Aufarbeitung von Fließbildinformationen für die Zuverlässigkeitsanalyse technischer Anlagen und ihre Umsetzung in einen Fehlerbaum*

Ch. Becker, H.-G. Schecker
Universität Dortmund
Fachbereich Chemietechnik
Arbeitsgruppe Physikalisch-Chemische Verfahrenstechnik

Zusammenfassung

Die von den Betreibern technischer Anlagen zur Zuverlässigkeitsanalyse verwendeten Methoden werden in der Regel unter großem Personalaufwand manuell durchgeführt. In diesem Artikel wird ein Verfahren vorgestellt, mit dessen Hilfe die Anlagentopologie aus dem Verfahrensfließbild in ein Computerprogramm eingelesen wird. Zu den einzelnen Anlagenkomponenten existiert eine Bibliothek, in der komponentenspezifische Mini-Fehlerbäume gespeichert sind. Zusammen mit den Fließbildinformationen lassen sich daraus die gewünschten Fehlerbäume generieren.

1 Einleitung

Bei der Planung und beim Betrieb technischer Anlagen ist der Betreiber daran interessiert, aber auch gesetzlich dazu verpflichtet, die Zuverlässigkeit seiner Anlage zu prüfen und zu maximieren. Die hierfür in der Praxis verwendeten Analyseverfahren sind jedoch sehr zeitaufwendig und nur von Experten durchführbar. Nach [1] benötigt eine Bearbeitergruppe mit mehreren Mitgliedern beispielsweise zwei bis vier Wochen für die Ereignisablaufanalyse [2] eines komplexeren Systems und mehrere Wochen für eine Fehlerbaumanalyse [3, 4]. Um den Aufwand solcher Analysen sowohl zeitlich als auch bezüglich der Qualifikation der Bearbeiter zu reduzieren, können sie durch ein Computerprogramm automatisiert werden. Hierfür müssen die über die zu untersuchende Anlage verfügbaren Informationen in eine computerlesbare Form überführt werden. Von besonderem Interesse sind hierbei die topologischen Informationen, die die logischen Verknüpfungen der einzelnen Komponenten enthalten. Bei verfahrenstechnischen Anlagen sind diese Daten in Form eines Verfahrensfließbildes abgelegt.

Mit der im Computer abgelegten Anlagenstruktur und zusätzlichen Informationen über

*Diese Arbeit wird durch die Deutsche Forschungsgemeinschaft im Rahmen des Sonderforschungsbereiches 531 „Computational Intelligence“ unterstützt.

die eingesetzten Komponenten und den durch die Anlage realisierten Prozeß kann dann ein Generierungsalgorithmus zum Beispiel die verschiedenen Komponentenausfälle in Fehlerbäume umsetzen und graphisch darstellen.

2 Die Fehlerbaumanalyse

Die in der DIN 25424 [3, 4] genormte Fehlerbaumanalyse ist eine Methode, mit der sich die logischen Verknüpfungen von Komponenten- und Teilsystemausfällen, die zu einem unerwünschten Ereignis führen, ermitteln lassen. Die erhaltenen Ergebnisse lassen sich sowohl qualitativ als auch — mit den Methoden der Logik-Algebra — quantitativ analysieren. Man kann also die verschiedenen Ausfallkombinationen, die zum unerwünschten Ereignis führen, mitsamt ihren Eintrittshäufigkeiten ermitteln.
Die Vorgehensweise ist hierbei deduktiv. Für ein vorgegebenes Ereignis werden die Ursachen bestimmt. Zur graphischen Darstellung der logischen Zusammenhänge im Fehlerbaum wird eine Reihe von Bildzeichen verwendet. Eine Auswahl davon ist in Tabelle 1 wiedergegeben.

	Standardeingang		Übertragungseingang
Kommentar	Kommentar	≥ 1	ODER-Verknüpfung
&	UND-Verknüpfung	$= 1$	Negation

Tabelle 1: Die Symbole der DIN 25424

Aus der graphischen Darstellung des Baumes läßt sich direkt die Menge der Minimalschnitte (engl.: minimal cuts) ermitteln, die jeweils zum TOP-Ereignis führen. Unter einem Minimalschnitt versteht man hierbei eine Ausfallkombination, die keine andere Ausfallkombination enthält und bei der die Instandsetzung einer der ausgefallenen Komponenten das System wieder in den Arbeitszustand überführt. Aus der Analyse dieser Minimalschnitte lassen sich die Komponenten ermitteln, die an vielen verschiedenen Ausfallszenarien beteiligt sind. Um den Einfluß eines Anlagenteils auf die Zuverlässigkeit der Gesamtanlage beurteilen zu können, muß die Eintrittshäufigkeit der einzelnen Szenarien ermittelt werden. Hierfür werden die Verknüpfungsoperatoren der Logik-Algebra verwendet.

3 Extraktion der Fließbildinformationen

Die einzelnen Komponenten einer verfahrenstechnischen Anlage sind über Ein- und Ausgänge miteinander verknüpft. Diese Verknüpfungspunkte kann man in drei Arten gliedern:

1. Stoffstromein- und -ausgänge

2. Informationsein- und -ausgänge

3. Energieflußein- und -ausgänge

Die verschiedenen Prozeßmedien fließen über die Stoffstromein- und -ausgänge durch die Anlage. Zwischen zwei Apparate bzw. zwischen einen Apparat und ein Ventil ist in der Regel eine Rohrleitung als Verbindung geschaltet. Der Informationsein- und Ausgänge werden mit Funktionen der MSR-Technik — hauptsächlich Meßwerten und Regelungsinformationen — belegt.
Unter Energieaustausch ist in diesem Zusammenhang sowohl der Wärmeübergang in dafür vorgesehenen Komponenten (Wärmeübertrager, Kühlschlangen, ...) als auch der Wärmeeintrag durch bewegte Teile (Rührer, ...) und die Versorgung der Komponenten mit Betriebsmitteln (Strom, Druckluft, ...) zu verstehen. Die Wärmeproduktion aufgrund einer chemischen Reaktion kann nicht über die Topologieinformationen erfaßt werden, sie muß als prozeßspezifische Eigenschaft über die Prozeßbeschreibung in die Modellierung gelangen. Über eine eindeutige Numerierung und die Koordinaten der Ein- und Ausgänge kann die Anlagentopologie aus dem Fließbild in den Computer übertragen werden. Ein derart aufgearbeitetes Fließbildobjekt ist in Abbildung 1 dargestellt. Die Numerierung der Verknüpfungspunkte wird bei der Fehlerbaumgenerierung für die korrekte Zuordnung der Komponentenausfälle benötigt.

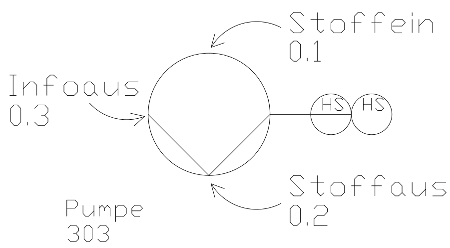

Abbildung 1: Fließbildobjekt Pumpe

4 Komponentenbezogene Teilbäume

Der Ausfall einer Anlagenkomponente kann entweder rein stochastischer Natur oder in dem nicht bestimmungsgemäßen Einsatz der Komponente begründet sein. Ein solcher Ausfall — in der Norm wird hier noch zwischen Sekundärausfällen und kommandierten Ausfällen unterschieden — läßt sich direkt mit mindestens einem Verknüpfungspunkt der

Komponente in Beziehung bringen. An diesem hängt eine andere Komponente, die eventuell für den Ausfall verantwortlich ist.
Nach Taylor [5] ist es möglich, für jede Anlagenkomponente einen Satz an Mini-Fehlerbäumen zu erstellen, die sich dann je nach TOP-Ereignis (Das TOP-Ereignis ist das erste unerwünschte Ereignis, die Wurzel des Fehlerbaums) zum Gesamtbaum kombinieren lassen. Für die verschiedenen Komponenten können sich hierbei bis zu 60 Mini-Fehlerbäume ergeben.
Bei der Modellierung der einzelnen Teilbäume einer Komponente wird zuerst durch eine detaillierte Analyse eine Liste der Ausfälle der Komponente erstellt. Hierfür kann z.B. das PAAG-Verfahren [6] verwendet werden. Für jeden der gefundenen Ausfälle wird dann ein Mini-Fehlerbaum erstellt, der aus den Primärausfällen der Komponente und Übertragungseingängen besteht. Jeder Übertragungseingang ist mit einem Verknüpfungspunkt der Komponente verbunden. An diese Punkte können später bei der Baumgenerierung die Ausfälle der benachbarten Fließbildobjekte angehängt werden. Abbildung 2 zeigt beispielhaft einen Mini-Fehlerbaum für eine Pumpe.

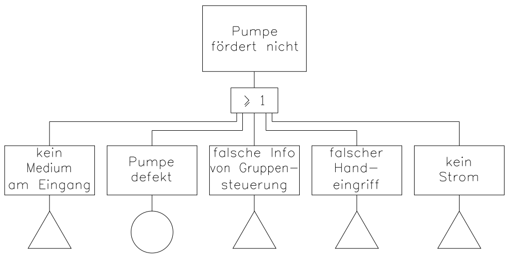

Abbildung 2: Mini-Fehlerbaum einer Pumpe

5 Generierung des Fehlerbaums

Hat man für jede Anlagenkomponente die Mini-Fehlerbäume erstellt, kann man mit den Fließbildinformationen den gewünschten Fehlerbaum erzeugen. Hierzu wählt man zuerst die ausgefallene Komponente und einen ihrer vormodellierten Ausfälle als TOP-Ereignis aus. Jedem der Übertragungseingänge des Mini-Fehlerbaums ist ein Verknüpfungspunkt und somit ein anderes Anlagenobjekt zugeordnet. Um den für den für den Übertragungseingang richtigen Mini-Fehlerbaum der zweiten Komponente zu identifizieren, muss neben der Zuordnung der Mini-Fehlerbäume zu den Verknüpfungsstellen eine weitere Klassifizierung erfolgen.
Hierfür werden Leitworte verwendet, die denen des PAAG-Verfahrens [6] ähneln, da die Sicherheitsingenieure in der chemischen Industrie in der Regel mit dieser Analysemethode vertraut sind. Die Leitworte enthalten zum einen den Prozeßparameter, der dem Ausfall zugeordnet wird und zum anderen eine Angabe darüber, wie der Parameter von seinem Sollwert abweicht. Diese Angabe wird — an das PAAG-Verfahren angelehnt — durch einen Wert aus der folgenden Liste belegt:

- zu hoch
- zu niedrig
- kein
- falsch

Die aus der Verknüpfung dieser Angabe mit dem Prozeßparameter entstehenden Leitworte sind vom Anwender leicht zu verstehen und ermöglichen die Konstruktion des Baumes. Im folgenden Kapitel soll diese Vorgehensweise an einem kurzen Beispiel erläutert werden.

6 Beispiel

Ein einfaches Regelventil besitzt fünf Verknüpfungspunkte in der Anlage. Neben dem Stoffstromein- und -ausgang sind dies die Leitung mit dem Regelungssignal, der Handeingriff sowie die Stromversorgung. Die möglichen Ausfälle eines solchen Ventils sind in der folgenden Tabelle 2 mit den zugehörigen Verknüpfungspunkten aufgeführt:

Nr.	Bezeichnung	Verknüpfungspunkt	Leitworte
1	zuwenig Medium am Ausgang	Stoffausgang	Durchfluß zu niedrig
2	zuwenig Medienfluß am Eingang	Stoffeingang	Durchfluß zu niedrig
3	zuviel Medium am Ausgang	Stoffausgang	Durchfluß zu hoch
4	Druck zu hoch am Ausgang	Stoffausgang	Druck zu hoch
5	Druck zu niedrig am Ausgang	Stoffausgang	Druck zu niedrig
6	Druck zu hoch am Eingang	Stoffeingang	Druck zu hoch
7	Druck zu niedrig am Eingang	Stoffeingang	Druck zu niedrig

Tabelle 2: Mögliche Ausfälle eines Regelventils

Zu jedem dieser Ausfälle kann ein Mini-Fehlerbaum generiert werden. Die sieben Bäume für das Ventil in Abbildung 3 sind aus [7] entnommen.
Für die Primärereignisse kann direkt ein Wert für die Ausfallhäufigkeit eingegeben werden. Die Übertragungseingänge sind mit den Verknüpfungspunkten verbunden. Für den ersten Mini-Fehlerbaum aus Abbildung 3 sind diese Beziehungen beispielhaft in Tabelle 3 mit den zugehörigen Leitworten aufgeführt:

Übertragungseingang	Verknüpfungspunkt	Leitworte
zuwenig Medium am Eingang	Stoffeingang	Durchfluß zu niedrig
kein Strom	Energieeingang	kein Strom
falsches Regelungssignal	Informationseingang	Information falsch

Tabelle 3: Verknüpfungspunkt–Ausfall-Beziehung für einen Mini-Fehlerbaum

Es ist zu beachten, daß die Leitworte in Tabelle 2 dazu dienen, den richtigen Ausfall für ein übergeordnetes Ereignis zu finden, während die Leitworte in Tabelle 3 mit den Ausfällen

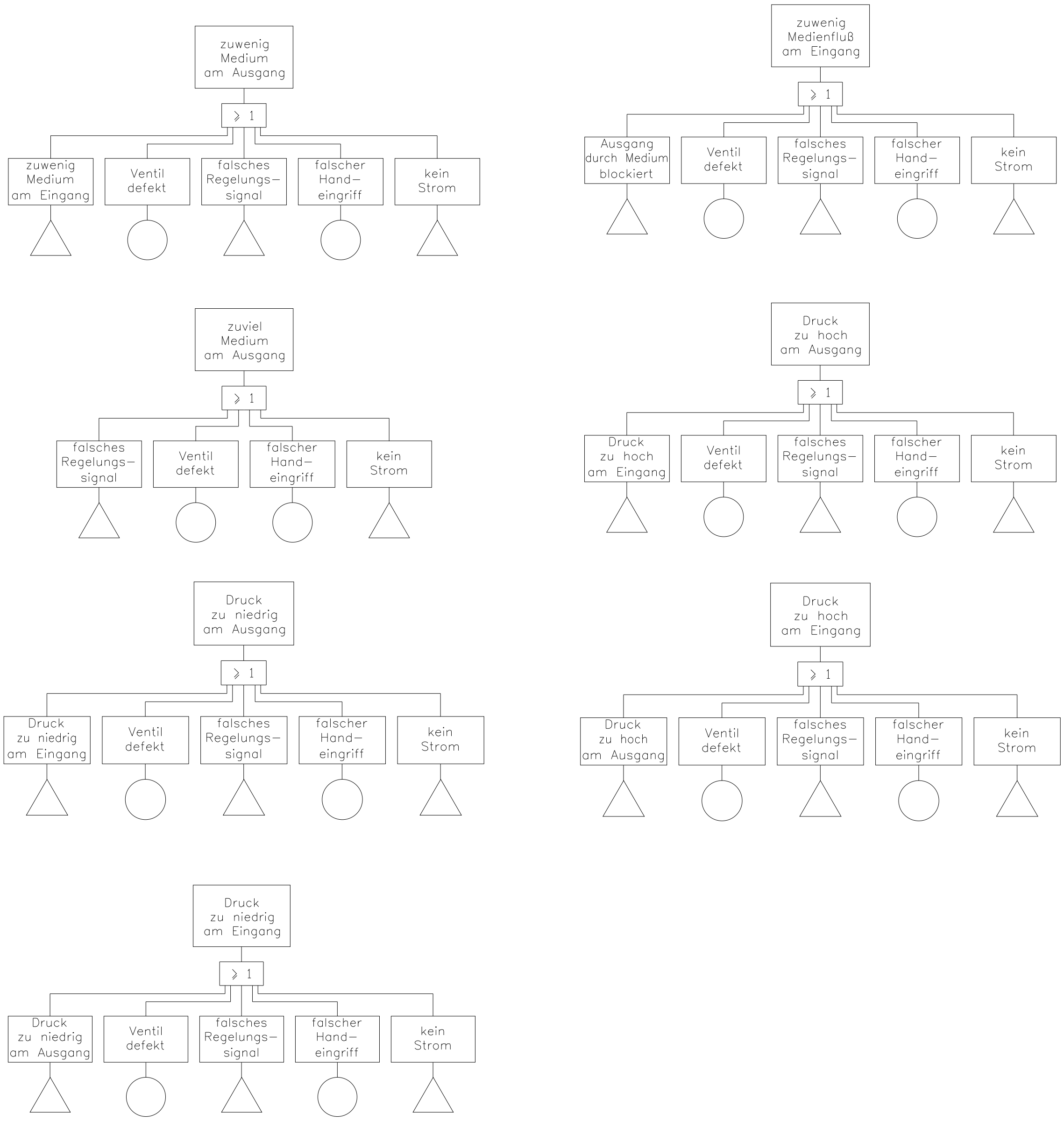

Abbildung 3: Mini-Fehlerbäume eines Regelventils

der Komponenten, die mit den Verknüpfungspunkten verbunden sind, verglichen werden. Wird bei der Generierung des Fehlerbaums eine Instanz des Ventils in den Baum eingebunden, so wird mit dem Leitwort des Übertragungseingangs der übergeordneten Komponente der richtige Ausfall des Ventils identifiziert. Der entsprechende Mini-Fehlerbaum wird an den Gesamtbaum angehängt. Bei den mit den Verknüpfungspunkten verbundenen Komponenten werden anhand der Leitworte aus Tabelle 3 dann die richtigen Ausfälle gefunden. Sind z.B. der Informationseingang über eine Informationsleitung mit einem Regler und der Stoffeingang über eine Rohrleitung mit einer Pumpe verbunden, ergibt sich daraus der Fehlerbaum in Abbildung 4.

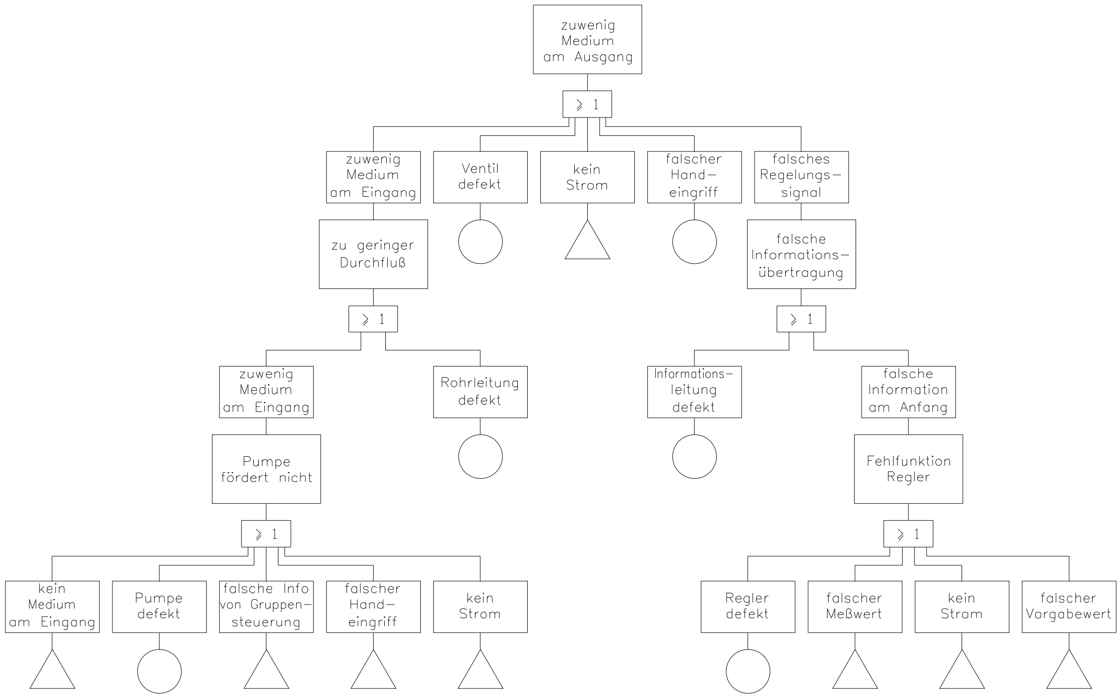

Abbildung 4: Ausschnitt aus einem generierten Fehlerbaums

7 Fazit

In dieser Arbeit wurde ein Verfahren vorgestellt, mit dem man aus den topologischen Fließbildinformationen einer verfahrenstechnischen Anlage und einer Bibliothek mit komponentenspezifischen Mini-Fehlerbäumen einen Fehlerbaum für das Gesamtsystem erstellen kann. Dieser Algorithmus wird im Rahmen eines Forschungsprojektes in einem Programm verwendet, das die Zuverlässigkeit eines technischen Systems bewertet und optimiert. Die Fehlerbaumanalyse dient hierbei als Basis, anhand der sich die Gütefunktion des Systems für die Optimierung aufstellen läßt.

Literatur

[1] J. Flanz, U. Hesener und H.-G. Schecker. Vergleich quantitativer Verfahren zur Risikoabschätzung verfahrenstechnischer Anlagen. Interner Bericht, Studie für das Landesumweltamt Nordrhein-Westfalen, 1993.

[2] DIN 25419: Ereignisablaufanalyse, November 1985. Beuth Verlag Berlin.

[3] DIN 25424 T1: Fehlerbaumanalyse, September 1981. Beuth Verlag Berlin.

[4] DIN 25424 T2: Fehlerbaumanalyse, April 1990. Beuth Verlag Berlin.

[5] J. Taylor. An algorithm for fault-tree construction. *IEEE Trans. Reliability*, **R31**(2), June 1982.

[6] K. Bartels, H. Hoffmann und L. Rossinelli. *Risikobegrenzung in der Chemie PAAG-Verfahren.* ISSA Prevention Series No. 2002. IVSS Internationale Vereinigung für Soziale Sicherheit, 1990.

[7] C. Becker. Entwicklung einer Methodik zur automatischen Generierung von Fehlerbäumen am Beispiel von Rührkesselreaktoren. Diplomarbeit, Universität Dortmund, 1997.