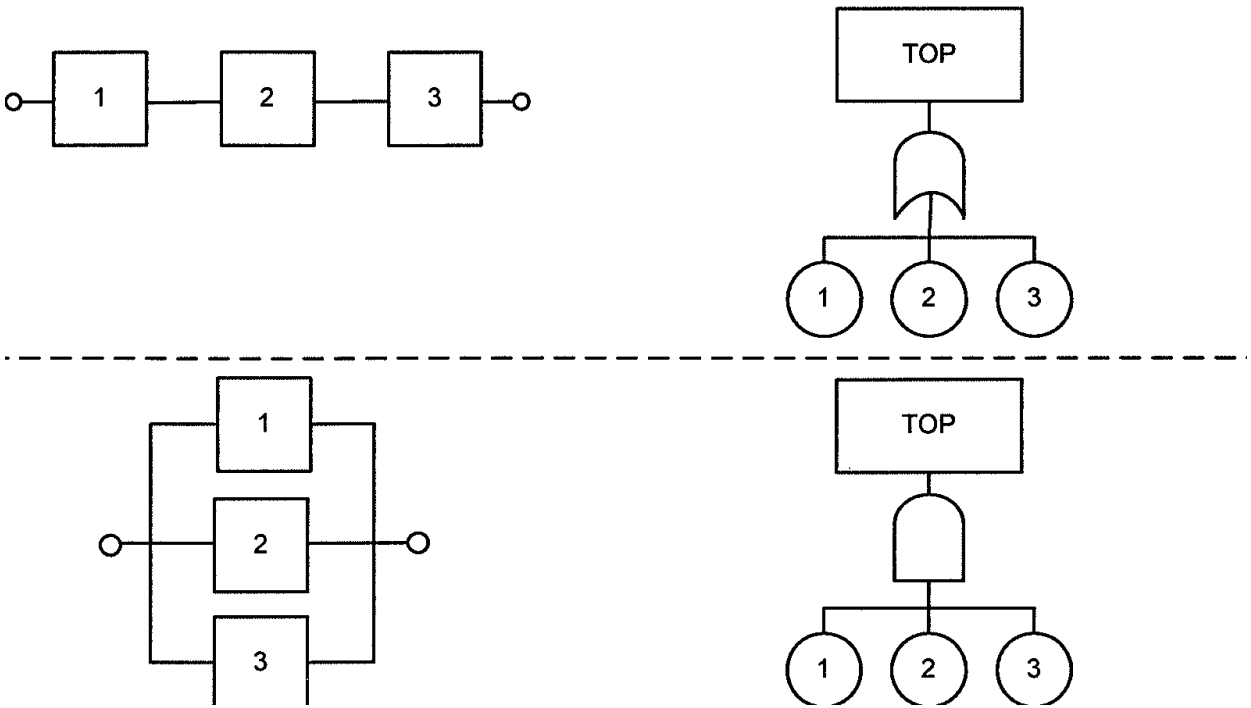
Reliability Block Diagramme und Fehlerbäume:





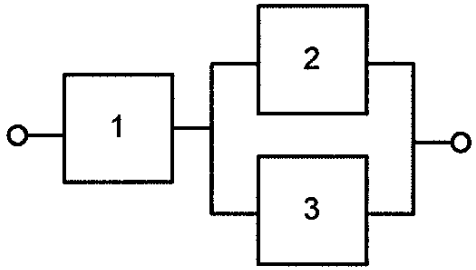
Reliability Blockdiagrammen

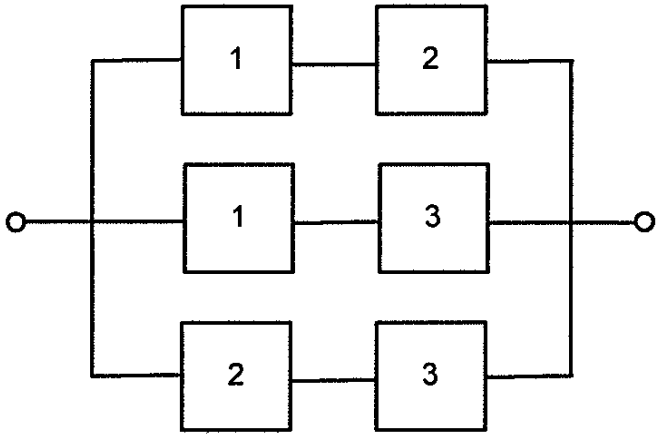
Reliability Block Diagramme und Fehlerbäume:



Reliability Blockdiagrammen

Reliability Block Diagramme und Fehlerbäume:





Reliability Blockdiagrammen

Reliability Block Diagramme und Fehlerbäume:

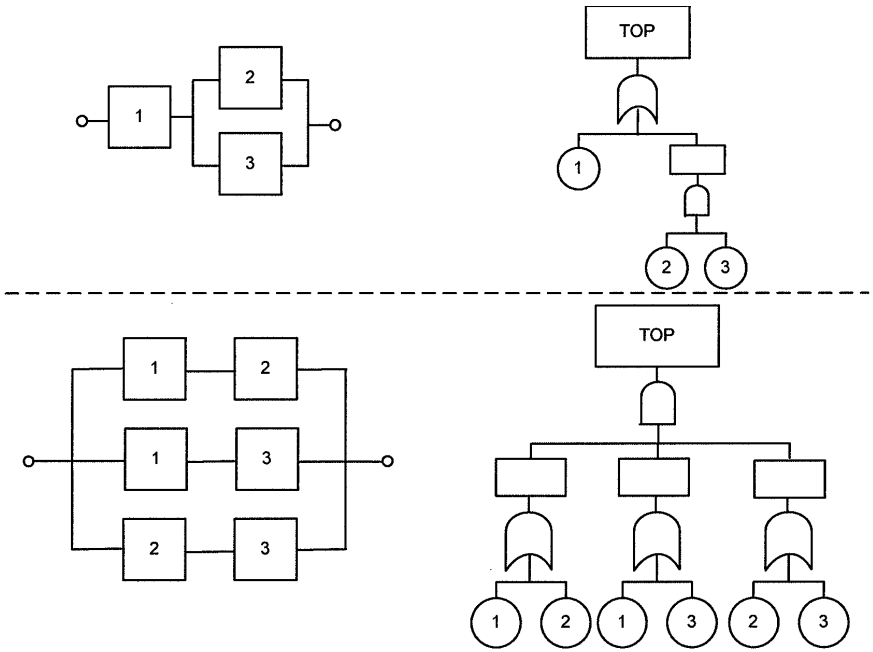


Abbildung :

Qualitative Analyse - *Minimal Cut Sets*

Definition

Eine Gruppe von Basis Ereignissen, deren Kombination bzw. gemeinsames Eintreten genügt, um das TOP Ereignis auszulösen heißt Cut Set. Kann man bei einen *Cut set* kein Basis Ereignis weglassen, so heißt dieser *minimal*.

Qualitative Analyse - *Minimal Cut Sets*

Definition

Eine Gruppe von Basis Ereignissen, deren Kombination bzw. gemeinsames Eintreten genügt, um das TOP Ereignis auszulösen heißt Cut Set. Kann man bei einen *Cut set* kein Basis Ereignis weglassen, so heißt dieser *minimal*.

- Anzahl der MCS heißt Ordnung;
- Wichtigste: MCSs erster Ordnung (Single Point Failure oder Singlet) und MCS zweiter Ordnung (Duplets).
- Wichtigste: Basis Ereignisse, die in vielen kleinen MSCs erscheint;

Qualitative Analyse - *Minimal Cut Sets*

Definition

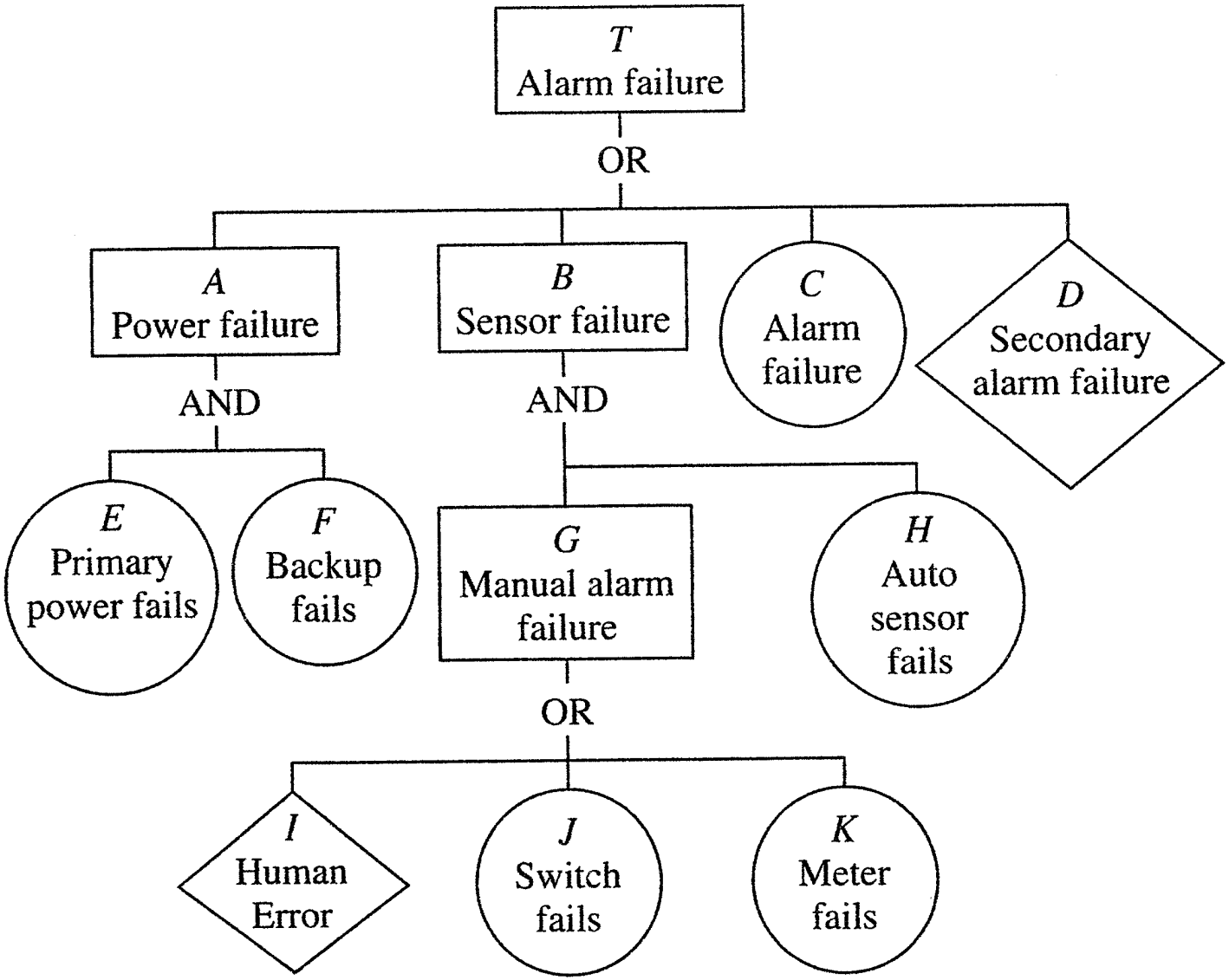
Eine Gruppe von Basis Ereignissen, deren Kombination bzw. gemeinsames Eintreten genügt, um das TOP Ereignis auszulösen heißt Cut Set. Kann man bei einen *Cut set* kein Basis Ereignis weglassen, so heißt dieser *minimal*.

Commen Causes

- Versorgungsausfall (z.B. von elektr. Spannung, Kühlwasser, Pneumatik, ...)
- Feuchtigkeit
- Korrosion
- mechanische Erschütterungen
- Staub
- Temperatur-Effekte (Frost/Überhitzung)
- elektromagnetische Störungen

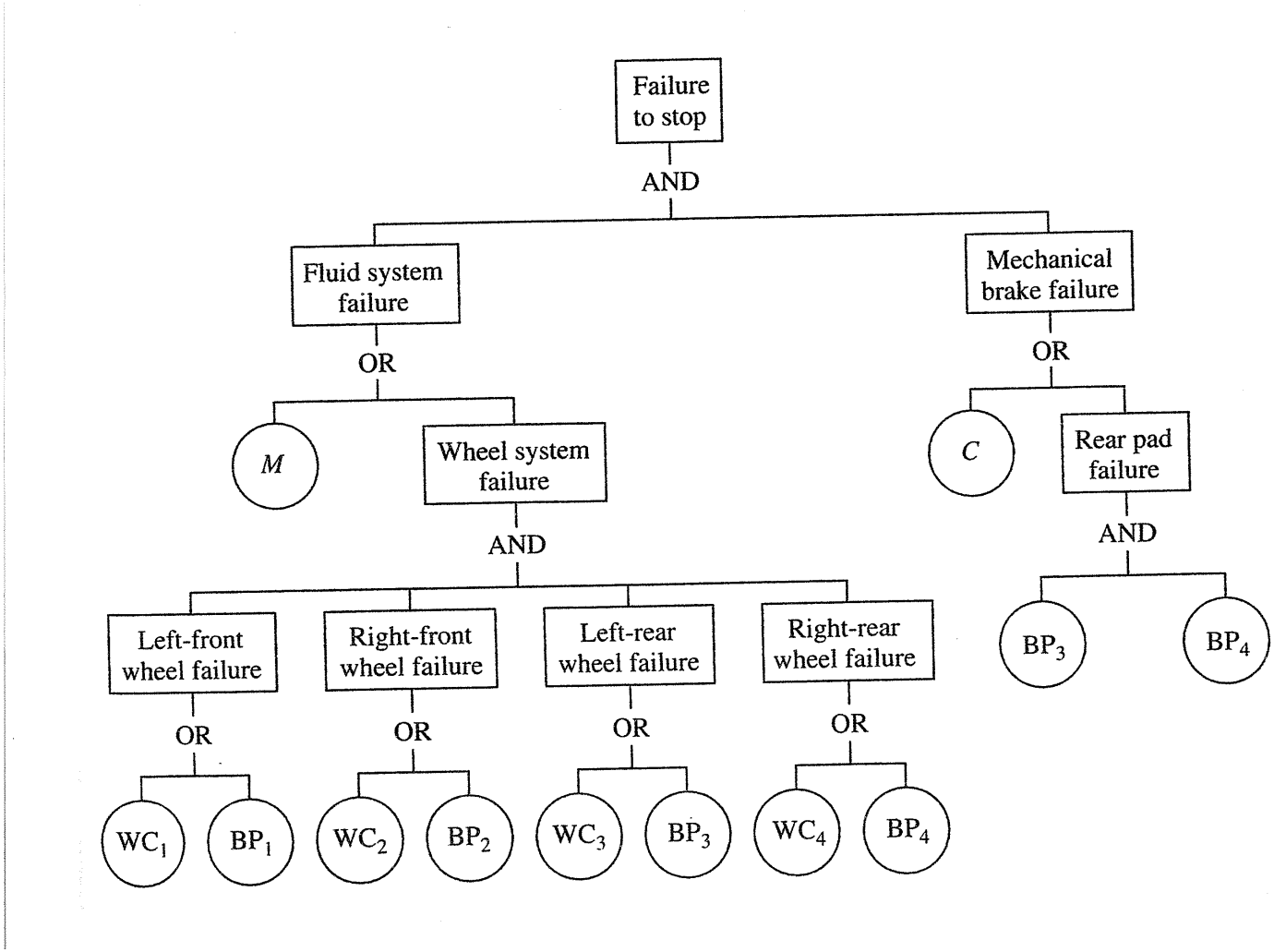
Ein Beispiel

Betrachten wir als Beispiel folgenden Fehlerbaum



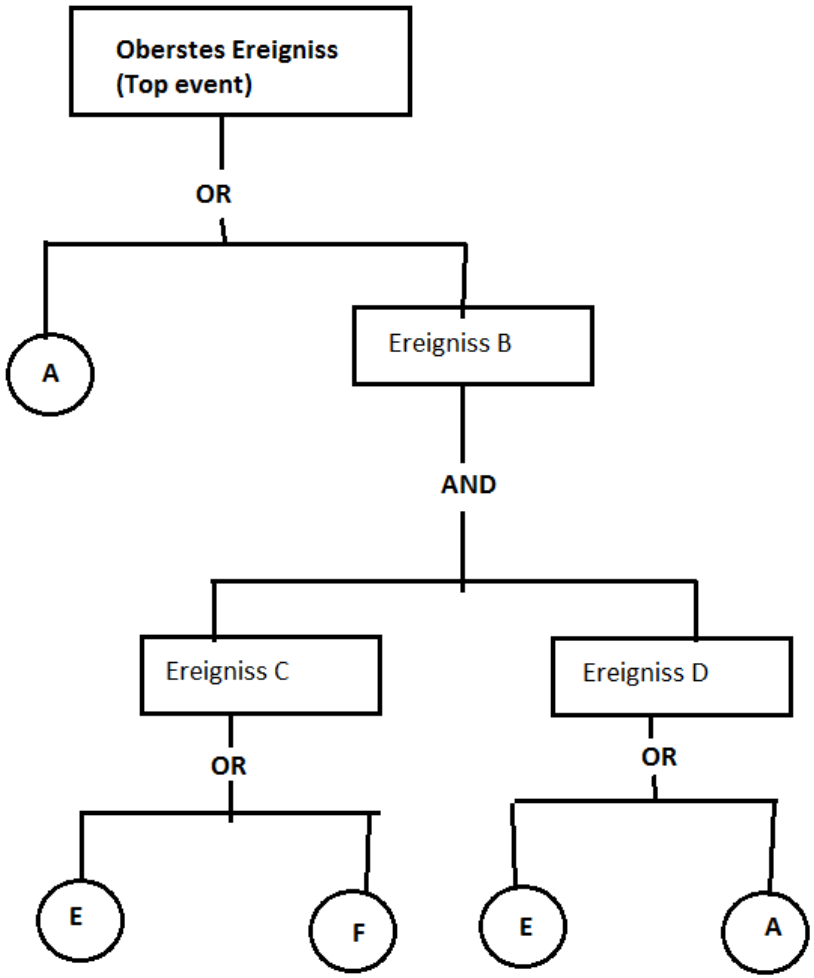
Qualitative Analyse - *Minimal Cut Sets*

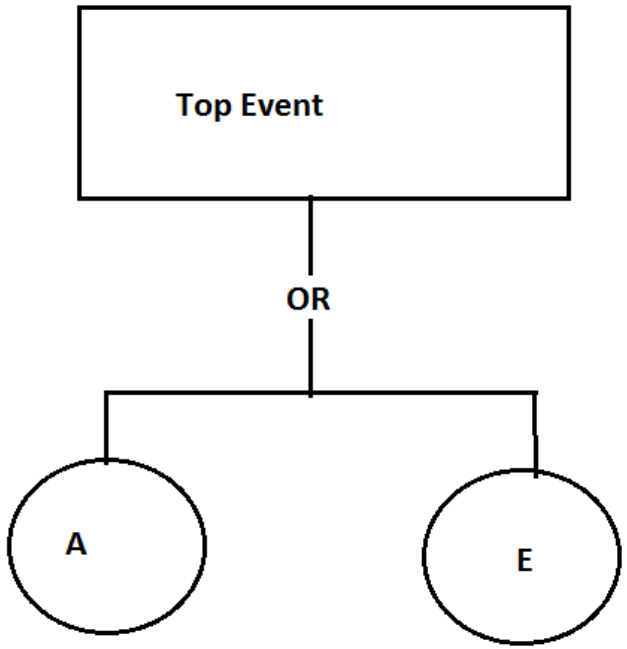
Finden Sie die MCS des Beispiels:



Auffinden von Redundanzen

Betrachtet man den linken Fehlerbaum in Bild unten, so sieht man bei genauer Analyse, dass das Basis Ereignis E nichts zum Ausgang beiträgt, also redundant ist. Der linke Fehlerbaum ist damit equivalent zum rechten Fehlerbaum in Bild unten.





Unter quanitativer Fehlerbaumanalyse versteht man die auf den Fehlerbäumen aufbauende quantitative Analyse: Den Basis Ereignissen werden Wahrscheinlichkeiten zugeordnet. Über die im Fehlerbaum festgelegten logischen Verknüpfungen wird die Wahrscheinlichkeit des Top-Ereignisses ermittelt.
Hier ist es wichtig, dass die Basis Ereignisse unabhängig und nach Möglichkeit disjunt sind.
Achtung:

- Ausfall-Rate - diese wird für Ereignisse angewendet und ist ein Maß für die Häufigkeit von Ausfällen eines Gerätes oder einer Komponente; sie wird üblicherweise in der Zahl der Ausfälle pro Jahr angegeben.
- Ausfall-Wahrscheinlichkeit - diese beschreibt die Wahrscheinlichkeit dafür, dass sich das Gerät in einem fehlerhaften Zustand befindet.

Mathematische Umsetzung

Der Wahrscheinlichkeitsraum $(\Omega, \mathcal{F}, \mathbb{P})$:

- Ω Wahrscheinlichkeitsraum,
- Ereignissystem $\mathcal{F} = \{$ Menge aller möglichen Teilmengen von $\Omega\}$;
- $\mathbb{P} : \mathcal{F} \to [0, 1]$ Wahrscheinlichkeitsmaß;

Rechenregeln:

- $A, B \in \mathcal{F}$: $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$;
- $A, B \in \mathcal{F}$, A, B sind unabhängig: $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$;
- $A, B \in \mathcal{F}$, A, B sind nicht unabhängig: $\mathbb{P}(A \cap B) = \mathbb{P}(A \mid B)\mathbb{P}(B)$;

Die Indikatorfunktion:

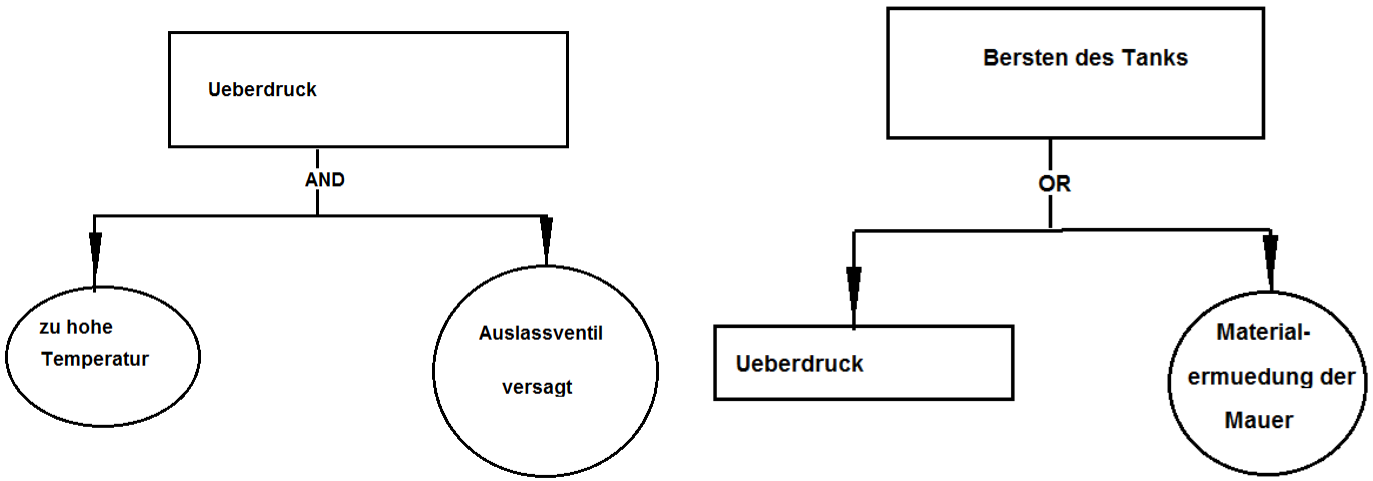
$$1_A(\omega) = \begin{cases} 1, & \text{falls } \omega \in A; \\ 0, & \text{falls } \omega \notin A. \end{cases}$$

- $A, B \in \mathcal{F}$: $\mathbb{E}[1_A] = \mathbb{P}(A)$;
- $A, B \in \mathcal{F}$, $\mathbb{E}[1_{A \cap B}] = \mathbb{E}1_A 1_B$;
- $A, B \in \mathcal{F}$, $\mathbb{E}[1_{A \cup B}] = \mathbb{E}1_A + \mathbb{E}1_B - \mathbb{E}1_A 1_B$;

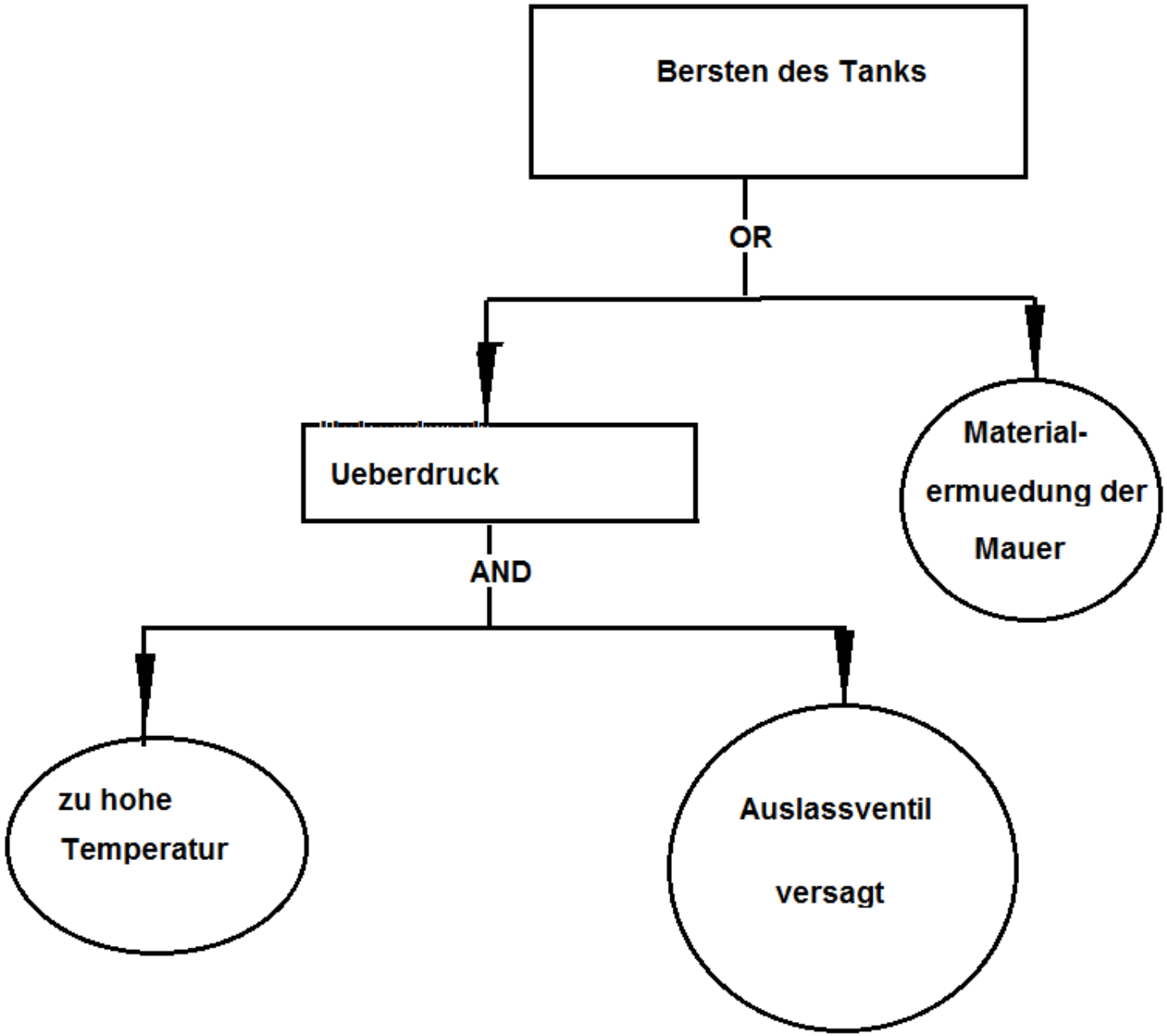
Beispiel 1.

Ein Wassertank kann durch Überdruck oder durch Materialermüdung der Mauer bersten. Materialermüdung ist in diesem Fall ein Basisereignis. Basisereignisse sind Ereignisse, über die man bereits genaue Kenntnisse und vor allem statistische Daten hat, und für die man nicht noch noch tiefer liegenden Ursachen suchen muss. Überdruck ensteht wenn einerseits das Ablassventil nicht funktioniert und andererseits der Kessel überhitzt wird.

Beispiel 1.


Ueberdruck
AND
zu hohe Temperatur
Auslassventil versagt
Bersten des Tanks
OR
Ueberdruck
Material-ermuedung der Mauer

Beispiel 1.


Bersten des Tanks
OR
Ueberdruck
Material-
ermuedung der
Mauer
AND
zu hohe
Temperatur
Auslassventil
versagt

Ein weiteres Beispiel

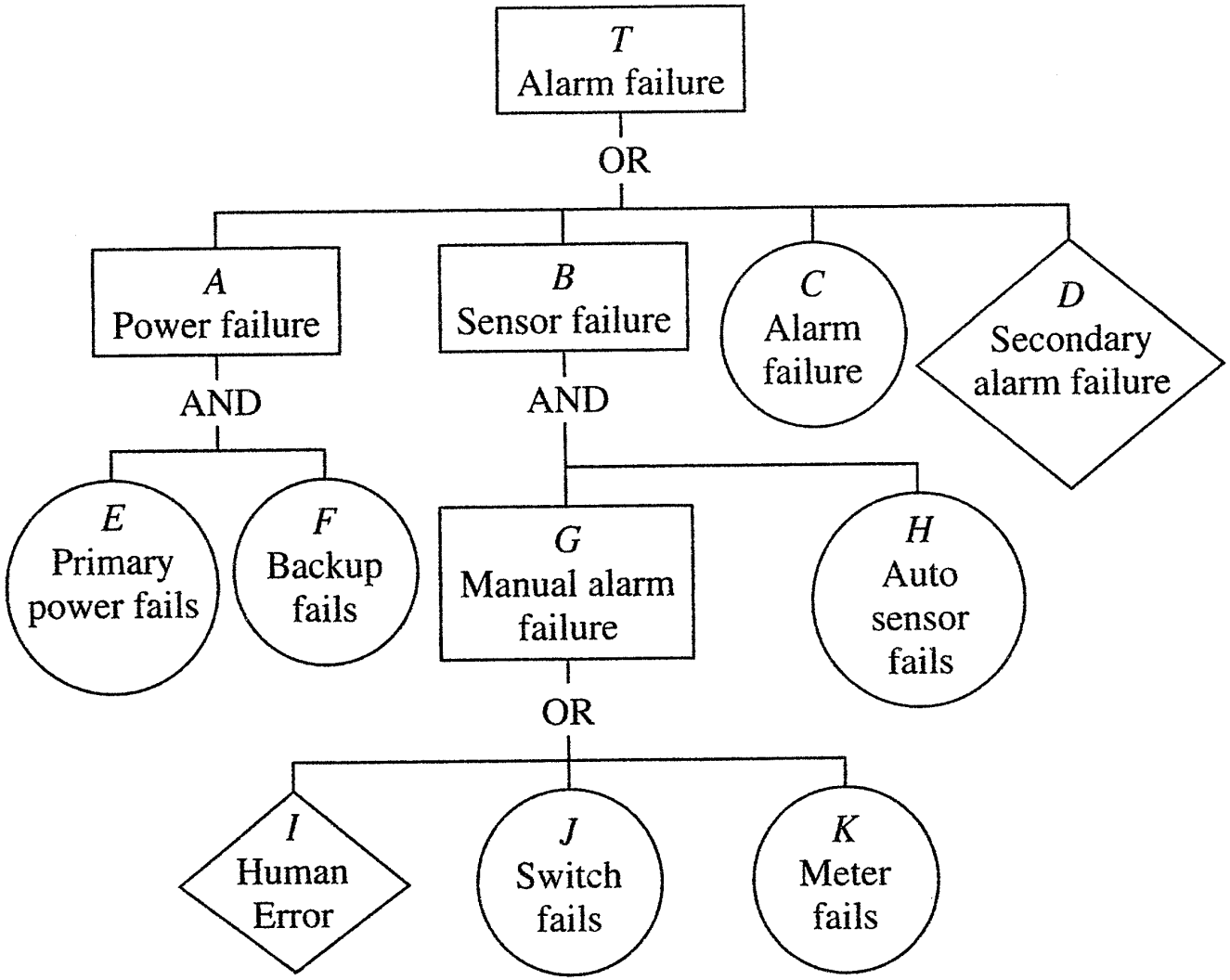


Abbildung :

Das Bremssystem