

# Chemische Prozesse in Mehrproduktanlagen sicher fahren



## Topic 1: Gefahrenpotentiale lauern überall

- Die unheilvolle Auswirkung des komplexen Zusammenspiels von Mehrproduktanlage, Prozessstufe und Organisation auf die chemische Prozesssicherheit
- Gefahrenpotential- und Risikoanalyse im Mehrproduktbetrieb

---

## INHALT

1	Allgemeine Erkenntnisse	1
1.1	Einleitung	1
1.2	Die Mehrproduktanlage (MPA)	1
1.3	Wie gefährlich ist der Mehrproduktbetrieb?	8
1.4	Ausblick: Anlagensicherheit bei der MPA	14
2	Gefahrenpotential- und Risikoanalyse	15
2.1	Einleitende Gedanken	15
2.2	Betriebszustände bei der MPA	17
2.3	Systematisches Vorgehen bei der Risikoanalyse	20
2.4	Klassifizierung von chemischen Prozessstufen	21
2.5	Risikobeurteilung mit modularen Fehlerbäumen	28
3	Fallbeispiel	33
3.1	Einleitung	33
3.2	Beschreibung der Prozessstufe	33
3.3	Sicherheitstechnische Untersuchung der Reaktionsstufe	36
3.4	Beurteilung der Reaktionsstufe	38
3.5	Festlegen der Kriterien für die Anlage, mit der es vielleicht möglich ist, ereignisverhindernde Massnahmen einzuleiten	37
3.6	Gefahrensuche	39
3.7	Gefahrenbeurteilung und Massnahmenplanung	39
3.8	Risikoanalyse der Sulfonierungs-Stufe	42
3.9	Auswertung der Fehlerbaumanalyse	44
3.10	Beurteilung des Risikos der Sulfonierungs-Stufe	48
4	Schlusswort	47

## Herausgeber

SCHNYDER Sicherheit in der Chemie AG  
Gewerbehäus Oederlin  
Landstrasse 2 b  
CH-5415 Rieden/Nussbaumen Switzerland  
Tel. +41-56-282 29 39  
Fax +41-56-282 28 52  
www.schnydersisticherheit.ch  
info@schnydersisticherheit.ch

## Autor



Alfred Schnyder  
Dipl. Chem. Ing. ETH  
info@schnydersisticherheit.ch

## Ausgabe

November 2002 (gedruckt im Juni 2007)

---

# Gefahrenpotentiale lauern überall

## Mehrproduktanlagen sicher betreiben

Von Alfred Schnyder

### 1 Allgemeine Erkenntnisse

#### 1.1 Einleitung

In der chemischen Industrie wird ein grosser Teil der Produktion in Mehrproduktanlagen (MPA) realisiert. Mit relativ einfachen apparativen Einrichtungen werden in MPA komplizierte, mehrstufige Prozesse gefahren. Die Prozessführung wird durch Merkmale der jeweiligen chemischen Reaktion und durch die Möglichkeiten der vorhandenen MPA bestimmt. Bei der MPA bestehen nicht für alle in der Anlage gefahrenen Prozesse massgeschneiderte Sicherheitseinrichtungen, da sonst ihre Flexibilität und ihr gewünschter Charakter verloren gehen. Die MPA ist so ausgelegt, dass eine grosse Anzahl von Verfahrensparametern in einem weiten Bereich variiert werden kann. Die gewünschte Variationsbreite überschreitet meist die für einen spezifischen Prozess zulässigen sicherheitstechnischen Grenzwerte. Mit Abschaltanlagen, die von Fall zu Fall verschieden eingestellt werden können, wird versucht, die Betriebsbedingungen für eine bestimmte Fahrweise auf einen sicherheitstechnisch unbedenklichen Bereich zu begrenzen. Mit der Möglichkeit der individuellen Anpassung der Grenzwerte steigt aber auch die Gefahr von menschlichen und organisatorischen Fehlhandlungen. Ein grosses Risiko der MPA liegt in den thermischen Potentialen der Stoffe und der Reaktionsmassen. Eine Untersuchung von thermischen Explosionen in MPA zeigt als Ursache:

- Ungenügende Kenntnisse der Thermo- und Prozesschemie,
- falsch ausgelegte Kühlsysteme,
- falsch ausgelegte Kontroll- und Sicherheitssysteme,
- falsche Prozessführung und
- ungenügend ausgebildetes Personal.

Um mit thermischen Gefahren sicher umzugehen, ist es notwendig, diese zu kennen, die Wahrscheinlichkeit der Schadeneintritte sowie die Dimensionen ihrer Auswirkungen abzuschätzen. Nur bei genauer Kenntnis der Gefahren kann eine für die betreffende Anlage sichere Fahrweise definiert werden.

#### 1.2 Die Mehrproduktanlage (MPA)

##### 1.2.1 Die wirtschaftliche Notwendigkeit der MPA

Der Markt verlangt hochwertige Chemikalien und Produkte mit vergleichsweise kleiner Produktionsmenge in immer kürzerer Zeit. Das stellt die Chemikalienhersteller vor die schwierige Aufgabe, eine Vielzahl von Produkten schnell und kostengünstig in kleinen Mengen zu produzieren. Damit das wirtschaftliche Risiko klein gehalten werden kann, sind angepasste Produktionsstrukturen und geeignete technische

Die Mehrproduktchemie ist wahrscheinlich der Industriezweig mit dem breitesten Gefahrenspektrum. Sie verarbeitet, feste, flüssige und gasförmige Stoffe, zum Teil unter hohem Druck und bei hoher Temperatur. Diese Stoffe können giftig sein, brennbar, zersetzlich und explosionsgefährlich. Die Mehrproduktchemie produziert, lagert und transportiert mit technischen Hilfsmitteln, bei denen Mängel, Störungen und Defekte möglich sind. Und das alles in Anlagen, die nicht massgeschneidert sind auf die jeweilige Problematik, arbeitsteilig organisiert und gesteuert durch Menschen, die gelegentlich auch Fehler machen.

Das Anforderungsprofil des Chargenprozesses stimmt in der Regel nicht mit dem Leistungsprofil der MPA überein. Aufgrund wirtschaftlicher Überlegungen werden Mängel durch entsprechende Ergänzungen behoben. Mängel, die aus wirtschaftlichen Gründen nicht behoben werden können, werden durch organisatorische Massnahmen überbrückt.

Der sichere Betrieb der MPA wird durch drei unterschiedliche Massnahmenblöcke gewährleistet:

- Verfahrenstechnische und apparative Massnahmen.
- PLT-Massnahmen
- Organisatorische Massnahmen

Die MPA ist so gebaut, dass in ihr eine Vielfalt von chemischen Reaktionstypen und Aufarbeitungen ihrer Reaktionsprodukte mit verschiedenen Fahrweisen durchgeführt werden können. Der Kern der MPA besteht aus einem Rührkesselreaktor mit aufgesetzter Kolonne und einem Sekundär-Heiz-Kühlkreis. Für das Handling von Edukt, Hilfsstoffen und Produkt sind Vorlagen, Ansatzbehälter und Apparate für die festflüssig Trennung installiert, die meist mit dem Rührkesselreaktor fest verrohrt sind. Die Werkstoffe und die Dichtungsmaterialien der MPA haben eine breite Chemikalienbeständigkeit. Die Volumina für den Rührkesselreaktor liegen bei 4 m<sup>3</sup> bis 12 m<sup>3</sup> und die Durchmesser der aufgesetzten Kolonne liegen bei 0,3 m bis 0,5 m. Die Zusatzapparate sind auf den Rührkesselreaktor abgestimmt. Die MPA deckt meist den Temperaturbereich von -15 °C bis 200 °C und den Druckbereich von 10 mbar bis ca. 6 bar ab. Die MSR-Ausstattung der MPA ist für eine Vielzahl von Anwendungen vorgeplant und dementsprechend mit Sensoren für einen grossen Messbereich und Aktoren für einen grossen Betriebsbereich eingerichtet.

und organisatorische Konzepte notwendig. Gefragt sind einerseits Chemieanlagen, mit denen der Feinchemikalien-Hersteller schnell und flexibel auf Marktanforderungen reagieren kann, die auch bei kleinen Produktionsmengen wirtschaftlich zu betreiben sind. Andererseits brauchen sie die Fähigkeit, sehr schnell chemische Verfahren aufzubauen und diese so zu modellieren, dass sie aus ihrer Chemieanlage einen optimalen Nutzen ziehen können.

Das technische Konzept, das diese Anforderungen besonders gut erfüllt, ist die MPA [1]. In der MPA ist die verfahrenstechnische Operation einem bestimmten Apparatemodul zugeordnet. Die Anzahl und Grösse der Module sind so bemessen, dass bestimmte Mengen unterschiedlicher Produkte innerhalb eines vorgegebenen Zeitraums hergestellt werden können. MPA müssen flexibel sein. Grun und Fichtner [2] unterscheiden drei Arten der Flexibilität.

- Die Strukturflexibilität ist die Eigenschaft eines Systems, sich durch Veränderungen der Verknüpfungen zwischen seinen Elementen an geänderte Funktionsanforderungen anzupassen.
- Die Sortimentsflexibilität ist die Eigenschaft eines Systems, ohne wesentliche Veränderungen seiner Elemente unterschiedliche Produkte erzeugen zu können.
- Die kapazitive Flexibilität ist die Eigenschaft eines Systems, veränderten Kapazitätsanforderungen gerecht zu werden.

Um diesen Flexibilitätsanforderungen zu genügen, wurden verschiedene technische Konzepte für Mehrproduktanlagen entwickelt und gebaut [3].

Ein Grossteil der MPA wurde allerdings nicht im Hinblick auf ihren eigentlichen Verwendungszweck gebaut. Sie entstanden vielmehr auf folgende Weise.

- Die Herstellung eines bestimmten Produkts wurde geplant.
- Die Anlage wurde für dieses spezielle Produkt gebaut und eingerichtet, und die entsprechende Infrastruktur wurde bereitgestellt.
- Nach der Inbetriebnahme der Anlage zeigte sich, dass die Anlage nicht voll ausgelastet werden konnte oder die Nachfrage nach dem Produkt ging zurück.
- Wegen der Notwendigkeit, die Wirtschaftlichkeit zu erhöhen, wurden in der gleichen Anlage auch andere Produkte hergestellt, um so die Fixkosten auf mehrere Produkte zu verteilen.
- Das führte dazu, dass die Anlage mit bestimmten Apparaten (Modulen) nachgerüstet wurde.
- Unter Nutzung von Einrichtungen an anderer Stelle entstand so die Mehrproduktanlage.

Mit einer auf diese Weise errichteten Mehrproduktanlage lassen sich auch solche Produkte wirtschaftlich erzeugen, deren Herstellung in einer Neuanlage unwirtschaftlich wäre.

---

## 1.2.2 Sicherheitsrelevante Merkmale von Chargenprozessen

In MPA werden chemische Spezialprodukte diskontinuierlich hergestellt. Dabei werden durch chemische Reaktionen aus kleineren molekularen Bausteinen grössere Moleküle synthetisiert. Solche Synthesen sind mit einer Abnahme von Entropie verbunden. Beim Ablauf derartiger Reaktionen wird beim Umsetzungsprozess ein entsprechender Betrag an freier Enthalpie freigesetzt. Daraus lässt sich als typisches Merkmal für die Synthese von Spezialprodukten folgendes ableiten:

- Der Chargenprozess ist meist mit erheblicher Wärmetönung verbunden.

Die für die Synthese von Spezialprodukten verwendeten Ausgangsstoffe besitzen eine hohe freie Enthalpie, sie sind also sehr reaktionsfreudig. Das bedeutet aber:

- Die gewünschten Umsetzungen sind meist von unerwünschten Parallelreaktionen und Folgereaktionen begleitet.

Die Synthese von chemischen Spezialprodukten verläuft in den meisten Fällen nach komplexen Reaktionsmechanismen. Die vollständige Aufklärung der Reaktionsmechanismen und die Bestimmung der kinetischen Daten zur Berechnung der optimalen Temperaturverläufe sind aus zeitlichen und wirtschaftlichen Gründen nicht möglich. Die Reaktionsparameter - insbesondere die für die bei chemischen Spezialprodukten entscheidende Qualität notwendige Temperaturführung - wird durch Laborversuche ermittelt.

- Die Reaktionstemperatur ist in der Praxis meist nur unter dem Gesichtspunkt der Produktqualität festgelegt.

Die Realisierung der vorgegebenen Reaktionsbedingungen erfolgt meist mit der Batch- und Semibatch-Technik,

- hier wird der Temperaturverlauf durch die Kühlung, sowie beim Semibatch-Reaktor zusätzlich über die Dosierung gesteuert.

Der zunehmend härter werdende Konkurrenzkampf bei chemischen Spezialprodukten verlangt auch beim Chargenprozess eine optimale «Raum-Zeit-Ausbeute». Die Optimierung dieses Kriteriums führt in der chemischen Technik zu konzentrierten Reaktionsmischungen. Meist wird aber die folgende Tatsache unterschätzt.

- Konzentrierte Reaktionssysteme ändern das Reaktionsmedium im Verlaufe der Reaktionszeit oft sehr stark.

Sowohl die Parameter, die die Wärmeentwicklung beeinflussen, wie auch diejenigen, welche die Wärmeabfuhr beeinflussen, sind eine - meist starke - Funktion der Reaktionszeit.

## 1.2.3 Die sicherheitsrelevante Eigenart von MPA

Bei der öffentlichen Diskussion über «Chemierisiken» wird von der chemischen Industrie oft darauf hingewiesen, dass chemische Prozesse in speziell gebauten Anlagen durchgeführt werden, in Anlagen, die mit risikomindernden Massnahmen nach dem Stand der Technik gebaut sind, um die entsprechenden chemischen Prozesse zu beherrschen. Dies trifft aber nur bei Grossprodukten zu. Je weiter wir uns von der Herstel-

lung von chemischen Grossprodukten entfernen, ist eine wirtschaftliche Produktion von Chemikalien nur in MPA möglich.

Die für die Herstellung von chemischen Grossprodukten gebauten Anlagen sind für die Durchführung eines bestimmten Verfahrens massgeschneidert. Vor dem Bau der Anlage werden die dem Prozess inhärenten Gefahren identifiziert und die für den sicheren Betrieb der Anlage notwendigen technischen Massnahmen abgeleitet. Ist der Entscheid für die Produktion eines chemischen Grossproduktes gefällt, durchläuft ein neues chemisches Verfahren eine Reihe von Entwicklungsstufen. Als Beispiel dient folgender Stufenplan zur Anlagensicherheit (Abb. 1)[4].

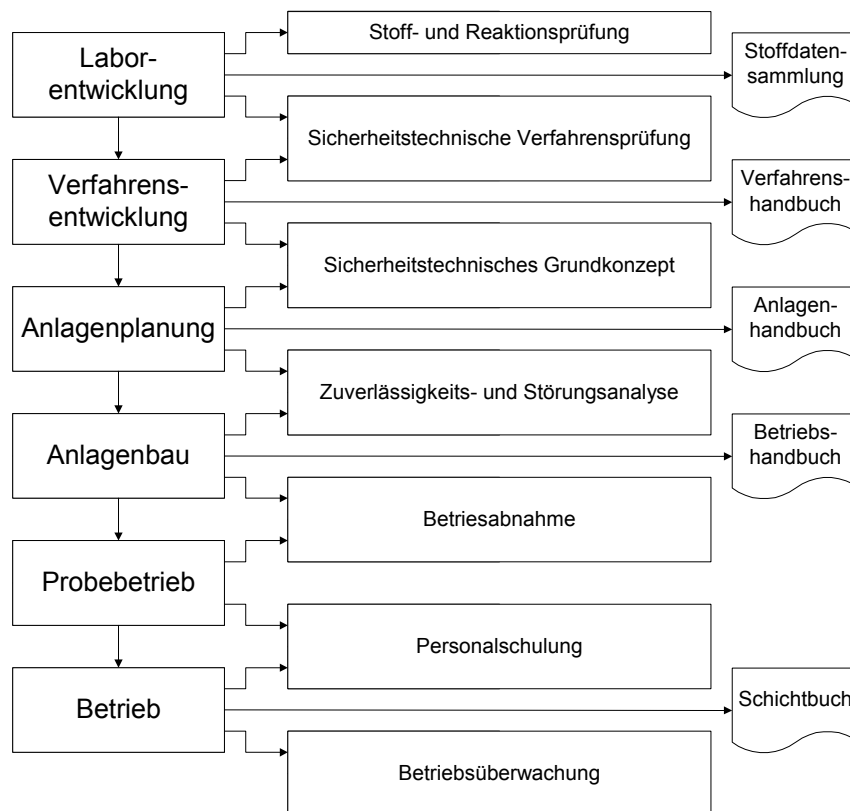


Abbildung 1

Bei der Projektierung einer MPA ist das nicht so. Hier stellt sich für die sicherheitstechnische Auslegung der Anlage ein grundlegendes Problem: In der Mehrproduktanlage sollen mehrere Hundert verschiedene chemische Prozessstufen gefahren werden. Die Crux ist nun, dass bei den Verantwortlichen oft ein nur ungenügendes Verständnis der Prozesschemie und der Thermochemie für alle diese Prozessstufen vorhanden ist.

Darum sind bei MPA nicht für alle in der Anlage durchgeführten chemische Prozesse massgeschneiderte Sicherheitseinrichtungen realisiert. Die von der MPA geforderte Flexibilität würde beeinträchtigt. Das Prozessleitsystem und das Energiekonzept sind regelmässig so ausgelegt, dass eine grosse Anzahl von Verfahrensparametern in einem weiten Bereich variiert werden kann. Die gewünschte Variationsbreite über-

schreitet aber meistens die für einen spezifischen Prozess zulässigen sicherheitstechnischen Grenzwerte. Bei der MPA wird versucht, mit variablen Abschaltvorrichtungen die Betriebsbedingungen für eine bestimmte Fahrweise auf einen sicherheitstechnisch unbedenklichen Bereich zu begrenzen. Mit der Möglichkeit, auch die Grenzwerte routinemässig und individuell anpassen zu können, steigt aber die Gefahr von menschlichen und organisatorischen Fehlhandlungen. Das Anforderungsprofil des Chargenprozesses stimmt in der Regel nicht mit dem Leistungsprofil der MPA überein. Aufgrund wirtschaftlicher Überlegungen werden Mängel durch entsprechende Ergänzungen behoben. Mängel, die aus wirtschaftlichen Gründen nicht behoben werden können, werden durch organisatorische Massnahmen überbrückt. Bei der MPA ist der notwendige sicherheitstechnische Planungsaufwand auf den Betreiber der MPA verlagert. Bei der MPA wird versucht, den sicheren Betrieb durch drei unterschiedliche Massnahmenblöcke zu gewährleisten:

- Verfahrenstechnische und apparative Massnahmen.
- PLT-Massnahmen
- Organisatorische Massnahmen

Anhand von drei Beispielen wird die Problematik bei der Festlegung eines Sicherheitskonzepts für eine MPA aufgezeigt.

**Beispiel 1:** In einem 4 m<sup>3</sup> Rührkessel wird aus einer gut rührbaren Destillationsmasse im Vakuum bei 140 °C, mit einer um 60 °C höheren Wandtemperatur, ein Lösungsmittel ausdestilliert. Die Destillationsmasse zersetzt sich unter adiabatischen Bedingungen ausgehend von 140 °C innerhalb von ca. 20 Stunden mit einer hohen Tragweite hinsichtlich eines möglichen Schadens. Vom Betreiber der Anlage wird nun aber diese Prozessstufe als sicher eingestuft. Dies ist jedoch eine Fehleinschätzung: Wenn sich nämlich zum Zeitpunkt, bei dem der Kessel noch zu 30 % gefüllt ist, ein Energieausfall ereignet, kann die Temperatur der Destillationsmasse von den anfänglichen 140 °C auf ca. 160 °C ansteigen [5]. Die thermoanalytische Untersuchung der Destillationsmasse zeigt, dass die TMR<sub>ad</sub> ausgehend von den 160 °C noch ca. 3 Stunden beträgt. Realistischerweise muss die Möglichkeit, den Eintritt des Schadens in drei Stunden abzuwenden, als sehr klein eingestuft werden.

**Beispiel 2:** In einer MPA werden während der grössten Zeit des Jahres Produkte hergestellt, bei denen während der Reaktionsstufe verdünnte Natronlauge zugegeben werden muss. Deshalb sind die Reaktoren an ein Verteilersystem für Natronlauge angeschlossen. Zwischendurch wird in dieser MPA ein Produkt gefahren, das bei der Zugabe von Natronlauge thermisch durchgeht. Es ist offensichtlich, dass wenn auf Grund einer Fehlhandlung Natronlauge irrtümlich zugegeben wird, eine Reaktorexlosion die Folge ist.

**Beispiel 3:** Bei einem Semibatchprozess wird ein Reaktand bei einer bestimmten Temperatur in einen Reaktor dosiert. Durch eine eigebaute Blende wird sichergestellt, dass die Dosierung nicht zu schnell erfolgt. Die Reaktionswärme wird über den mit Wasser gekühlten Reaktorman-

Das systematische Vorgehen bei der Risikoermittlung auf jeder Entwicklungsstufe zu einem chemischen Grossverfahren hin hat dazu geführt, dass heute die Risiken bei der Produktion von chemischen Grossprodukten geringer sind als in anderen chemischen Bereichen. Die Ereignisse bei der Produktion von chemischen Grossprodukten betragen ca. 20 % der Gesamt Ereignisse im Bereiche der Chemieproduktion.

Eine für die chemische Prozesssicherheit der MPA wichtige Tatsache ist, dass Stoffumsetzungen in technischen Systemen durchgeführt werden, die nicht für diese spezielle Aufgabe geplant und gebaut worden sind.

Die Prozessführung in MPA ist wesentlich durch individuelle Merkmale des chemischen Reaktionssystems bestimmt. Die Taktik der Prozessführungen erfolgen überwiegend aufgrund empirischer Erkenntnisse. In der Regel wird ein Chargenprozess wegen der meist geringen Mengenproduktion weniger umfassend durchleuchtet. Nicht selten werden in kleineren und mittleren Betrieben chemische Prozesse vom Labor mit einem Vergrösserungsfaktor von 10'000 direkt in die Produktion übertragen. Die Prozessführung für jedes Produkt ist durch Rezepturen festgelegt. Meist fehlt die Kenntnis darüber, welcher Teil der Gefahren des Prozesses durch die Anlage kontrolliert wird und welcher Teil durch die Anlagenoperateure sichergestellt sein muss.

tel abgeführt. Auch hier ist die Sicherheit, in der sich die Betreiber wöhnen, trügerisch. Wenn nämlich das Kühlwasser sehr kalt ist, sinkt die Temperatur im Reaktor ab. Dadurch wird die chemische Reaktion langsamer und es kommt zu einer Akkumulation von Reaktanden. Bei einem Kühlerausfall kann es also zu einer Runawayreaktion kommen.

### 1.3 Wie gefährlich ist der Mehrproduktbetrieb?

#### 1.3.1 Einleitung

Wegen der grossen wirtschaftlichen Bedeutung der MPA besteht ein besonderes Interesse, die Ereignisse, die in der Chemischen Industrie aufgrund von Runawayreaktionen eingetreten sind, zu untersuchen und aus den Ergebnissen methodische Systeme abzuleiten, die es erlauben,

- die Gefahren von chemischen Prozessen in MPA zu erkennen
- und Massnahmen abzuleiten, die ein sicheres Produzieren in MPA ermöglichen.

In Grossbritannien sind mit mehreren Studien solche Ereignisse untersucht worden[6][7][8].

#### 1.3.2 Einige interessante Zahlen aus diesen Studien

- **Welcher Anteil der Unfälle fällt auf die Mehrproduktchemie?**

J. A. Barton und P. F. Noland [9] differenzierten die Ereignisse, die in der Chemischen Industrie zwischen 1962 und 1987 eintraten, nach Industriebereichen.

Industriezweig	Ereignisse in % (gerundet)
Feinchemikalien und Zwischenprodukte	27
Kunststoffe, Gummi und Harze	22
Pharmazeutische und Tiermedizin-Produkte	7
Verschiedene Produkte	12
Farbstoffe	7
Organische Grossprodukte	11
Agrikulturchemikalien	3
Metallurgische und Metallverarbeitung	7
Lebensmittel und Aromastoffe	3
Farben und Lacke	3

Tabelle 1

Bei den in der Tabelle 1 gelb markierten Industriebereichen wird vorwiegend in MPA produziert. Ihr Anteil beträgt ca. 75 %. Nach einer anderen Schätzung ist die Produktion von chemischen Grossprodukten, die in Monoanlagen produziert werden, zu ca. 20 % an den Ereignissen beteiligt[10]. Auf die Mehrproduktchemie fällt also der Hauptteil der Ereignisse.

Interessant sind die Schlussfolgerungen, die aus einer Studie von Industrieversicherern (Norstrom Paper [10]) abgeleitet werden können. Aufgrund dieser Studie sind die Hauptursachen, die zu Versicherungsleistungen an die chemische Industrie führten, folgende:

- **Feuer** verursacht 20 % der Kosten mit der Häufigkeit von 41 %.



- **Explosionen** verursachen 66 % der Kosten mit der Häufigkeit von 23 %.

Die Autoren der Studie fassten die Runawayreaktionen und die Explosionen zusammen. Sie unterteilten die Ereignisse in drei Klassen:

- Petrochemische Industrie
- Die «extra heavy hazard class» umfasst die Herstellung von organischen Peroxiden, Sprengstoffen, Nitrierungen und Grignard-Reaktionen.
- Die «heavy hazard class» umfasst die meisten Polymerisationsprozesse, Sulfonierungen, Niederdruckhydrierungen, allgemeine organische Reaktionen und Lösungsmittelextraktionen.

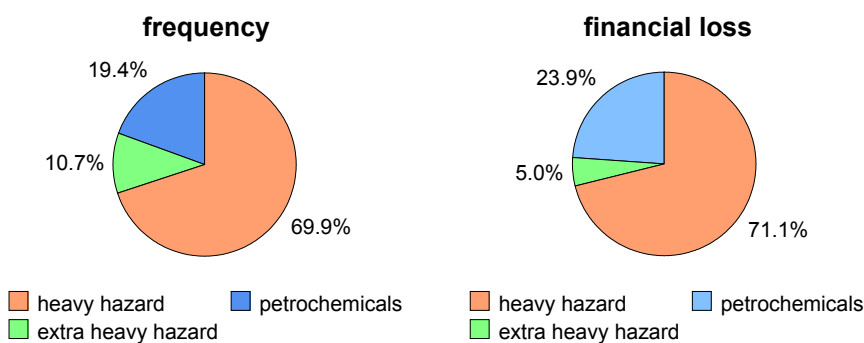


Abbildung 2

Die Abbildung 2 zeigt, dass für die Versicherungen der Hauptteil der Kosten in der «heavy hazard class», also in der Mehrproduktchemie, anfallen.

• **Welche Reaktionstypen sind besonders gefährlich?**

Die Tabelle 2 zeigt eine Auflistung von Reaktionstypen, die aus 263 Ereignissen als Einheitsprozesse identifiziert wurden.

Ereignisse nach Reaktionstypen differenziert <sup>1)</sup>			
Reaktionstyp	Anzahl [%]	Reaktionstyp	Anzahl [%]
Alkoholyse	2.24	Isomerisierungen	1.49
Aminierung	2.24	Methylierungen	1.49
Cyclisierung	2.24	Nitrierungen	24.6
Diazotierung	1.49	Oxidationen	2.98
Elektrolyse	0.75	Polymerreaktionen	(42.5)
Veresterung	1.49	Phenolharze	8.95
Halogenierung	(6.7)	Andere Harze	12
Chlorierung	4.47	Polykondensationen	3
Bromierung	2.24	Polymerisationen	9.7
Hydrierung	5.2	Sulfonierungen	8.95
Hydrolyse	4.47		

<sup>1)</sup> 134 aus 263 Ereignissen

Tabelle 2

Die in der Tabelle erwähnten Polymerreaktionen machen den Hauptanteil der Ereignisse aus, gefolgt von Nitrierungen, Sulfonierungen etc.

• **Wie lange werden Reaktoren im Betrieb genutzt?**

Aufgrund einer Schätzung des Reaktorinventars waren in der Periode von 1970 bis 1987 in Grossbritannien ungefähr 2'100 Reaktoren in Be-

trieb. Die Tabelle 3 gibt einen Eindruck über das Alter der Reaktoren und über die Langlebigkeit von Chemieanlagen.

Baujahr von Reaktoren	
Gebaut zwischen	Anzahl in %
1914 - 1950	2.5
1951 - 1960	12.2
1961 - 1970	25.7
1971 - 1980	45.1
1981 - 1985	14.5

Tabelle 3

Es zeigt sich, dass chemische Prozesse häufig auf recht alten Anlagen gefahren werden.

- **Unfallhäufigkeit**

Von 1970 bis 1981 haben sich in Grossbritannien 66 Reaktorexplosionen ereignet. Die Tabelle 4 zeigt die abgeleitete Unfallhäufigkeit.

Einige Daten zu Rührkesselunfällen infolge Überdrucks (Quelle Marrs et al. 1989)	
betrachteter Zeitraum	1970 bis 1981 (12 Jahre)
geschätzte Anzahl eingesetzter Rührkessel	2'100
Anzahl Ereignisse	66
geschätzte Anzahl Prozesse pro Jahr	250
geschätzte Dauer eines Prozesses	16 Stunden
$\text{Unfallhäufigkeit} = \frac{66}{12 \cdot 2100} = 2.62 \cdot 10^{-3} \frac{\text{Unfälle}}{\text{Jahr}}$	

Tabelle 4

- **Häufigkeit von Prozessabweichungen**

Nicht jede Prozessabweichung, die zu einem Reaktorüberdruck führt, endet in einer Runawayreaktion mit anschliessender Reaktorexplosion. Aufgrund der Umfragen in der Industrie wird das Verhältnis auf

$$\frac{\text{Prozessabweichungen}}{\text{Reaktorexplosionen}} = \text{ca. } 0.05 \text{ geschätzt.}$$

Diese Schätzung wird durch eine unabhängige Untersuchung erhärtet [11].

- **Todesfallrisiko**

Aus den durch die Reaktorexplosionen verursachten Todesfällen ist die tödliche Unfallrate FAR (Fatal Accident Risk) abgeschätzt worden (Tabelle 5). Die tödliche Unfallrate FAR ist definiert als die Todesfälle pro  $10^8$  exponierte Stunden. Für die Schätzung wurde angenommen, dass eine Mehrproduktanlage aus 10 Reaktoren besteht, die über das ganze Jahr von 2 Anlagenoperatoren rund um die Uhr betreut werden.

- Die Expositionszeit wird zu:  $\frac{(1'987 \cdot 15 \cdot 8760 \cdot 2)}{10} = 5.22 \cdot 10^7$
- Die Schätzung für FAR wird zu:  $\frac{2}{(5.22 \cdot 10^7) \cdot 10^8} = 3.83$

Die aus den Ereignissen abgeleitete FAR liegt beträchtlich höher als die angestrebte FAR, die mit 0.4 angegeben wird [12]. Für einen Anlagenoperateur ist das Risiko also signifikant durch eine Runawayreaktion in chemischen Reaktoren zu sterben [13].

Todesfallrisiko (Quelle Marrs et al. 1989)	
betrachteter Zeitraum	1967 bis 1981 (15 Jahre)
geschätzte Anzahl eingesetzter Reaktoren	1'987
Anzahl Todesfälle	2
$\text{Todesfallhäufigkeit} = \frac{2}{15 \cdot 1987} = 6.71 \cdot 10^{-5} \left( \frac{\text{Todesfälle}}{\text{Reaktorjahr}} \right)$	

Tabelle 5

### 1.3.3 «Auslösende Ereignisse» als Unfallursachen

Eine Studie von 100 Ereignissen, die in der Chemischen Industrie in Italien aufgrund von Runawayreaktionen eingetreten sind, zeigt die häufigsten Unfallursachen [14].

- 42 % basieren auf mangelnden Kenntnissen des chemischen Prozesses (Chemie, Kinetik und thermische Potentiale);
- 23 % basieren auf ungenügender Qualität der Reaktanden;
- 25 % basieren auf Nichtbefolgen von Prozessvorschriften und auf Fehlern beim Scale-up.
- 10 % basieren auf ungenügender Kühlung und/oder ungenügender Durchmischung.

Nolan [9] teilt die Ereignisse ein nach den Ursachen für die Prozessabweichungen [15], sowohl nach allen Reaktionen als auch nach Einheitsprozessen wie Sulfonierung, Nitrierung und Polymerisation (Tabelle 6).

Identifizierte Ursachen für Prozessabweichungen die zu Überdruckereignissen führten				
Ursache der Prozessabweichung	Alle Reaktionen [%] <sup>1)2)</sup>	Sulfonierung [%] <sup>1)2)</sup>	Nitrierungen [%] <sup>1)2)</sup>	Polymerreaktionen [%] <sup>1)2)</sup>
Ungenügende Kenntnis der erwünschten Reaktion	3.5 (3.7)	9.1	0	7.1 (8.6)
Nicht erkannte Zersetzungsreaktionen der Reaktanden	8.1 (8.6)	18.2	10.3	0
Exothermien unbekannter Ursache	3.5 (3.7)	0	10.3	0
Falsches Beladen von Reaktoren	17.2 (18.3)	0	13.8	14.3 (17.4)
Ungenügendes Kühlen	13.1 (14)	0	6.9	28.6 (34.8)
Übermässiges Heizen	9.6 (10.2)	9.1	17.2	14.3 (17.4)
Falsches Rühren	10.1 (10.8)	36.4	13.8	7.1 (8.6)
Falsche Reaktorkontrolle	9.1 (9.7)	0	13.8	3.6 (4.4)
Unerwünschte Katalyse	2.5 (2.7)	0	0	3.6 (4.4)
Exotherme Reaktionen durch Verunreinigungen	10.6 (11.3)	27.3	3.4	0
Wassereintritt und Verdampfungen	0.5 (0.5)	0	3.4	0
Luftintritt und Zündung	3.5 (3.7)	0	3.4	0
Eintritt von Gasen unter Druck	0.5 (0.5)	0	0	
Zurückführen aus Prozessabweichungen	2 (2.2)	0	6.9	3.4 (4.4)
Unbekannte Ursachen	0			0

<sup>1)</sup> Für die Untersuchung konnten die Aufzeichnungen von 199 Chemieunfällen verwendet werden.  
<sup>2)</sup> Bei den Zahlen in Klammern wurden die Fälle mit unbekannter Ursache mit den relativen Häufigkeiten der bekannten Ursachen umgerechnet und zu diesen addiert.

Tabelle 6

Die Ereignisursachen führen in einer bestimmten Anzahl von Fällen zu einer Runawayreaktion, die eine Reaktorexlosion auslösen kann. Die Ereignisursachen [(1) ungenügende Kenntnis der erwünschten Reaktion, (2) nicht erkannte Zersetzungsreaktionen der Reaktanden und (3) Exothermien unbekannter Ursache] haben alle die gleiche Basis, nämlich mangelnde Kenntnis der Prozesschemie und Thermochemie, die als ein «auslösendes Ereignis» zusammengefasst werden können. Tabelle 7 enthält eine Rangliste der abgeleiteten auslösenden Ereignisse, die 90 % aller Fälle abdeckt, zusammen mit einer Expertenbefragung, die Marrs' Studie ergänzt, die aber zu anderen Schlüssen kam.

Auslösendes Ereignis	Untersuchungsergebnis (Quelle Marrs)		Expertenmeinung
	Anteil [%]	Rang [-]	Rang [-]
Falsches Beladen von Reaktoren	18.3	1	1
Mangelnde Kenntnisse der Prozesschemie und der Thermochemie	16	2	6
Ungenügendes Kühlen	14	3	3
Exotherme Reaktionen aufgrund von Verunreinigungen	11.3	4	7
Falsches Rühren	10.8	5	5
Übermässiges Heizen	10.2	6	4
Falsche Reaktorkontrolle	9.7	7	2
Total	90.3		

Tabelle 7

Die wesentlichen Unterschiede zwischen Marrs' Studie und der Expertenbefragung können wie folgt zusammengefasst werden.

- Zwei auslösende Ereignisse sind von den Experten als weit weniger häufig eingestuft worden, nämlich (1) die exothermen Zersetzungen aufgrund ungenügender Kenntnis der Prozesschemie sowie der Thermochemie und (2) die exothermen Reaktionen aufgrund von Verunreinigungen.
- Zwei auslösende Ereignisse [(1) übermässiges Heizen und (2) falsche Reaktorkontrolle] sind von den Experten überschätzt worden.
- Für drei auslösende Ereignisse [(1) falsches Beladen von Reaktoren, (2) ungenügendes Kühlen und (3) falsches Rühren] stimmt die Schätzung der Experten mit den tatsächlichen Ereignissen überein.

### 1.3.4 Trägerischer Reaktorschutz

#### 1.3.4.1 Wie werden Reaktoren gegen Explosionen geschützt?

Für den Schutz von Reaktoren werden Entlastungssysteme und Instrumentensystemen eingesetzt. G. P. Marrs et al. [8] untersuchten Reaktorexlosionen, die durch Überdruck verursacht wurden, sowie die Wirksamkeit von Schutzmassnahmen gegen Reaktorexlosionen.

#### 1.3.4.2 Wie ist die Schutzwirkung von Entlastungssystemen?

Bei 66 untersuchten Chemieunfällen, die zu einer Reaktorexlosion führten, waren 48 Reaktoren geschlossen und 18 Reaktoren offen.

- Bei 21 (32 %) Fällen hatten die Reaktoren eine Entlastungseinrichtung: Entweder eine Berstscheibe oder ein Entlastungsventil oder beides. Diese waren bei der Inspektion durch die Behörden akzeptiert worden.
- Bei den übrigen Fällen waren die Reaktoren weder mit einer Berstscheibe noch mit einer anderen adäquaten Entlastungseinrichtung ausgerüstet.

Die 48 Explosionen bei den geschlossenen Reaktoren zeigen folgendes:

- Bei 10 (21 %) Fällen funktionierte die Entlastungsöffnung. Der Unfall konnte trotzdem nicht verhindert werden.
- Bei 13 (27 %) Fällen wurde eine Entlastungseinrichtung speziell dimensioniert. Aus nicht bekannten Gründen scheiterte die Entlastung trotzdem, sie konnte das Ereignis zu verhindern.
- In den Fällen, in denen keine Entlastungseinrichtung installiert war (einschliesslich der Fälle, in denen die Art der Entlastungseinrichtung aus den Daten nachträglich nicht eruiert werden konnte, aber wahrscheinlich keine korrekte Entlastung installiert war), zerbarsten bei 10 (21 %) Ereignissen Glasaufbauten und bei 11 (23 %) Ereignissen Reaktoren.

Die Studie zeigt, dass die Ursache für die ungenügende Schutzwirkung vor Reaktorexlosionen darin liegt, dass bei den Reaktoren keine oder ungenügend dimensionierte Entlastungsöffnungen bzw. Berstscheiben installiert waren. Beachtlich ist die grosse Zahl von Reaktorexlosionen, die bei offenem Reaktor, meist mit offenem Mannloch, aufgetreten sind. Diese Vorfälle könnten also auch mit richtig dimensionierten Entlastungsöffnungen nicht verhindert werden. Bei Reaktorexlosionen ist der Ausfall der Entlastungseinrichtungen signifikant. Bei MPA ist die Wahrscheinlichkeit also gross, dass ein Entlastungssystem versagt,

- weil dieses unterdimensioniert oder sonst falsch ausgelegt ist,
- weil die Berstscheibe nicht anspricht,
- oder weil die Entlastungsöffnung blockiert ist.

#### 1.3.4.3 Wie ist die Schutzwirkung von Instrumentensystemen?

Prozessabweichungen - verursacht durch auslösende Ereignisse - treten relativ häufig ein, aber nur wenige eskalieren zu einer Reaktorexlosion. Es gibt also ereignisverhindernde Möglichkeiten, die manchmal eine Eskalation des Ereignisses wirksam verhindern. Bedeutsam ist in diesem Zusammenhang, dass ein auslösendes Ereignis meist nur eine kurze Zeit wirksam ist, weil der Anlagenoperator durch Korrekturen die Abweichungen vom Normalbetrieb erfolgreich zurückführen kann.

Ist es möglich, die Schutzwirkung dieser ereignisverhindernden Möglichkeiten mittels Hardware (Mess- und Regelungstechnik) oder Software (Betriebsverfahren oder Computerprogramme) zu vergrössern?

G. P. Marrs et al. haben jedes auslösende Ereignis daraufhin beurteilt, wie gross der Anteil war, bei denen es im Prinzip möglich gewesen wäre, ein wirksames Instrument für Gegenmassnahmen vorzusehen. Das Resultat wurde einer Schätzung des Anteils an Fällen gegenüber gestellt, bei denen solche Gegenmassnahmen, wären sie angewendet wor-

Die Entlastungseinrichtung hat zwei Aufgaben zu erfüllen.

- Sie muss die Fähigkeit haben, die Funktion, für die sie bestimmt ist, auszuführen.
- Sie muss diese Funktion, wenn sie angefordert wird, zuverlässig ausführen.

Neuere Studien über die Zuverlässigkeit zeigen

- die Wahrscheinlichkeit des Ausfalls richtig dimensionierter Berstscheiben ist sehr tief;
- die Wahrscheinlichkeit des Nichtfunktionierens richtig dimensionierter Entlastungsöffnungen ist auch sehr tief.

Der Widerspruch, dass einerseits die Zuverlässigkeit von Entlastungseinrichtungen als relativ hoch beurteilt wird, dass aber andererseits bei Reaktorexlosionen ein Ausfall der Entlastungseinrichtungen in einem signifikanten Ausmass auftritt, zeigt auf, dass die meisten Ausfälle der Entlastungseinrichtungen auf falsche Dimensionierungen zurückzuführen sind.

Das wiederum berechtigt zur Frage, ob bei Mehrprodukthanlagen die Entlastungseinrichtungen überhaupt richtig dimensioniert werden können angesichts der Tatsache, dass der Anlagenbauer noch gar nicht weiss, welche Prozesse in der MPA später gefahren werden sollen.

### Wie steht es um die Kenntnis der Gefahrenpotentiale bei Mehrproduktanlagen?

Eine von den Berufsgenossenschaften Chemie Deutschland nach dem Störfall bei der Firma Höchst im Werk Frankfurt-Griesheim 1993 bei etwa 100 Mitgliederbetrieben durchgeführte Befragung sollte klären, ob die Gefahrenpotentiale in den Mitgliederbetrieben erkannt und welche Massnahmen zur Vermeidung von Störfällen getroffen wurden.

Diese Befragung zeigte, dass Kenntnisse über Reaktionskenndaten - Reaktionswärme und Reaktionsgeschwindigkeit, Zersetzungsbeginn und Zersetzungsenergie - wesentlich von der Grösse des Betriebs abhängen. Grossbetriebe verfügen über die gerätetechnische Ausstattung zur kalorimetrischen Untersuchung von Stoffen und Reaktionsgemischen und nutzen diese auch. Dabei wird in der Regel nicht nur der Normalbetrieb untersucht, sondern auch Abweichungen davon. Mittelständische Betriebe haben diese Möglichkeiten nur in Einzelfällen. Aber bei der Mehrzahl kleinerer Betriebe liegen thermoanalytische Daten zum Reaktionsverhalten nicht oder nur als Schätzungen vor.

den, tatsächlich zu einer Verhinderung des Ereignisses geführt hätten. Bei zwei von drei Kategorien von auslösenden Ereignissen wäre es möglich gewesen, wirksame Schutzmassnahmen vorzusehen.

- In die erste Kategorie gehören (1) ungenügende Kenntnis der Prozesschemie und der Thermochemie und (2) ungenügendes Rühren. Hier wird die Wahrscheinlichkeit, dass die eingetretenen Vorfälle durch entsprechende Gegenmassnahmen hätten verhindert werden können, etwa mit 90 % beurteilt.
- In die zweite Kategorie gehören (1) falsches Beladen, (2) falsch ausgelegte Kühlsysteme und (3) übermässiges Heizen. Hier wird die Wahrscheinlichkeit, dass die eingetretenen Vorfälle durch entsprechende Gegenmassnahmen hätten verhindert werden können, etwa mit 50 % beurteilt.
- In die dritte Kategorie gehören (1) unerwünschte Katalyse, (2) exotherme Reaktionen durch Verunreinigungen, (3) Wassereintritt und Druckaufbau durch spontane Verdampfung, (4) zu hoher Druck durch Eintritt von Gasen aus Druckbehältern und (5) Ereignisse, die nach dem Zurückführen aus Prozessabweichungen eintreten. Hier ist die Wahrscheinlichkeit, dass die eingetretenen Vorfälle durch entsprechende Gegenmassnahmen hätten verhindert werden können, praktisch null.

Die Studie über die Wirksamkeit von MSR- und PLT-Massnahmen zum Schutz gegen Reaktorexpllosionen lässt sich wie folgt zusammenfassen.

- Die Wahrscheinlichkeit, das auslösende Ereignis «falsches Rühren» technisch wirksam abzusichern, wird als hoch eingestuft.
- Wenn eine Runawayreaktion aufgrund des auslösenden Ereignisses «Rührerausfall» eintritt, ist es schwierig, dieses technisch abzusichern, es sei denn, dass es zur Verhinderung der Runawayreaktion genügt, die Dosierung zu unterbrechen.
- Ebenso schwierig ist es, die auslösenden Ereignisse «unerwünschte Katalyse» und «Wassereintritt, der zu einem Druckaufbau durch Verdampfung oder durch Gasentwicklung führt», mit technischen Massnahmen wirksam abzusichern.

#### 1.4 Ausblick: Anlagensicherheit bei der MPA

Wir halten folgende Tatsachen fest.

- Ein wachsender Anteil von Chemikalien kann nur in flexiblen MPA wirtschaftlich hergestellt werden.
- 75 % der Ereignisse, die in der chemischen Industrie aufgrund von Runawayreaktionen eintreten, fallen auf die Mehrproduktchemie.
- Mehr als 90 % der Ereignisse, die beim Betreiben der MPA auftreten, können auf sieben «auslösende Ereignisse» zurückgeführt werden: (1) falsches Beladen von Reaktoren, (2) mangelnde Kenntnisse der Prozesschemie und der Thermochemie, (3) ungenügendes Kühlen, (4) exotherme Reaktionen aufgrund von Verunreinigungen, (5) falsches Rühren, (6) übermässiges Heizen und (7) falsche Reaktorkontrolle.

- Es ist unmöglich, die MPA mit technischen Massnahmen wirksam gegen diese «auslösende Ereignisse» zu schützen. Diese Tatsache ist darauf zurückzuführen, dass bei der Projektierung einer MPA noch nicht bekannt war, welche chemischen Prozessstufen in ihr gefahren werden sollen – Prozessstufen notabene, von denen meist ein nur ungenügendes Verständnis der Prozesschemie und der Thermochemie vorhanden ist.

Für den Mehrproduktbetrieb gilt folgendes: Weil die MPA gegeben ist, können zwei der definierten auslösenden Ereignisse, nämlich (1) ungenügendes Kühlen und (2) falsches Rühren, nur insoweit beeinflusst werden, dass die Eignung oder die Nichteignung der Anlage festgestellt wird. Um diese Aussage machen zu können, muss die Relevanz dieser auslösenden Ereignisse als Schutzwirkung erkannt sein. Das ist aber nur auf der Basis von genügenden Prozesskenntnissen möglich.

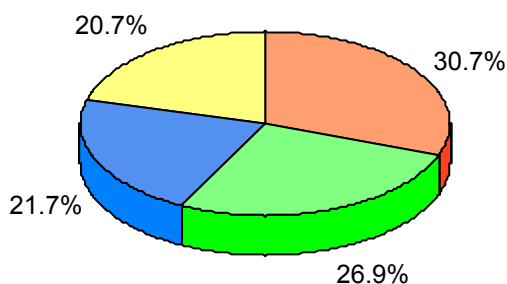
Die Ursache «ungenügende Prozesskenntnis» wird sowohl von der Industrie als auch von den Behörden immer noch stark unterschätzt.

Ebenso stark unterschätzt wird das wirtschaftliche Potential, welches eine gute Prozesskenntnis in sich birgt.

Siehe Glossarkasten auf Seite 12.

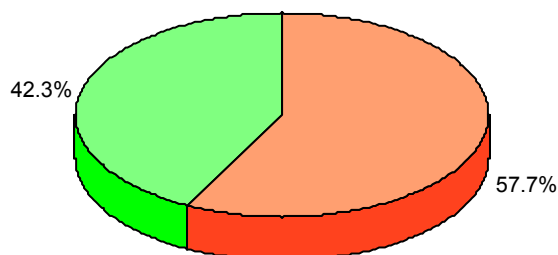
### Ungenügende Prozesskenntnis

- Mangelnde Kenntnisse der Prozesschemie und der Thermochemie
- Exotherme Reaktionen aufgrund von Verunreinigungen
- Ungenügendes Kühlen
- Falsches Rühren



### Ursache

- Ungenügende Prozesskenntnisse
- Menschliche Fehler



### Menschliche Fehler

- Falsches Beladen von Reaktoren
- Übermässiges Heizen
- Falsche Reaktorkontrolle

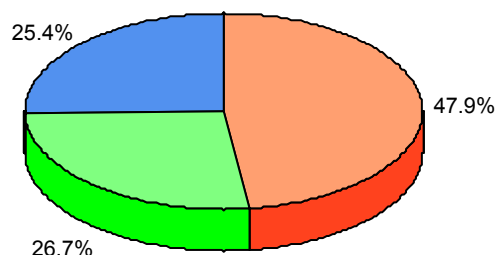


Abbildung 3

In der Abbildung 3 sind die sieben «auslösenden Ereignisse» in den zwei Ursachengruppen «ungenügende Prozesskenntnis» und «menschliche Fehler» zusammengefasst. Bei dieser Einteilung wird ersichtlich, dass nahezu 60 % der Reaktorunfälle durch ungenügende Prozesskenntnisse verursacht werden. Bei genauem Hinsehen ist der Anteil noch grösser, denn viele dieser «menschlichen Fehler» können nur

---

darum begangen werden, weil die Auswirkungen entsprechenden Verhaltens auf die Prozesschemie nicht verstanden und deshalb die Anlage technisch nicht abgesichert wird.

Die mehrjährige Erfahrung, die wir beim Aufzeigen von thermischen Gefahrenpotentialen bei chemischen und thermischen Prozessstufen und durch die Unfallabklärung nach Reaktorunfällen in der chemischen Industrie gemacht haben, hat uns folgendes gezeigt.

- Vielfach fehlt das Bewusstsein, dass bei der MPA der notwendige sicherheitstechnische Planungsaufwand vom Betreiber der MPA bei jedem neu in Betrieb genommenen Prozess vorzunehmen ist.
- Meist ist von den in MPA gefahrenen chemischen Prozessstufen nur ein ungenügendes Verständnis der Prozesschemie und der Thermochemie dieser Prozessstufen vorhanden.
- Selten wird bei der Einführung von chemischen Prozessen in die MPA mit einer dem Stand der Technik angepassten Systematik – Gefahrensuche, Gefahrenminimierung und Risikoanalyse – aufgezeigt, ob die bestehende Anlage und die bestehende Organisation in der Lage sind, die Gefahren des Prozesses zu beherrschen.
- Oft fehlt bei der Einführung von chemischen Prozessen in die MPA der effiziente Dialog zwischen Prozesschemikern einerseits und Sicherheitsverantwortlichen andererseits.

Mit diesem Aufsatz wollen wir das komplexe Zusammenspiel von *Mehrproduktanlage*, *Prozessstufe* und *Organisation* aufzeigen. Dieses Verständnis ist für den sicheren Betrieb der MPA unabdingbar. Der Aufsatz ist bewusst breit angelegt. Er soll zeigen, dass es für die Anlagensicherheit wichtig ist, chemische Prozessstufen in MPA ganzheitlich zu beurteilen. Unser Ziel ist es zu zeigen, dass es möglich ist, wirtschaftlich zu beurteilen, ob ein chemischer Prozess in einer gegebenen Anlage sicher gefahren werden kann.



## 2 Gefahrenpotential- und Risikoanalyse

### 2.1 Einleitende Gedanken

Die Analyse von thermischen Explosionsgefahren zeigt, dass es zum sicheren Betrieb von MPA nicht genügt, Daten über die Thermostabilität der Reaktanden und der Reaktionsgemische zu erarbeiten. Die Möglichkeiten für die Auslösung des Potentials einer Stofffreisetzung aufgrund einer "Runawayreaktion" sind vielschichtig. Diese bestehen immer aus einem Zusammenspiel von Eigenschaften, die aus verschiedenen Gefahrenfeldern stammen. Zu beachten sind verschiedene Ursachen, die aus den Gefahrenfeldern «Prozess», «Anlage» und «Organisation» stammen (Abb. 4, [16]).

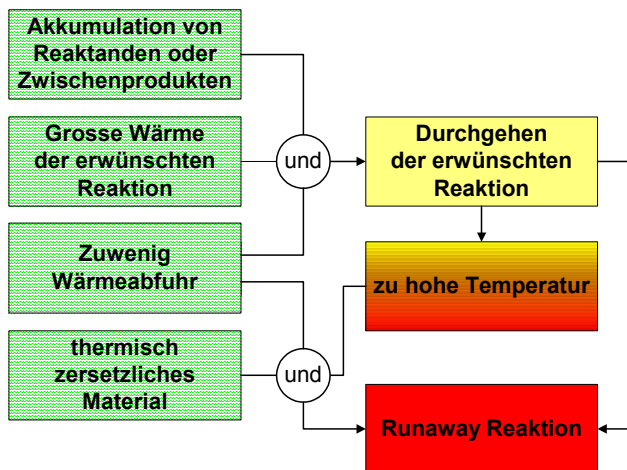


Abbildung 4

#### Ursachen für die Akkumulation von Reaktanden oder Zwischenprodukten:

- falsche Annahmen der Reaktionskinetik
- zu hohe Dosiergeschwindigkeit
- zu tiefe Prozesstemperatur
- ungenügendes Mischen
- falsche oder unterlassene Initiierung
- inhibierende Verunreinigungen

#### Ursachen für zu wenig Wärmeabfuhr:

- Rührerausfall
- ungenügende Kühlkapazität
- zu grosse Wärmeisolierung
- falsche Annahmen über den Wärmetransport
- Kühlerausfall

#### Ursachen für zu hohe Temperatur:

- falsche Temperaturwahl
- unbeabsichtigtes Heizen
- Energieeintrag durch Rühren
- Einbruch von Wärmeträgerflüssigkeit
- katalysierende Verunreinigungen

Im Folgenden wollen wir zeigen, wie die Gefahren, die durch das komplexe Zusammenspiel der Elemente der Undverknüpfungen entstehen,

Der sichere Betrieb der MPA erfordert ein Konzept das es dem Betreiber ermöglicht,

- Risiken zu erkennen,
- Risiken zu beurteilen
- und Risiken durch geeignete Massnahmen zu verringern.

Ein solches Konzept ist auf drei Grundsätzen gebaut.

- Der **erste Grundsatz** verlangt, dass Anlagenbetreiber die Eigenschaften und das Verhalten der Stoffe, sowie die Möglichkeit und die Grenzen ihrer apparativen Hilfsmittel, mit denen in ihrem Betrieb gearbeitet wird, kennen müssen.
- Der **zweite Grundsatz** verlangt, dass eine Unternehmung den neuesten Stand der Technik im Aufzeigen der inhärenten Gefahren von Prozessstufen kennt und diesen für die Gefahrensuche selbst dann nutzt, wenn es nicht über die notwendige technische Infrastruktur verfügt.
- Der **dritte Grundsatz** verlangt, dass sich der Anlagebetreiber Rechenschaft darüber geben muss, was er von seinen Mitarbeitern an Wissen, Können und Zuverlässigkeit erwarten darf, welche Risiken organisatorisch und welche Risiken technisch abzusichern sind.

*Zitat: «Tragbarkeit von Risiken, Konzept eines multinationalen Chemieunternehmens» Kaspar Eigenmann, Dr. Chem. ETH, Ciba-Geigy AG, Basel. Vortrag im Rahmen der Tagung: Umweltrecht in der Praxis, Rechtsfragen des Vollzugs der Störfallverordnung, Solothurn 1992.*

---

sichtbar gemacht werden können. Durch das Einhalten einer dem Stand der Technik angepassten Systematik – Gefahrensuche, Gefahrenminimierung und Risikoanalyse – kann aufgezeigt werden, ob die bestehende Anlage und die bestehende Organisation in der Lage sind, die Gefahren des Prozesses zu beherrschen. Durch die Systematik wird das Risiko so aufgezeigt, dass die Verantwortlichen in der Lage sind, gefahrenmindernde Massnahmen zu ergreifen und schnelle Produktionsentscheide zu treffen.

Das systematische Vorgehen besteht aus vier Teilaufgaben:

- Zuerst werden die inhärenten Gefahren des chemischen Systems beim definierten Normalbetrieb in jeder Prozessstufe aufgezeigt. Dadurch wird die Menge der Gefahren der Prozessstufen sichtbar. Die Prozessstufen werden klassifiziert.
- Mit der Kenntnis der Gefahren der jeweiligen Prozessstufe können sichere Prozessbedingungen definiert werden, ebenso wie das Anforderungsprofil für die bestehende Mehrproduktanlage, das notwendig ist, um die inhärenten Gefahren der Prozessstufe zu kontrollieren. Es wird offenbar, welche «Module» schliesslich die bestehenden Gefahren kontrollieren. Dadurch werden auch die Anforderungen an die Organisation erkennbar, die die Mängel der Anlage überbrücken müssen, und bei der Mehrproduktanlage notwendig sind, um die der Prozessstufe inhärenten Gefahren zu kontrollieren.

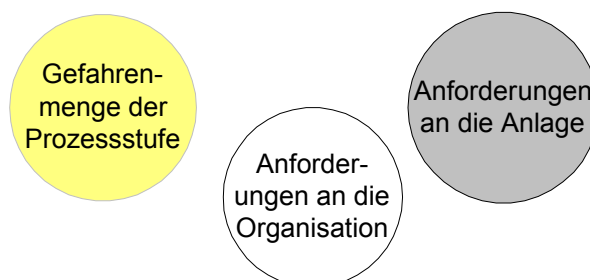


Abbildung 5

- Durch dieses Vorgehen wird sichtbar, welcher Teil der Gefahren durch die Anlage abgedeckt wird, aber auch, welcher Teil der Gefahren durch die Organisation abgedeckt werden muss (Abb. 5).

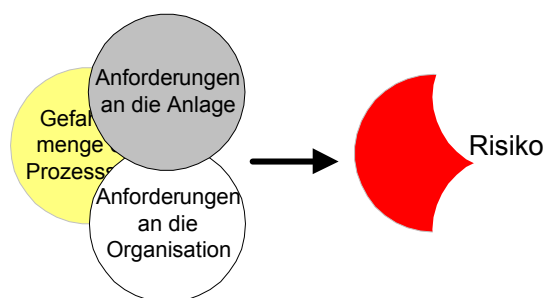


Abbildung 6

- Durch Überlagern der Gefahrenmenge des Prozesses mit den Möglichkeiten der Anlage und den Anforderungen an die Organisation wird überprüft, ob die Anlage und die Organisation den Anforderungen der Prozessstufe genügen (Abb. 6).

Durch dieses Vorgehen wird das verbleibende Risiko sichtbar und die Frage kann beantwortet werden: «Ist das Risiko tragbar»

Die Kenntnis des Risikos erlaubt dem Anlagebetreiber, die für den sicheren Betrieb seiner Anlage richtigen technischen, organisatorischen und personellen Massnahmen zu realisieren. Ist das Risiko zu gross, darf die Prozessstufe nach dem bestehenden Verfahren nicht gefahren werden. Das Verfahren muss «entschärft» werden.

## 2.2 Betriebszustände bei der MPA

Für die sicherheitstechnische Beurteilung von chemischen Prozessstufen in Mehrproduktanlagen unterscheiden wir folgende Betriebszustände (Abb. 7) [17]:

- den Normalbetrieb
- den gestörten Betrieb
- den bestimmungsgemässen Betrieb
- den Störfall

Der *Normalbetrieb* ist durch Betriebsvorschriften definiert und beim Normalbetrieb läuft ein Prozessschritt innerhalb der Parameterbereiche ab, die, wenn sie eingehalten werden können, zur gewünschten Qualität des zu produzierenden Produktes führen. Der Normalbetrieb wird durch Betriebseinrichtungen (technische Einrichtungen und organisatorische Anweisungen) gewährleistet.

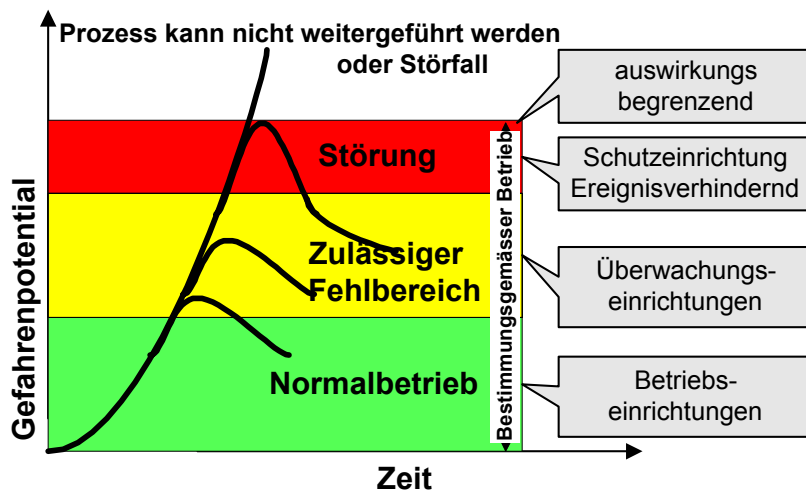


Abbildung 7

Bei einer Abweichung vom Normalbetrieb kommt es zum *gestörten Betrieb*, wobei solche Abweichungen von den Betriebseinrichtungen erkannt werden müssen. Wenn der entsprechende Prozessschritt aus dem gestörten Betrieb in den Normalbetrieb zurückgeführt werden und der Prozessschritt ohne Gefährdung weitergeführt werden kann, liegt lediglich eine Störung vor. Die eingesetzten MSR-Einrichtungen werden als *Überwachungseinrichtungen* bezeichnet. Wenn die Rückführung in den Normalbetrieb nicht mehr gelingt und eine Substanz in gefährbringender Menge für Mensch und Umwelt freigesetzt wird, muss der Stoffaustritt durch *ereignisverhindernde Massnahmen* verhindert werden. Der Bereich, in dem sowohl Überwachungseinrichtungen als auch eintrittsverhindernde Massnahmen wirksam sind, ist der *zulässige*

*Fehlbereich. Der bestimmungsgemäße Betrieb* besteht mithin aus dem Normalbetrieb und dem zulässigen Fehlbereich. Wenn der bestimmungsgemäße Betrieb, den Austritt einer für Mensch und Umwelt gefährbringende Menge Substanz nicht verhindern kann, kommt es zum *Störfall*. Ist die Prozessstufe so ausgelegt, dass sie beim Verlassen des Normalbetriebs auch ohne Eingriff von MSR-Einrichtungen oder des Anlagenfahrers den bestimmungsgemäßen Betrieb nicht verlässt, so ist sie **inhärent sicher**.

### 2.3 Systematisches Vorgehen bei der Risikoanalyse

Durch die dem Stand der Technik angepasste Systematik – Gefahrensuche, Gefahrenminimierung und Risikoanalyse – muss gezeigt werden, ob die bestehende Anlage und die bestehende Organisation in der Lage sind, die Gefahren des durchzuführenden Prozesses zu beherrschen. Zur Systematik gehören die Gefahrensuche, die Bewertung der gefundenen Gefahren in Form von Risiken und das Management der abgeleiteten Massnahmen [18].

Dazu wird der Prozess in Stufen aufgeteilt. Die Prozessstufen entsprechen den Aggregaten der MPA, in denen die Prozessoperationen durchgeführt werden. Die Prozessstufen ihrerseits werden in sicherheitsrelevante Arbeitsschritte aufgeteilt, damit die Gefahren analysierbar werden (Abb. 8).

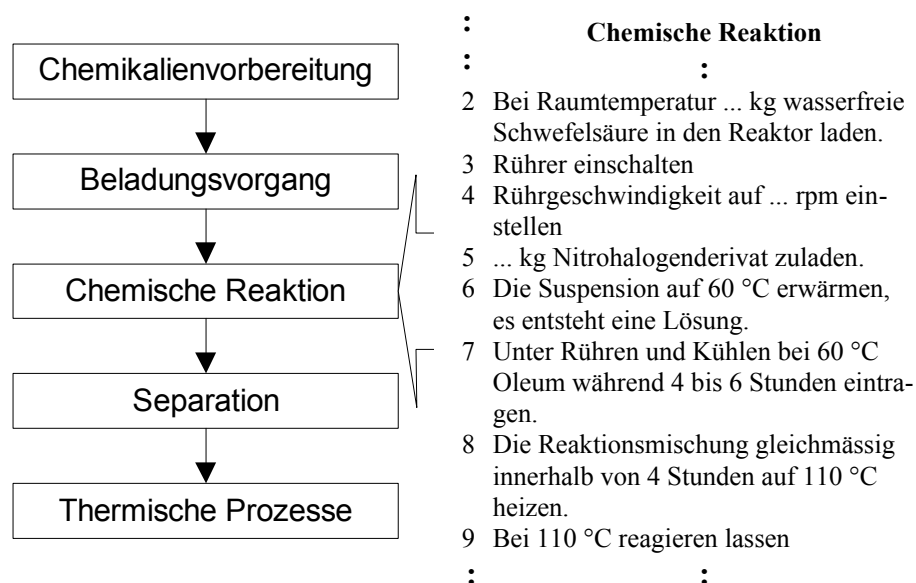


Abbildung 8

#### 2.3.1 Die Ebenen der Prozessrisikoanalyse

Die Systematik verläuft über sechs Ebenen (Abb. 9).

##### **Ebene 1: Ermittlung der Basisdaten**

Für die Durchführung der Prozessrisikoanalyse werden Daten zu folgenden Problemkreisen benötigt [19]:

- Die sicherheitsrelevanten Stoffdaten der eingesetzten Chemikalien.
- Prozessdaten (erwünschte und unerwünschte chemische Reaktionen). Die der Reaktionsstufe inhärenten Gefahren müssen aufgezeigt werden mit Bezug auf die sicherheitstechnische Bewertung

---

der Prozessstufe beim Normalbetrieb einerseits und die sicherheitstechnische Bewertung der Prozessstufe bei Abweichungen vom Normalbetrieb andererseits.

- Daten zur Anlage und zur Steuerung der Anlage.
- Daten zu menschlichen Handlungen und Fehlhandlungen.
- Daten zu externen Einflüssen.

Die Qualität der Risikoanalyse hängt von den vorhandenen Basisdaten ab. Stoffdaten sind leichter zu beschaffen als Prozessdaten. Prozessdaten liegen in vielen Fällen nur ungenügend vor [20]. Sehr schwierig ist es, aussagekräftige Daten über menschliche Fehlhandlungen zu erhalten [21].

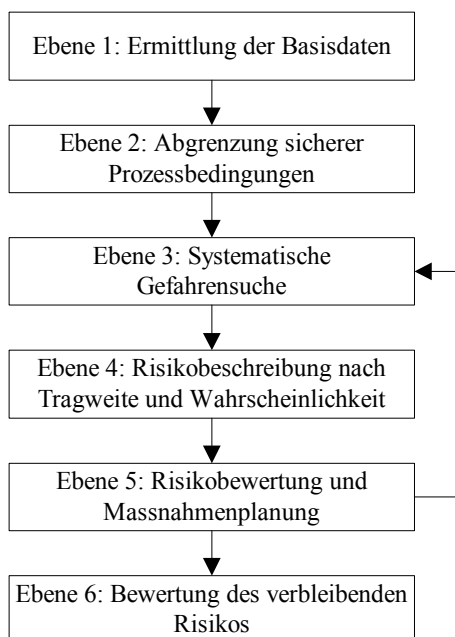


Abbildung 9

## **Ebene 2: Abgrenzung sicherer Prozessbedingungen**

Aufgrund der erhobenen Basisdaten können die Bedingungen, Grenzen und Bandbreiten festgelegt werden, die zur sicheren Durchführung der einzelnen Prozessschritte eingehalten werden müssen. Sichere Prozessbedingungen werden definiert und damit die Voraussetzungen an das Anforderungsprofil für die bestehende Mehrproduktanlage, das notwendig ist, um die inhärenten Gefahren der Prozessstufe zu kontrollieren. Es wird aufgezeigt, welche «Module» schliesslich die bestehenden Gefahren kontrollieren. Dadurch werden auch die Anforderungen an die Organisation sichtbar, welche die Mängel der Anlage überbrücken müssen, und bei der Mehrproduktanlage notwendig sind, um die der Prozessstufe inhärenten Gefahren zu kontrollieren.

## **Ebene 3: Systematische Gefahrensuche**

Der Prozess wird in seinem Umfeld (Anlage, Personal, Arbeitsabläufe und Umgebung) auf Möglichkeiten untersucht, die zu Abweichungen von den sicheren Prozessbedingungen führen können. Die Gefahrensuche erstreckt sich auf folgende kritische Bereiche:

Beim Aufbau von chemischen Prozessen müssen mit einer systematischen Prozessentwicklung - Synthesewahl, Prozesskonzept etc. - von Anfang an hohe Tragweiten von möglichen Ereignissen reduziert werden. Von Anfang an muss die Fahrweise so aufgebaut werden, dass die Zeitdauer, bis sich ein Ereignis mit hoher Tragweite bei einer Prozessabweichung manifestiert, möglichst gross wird.

- Chemikalien
- Prozessstufen (Reaktionen, thermische Belastungen etc.)
- Anlage, Steuerung, Energieversorgung
- Mensch-Maschine-Interaktionen
- Umfeld, äussere Einwirkung

Die Gefahrensuche muss das technische System und die Schnittstellen umfassen.

Das Ergebnis der systematischen Gefahrensuche ist die Auflistung von möglichen Abweichungen vom Normalbetrieb und von Schadensszenarien. Diese können mit ihren Verknüpfungen auch durch einen Fehlerbaum dargestellt sein und müssen im folgenden Schritt genauer analysiert werden.

#### **Ebene 4: Risikobeschreibung**

Die gefundenen Gefahren müssen beurteilt und als Risiko formuliert werden. Das Risiko wird als Funktion von Eintrittswahrscheinlichkeit und Tragweite beschrieben. Die Bestimmung der Terme Eintrittswahrscheinlichkeit und Tragweite erfolgt mit einem qualitativen oder mit einem halbquantitativen Ansatz. Für die Beschreibung des thermischen Risikos des Bereichs Prozess in der MPA genügen drei Niveaus für die Wahrscheinlichkeit und die Tragweite, nämlich tief, mittel und hoch (siehe Tabelle 8).

#### **Ebenen 5 und 6: Massnahmen und Bewertung**

Die signifikanten Risiken sollen durch die Massnahmen auf ein tragbares Mass reduziert werden. Wichtige Hinweise für die Massnahmenplanung gibt eine Sensitivitätsanalyse (Einfluss von technischen Systemparametern auf kritische Risiken). Bei der Massnahmenplanung gilt folgende Hierarchie:

- Aufbau von inhärent sicheren Prozessen in Bezug auf Chemie, Verfahren und Apparate wählen.
- Bei Risiken werden primär hohe Tragweiten durch technische Massnahmen minimiert, z.B. durch Reduzieren der Gefahrenmenge durch die Wahl eines Dünnschichtverdampfers anstelle der Batchdestillation. Erst in zweiter Linie werden die Eintrittswahrscheinlichkeiten reduziert (Prozessüberwachung).
- Risiken durch technische und organisatorische Massnahmen bezüglich Ereignistragweite reduzieren (Prozessabsicherung, Notmassnahmen).

Die Risikoanalyse soll die Verfahrensentwicklung iterativ von Anfang an begleiten (siehe Abb. 9). Nur so können die Sicherheitsmassnahmen gemäss Bearbeitungstiefe und Informationsstand stufenweise ausgebaut werden. Schliesslich ist bei der Planung von Sicherheitsmassnahmen noch auf folgende Punkte zu achten:

- Sicherheitsmassnahmen sind sorgfältig auf neue Risiken zu überprüfen (bei der Montage eines Sicherheitsventils zur Druckabsicherung eines Reaktors tritt eine neue Gefahr auf, nämlich die der Freisetzung von toxischen oder explosionsgefährlichen Stoffen).

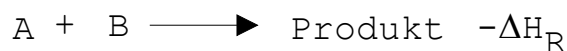
- Die optimale Mensch-Maschine-Interaktion ist bei Sicherheitsmassnahmen besonders wichtig. Dabei tritt das Problem auf, dass in einem voll automatisierten Betrieb im Normalfall der Mensch durch die Technik bestimmt wird, dass jedoch, um Störfälle zu verhindern, die Technik durch den Menschen kontrollierbar sein muss.
- Sicherheitsmassnahmen sind so auszulegen, dass ein einfacher Fehler nicht zu einem Ereignis mit hoher Tragweite führen kann.
- Der Nutzen der Risikoanalyse ist stark abhängig von einer hohen Sicherheitskultur, welche erst die sorgfältige Implementierung und die nachfolgende Erhaltung der gewählten Schutzmassnahmen ermöglicht.

Sicherheitskultur bedeutet im Betrieb unter anderem, ein hohes Niveau des technischen Unterhalts und der Sicherheitsausbildung zu erreichen.

Sicherheitskultur bedeutet auch, dass die Risikoanalyse die Verfahrensentwicklung iterativ von Anfang an begleitet, damit die Sicherheitsmassnahmen gemäss Bearbeitungstiefe und Informationsstand stufenweise ausgebaut werden können.

## 2.4 Klassifizierung von chemischen Prozessstufen [22]

Am Beispiel einer exothermen Semibatch Reaktion wird gezeigt, wie sich ein chemisches System während einer Abweichung vom Normalbetrieb verhält: In einer Mehrproduktanlage wird Stoff A mit Stoff B bei einer vorgegebenen Reaktionstemperatur  $T_R$  umgesetzt (Abb. 10), wobei Wärme freigesetzt wird.



Oberhalb der Reaktionstemperatur erreicht eine Zersetzungsreaktion eine sicherheitsrelevante Geschwindigkeit.

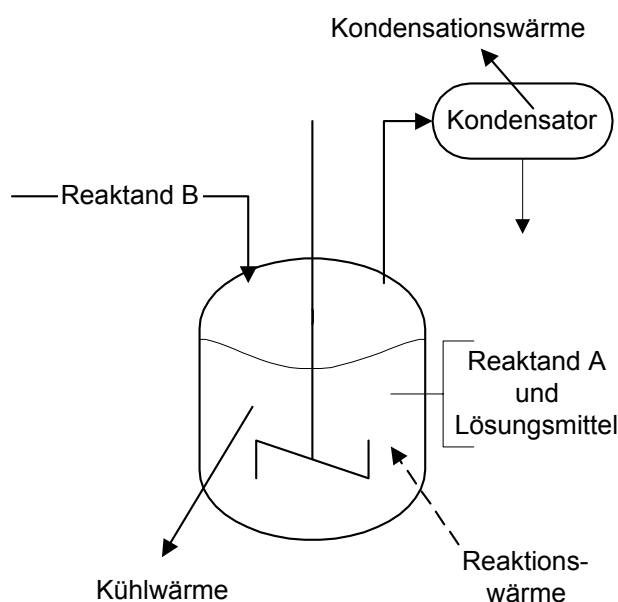


Abbildung 10

Der Normalbetrieb der Prozessstufe stellt sich wie folgt dar:

- Reaktand A und das Lösungsmittel werden in einen Reaktor bei Raumtemperatur vorgelegt und bis zu der Reaktionstemperatur  $T_R$  erhitzt.
- Reaktand B wird dann während einer festgelegten Zeitdauer in den Reaktor dosiert, wobei die Temperatur  $T_R$  durch Kühlen konstant gehalten wird.

- Nach beendeter Dosierung wird die Temperatur während einer vorgegebenen Zeit konstant gehalten.
- Der Reaktor wird abgekühlt und entleert.

Damit der Normalbetrieb eingehalten und die vorgegebene Reaktionstemperatur durch Kühlen gehalten werden kann, muss die abgeführte Wärme gleich gross sein wie die Wärme, die durch die chemische Reaktion in den Reaktor gebracht wird [23].

Das Risiko einer thermischen Explosion wird sichtbar gemacht mit dem *Szenario einer Kühlpanne* mit nachfolgender Zersetzungsreaktion (Abb. 11). Das Kühlpannen-Szenario basiert auf adiabatischen Bedingungen, denn

- durch die Kühlpanne ist die Wärmeabfuhr stark eingeschränkt,
- und das adiabatische System ist unabhängig von technischen Betriebsparametern.

Darum ist das adiabatische System für den Betriebsmassstab eine sichere Näherung.

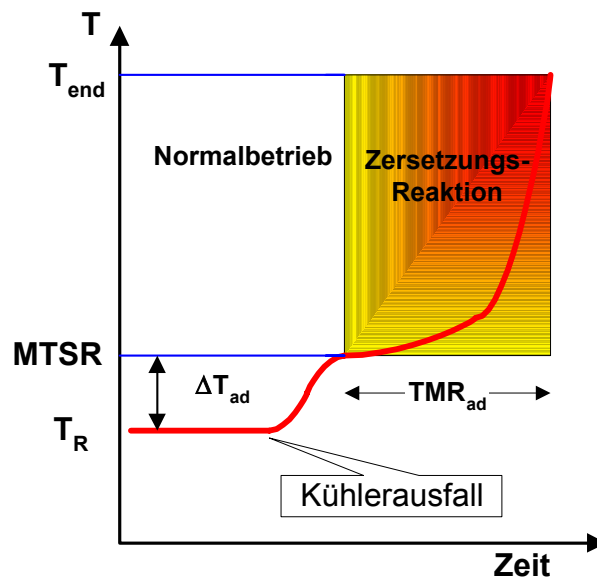


Abbildung 11

Es sind nunmehr zwei Fragenkomplexe zu beantworten.

#### Fragenkomplex zur Thermodynamik

- Kann die Prozesstemperatur  $T_R$  vom Kühlsystem kontrolliert werden?
- Wie hoch steigt die Temperatur beim Kühlerausfall? In den Abbildungen 11 und 12 ist dies mit MTSR (Maximale Temperatur der Synthese-Reaktion) bezeichnet.
- Wie ist die Siedetemperatur  $T_b$  der Reaktionsmasse im Verhältnis zur MTSR?
- Welche Menge der Reaktionsmasse kann bei Einstellung der MTSR verdampfen?
- Welche Temperatur  $T_{end}$  und welcher Druck  $P(T_{end})$  wird - ausgehend von der MTSR - durch die Zersetzungsreaktion erreicht?



---

## Fragenkomplex zur Kinetik

- Zu welchem Zeitpunkt der Prozessführung ist eine Kühlpanne kritisch?
- Wieviel Zeit braucht das Durchgehen der erwünschten Reaktion?
- Wie schnell verdampft die potentielle Menge der Reaktionsmasse?
- Wieviel Zeit braucht der Runaway aufgrund der Zersetzungsreaktion?

Die Temperatur  $T_{\text{end}}$  bzw.  $\Delta T_{\text{ad}}$  ist ein *Mass für die Tragweite* einer thermischen Explosion. Die Zeit bis zum Erreichen der Temperatur  $T_{\text{End}}$  - **Time to Maximum Rate** ( $\text{TMR}_{\text{ad}}$ ) - gilt als *Mass für die Eintrittswahrscheinlichkeit* einer thermischen Explosion. Die Wahrscheinlichkeit ist nämlich gross, dass bei Prozessabweichungen in der MPA ein Ereignis mit grosser Tragweite eintritt, wenn nur wenig Zeit für Gegenmassnahmen zur Verfügung steht. Für die Beurteilung der thermischen Prozessrisiken benötigen wir also thermodynamische Grössen wie  $\Delta T_{\text{ad}}$  und kinetische Grössen wie  $\text{TMR}_{\text{ad}}$ .

Für die Beschreibung des thermischen Risikos des Bereichs Prozess in der MPA genügen drei Niveaus für die Wahrscheinlichkeit und die Tragweite, nämlich tief, mittel und hoch (Tabelle 8).

	<b>Tragweite</b>	<b>Wahrscheinlichkeit</b>
<b>hoch</b>	$\Delta T_{\text{ad}} > 200 \text{ K}$	$\text{TMR}_{\text{ad}} < 8 \text{ h}$
<b>mittel</b>	$50 \text{ K} < \Delta T_{\text{ad}} < 200 \text{ K}$	$8 \text{ h} < \text{TMR}_{\text{ad}} < 24 \text{ h}$
<b>tief</b>	$\Delta T_{\text{ad}} < 50 \text{ K} *$	$\text{TMR}_{\text{ad}} > 24 \text{ h}$
* Wenn ein Stoffaustritt ausgeschlossen werden kann. (Vorsicht bei geschlossenen Systemen)		

Tabelle 8

Aus dem Pannenszenario ist ersichtlich, dass vier Temperaturen wichtig sind:

- Die Prozesstemperatur  $T_p$
- Die maximale Temperatur (MTSR), die aufgrund des Durchgehens der erwünschten Reaktion erreicht wird, wenn keine Wärme mehr abgeführt werden kann (Kühlpanne oder Rührerunterbruch). Sie ist eine Funktion der Akkumulation nicht verbrauchter Reaktanden.
- Die Temperatur, ab welcher die Zersetzungsreaktion kritisch wird, also die Temperatur, bei der die  $\text{TMR}_{\text{ad}}$  24 Stunden unterschreitet.
- Die maximal tolerierbare Temperatur. Im offenen System ist es der Siedepunkt ( $T_b$ ), im geschlossenen System ist es diejenige Temperatur, bei welcher der Druck so gross ist, dass das Sicherheitsventil oder die Berstscheibe der Anlage ansprechen.

Aufgrund dieser vier Temperaturen sind fünf Szenarien möglich. Sie sind nach F. Stössel [21] mit steigender Kritikalität [24] in der Abbildung 12 klassifiziert.

**Klasse 1:** Wenn die Synthesereaktion nicht mehr kontrolliert werden kann, genügt die akkumulierte Wärme nicht, um die Reaktionsmasse auf die Siedetemperatur zu erhitzen. Die Zersetzungsreaktion kann nicht ausgelöst werden. Nur wenn die Reaktionsmasse während längerer Zeit unter Wärmestaubedingungen gehalten wird, könnte die Siede-

temperatur erreicht werden. In diesem Fall würde die Verdampfungskühlung als zusätzliche «Sicherheitsbarriere» wirken. Die Reaktionsstufe ist in dieser Situation thermisch sicher.

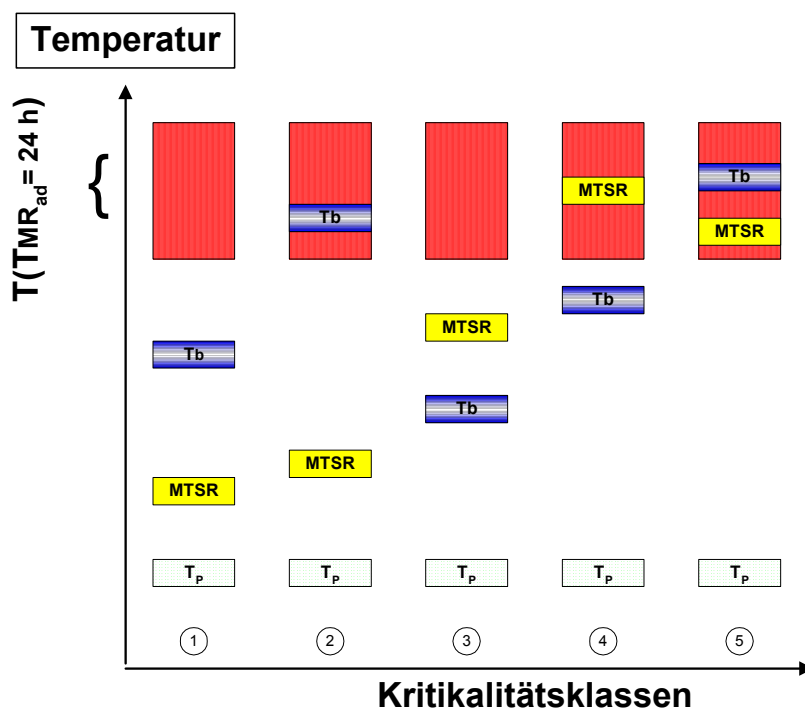


Abbildung 12

**Klasse 2:** Wenn die Synthesereaktion nicht mehr kontrolliert werden kann, genügt die akkumulierte Wärme nicht, um die Reaktionsmasse auf die Siedetemperatur zu erhitzen. Die Zersetzungsreaktion kann nicht ausgelöst werden. Wenn die Reaktionsmasse während längerer Zeit unter Wärmestaubedingungen gehalten wird, könnte die Zersetzungsreaktion ausgelöst und die Siedetemperatur erreicht werden. Wenn aufgrund der Wärmeleistung der Zersetzungsreaktion eine grosse Verdampfungsgeschwindigkeit entsteht, kann es zu einem gefährlichen Betriebszustand kommen.

**Klasse 3:** Wenn die Synthesereaktion nicht mehr kontrolliert werden kann, genügt die akkumulierte Wärme, um die Reaktionsmasse auf die Siedetemperatur zu erhitzen. Die Zersetzungsreaktion kann aber nicht ausgelöst werden. Die Sicherheit der Prozessstufe hängt hier davon ab, wie gross die Wärmeleistung bei der Siedetemperatur ist.

**Klasse 4:** Wenn die Synthesereaktion nicht mehr kontrolliert werden kann, genügt die akkumulierte Wärme, um die Reaktionsmasse auf die Siedetemperatur zu erhitzen. Die Zersetzungsreaktion kann aber ausgelöst werden. Bei diesem Szenario hängt die Sicherheit der Prozessstufe davon ab, wie gross die Summe der Wärmeleistungen der Synthesereaktion und der Zersetzungsreaktion ist. In einem offenen System kann die Verdampfungskühlung als Sicherheitsbarriere wirken. Die Auslegung des Destillationssystems ist in diesem Fall entscheidend.

**Klasse 5:** Wenn die Synthesereaktion nicht mehr kontrolliert werden kann, genügt die akkumulierte Wärme, um die Reaktionsmasse auf die Temperatur zu erhitzen, bei der die Zersetzungsreaktion ausgelöst wird.

Es ist unwahrscheinlich, dass die Verdampfungskühlung in dieser Situation als Sicherheitsbarriere wirken kann.

Die Abbildung 13 zeigt die notwendigen Untersuchungen für die Klassifizierung von chemischen Prozessstufen.

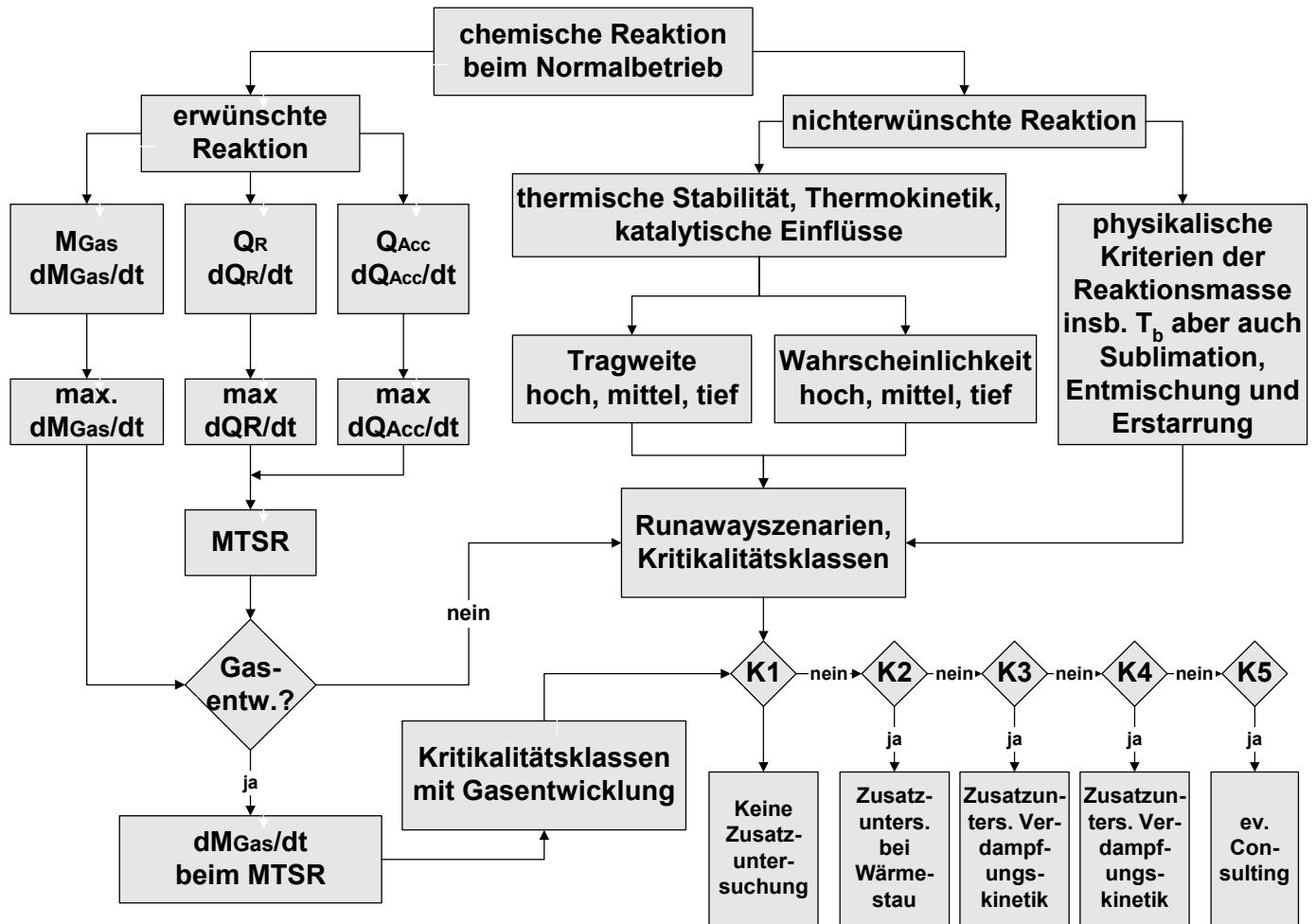


Abbildung 13

Wird zusätzlich zu den Temperaturen  $T_R$ ,  $MTSR$ ,  $T_b$  und  $T(TMR_{ad} = 24 \text{ h})$  noch die Gasentwicklung berücksichtigt, so gelangen wir zu einer Erweiterung der Klassifizierung (Abb. 14).

Beim Entwickeln von chemischen und thermischen Prozessstufen soll die Fahrweise von Anfang an so aufgebaut werden, dass die Zeitdauer, bis sich bei einer Prozessabweichung ein Ereignis mit hoher Tragweite manifestiert, möglichst gross wird.

Die Kritikalitätsklassen bilden die Grundlage zur Ausarbeitung von risikomindernden Massnahmen

Die **modulare Fehlerbaumanalyse** basiert auf der Fehlerbaumtechnik.

Bei ihr werden vorgefertigte «modulare» Fehlerbäume, die aus dem Gesamtsystem «Prozess, MPA und Organisation» stammen, zu Freisetzungsszenarien zusammengestellt.

Damit die Fehlerbaumanalyse erfolgreich auf die MPA angewendet werden kann, muss ein vollständiges Verständnis des modularen Aufbaus des Systems «Prozess - MPA» einerseits und der Zuverlässigkeit der Betriebsmodule und der Schutzmodule andererseits, vorhanden sein.

Aber genau das verlangen die Grundsätze für die Risikoanalyse bei MPA (siehe dazu Glossarkasten auf Seite 15).

Auf dieser Basis eignet sich die modulare Fehlerbaumanalyse vorzüglich für den effizienten Dialog zwischen den Prozesschemikern einerseits und den Sicherheitsingenieuren andererseits.

Das Ziel der quantitativen Risikoanalyse ist die Bewertung des Risikos in Zahlen in Bezug auf die Eintretenswahrscheinlichkeit und die Tragweite. Das Resultat der quantitativen Risikoanalyse ist ein Zahlenwert, der die Dimension Schaden pro Zeiteinheit hat. Die quantitative Risikoanalyse setzt voraus, dass das analysierte Risiko bereits durch die systematische Gefahrensuche als Gefahr erkannt worden ist. Mit der quantitativen Risikoanalyse können keine neuen Gefahren gefunden werden.

## 2.5 Risikobeurteilung mit modularen Fehlerbäumen [25]

### 2.5.1 Einleitung

Im Folgenden wollen wir den grossen Nutzen zeigen, der durch die Klassifizierung der chemischen Prozessstufen für den Mehrproduktbetrieb entsteht. Es ist nämlich möglich, auf der Basis der Klassifizierung von chemischen Prozessstufen einerseits und der modular aufgebauten MPA andererseits, eine Fehlerbaumanalyse durchzuführen, und so für die Risikoanalyse von chemischen Prozessen in MPA ein Werkzeug bereitzustellen, das sich bei der Beurteilung von Monoanlagen bewährt hat.

Die Fehlerbaumanalyse ist eine graphische Methode, sie geht deduktiv vom unerwünschten Ereignis aus und analysiert alle möglichen Wege und Verknüpfungen, die zu diesem Ereignis führen können. Mit der Fehlerbaumanalyse werden diejenigen logischen Verknüpfungen von Komponenten- oder Teilsystem-Ausfällen ermittelt, die zum unerwünschten Ereignis führen. Der Fehlerbaum ist ein Modell des Ausfallverhaltens des zu sichernden Systems. Er besteht aus Bildzeichen für die Eingänge und die Verknüpfungen. Innerhalb des Fehlerbaums stellen die Verknüpfungen die logischen Zusammenhänge dar und formen die Eingangssignale gemäss ihren Regeln in Ausgangssignale um. Bei der Fehlerbaumanalyse wird vom unerwünschten Ereignis ausgegangen, die Eingänge der Verknüpfungsbausteine sind unten und die Ausgänge oben abgebildet. Es werden nur diejenigen Verknüpfungen dargestellt, die ein unerwünschtes Ereignis zur Folge haben.

Die verschiedenen Wege, die zum betrachteten Ereignis führen, werden durch zwei Kombinationen von zwei oder mehreren «auslösenden Ereignissen» beschrieben:

- Die Kombination der «Und-Verknüpfung»
- Die Kombination der «Oder-Verknüpfung»

Bei der **«Und-Verknüpfung»** müssen die «auslösenden Ereignisse» gleichzeitig erfüllt sein, damit das Ereignis eintreten kann. Darum ist die Wahrscheinlichkeit, dass das Folge-Ereignis eintritt, kleiner als die der «auslösenden Ereignisse». Wenn die auslösenden Ereignisse voneinander unabhängig sind, so ist die Wahrscheinlichkeit des Folge-Ereignisses gleich dem Produkt der Einzelwahrscheinlichkeiten:

Bei der **«Oder-Verknüpfung»** reicht jedes auslösende Ereignis aus, um das betrachtete Folge-Ereignis auszulösen. Das heisst, die Wahrscheinlichkeit ist die Summe der einzelnen Ereigniswahrscheinlichkeiten.

Mit Fehlerbaumanalysen werden speziell Systeme von zeitinvarianten Eigenschaften modelliert. Sie eignen sich besonders für die Analyse von kontinuierlichen Prozessen und für die Analyse von zeitinvarianten Einrichtungen in diskontinuierlichen Teilprozessen wie z.B. Schutzeinrichtungen.

Chemische Prozesse in MPA sind aber zeitabhängig. Die Prozessparameter (Temperatur, Druck, Konzentration usw.) sind vom jeweiligen Prozessschritt abhängig und innerhalb des Prozessschrittes von der Zeit. Wenn wir nun das zu analysierende System in die Bereiche «tech-

nisches System» und «Prozess» unterteilen, können für beide Bereiche unabhängige Teilfehlerbäume erstellt werden, die zeitinvariante Strukturen darstellen, welche sich für die Modellierung von Freisetzungsszenarien eignen. Diese zeitinvarianten Strukturen können mit Fehlerbäumen modelliert werden.

- Die Fehlerbäume für den Bereich «Prozess» folgen aus den Kritikalitätsklassen (Abb. 12 und 14). Sie beschreiben die übergeordneten Strukturen der Gesamtfehlerbäume und lassen sich unabhängig von standardisierten Teilsystemen bilden.
- Die Fehlerbäume für den Bereich «technisches System» folgen aus den standardisierten Modulen der Mehrproduktanlage (Abb. 20). Die Fehlerbäume des Bereichs «technisches System» werden mit der übergeordneten Struktur gekoppelt, sie bilden die Systemebene.

### 2.5.2 Übergeordnete Fehlerbäume

Die übergeordneten Fehlerbäume ergeben sich aus der Klassifizierung der Prozessstufe. Mit einem Entscheidungsbaum (Abb. 14, [26]) können Szenarien, welche die übergeordneten Strukturen für die Bildung von Fehlerbäumen zum Prozessmodul bilden, abgeleitet werden.

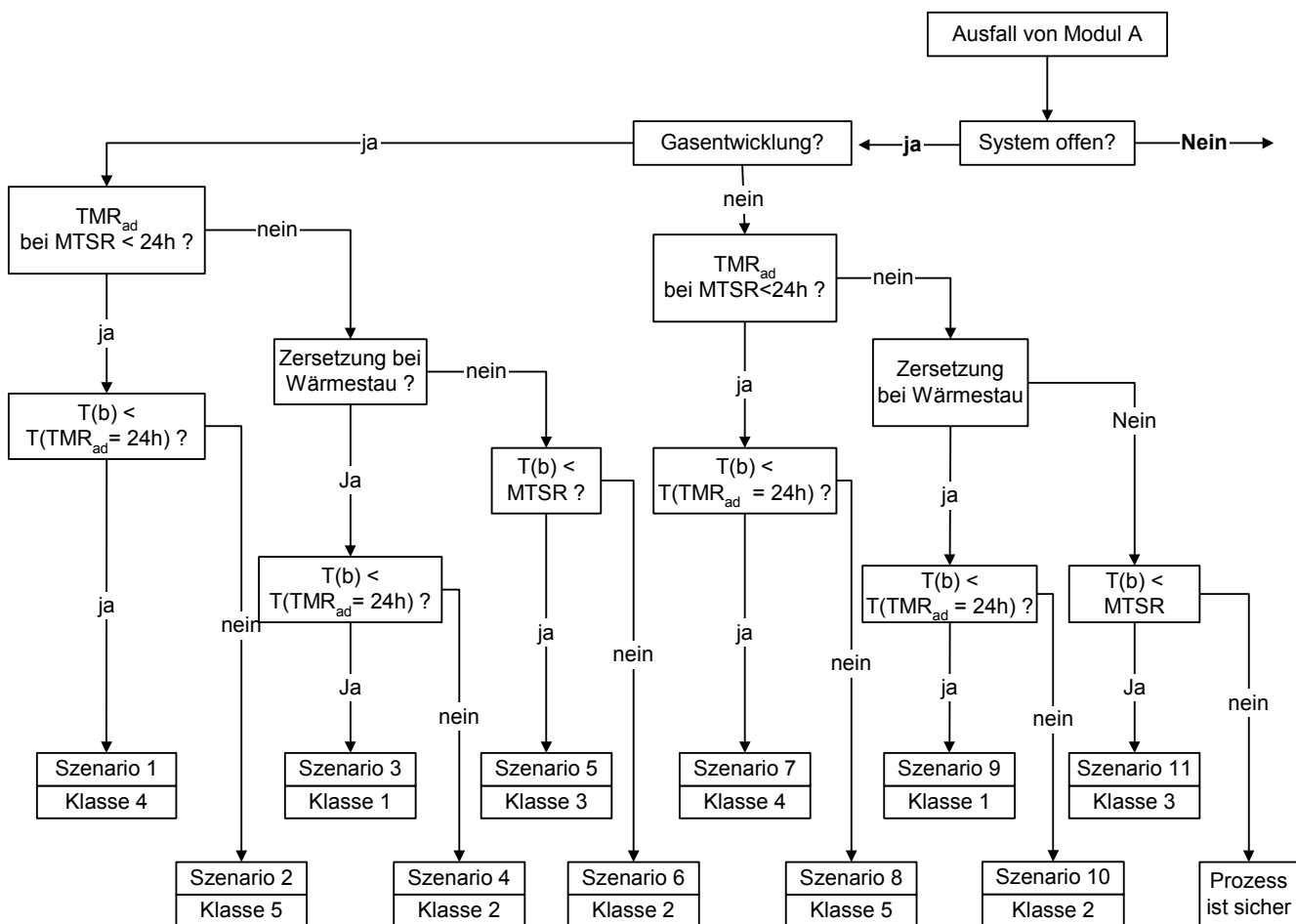


Abbildung 14

Die Entscheidungen werden aufgrund folgender Kriterien gefällt:

- Frage nach dem System: offen oder geschlossen.

Chemische Prozesse in MPA sind zeitabhängig. Die Prozessparameter (Temperatur, Druck, Konzentration usw.) sind vom jeweiligen Prozessschritt abhängig und innerhalb des Prozessschrittes von der Zeit.

Wird das System «Prozess-Mehrproduktanlage-Organisation» in die Teilsysteme «technisches System» und «Prozess» unterteilt, können für diese Teilfehlerbäume modelliert werden. Diese sind voneinander unabhängig und auch zeitunabhängig.

Die Teilfehlerbäume können zu «modularen» Fehlerbäumen verknüpft werden. Dadurch entsteht ein Instrument mit dem beim System «Prozess-Mehrproduktanlage-Organisation» Freisetzungsszenarien analysiert werden können.

Die Fehlerbäume für das Teilsystem «Prozess» folgen aus den Kritikalitätsklassen, die aus der sicherheitstechnischen Untersuchung abgeleitet werden. Sie beschreiben die übergeordneten Strukturen der Gesamtfehlerbäume und lassen sich unabhängig von standardisierten Teilsystemen bilden.

Die Fehlerbäume für das Teilsystem «technisches System» folgen aus den standardisierten Modulen der Mehrproduktanlage. Sie sind prozessunabhängig. Die Fehlerbäume des Bereichs «technisches System» werden mit der übergeordneten Struktur gekoppelt.

Die prozessunabhängigen Fehlerbäume der technischen Module werden mit prozessunabhängigen Fehlerbäumen (Komponentenausfälle, Versorgungsausfälle und menschliche Fehlhandlungen) und prozessabhängigen Fehlerbäumen, die aufgrund der Durchführung eines bestimmten Prozesses möglich sind, gekoppelt.

- Frage zur Gasentwicklung: ja/nein
- $TMR_{ad}$  bei  $MTSR < 24$  h: ja/nein
- Zersetzung bei Wärmestau: ja/nein
- $T_b < T(TMR_{ad} = 24 \text{ h})$ : ja/nein (Frage nach der Siedebarriere)

Die Siedebarriere wird gesondert von den Schutzmodulen betrachtet, sie ist eine inhärente Eigenschaft der Prozessstufe und ist eine vom technischen System unabhängige Sicherheitsmassnahme [27].

Es sind folgende Szenarien denkbar, die zur Reaktorexlosion durch Zersetzung führen können[28].

- **System offen und Gasentwicklung**

- **Szenario 1:** Der Siedepunkt kann als Barriere dienen. Erst durch das Versagen von Siedebarriere und Schutzmassnahmen kann das unerwünschte Ereignis eintreten (geringere Anforderung an das technische System).

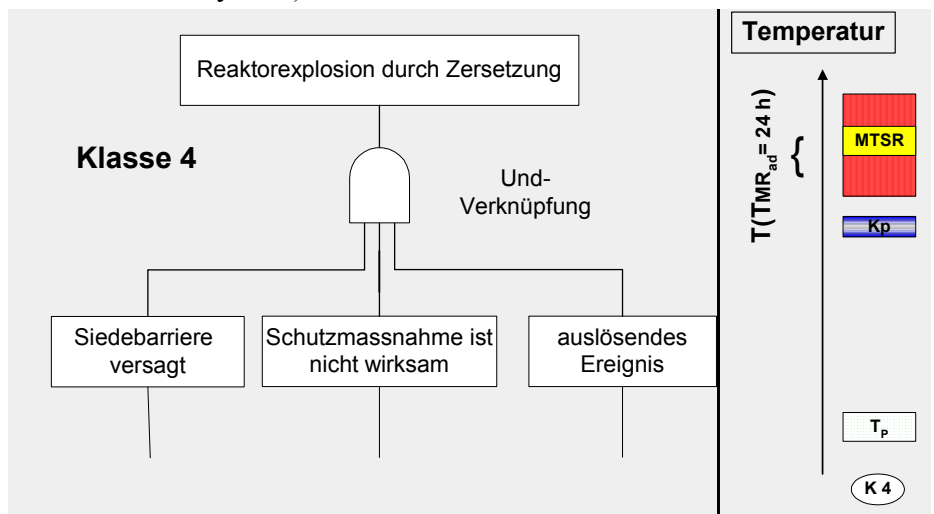


Abbildung 15

Hier ist die Gasbildung als zusätzlicher Faktor zum Druckaufbau zu beachten. Das Szenario entspricht der Klasse 4 (Abb. 15).

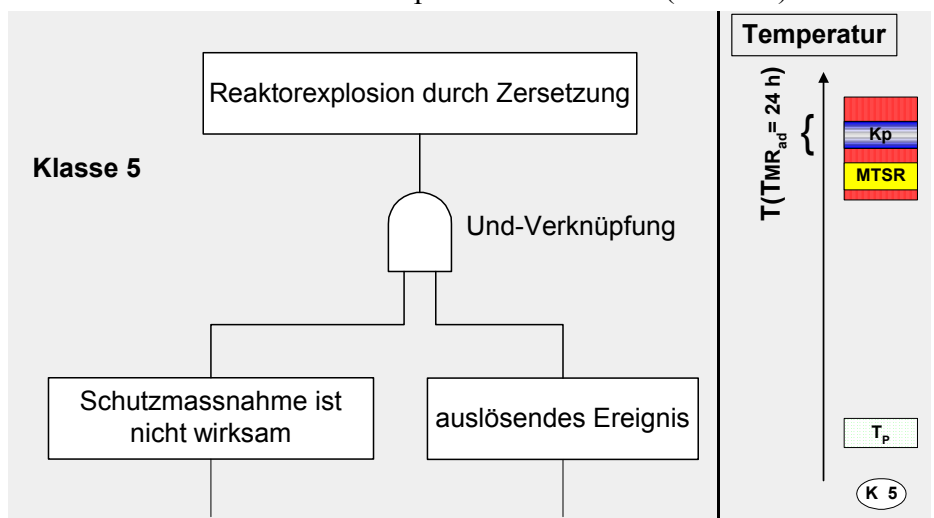


Abbildung 16

- **Szenario 2:** Der Siedepunkt dient nicht als Barriere, der Reaktionsablauf muss mit Hilfe technischer Massnahmen unterbrochen werden, was hohe Anforderung an das technische System stellt. Auch hier ist die Gasbildung als zusätzlicher Faktor zum Druckaufbau zu beachten. Das Szenario entspricht der Klasse 5 (Abb. 16).
- **Szenario 3:** Nur durch Wärmestau kann eine Zersetzung ausgelöst werden. Der Siedepunkt kann als Barriere dienen. Das Szenario stellt geringere Anforderung an das technische System, eventuell sind zusätzlich organisatorische Massnahmen nötig. Wiederum ist die Gasbildung als zusätzlicher Faktor zum Druckaufbau zu beachten. Das Szenario entspricht der Klasse 1 (Abb. 17).

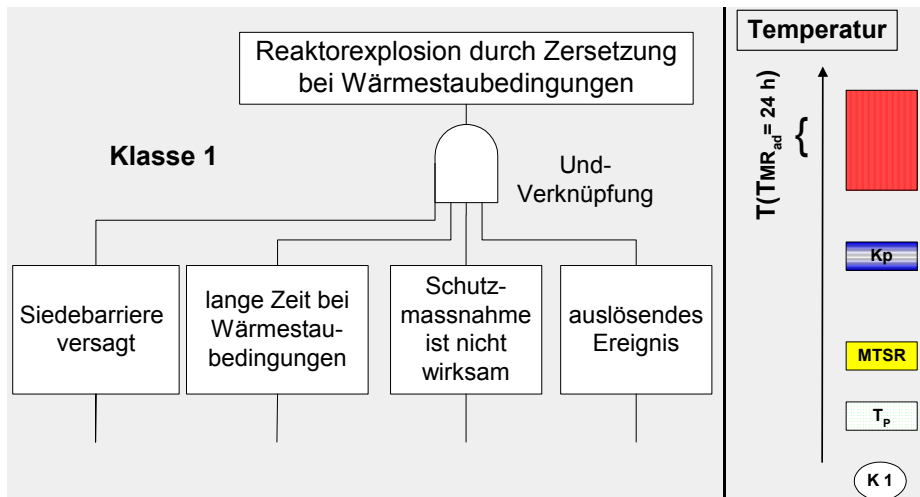


Abbildung 17

- **Szenario 4:** Nur durch Wärmestau kann eine Zersetzung ausgelöst werden; es ist keine Siedebarriere vorhanden (geringere Anforderung an das technische System, zusätzlich organisatorische Massnahmen). Gasbildung als zusätzlicher Faktor zum Druckaufbau ist zu beachten. Das Szenario entspricht der Klasse 2 (Abb. 18).

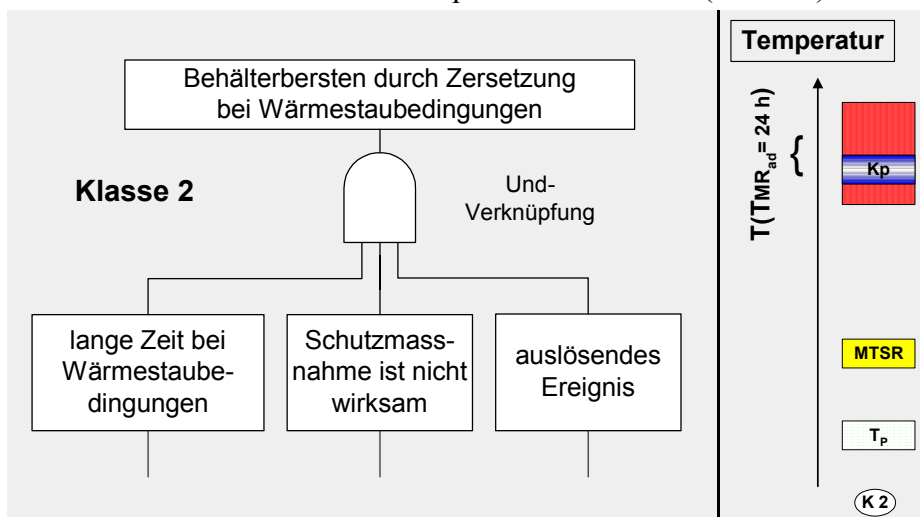


Abbildung 18

- **Szenario 5:** Durch Verdampfung und Gasbildung kann Druck aufgebaut, jedoch keine Zersetzung erreicht werden. Der Druckaufbau

muss genügend gross sein, um eine Reaktorexlosion zu erzeugen (höhere Anforderung an das technische System). Das Szenario entspricht der Klasse 3 (Abb. 19).

- **Szenario 6:** Durch Gasbildung kann Druck aufgebaut werden, es wird jedoch keine Zersetzung erreicht. Der Druckaufbau muss genügend gross sein, um eine Reaktorexlosion zu erzeugen (höhere Anforderung an das technische System). Das Szenario entspricht der Klasse 3.

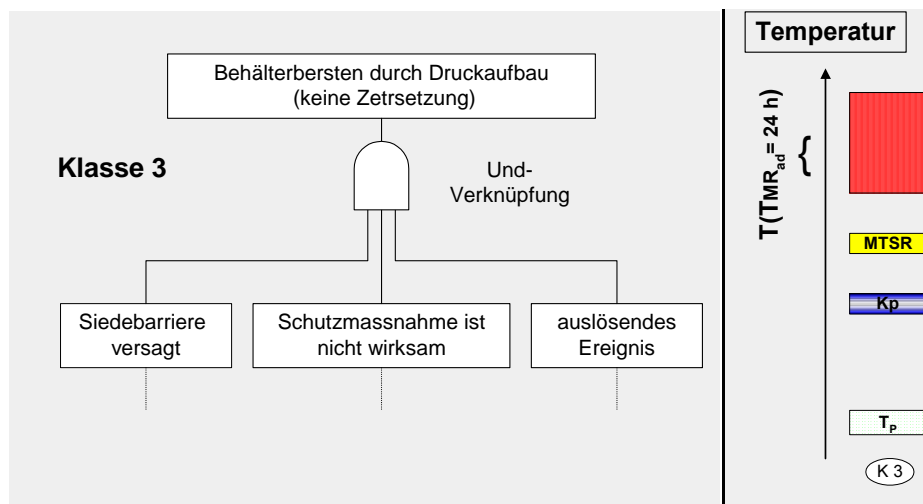


Abbildung 19

- **System offen, keine Gasentwicklung**
  - **Szenario 7:** Analog zu Szenario 1, jedoch ohne zusätzliche Gasbildung. Das Szenario entspricht der Klasse 4.
  - **Szenario 8:** Analog zu Szenario 2, jedoch ohne zusätzliche Gasbildung. Das Szenario entspricht der Klasse 5.
  - **Szenario 9:** Analog zu Szenario 3, jedoch ohne zusätzliche Gasbildung. Das Szenario entspricht der Klasse 1.
  - **Szenario 10:** Analog zu Szenario 5, jedoch ohne zusätzliche Gasbildung. Das Szenario entspricht der Klasse 2.
  - **Szenario 11:** Analog zu Szenario 4, jedoch ohne zusätzliche Gasbildung. Das Szenario entspricht der Klasse 3.

### 2.5.3 Die Systemebene: Fehlerbäume für technische Module

Die Fehlerbäume für die technischen Module sind vom chemischen Prozess losgelöst, sie bilden die Systemebene der modularen Fehlerbaumanalyse. Die technischen Module beschreiben Teilsysteme, die dem Betrieb, der Überwachung und dem Schutz der Anlage dienen. Es gibt zwei Gruppen von Modulen, die voneinander unabhängig gebildet werden (Abb. 20).

- Betriebsmodule stellen, wenn sie versagen, ein auslösendes Ereignis dar. Diese Einrichtungen sind bei Mehrproduktanlagen nur zeitweise aktiv.
- Überwachungs- und Schutzmodule führen die Anlage nach einer Abweichung in den sicheren Zustand. Im Gegensatz zu den Betriebseinrichtungen sind diese im Hintergrund dauernd aktiv.



Die Module können in eindeutige, prozessunabhängige Funktionen unterteilt werden (Tabellen 9 und 10).

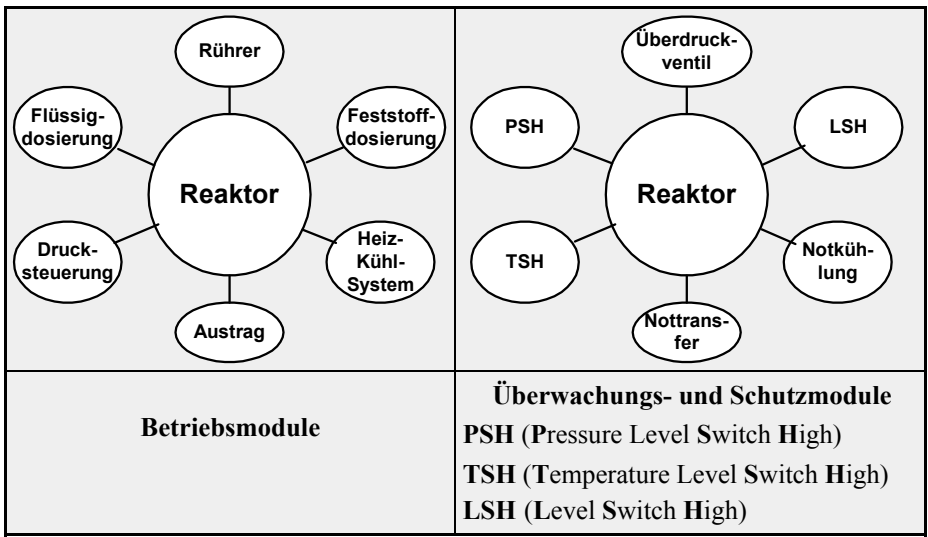


Abbildung 20

Betriebsmodul	Prozessunabhängige Funktionsdefinition
Heiz- Kühlsystem	Kühlen mit Wärmeträgermedium zwischen .. °C und ... °C Heizen mit Wärmeträgermedium zwischen ... und ... °C Durchflussmenge Wärmeträgermedium ... L/min
Rührer	Rührerdrehzahl ...rpm
Dosierung	Eintrag von ...kg/min

Tabelle 9

Diese Funktionen ergeben zusammen mit Rohrleitungs- und Instrumentenflussbilder der Teilsysteme [29] prozessunabhängige Fehlerbäume.

Überwachungs- und Schutzmodul	Prozessunabhängige Funktionsdefinition
TSH	Verriegelung der Dosierung oberhalb .... °C
LSH	Verriegelung des Eintrags ab Füllstand ... L
Notkühlung	Kühlung mit Trinkwasser mit Durchfluss ... L/min
Nottransfer	Transfer des Reaktorinhalts innerhalb der Zeitdauer von ...min

Tabelle 10

**2.5.4 Die Subsystemebene**

In der Subsystemebene werden die prozessunabhängigen Fehlerbäume der technischen Module mit den prozessunabhängigen Fehlerbäumen (Komponenten- und Versorgungsausfälle sowie menschliche Fehlhandlungen) und den prozessabhängigen Fehlerbäumen gekoppelt (siehe Abb. 21). *Prozessabhängige Fehler sind aufgrund der Durchführung eines bestimmten Prozesses möglich. Durch den Einfluss des chemischen Prozesses können Zuverlässigkeitskenngrößen verändert werden, z.B. kann sich die Ausfallwahrscheinlichkeit eines Ventils, das ein Schutzmodul darstellt, infolge korrosiver Medien erhöhen. Bei der Durchführung von chemischen Prozessen können auch neue auslö-*

Für die Beurteilung von ereignisverhindernden Massnahmen ist die Analyse der «Minimal Cut Sets» ein wichtiges Instrument. Ein «Minimal Cut Set» ist die minimale Kombination von Fehlern (Ausfällen), die ausreichen, um ein System vom Zustand der Funktion in den Zustand des Ausfalls zu führen. Die «Minimal Cut Sets» werden mit der Fehlerbaumtechnik ermittelt. Ein bestimmtes Ereignis wird unter Berücksichtigung der logischen Verknüpfungen durch die Basisereignisse ausgedrückt. Mit den Regeln der Booleschen Algebra wird der Ausdruck der Verknüpfungen soweit umgeformt, dass die «Minimal Cut Sets» sichtbar werden.

Wenn bei der Berechnung eines Freisetzungsszenarios

- ein oder mehrere «Minimal Cut Sets» auftreten, die nur ein Ereignis haben (ein Einzelausfall führt zur Freisetzung) so erfordern diese Szenarien zusätzliche Massnahmen;
- nur «Minimal Cut Sets» mit zwei Ereignissen auftreten (zwei unabhängige Fehler führen zum übergeordneten Ereignis) so muss, je nach Eintrittswahrscheinlichkeit und Art der Einzelereignisse, entschieden werden, ob diese akzeptiert werden können oder ob zusätzliche Massnahmen zu ergreifen sind;
- nur «Dreier Cut Sets» auftreten und besitzt jedes Ereignis eine geringe Eintrittswahrscheinlichkeit, so erübrigt sich in den meisten Fällen der Einsatz zusätzlicher Massnahmen.

sende Ereignisse entstehen. Beispielsweise kann sich die Ausfallwahrscheinlichkeit des Kühlmoduls erhöhen, weil ein Stoff aus der Reaktionsmasse kristallisiert, das die Wärmeleitfähigkeit erniedrigt.

### 2.5.5 Systemmodellierung

Mit den vorgefertigten Teilfehlerbäumen kann nun der Fehlerbaum aufgebaut werden (Abb. 21).

- Zuerst wird auf der Basis der Kritikalitätsklassen die Ebene der «Übergeordneten Struktur», das Prozessmodul, gebildet.
- In der Systemebene werden die unabhängig vom Prozess erstellten Fehlerbäume für technische Ausfälle an die «Übergeordnete Struktur» gekoppelt.
- In der Subsystemebene werden die Wechselwirkungen von Prozess und Anlage, die zu «auslösenden Ereignissen» führen, an die Systemebene gekoppelt.

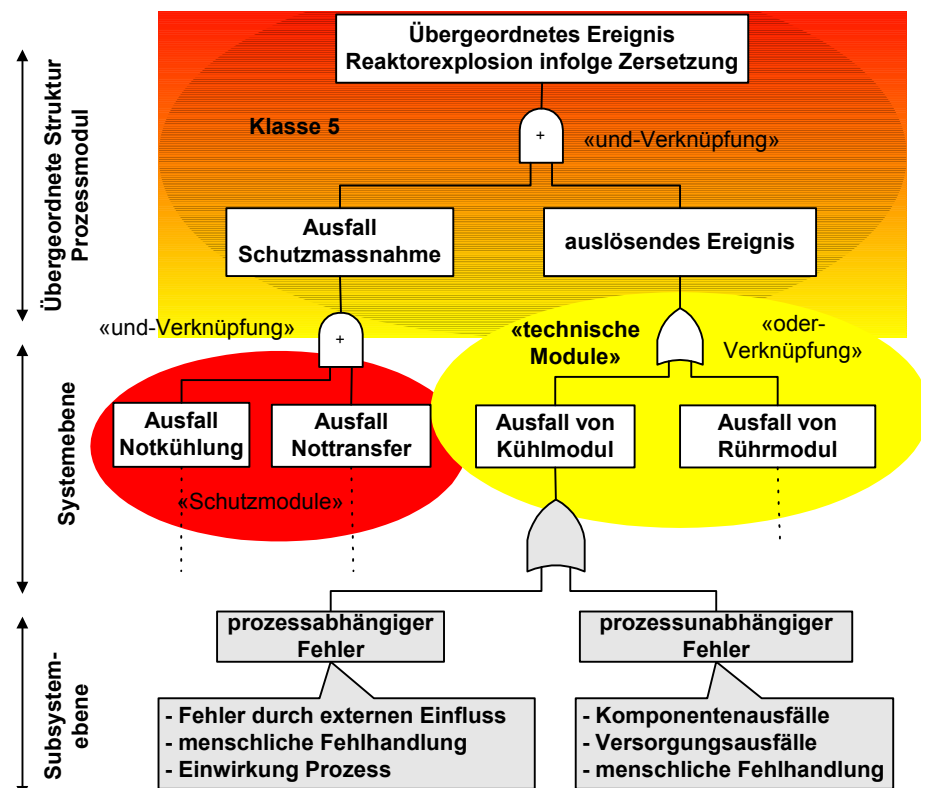


Abbildung 21

Auf diese Weise werden die Wechselwirkungen von Prozess, Anlage und Organisation, die zu auslösenden Ereignissen führen, sichtbar und Schwachstellen im System «Prozess-Mehrproduktanlage-Organisation» werden erkannt (Abb. 6).

### 2.5.6 Systembeurteilung

Von den Freisetzungsszenarios werden die Eintrittswahrscheinlichkeiten der einzelnen Ereignisse bestimmt.

Die Suche der relevanten Ausfälle besteht aus drei Schritten:

- Ermitteln der minimalen Kombinationen von Fehlern, die ausreichen, um ein System vom Zustand der Funktion in den Zustand des Ausfalls zu führen, kurz «Minimal Cut-Sets»[30].

- Aufspüren der kritischen Pfade, die sich aus denjenigen «Minimal Cut-Sets» mit wenigen Ereignissen und hohen Wahrscheinlichkeiten ergeben.
- Überprüfen der eingesetzten Daten für die kritischen Pfade auf ihre Plausibilität hin.

Die Prozessstufe in der MPA kann nun beurteilt werden. Weil die «Minimal Cut-Sets» diejenigen Ereignisketten mit den grössten Anteilen am Gesamtversagen zeigen, können Massnahmen gezielt dort eingesetzt werden, wo sie die Systemzuverlässigkeit am stärksten beeinflussen.

### 3 Fallbeispiel

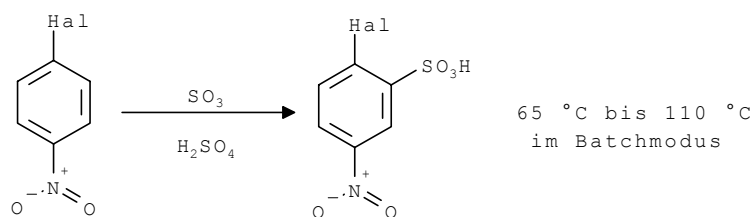
#### 3.1 Einleitung

Mit einem vereinfachten Fallbeispiel[31], der Sulfonierung eines Nitrohalogenderivates, soll das Vorgehen bei der sicherheitstechnischen Beurteilung von chemischen Reaktionsstufen demonstriert werden. Die sicherheitstechnische Beurteilung der Sulfonierungs-Stufe umfasst folgende Schritte:

- Aufzeigen der inhärenten Gefahren der Prozessstufe.
- Klassifizierung der Prozessstufe.
- Beurteilung der vorgesehenen Fahrweise und Definition von ereignisverhindernden Massnahmen.
- Festlegung der Kriterien, denen die Anlage genügen muss, um ereignisverhindernde Massnahmen einzuleiten.
- Modulare Fehlerbaumanalyse des Systems «Prozess-Mehrproduktanlage-Organisation».

#### 3.2 Beschreibung der Prozessstufe

Ein Nitrohalogenderivat wird in einer MPA in einem 8 m<sup>3</sup> Reaktor sulfoniert. Sowohl die Temperaturführung als auch die Dosierung erfolgen bei der vorhandenen Anlage von Hand.



#### Der definierte Normalbetrieb

- Bei 25 °C wasserfreie Schwefelsäure in den Reaktor laden.
- Unter Rühren das Nitrohalogenderivat zuladen.
- Die entstandene Suspension auf 60 °C erwärmen; es entsteht eine Lösung.
- Unter Rühren und Kühlen bei 60 °C Oleum während 4 Stunden eintragen.
- Die Reaktionsmischung gleichmässig innerhalb von 4 Stunden auf 110 °C heizen.

- Mehrere Stunden bei 110 °C reagieren lassen.

### 3.3 Sicherheitstechnische Untersuchung der Reaktionsstufe

Die der Reaktionsstufe inhärenten Gefahren müssen aufgezeigt werden mit Bezug auf

- die sicherheitstechnische Bewertung der Prozessstufe beim Normalbetrieb einerseits
- und die sicherheitstechnische Bewertung der Prozessstufe bei Abweichungen vom Normalbetrieb andererseits.

#### (1) Untersuchung der erwünschten Reaktion

Die Abbildung 22 zeigt den Wärmefluss (rote Kurve) der betriebsnah durchgeführten reaktionskalorimetrischen Untersuchung. Während der 4-stündigen Dosierung von Oleum (blaue Kurve) wird die Summe der Mischwärme, der Lösungswärme und der Reaktionswärme frei. Die Exothermiespitze am Anfang der Dosierung von Oleum zeigt die Hydratisierung von Oleum mit in der Schwefelsäure gelöstem Wasser. Während der Aufheizphase (schwarze Kurve) steigt der Wärmefluss langsam an und erreicht bei 90 °C das Wärmeleistungsmaximum. Die gemessene Reaktionswärme ist 136 kJ/kg, die Wärmekapazität der Endreaktionsmasse ist 1.86 kJ/kg/K.

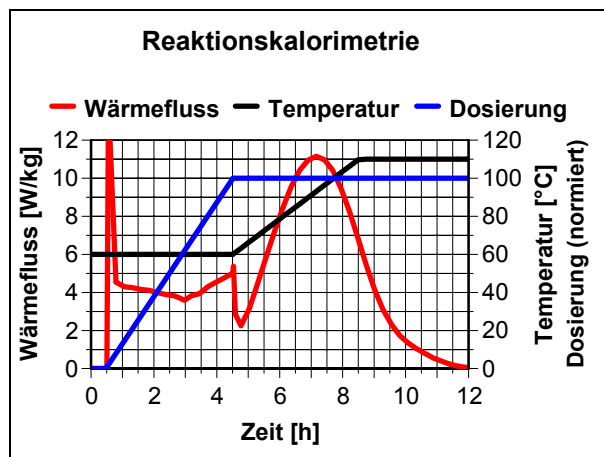


Abbildung 22

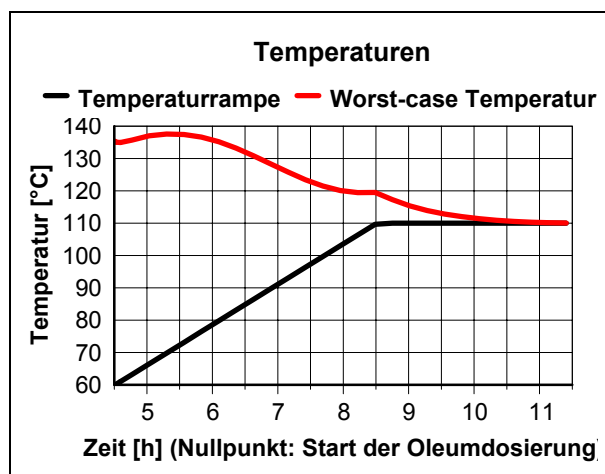


Abbildung 23

In der Abbildung 23 ist die Temperatur, die sich bei einer Kühlpanne einstellen wird (die «Worst-case-Temperatur») zusammen mit der Kurve der Reaktionstemperatur dargestellt. Die Temperatur, die sich beim Normalbetrieb durch eine Kühlpanne oder einen Rührerausfall im schlimmsten Fall einstellen kann, beträgt im Fallbeispiel ca. 140 °C.

## (2) Untersuchung der unerwünschten Reaktion

Die mikrothermoanalytische Untersuchung zeigt, dass sich die Endreaktionsmasse mit dem Potential einer hohen Tragweite thermisch zersetzt (Abb. 24).

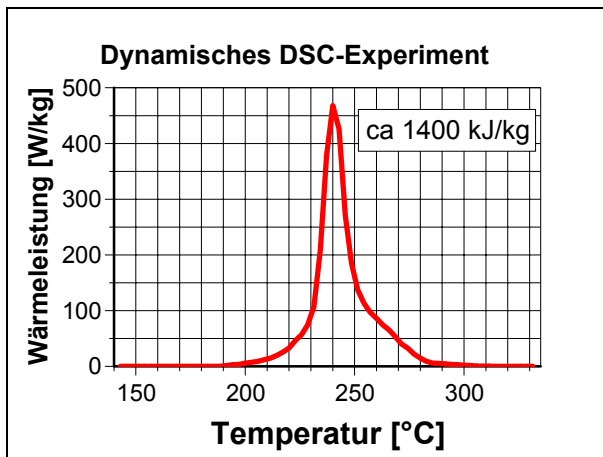


Abbildung 24

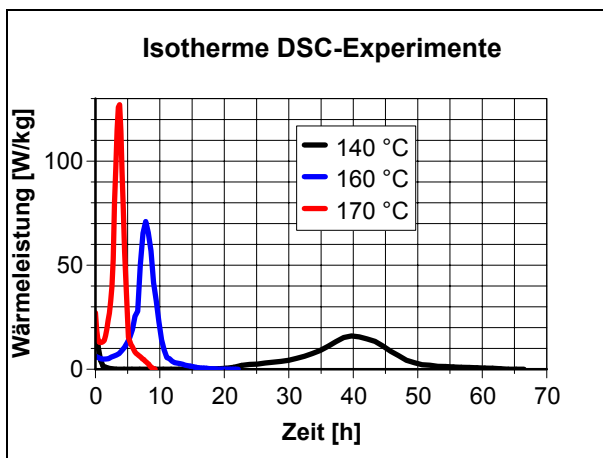


Abbildung 25

Isotherme DSC-Experimente zeigen, dass die Wärmeleistung der Exothermie ihr Maximum jeweils erst nach einer «Induktionszeit» durchläuft, die zu höheren Temperaturen hin kürzer wird (Abb. 25). Die Zersetzung der Reaktionsmasse zeigt ein autokatalytisches Verhalten. Eine Aussage über die Stabilität dieser Reaktionsmasse ist prinzipiell nur durch die Temperatur- und Zeitangabe möglich. Deshalb wurden aus vier adiabatischen Experimenten die thermokinetischen Parameter abgeleitet. Die Abbildung 26 zeigt zwei adiabatische Experimente, ausgehend von 140 °C und 147.5 °C.

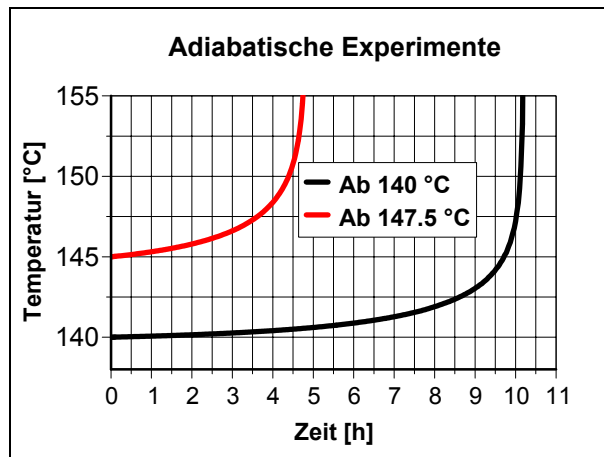


Abbildung 26

Die Abbildung 27 zeigt die Extrapolation der  $TMR_{ad}$  auf den Temperaturbereich von 130 °C bis 180 °C.

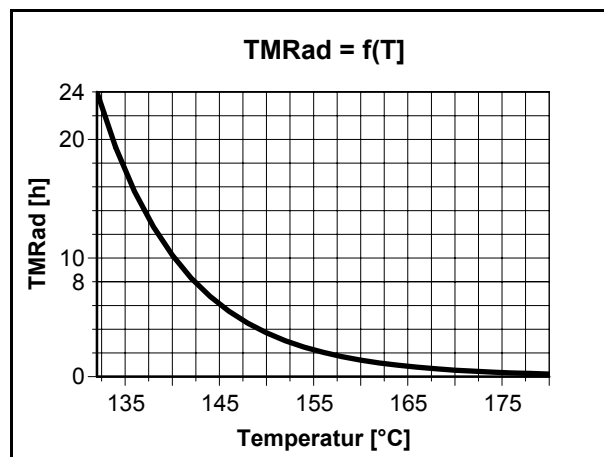


Abbildung 27

### 3.4 Beurteilung der Reaktionsstufe

Die Abbildung 22 zeigt, dass die Sulfonierung erst innerhalb der Temperaturrampe von 60 °C - 110 °C stattfindet. Das heisst, dass nach beendeter Dosierung von Oleum nahezu die gesamte Reaktionswärme akkumuliert ist. Die Abbildung 23 zeigt, dass wenn innerhalb der Temperaturrampe bei 70 °C die Kühlung oder die Rührung ausfällt, die Reaktionstemperatur auf ca. 140 °C steigt. Das adiabatische Experiment, ausgehend von der MTSR von 140 °C, zeigt die  $TMR_{ad}$  von 10 Stunden (Abb. 26). Ausgehend von 145 °C, derjenigen Temperatur, die sich einstellt, wenn die Temperatur nach der Dosierung von Oleum 65 °C statt der vorgeschriebenen 60 °C beträgt, ist die  $TMR_{ad}$  schon derart kurz, dass es bei Abweichungen vom Normalbetrieb in einer MPA kaum mehr möglich sein wird, Gegenmassnahmen einzuleiten (Abb. 27).

Im Fallbeispiel ist die Sulfonierungs-Stufe thermisch nicht sicher. Die Tragweite und die Wahrscheinlichkeit, dass eine thermische Explosion eintritt, sind hoch. Die Reaktionsstufe kann bei Abweichungen vom Normalbetrieb nur mit Notmassnahmen beherrscht werden. Die Klassifizierung der Prozessstufe für die Bildung des übergeordneten Fehler-

baums zeigt die Abbildung 28. Die Entscheidungen, die schliesslich zur Kritikalitätsklasse 5 führen, sind in der Abbildung rot eingezeichnet. Diese Prozessstufe darf in der von Hand gesteuerten Anlage nicht gefahren werden. Wenn innerhalb der Temperaturrampe Fehler gemacht werden, ist die Gefahr zu gross, dass die MTSR höher ist als 140 °C. Eine höhere MTSR führt aber zu einer kürzeren  $TMR_{ad}$ .

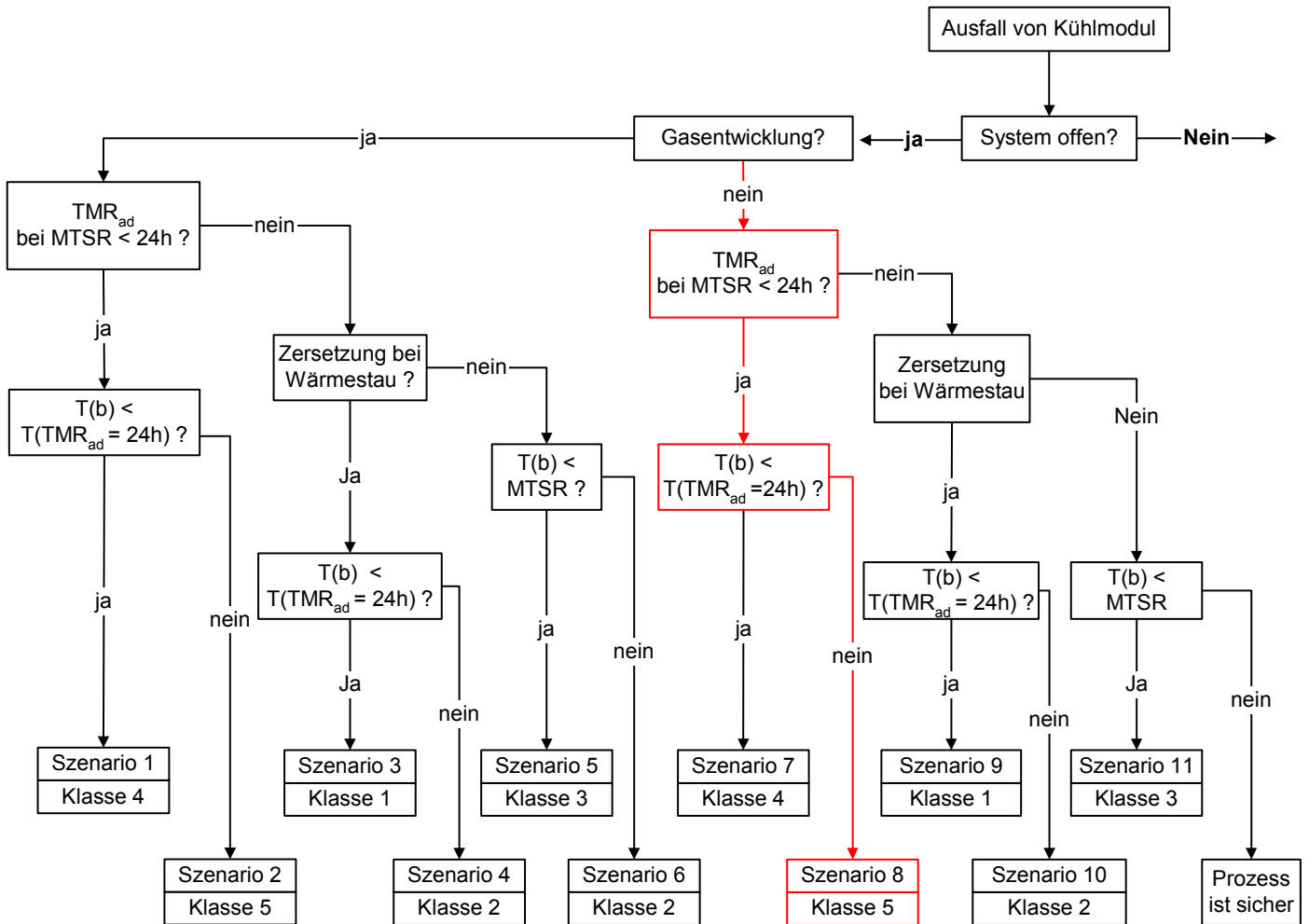


Abbildung 28

### 3.5 Festlegen der Kriterien für die Anlage, mit der es vielleicht möglich ist, ereignisverhindernde Massnahmen einzuleiten

Die sicherheitstechnische Untersuchung hat gezeigt,

- dass die Abweichung vom Normalbetrieb aufgrund einer Kühlpanne oder eines Rührunterbruchs - wegen der dadurch entstehenden Wärmestausituation - zu einem Ereignis mit grosser Tragweite führt,
- und dass dieses Ereignis mit grosser Wahrscheinlichkeit eintritt, wenn durch die Abweichung vom Normalbetrieb die entstandene Wärmestausituation einige Stunden andauert.

Damit diese Prozessstufe - mit der gegebenen hohen Tragweite - sicher durchgeführt werden kann, ist eine Anlage notwendig, die durch ereignisverhindernde Massnahmen die Wärmestausituation ausschliesst.

Eine mögliche ereignisverhindernde Massnahme, die den Wärmestau ausschliesst, ist ein Nottransfer der Reaktionsmasse in einen Behälter, in dem sich die notwendige Menge Eis und Wasser befindet. Die Abbildung 29 zeigt das Schema einer Anlage, in der ein solcher Nottransfer durchgeführt werden kann [32]. Die Anlage besteht aus den Reaktoren R0, R1 und R2 und einem gummierten Kessel R3, der als Notkessel gebraucht werden kann. R0 ist mit einem Warmwasserkreislauf ausgerüstet. R1 und R2 sind an Wärmeträgeranlagen angeschlossen. Die Durchführung der Sulfonierungs-Stufe ist wie folgt geplant:

- In R0 wird die Lösung von Nitrohalogenderivat in Schwefelsäure bei 60 °C hergestellt. Diese Lösung wird nach R1 verschoben.
- In R1 wird die Dosierung von Oleum vorgenommen und anschliessend die Temperaturrampe durchgeführt. Danach wird die Reaktionsmasse nach R2 verschoben.
- In R2 wird die Nachreaktion durchgeführt.

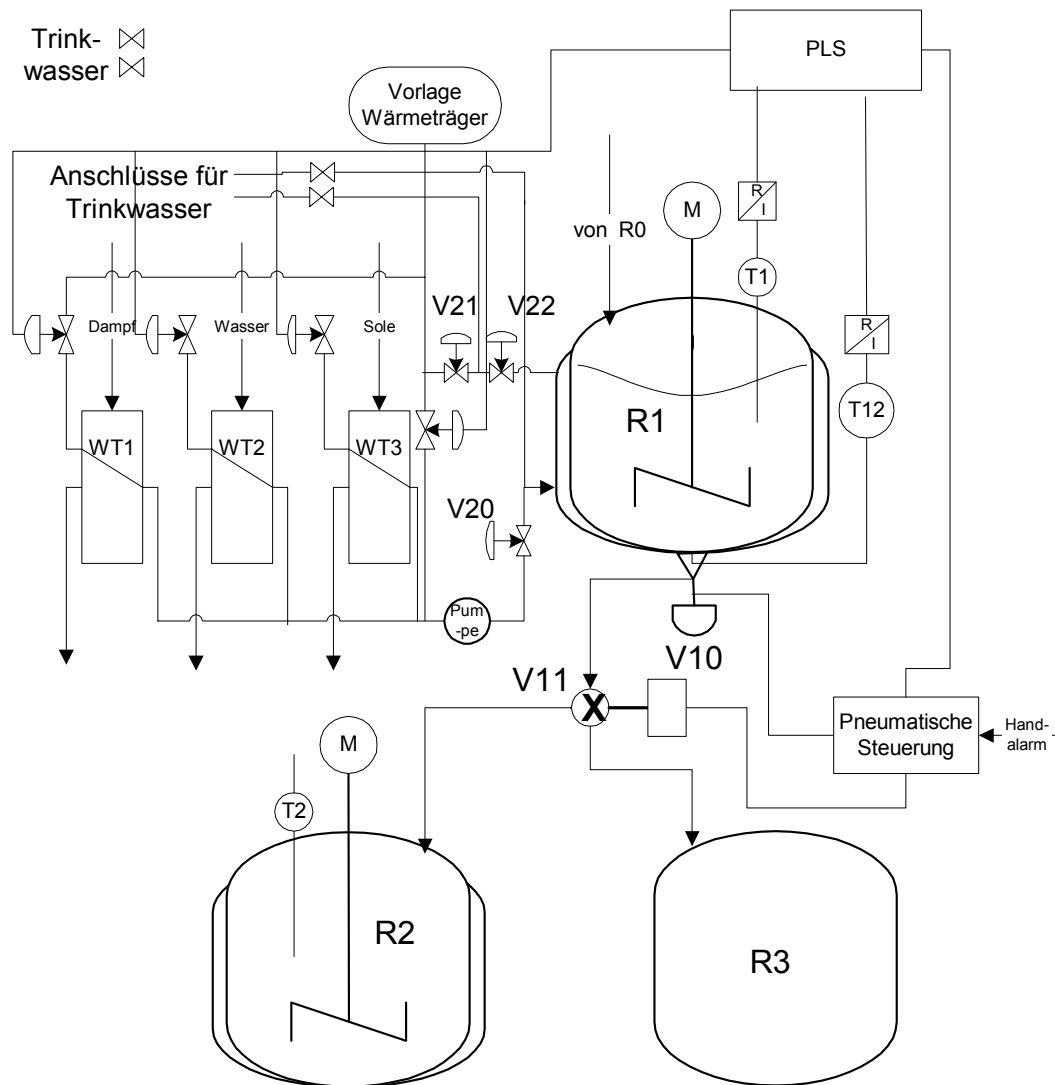


Abbildung 29



### 3.6 Gefahrensuche

Wie wir in Abschnitt 2.3 gezeigt haben, wurde auf der Basis der in Abschnitt 3.5 definierten Produktionsanlage (Abb. 29) und der Betriebsvorschrift (Abb. 8) eine Gefahrensuche durchgeführt. Die Abbildung 30 zeigt zur Veranschaulichung einen Auszug aus der Gefahrensuche.

Prozessanalyse (Fehlersuche)		Ebene III. Formular 1							
Projekt: Sulfonierung, Reaktionsstufe									
Code:									
Datum									
		Arbeitsschritt (Arbeitsschritt Nr.)							
Kritische Abweichung		2	3	4	5	6	7	8	9
Energieversorgung	Strom		X	X	X	X	X	X	X
	Wasser					X	X	X	X
	Dampf					X	X	X	X
	Sole / Eis								
	Stickstoff	X	X	X	X	X	X	X	X
	Steuerluft	X	X	X	X	X	X	X	X
	Servoluft								
	Vakuum	X							
	Ventilation	X							
Prozessbedingungen / Vorschrift	Reinigung	X							
	Kontrolle der Anlage	X							
	Evakuieren / Entlasten	X			X				
	Apparateventilation	X			X				
	Eintragen / Zudosieren	X			X		X		
	Menge	X			X				
	Reihenfolge	X			X				
	Zugabegeschwindigkeit								
	Verwechslung	X			X		X		
	Elektrostatische Aufladung								
	Temperatur				X	X	X	X	X
	Druck								
	pH-Wert								
	Heizen					X	X	X	X
	Kühlen					X	X	X	X
	Rührgeschwindigkeit			X	X	X	X	X	X
	Reaktion mit Wärmeträger	X	X	X	X	X	X	X	X
	Katalysator / Inhibitor								
	Verunreinigungen	X							
	Abtrennung / Dekantieren								
	Verbr. Leitung., Ventile	X			X		X		
	Pumpen, Leeren								
Abfallbeseitigung									
Prozessunterbruch				X	X	X	X	X	
Chemikalienaustritt	X			X		X			

Abbildung 30 (angelehnt an ETH/ESCIS [33])

### 3.7 Gefahrenbeurteilung und Massnahmenplanung

Aus den Abweichungen, die sich in der Reaktionsstufe bei den Arbeitsschritten (Abb. 30) als kritisch erweisen, wurden Szenarien gebildet und deren Tragweiten und Eintrittswahrscheinlichkeiten bestimmt. Für jede Gefahr wurden Massnahmen abgeleitet durch welche die signifikanten Risiken auf ein tragbares Mass reduziert werden sollen. Die Abbildung 31 zeigt zur Veranschaulichung einen Auszug der Szenarien mit hoher Tragweite.

RISIKOANALYSE		Ebene IV und V Risikokatalog / Risikobeurteilung / Massnahmen		
PROJEKT: Code: Datum:				
Arbeitsschritt	Gefahr	Risiko		Massnahmen
		W	T	
	<b>Rührerausfall:</b> Ohne Rührung kann keine Wärme Abgeführt werden. Ohne Wärmeabfuhr steigt die Temperatur in den Zersetzungsbereich. Ohne Rührung ist die Notkühlung unwirksam.	M	H	<ul style="list-style-type: none"> <li>○ Rührerüberwachung</li> <li>○ Während Stillstand Temperaturüberwachung der Reaktionsmasse</li> <li>○ Nottransfer</li> <li>○ .....</li> <li>○ .....</li> </ul>
	<b>Kühlungsausfall:</b> Ohne Wärmeabfuhr steigt die Temperatur in den Zersetzungsbereich	H	H	<ul style="list-style-type: none"> <li>○ Notkühlung aktivieren (organisatorische Massnahme)</li> <li>○ Während Stillstand Temperaturüberwa-</li> </ul>

Abbildung 31 (angelehnt an ETH/ESCIS [32])

### 3.8 Risikoanalyse der Sulfonierungs-Stufe

#### 3.8.1 Vorgehen [34]

Die Szenarien, die aufgrund der systematischen Gefahrensuche zu Ereignissen mit grosser Tragweite führen, werden mit der modularen Fehlerbaumanalyse analysiert. Diese Szenarien enthalten die technischen Ausfälle und die technischen Ausfälle, die in Kombination mit menschlichen Fehlhandlungen relevant sind. Durch die detaillierte Modellierung werden abhängige Ausfälle durch gemeinsam genutzte Hilfseinrichtungen sowie Ausfälle durch Komponentenversagen berücksichtigt.

#### 3.8.2 Betrachtete Ereignisse

Das übergeordnete Ereignis der modularen Fehlerbäume ist die Runawayreaktion im Sulfonierungs-Reaktor. Die Sulfonierungs-Stufe wurde aufgrund der sicherheitstechnischen Untersuchung in die Kritikalitätsklasse 5 eingeteilt.

Zu modellierende Szenarien		
Nr.	Auslösendes Ereignis	Schutzmassnahme
1	Kühlerausfall	Nottransfer und Notkühlung
2	Rührerausfall	Nottransfer und Notkühlung
3	Kühler- und Rührerausfall	Nottransfer und Notkühlung

Tabelle 11

---

Die Abbildung 16 zeigt die übergeordnete Struktur des Gesamtfehlerbaums für das Szenario «Reaktorexlosion infolge einer Zersetzungsreaktion». Dieser Fehlerbaum wird auf die auslösenden Ereignisse und Schutzmassnahmen angewendet (Tabelle 11).

### 3.8.3 Beschreibung der technischen Teilsysteme

Anhand des Anlageschemas in der Abbildung 29 werden die modellierten technischen Module beschrieben (Abb. 20). Die Fehlerbäume zu den beschriebenen technischen Modulen werden in diesem Aufsatz nicht diskutiert [35].

Das **Heiz- und Kühlmodul** ist ausgelegt für den Temperaturbereich von -30 °C bis 170 °C.

- Oberhalb von 45 °C kommt der mit Wasser betriebene WT2 zum Einsatz.
- Unterhalb von 35 °C wird im Wärmetauscher WT1 mit Sole gekühlt.
- Zwischen 35 °C und 45 °C findet ein gleitender Übergang vom Kühlen mit Sole zum Kühlen mit Wasser statt.

Die Temperaturregelung erfolgt über zwei Messfühler:

- Messfühler T1 im Stromstörer
- Messfühler T2 im Bodenablassventil

Beim **Rührmodul** lässt sich die Rührerdrehzahl mittels Frequenzumformer stufenlos regeln. Sowohl der Frequenzumformer als auch die Sperrflüssigkeitspumpe sind überwacht. Bei einer Störung wird der energielose Zustand herbeigeführt. Alle Ventile werden geschlossen und der Motor wird ausgeschaltet.

Bei einer kritischen Temperaturerhöhung wird automatisch der **Nottransfer** ausgelöst. Der Inhalt des Reaktors wird in den Notablasstank entleert. Im Notablasstank ist Eis und Wasser vorgelegt. Die pneumatische Ansteuerung der Ventile erfolgt entweder über das Prozessleitsystem, den lokalen Rechner oder von Hand über einen plombierten Notstahnhahn. Falls die Steuerluft ausfällt, dient ein Druckluftnottank als Druckpolster. Das Bodenablassventil V10 ist im druckluftlosen Zustand geschlossen und das Dreiwegventil V11 steht in Stellung zum Folgekessel.

Die Kriterien für die Nottransferauslösung sind wie folgt definiert:

- Überschreitet die Temperatur 115 °C, so erfolgt entweder über das Prozessleitsystem oder über den lokalen Rechner eine Alarmierung.
- Überschreitet die Temperatur 118 °C, so wird der Nottransfer automatisch ausgelöst. Wenn die Automatik versagt, kann der Nottransfer über eine Handtaste ausgelöst werden.

Die Messfühler T1 und T2 sind sowohl dem Heizmodul als auch dem Kühlmodul zugeordnet. T1 und T2 werden auch zur Auslösung des Nottransfers eingesetzt. Das beeinflusst die Berechnungen nicht. Bei der Ermittlung der «Minimal Cut Sets» werden auslösende Ereignisse, die mehrmals in einem Fehlerbaum auftreten, zu einem Ereignis reduziert.

Die Aufstellung von Fehlerbäumen erfordert viel Fachwissen und Erfahrung. Die Quantifizierung ist auch heute noch problematisch, sie kann nur so gut sein, wie es die Qualität der verfügbaren Datenbasen zur Ermittlung von Ausfallwahrscheinlichkeiten von Komponenten und anderen Zuverlässigkeitsdaten sind.

Der grosse Nutzen der modularen Fehlerbaumanalyse liegt darin, dass sich die mit den verfügbaren Datenbasen berechneten Eintrittswahrscheinlichkeiten der einzelnen Szenarien für die vergleichende Beurteilung bei der Planung von risikominierenden Massnahmen eignen.

Für das Fallbeispiel gelten folgende Annahmen:

- Die Temperaturmessgruppen des Heiz- und Kühlsystems und des Nottransfersystems sind unabhängig.
- Die Temperaturmessgruppen des Heiz- und Kühlsystems und des Nottransfersystems sind voneinander unabhängig, da sie separaten Teilsystemen angehören und auch einem unterschiedlichen Instandhaltungsprogramm unterworfen sind.

Die abhängigen Ausfälle bei redundanten Einrichtungen (z. B. Temperaturfühler) wurden in der Analyse berücksichtigt.

Weiter gelten die Annahmen:

- Das Ventil V10 wird einmal pro Prozesszyklus betätigt.
- Das Dreiwegventil V11 wird im störungsfreien Betrieb nur einmal pro Monat, während der Simulation eines Nottransfers, betätigt.

Das Modul zur **Notkühlung** ist in der Abbildung 29 dargestellt. Mit einer organisatorischen Massnahme kann von Hand Trinkwasser angeschlossen werden. Damit mit der Notkühlung genügend Wärme abgeführt werden kann, muss das Rührmodul funktionieren. Ein Rührerausfall bewirkt somit auch den Ausfall der Notkühlung.

### 3.9 Auswertung der modularen Fehlerbaumanalyse

#### 3.9.1 Allgemeines

Die folgenden Ausführungen dienen nur der Demonstration des Vorgehens, sie ist nicht vollständig. Die Darstellung der modularen Fehlerbäume für das Kühlmodul und für das Rührmodul würden den Rahmen dieses Aufsatzes sprengen. Die berechneten «Minimal Cut Sets» werden soweit dargestellt, dass die Schwachstellen der Teilsysteme sichtbar werden.

#### 3.9.2 Szenario 1: Reaktorexlosion durch Kühlmodulsausfall

Die Abbildung 32 zeigt die übergeordnete Struktur für das Szenario Kühlmodulsausfall. Dieses wurde mit den modularen Fehlerbäumen zum Ausfall des Kühlmoduls, Notkühlmoduls und des Nottransfermoduls verknüpft. Das übergeordnete Ereignis «Reaktorexlosion durch Zersetzung» wurde anhand der Minimal Cut Set-Bestimmung [36] berechnet. Für dieses Szenario wurde die auf einen Prozesszyklus bezogene Eintretenswahrscheinlichkeit von  $3.3 \cdot 10^{-6}$  berechnet.

Die Möglichkeit des Stromausfall wurde unterteilt in

- totaler Stromausfall
- und Stromausfall im Betrieb.

Ein totaler Stromausfall führt zum Ausfall aller Hilfsenergien, ein Stromausfall im Betrieb betrifft dagegen nur die Stromversorgung der betrachteten Anlage.

Die Tabelle 12 zeigt die auslösenden Ereignisse deren «Minimal Cut Sets» 98.8 % zum Ereignis «Reaktorexlosion durch Zersetzung» beitragen. Der hohe Anteil der ersten beiden auslösenden Ereignisse hängt von der Ausfallwahrscheinlichkeit des Ventils V11 ab. Natürlich gibt es noch mehr «Minimal Cut Sets» mit zwei und mehr Ereignissen, diese tragen aber nur noch wenig zum übergeordneten Ereignis bei.

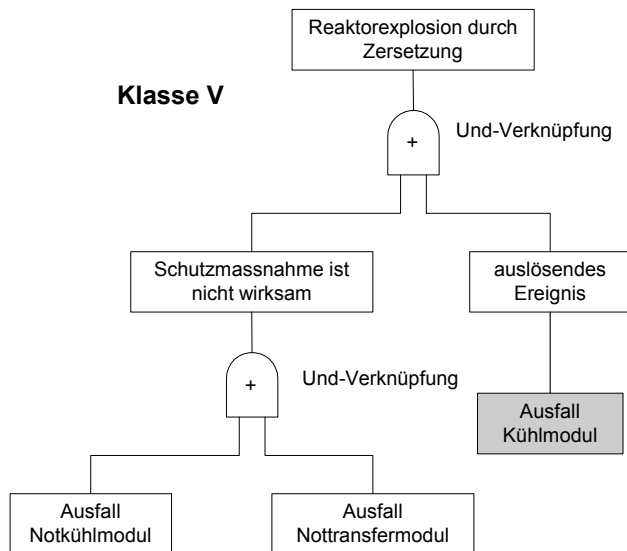


Abbildung 32

Sicherheitsrelevante «Minimal Cut Sets» für das Szenario «Reaktorexlosion durch Kühlmodulsausfall» (Minimal Cut Sets mit zwei Ereignissen)	
V11 geht nicht in Transferstellung / kein Strom im Areal (inkl., keine Steuerluft)	70
V11 geht nicht in Transferstellung / kein Strom intern	17.5
Ausfall Nottank Druckluft kein / Strom im Areal (inkl., keine Steuerluft)	7.7
Nothahn in falscher Stellung / kein Strom im Areal	1
kein Wasser im Nottank (Notkessel) / kein Strom im Areal (inkl., keine Steuerluft)	1
Ventil V10 öffnet nicht / kein / Strom im Areal (inkl., keine Steuerluft)	0.8
Ausfall Druckreduzierventil / kein Strom im Areal (inkl., keine Steuerluft)	0.8
Andere *	1.2

\* Diese enthalten sehr viele «Minimal Cut Sets» mit zwei und drei Ereignissen.

Tabelle 12

### 3.9.3 Szenario 2: Reaktorexlosion durch Rührmodulsausfall

Die Abbildung 33 zeigt die übergeordnete Struktur für das Szenario Rührmodulsausfall. Dieses wurde mit den modularen Fehlerbäumen zum Ausfall des Rührmoduls, Notkühlmoduls und des Nottransfermoduls verknüpft. Das übergeordnete Ereignis «Reaktorexlosion durch Zersetzung» wurde anhand der Minimal Cut Set-Bestimmung [37] berechnet.

Für dieses Szenario wurde die auf einen Prozesszyklus bezogene Eintretenswahrscheinlichkeit von  $4.6 \cdot 10^{-6}$  berechnet. Die Tabelle 13 zeigt die auslösenden Ereignisse deren «Minimal Cut Sets» 96 % zum Ereignis «Reaktorexlosion durch Zersetzung» beitragen. Die Analyse der «Minimal Cut Sets» zeigt, dass hauptsächlich das Ventil V11 zu dieser Ausfallwahrscheinlichkeit beiträgt. Dieses ist an ca. 90 % der Ausfallkombinationen, die zur Reaktorexlosion führen, beteiligt. Auch für dieses Szenario gibt es noch mehr «Minimal Cut Sets» mit zwei und

mehr Ereignissen, die aber nur noch wenig zum übergeordneten Ereignis beitragen.

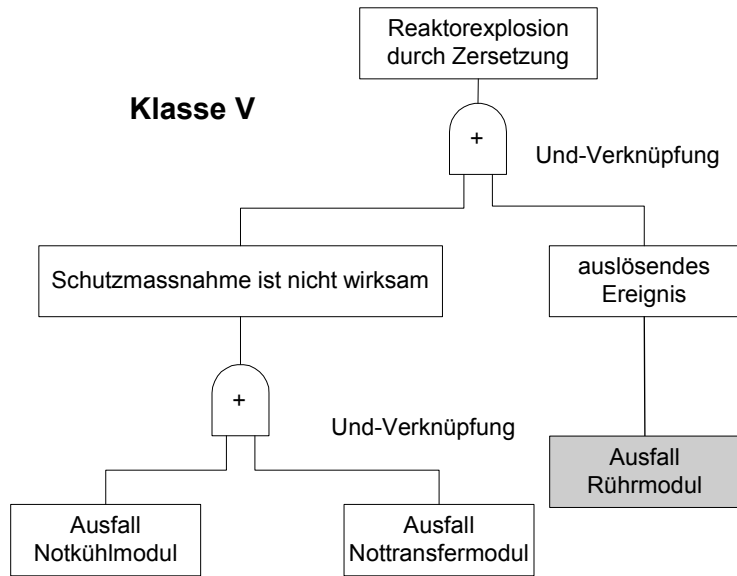


Abbildung 33

<b>Sicherheitsrelevante «Minimal Cut Sets» für das Szenario «Reaktorexlosion durch Rührmodulsausfall» (Minimal Cut Sets mit zwei Ereignissen)</b>	
V11 geht nicht in Transferstellung / kein Strom im Areal (inkl., keine Steuerluft)	50
V11 geht nicht in Transferstellung / Motor defekt	12.5
V11 geht nicht in Transferstellung / Frequenzumformer defekt	12.5
V11 geht nicht in Transferstellung / kein Strom im Areal	12.5
Ausfall Nottank (Druckluft) / kein Strom im Areal (inkl., keine Steuerluft)	5.5
V11 geht nicht in Transferstellung / Rührwelle gebrochen	1
V11 geht nicht in Transferstellung / Rührblatt abgefallen	1
V10 öffnet nicht / kein Strom im Areal (inkl. keine Steuerluft)	0.5
Ausfall Druckreduzierventil / kein Strom im Areal (inkl. keine Steuerluft)	0.5
Andere *	4

Tabelle 13

### Szenario 3: Reaktorexlosion durch gleichzeitigen Rühr- und Kühlmodulsausfall

Das dritte Szenario stellt den gleichzeitigen Ausfall des Rühr- und Kühlmodus dar. Es soll zeigen, ob der **gleichzeitige** Ausfall des Kühl- und Rührmoduls weniger wahrscheinlich ist als derjenige der Einzelausfälle, ob also diese Teilsysteme voneinander unabhängig sind. Dieses Szenario darf nicht verwechselt werden mit der «Oder-Verknüpfung» (vergl. Abschnitt 3.10) Die Abbildung 34 zeigt die übergeordnete Struktur für das Szenario gleichzeitige Ausfall des Kühl- und Rührmoduls.

Für das Szenario Kühlmodulsausfall mit gleichzeitigem Rührmodulsausfall wurde die auf einen Prozesszyklus bezogene Eintretenswahrscheinlichkeit von  $3.3 \cdot 10^{-6}$  berechnet. Wie erwartet ist die Wahrscheinlichkeit dieses Szenarios gleich gross wie das Szenario «Reaktorexpllosion durch Kühlmodulsausfall». Der gleichzeitige Ausfall von Rühr- und Kühlmodul ist also nicht unwahrscheinlicher als der Ausfall des Kühlmoduls. Dies wird durch die «Minimal Cut Sets» erklärt. Die Tabelle 14 zeigt, dass bei allen relevanten «Minimal Cut Sets» der Stromausfall als auslösendes Ereignis vorhanden ist. Weil das Funktionieren des Rührmoduls und des Kühlmoduls von der Stromversorgung abhängt, löst ein Stromausfall den gleichzeitigen Ausfall beider Teilsysteme aus.

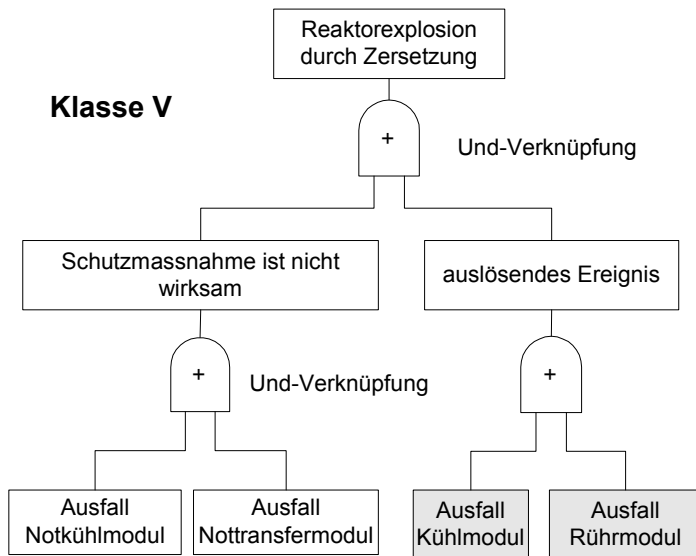


Abbildung 34

Sicherheitsrelevante «Minimal Cut Sets» für das Szenario «Reaktorexpllosion durch gleichzeitigen Rühr- und Kühlmodulsausfall» (Minimal Cut Sets mit zwei Ereignissen)	
V11 geht nicht in Transferstellung / kein Strom im Areal (inkl., keine Steuerluft)	70
V11 geht nicht in Transferstellung / kein Strom intern	17.5
Ausfall Nottank Druckluft / kein Strom im Areal (inkl., keine Steuerluft)	7.7
Nothahn in falscher Stellung / kein Strom im Areal	1
Kein Wasser im Nottank (Notkessel) / kein Strom im Areal (inkl., keine Steuerluft)	1
Ventil V10 öffnet nicht / kein Strom im Areal (inkl., keine Steuerluft)	0.8
Ausfall Druckreduzierventil / kein Strom im Areal (inkl., keine Steuerluft)	0.8
Andere *	1.2

\* Diese enthalten sehr viele «Minimal Cut Sets» mit zwei und drei Ereignissen.

Tabelle 13

Alle ermittelten «Minimal Cut Sets» mit zwei Ereignissen enthalten den Stromausfall als eines der auslösenden Ereignisse [38].

### 3.10 Beurteilung des Risikos der Sulfonierungs-Stufe

Für das Szenario **Reaktorexlosion durch Kühlmodulsausfall** wurde eine auf die Reaktorbelegung bezogene Wahrscheinlichkeit von  $3.3 \cdot 10^{-6}$  ermittelt. Wenn der Prozess in der MPA 300 Tage im Jahr mit drei Schichten pro Tag gefahren wird, so ist die Unfallhäufigkeit für dieses Szenario  $3 \cdot 300 \cdot 3.3 \cdot 10^{-6} = 2.97 \cdot 10^{-3}$  **pro Jahr**.

Für das Szenario **Reaktorexlosion durch Rührmodulsausfall** wurde eine auf die Reaktorbelegung bezogene Wahrscheinlichkeit von  $4.6 \cdot 10^{-6}$  ermittelt. Wenn der Prozess in der MPA 300 Tage im Jahr mit drei Schichten pro Tag gefahren wird, so ist die Unfallhäufigkeit für dieses Szenario  $3 \cdot 300 \cdot 4.6 \cdot 10^{-6} = 4.14 \cdot 10^{-3}$  **pro Jahr**.

Ohne Rührung kann keine Wärme abgeführt werden und ohne Wärmeabfuhr steigt die Temperatur in den Zersetzungsbereich.

Die Reaktorexlosion wird sowohl durch den Rührmodulsausfall als auch durch den Kühlmodulsausfall ausgelöst. Der Fehlerbaum in Abbildung 21 macht diese «Oder-Verknüpfung» deutlich. Bei der «Oder-Verknüpfung» reicht jedes auslösende Ereignis aus, um das betrachtete Ereignis auszulösen. Das heisst, die Wahrscheinlichkeit ist die Summe der einzelnen Ereigniswahrscheinlichkeiten.

Somit berechnet sich die Unfallhäufigkeit zu

$$3 \cdot 300 \cdot (3.3 + 4.6) \cdot 10^{-6} = 7.1 \cdot 10^{-3} \text{ pro Jahr.}$$

Die Frage nun, ob die Sulfonierungs-Stufe in der betrachteten Anlage gefahren werden darf, wird anhand einer halb-quantitativen Betrachtungsweise beurteilt [39]. Die Tabelle 15 zeigt ein Beispiel einer halb-quantitativen Abschätzung der Tragweite.

Tragweiteklasse	Beschreibung	
I	Mensch Umwelt Sachwerte	Tote, ausserhalb des Areals evakuierte Arealüberschreitende Langzeitschäden > 10 Millionen CHF, > 1 Jahr Ausfall der Anlage
II	Mensch Umwelt Sachwerte	Verletzte, ausserhalb des Areals Reizungen reversible Schäden in der Nachbarschaft < 10 Millionen CHF, < 1 Jahr Ausfall der Anlage
III	Mensch Umwelt Sachwerte	Verletzte nur im Areal, Belästigung Areal, allenfalls Abwasseranlage betroffen < 2 Millionen CHF, Ausfall der Anlage: Wochen
IV	Mensch Umwelt Sachwerte	Leichtverletzte nur im Areal Nur Anlage bis Areal betroffen < 2 Millionen CHF, Ausfall der Anlage: Tage

Tabelle 14

Wahrscheinlichkeit	Beschreibung	
A	häufig	mehr als einmal pro Jahr
B	oft	1 mal pro Jahr
C	gelegentlich	1 mal in 5 Jahren
D	selten	1 mal in 30 Jahre
E	unwahrscheinlich	1 mal in 100 Jahren
F	sehr unwahrscheinlich	1 mal in 1000 Jahren

Tabelle 15



Die Tabelle 16 zeigt ein Beispiel einer halb-quantitativen Bewertung der Wahrscheinlichkeit auf Prozessebene. Die Klasseneinteilung erfolgt hier aufgrund von Kriterien, die für Mitglieder von Risikoanalyse-Teams mit unterschiedlichen Spezialisierungen vorstellbar und kommunizierbar sind.

Im Fallbeispiel ist die Sulfonierungs-Stufe thermisch nicht sicher. Die Tragweite ist hoch, wenn eine thermische Explosion eintritt. Die Tragweite kann in Klasse I (Tabelle 15) eingeteilt werden.

Mit der Fehlerbaumanalyse wurde die Häufigkeit, dass eine Reaktor-explosion durch den Rührmodul-ausfall oder durch den Kühlmodul-ausfall ausgelöst wird, als  $7.1 \cdot 10^{-3}$  pro Jahr berechnet. Die Wahrscheinlichkeit kann in die Klasse E (Tabelle 16) eingeteilt werden.

Das Risiko der Sulfonierungs-Stufe wird nun anhand einer Risikomatrix mit den Tragweiten- und Wahrscheinlichkeitsklassen als Achsen dargestellt.

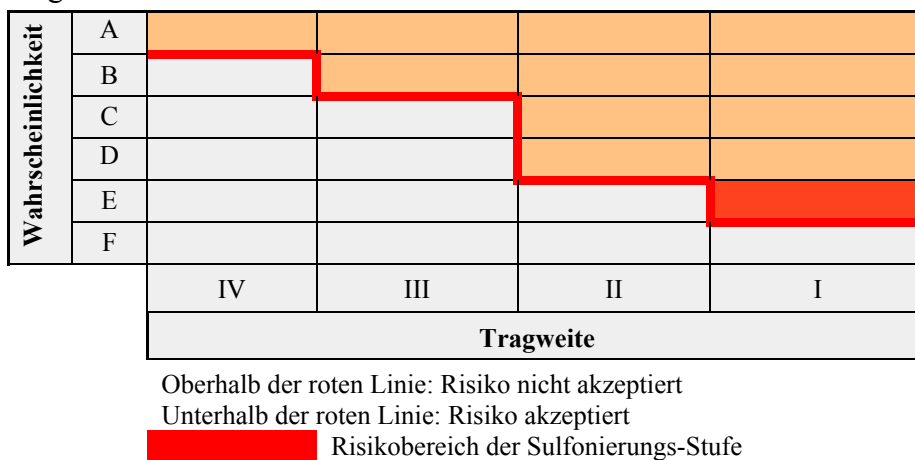


Abbildung 35

Die Abbildung 35 zeigt, dass das Risiko, das die Sulfonierungs-Stufe in der gewählten Anlage darstellt, nicht akzeptiert werden kann.

#### 4 Schlusswort

Die Risikoabschätzung für Chemieanlagen ist komplex. Die Frage, durch welche Massnahmen und mit welchen Mitteln die Forderung der Öffentlichkeit nach Sicherheit, bei der chemischen Produktion, bei der Lagerung und beim Transport, erfüllt werden kann, wird unterschiedlich beantwortet [40]. Für die sicherheitstechnische Beurteilung von MPA gelten die folgenden Leitsätze [41]:

**Leitsatz 1:** Risikoanalysen, die das Ziel haben quantitative Abschätzungen von Risiken zu erarbeiten, erhöhen den Sicherheitsstandard der Mehrproduktchemie nicht, denn

- die Unschärfen der Risikowerte sind zu gross,
- sehr viele Einflussgrössen können nicht objektiviert werden,
- die Quantifizierung des maximalen Schadensausmasses ist schwierig.

---

**Leitsatz 2:** Das wirksamste Sicherheitskonzept für die Mehrproduktchemie ist dasjenige, welches die Gefahrenpotentiale selbst minimiert und nicht deren Eintrittswahrscheinlichkeiten. Die durch die Prozessentwicklung erreichte inhärente Sicherheit des Systems *Mehrproduktanlage, Prozessstufe* und *Organisation* ist einem nachträglich festgestellten Risikowert vorzuziehen, denn

- die inhärente Sicherheit einer Prozessstufe minimiert eine Gefährdung von Mensch und Umwelt,
- die inhärente Sicherheit eines Systems kann durch keine Unsicherheit beeinflusst werden,
- Risikoberechnungen als Gegensatz zur inhärenten Sicherheit eines Systems sind für mathematische Manipulationen offen.

Das Risiko einer thermischen Explosion, der im Fallbeispiel untersuchten Sulfonierungs-Stufe, kann nur nachhaltig gesenkt werden, wenn das Verfahren so umgearbeitet wird, dass in ihr nicht die Energiemenge akkumulieren kann, die bei einer Prozessabweichung die thermische Explosion auslöst. Die Sicherheit des Systems *Mehrproduktanlage, Prozessstufe* und *Organisation* der Sulfonierungs-Stufe kann nicht dadurch vergrößert werden, dass – durch technische Raffinesse – die Ausfallwahrscheinlichkeit eines Ventils verkleinert wird.

**Leitsatz 3:** Für die Mehrproduktchemie ist es nicht notwendig, dass die Methoden der quantitativen Risikoabschätzung weiterentwickelt werden, weil die Problemstellung nicht in den Methoden selber zu suchen ist, sondern in den Zielen, die damit verfolgt werden.

- Wenn die Fehlerbaumanalyse dazu eingesetzt wird, die Wirksamkeit verschiedener Alternativen eines Systems *Mehrproduktanlage, Prozessstufe* und *Organisation* zu beurteilen, ist die Fehlerbaumanalyse ein geeignetes Instrument.
- Wenn die Fehlerbaumanalyse dagegen dazu eingesetzt wird, Frequenzen für Störereignisse zu ermitteln, so muss sie scheitern.

**Leitsatz 4:** Das Ziel der quantitativen Risikoanalyse ist die Bewertung des Risikos in Zahlen in Bezug auf die Eintretenswahrscheinlichkeit und die Tragweite. Das Resultat der quantitativen Risikoanalyse ist ein Zahlenwert, der die Dimension Schaden pro Zeiteinheit hat. Die quantitative Risikoanalyse setzt voraus, dass das analysierte Risiko bereits durch die systematische Gefahrensuche als Gefahr erkannt worden ist. Mit der quantitativen Risikoanalyse können keine neuen Gefahren gefunden werden. Darum ist es für die Mehrproduktchemie wichtig, dass eine Unternehmung den neuesten Stand der Technik im Aufzeigen der inhärenten Gefahren von Prozessstufen kennt und diesen für die Gefahrensuche selbst dann nutzt, wenn es nicht über die notwendige technische Infrastruktur verfügt.

---

## Anmerkungen und Literaturverzeichnis

- [1] Furer, S.; Rauch, J.; Sanden, F. J.; Chem. Ing. Tech. 68 (1996) Nr. 4, S.375/381
- [2] Gruhn, G.; Fichtner, G.; Chem. Tech. (Leipzig) 40 (1988) Nr. 12, S.505/512
- [3] Rauch, J.; «Mehrproduktanlagen», Wiley VCH Verlag GmbH, Weinheim, 1998
- [4] Quelle: Pilz V.; «Zur Bedeutung der Storfallverordnung », CIT 8, 1982
- [5] Die Begrundung fur diese Temperaturerhohung finden Sie in unserer Jubilaumspublikation, Topic 2 «Gefahren sichtbar machen».
- [6] Nolan hat Daten uber weltweit dokumentierte Ereignisse der Jahre 1970 bis 1981 zusammengetragen. Nolan, P. F., 1983; «The Case Histories of Runaway Reactions», Report to U.K. Health and Safety Executive.
- [7] Nolan und Barton haben auf der Basis der 263 untersuchten Falle die Ereignisse nach Reaktionstypen zusammengefasst und nach Unfallursache differenziert. Barton, J. A. and Nolan, P. F., 1984; «Runaway Reactions in Batch Reactors» I. Chem. E Symposium Series No. 85, 13.
- [8] Marrs et al. untersuchten Reaktorexpllosionen, die durch Uberdruck verursacht wurden, sowie die Wirksamkeit von Schutzmassnahmen gegen Reaktorexpllosionen. Marrs, G. P.; Lees, F. P.; Barton, J.; Scilly, N.; Chem. Eng. Res. Des, Vol 67, pp 381/406, July 1989.
- [9] Barton, J. A.; Nolan, P. F.; «Incidents in the chemical industry due to thermal runaway chemical reactions», Chemical Reaction Symposium, 12-13 December 1990 Amsterdam.
- [10] Norstrom, G. P.; (1982) «An Insurer's Perspective of the Chemical Industry» in Fawcett, H.H. and Wood, W.S. (Ed), Safety and Prevention in chemical Operations, pp. 509/527, J. Wiley, zit. in Lecture Series, «Loss Prevention / Plant Safety», S. Banerjee, Department of Chemical and Nuclear Engineering, University of California.
- [11] Prugh, R. W.; 1981 in Loss Prevention, Vol 14 (AIChE, New York) p. 1. Er schatzte die Wahrscheinlichkeit, dass eine Runawayreaktion erfolgreich verhindert werden kann, als 95 %. Dieses Resultat impliziert, dass 95 % der Prozessabweichungen die zu einem Reaktoruberdruck fuhren, nicht zu einem Unfall fuhren.
- [12] Kletz, T. A.; (1971), In «Major Loss Prevention in the Process Industry's» (IChemE, London), p. 75. In the original work on the FAR as a risk criterion the overall industry, or chemical industry, FAR was taken as 4. Allowing half of this for everyday hazards, such as falling down steps, etc., and half for special technological hazards, and assuming there might be up to five of the latter, gives a target FAR for any single technological hazard of 0.4.
- [13] Weltweit gesehen treten ab und zu Chemieunfalle auf, die sehr viele Todesfalle zu verzeichnen haben. Tritt nur ein solcher Unfall auf, so steigt das Todesfallrisiko dramatisch an.
- [14] Nebuloni, M.; Paper presented at RC User Forum Europe 1988.
- [15] Typische Ereignisursachen sind, ungenugende Kuhlung und ubermassiges Heizen. Eine Ereignisursachen kann vielfach in Unterereignisse eingeteilt werden. Zum Beispiel besteht die Ereignisursachen ungenugendes Kuhlen aus den Unterereignissen, Kuhlmittelzirkulationsfehler und Kondensatorfehler.
- [16] In unserer Jubilaumspublikation, Topic 2 «Gefahren sichtbar machen», werden diese Gefahren und ihre Wechselwirkungen ausfuhrlich diskutiert.
- [17] Steinbach, J.; «Chemische Sicherheitstechnik» VCH Verlag GmbH Weinheim, 1998
- [18] Die Systematik basiert auf: Expertenkommission fur Sicherheit in der Chemischen Industrie der Schweiz (1986), «Einfuhrung in die Risikoanalyse». Heft 4, Basel.
- [19] Damit die Erfassung der Basisdaten wirtschaftlich erfolgen kann, ist es sinnvoll, fur Ihren Betrieb massgeschneiderten Formulare zu verwenden.
- [20] Siehe dazu Glossarkasten auf Seite 12.
- [21] Literaturdaten zu menschlichen Fehlhandlungen. Siehe Madjar (Literatur [25]).
- [22] Stossel, F.; What is your thermal Risk?, Chem. Eng. Prog. 89, (1993),10, 68/75

- 
- [23] Die Problematik der Wärmeabfuhr wird ausführlich behandelt im Publikationsteil, Topic 2 «Gefahren sichtbar machen».
- [24] Der Begriff Kritikalität stammt aus der Kerntechnik. Er beschreibt den Zustand eines Kernreaktors, bei dem die zur fortgesetzten Kernspaltung notwendige Kettenreaktion nicht mehr von selbst erlischt (zu kritisch im Sinne von «bedrohlich»).
- [25] Madjar, M.; Methoden zur Risikoanalyse in der Fein- und Spezialitätenchemie, ETH (Eidgenössisch Technische Hochschule Zürich), Dissertation Nr. 11317
- [26] Das Abfrageschema ist angelehnt an Abb. 9-3 in Madjar (Literatur [25]).
- [27] Der Einfluss durch die Technik besteht darin, dass die Dampfabfuhr und die Dampfkondensation sichergestellt sein muss.
- [28] Die Szenarien für das geschlossene System werden nicht diskutiert.
- [29] Anhand der Rohrleitungsbilder und Instrumentenfließbilder werden diejenigen Komponenten, Versorgungsausfälle und Fehlhandlungen ermittelt, die eine Abweichung der festgelegten Funktion und somit den Ausfall des Moduls zur Folge haben kann.
- [30] Siehe dazu Glossarkasten auf Seite 32.
- [31] Im Jahre 1974 ereignete sich bei der Firma Höchst, bei der Herstellung von 2-Chlor-5-nitro-benzolsulfonsäure nach einem etwas anderen Verfahren, eine Reaktorexlosion. Das Verfahren zu diesem Fallbeispiel wurde von uns als Demonstrationsbeispiel massgeschneidert und sicherheitstechnisch untersucht.
- [32] Imaginäre Anlage. Angelehnt an Abb. 10-14 in Madjar (Literatur [25]). Das Verfahren zu diesem Fallbeispiel wurde von uns als Demonstrationsbeispiel so massgeschneidert, dass die Fehlerbaumanalyse analog zu dem in der zitierten Literatur analysierten Beispiel durchgeführt werden konnte.
- [33] Sicherheit in chemischen und verfahrenstechnischen Anlagen, Fortbildungskurs am Institut für Verfahrens- und Kältetechnik, März 1990.
- [34] Das Vorgehen ist eng an die «Modulare Fehlerbaumanalyse» Madjar (Literatur [25]) angelehnt worden. Die Zahlenwerte für die Zuverlässigkeitskenngrößen stammen aus dieser Quelle.
- [35] Es ist das Ziel des Aufsatzes den grossen Nutzen herauszuarbeiten, der durch die Klassifizierung der chemischen Prozessstufen entsteht. Damit die Übersichtlichkeit der Darstellung nicht ein Opfer der Vollständigkeit wurde, sind die Fehlerbäume zu den beschriebenen Teilsystemen in dieser Darstellung nicht diskutiert worden. Wir verweisen auf Madjar (Literatur [25]).
- [36] Siehe dazu Glossarkasten auf Seite 32.
- [37] Siehe dazu Glossarkasten auf Seite 32.
- [38] Abgesehen von diesen Ereignissen existieren «Minimal Cut Sets», die aus drei unabhängigen Ereignissen bestehen, ihre Wahrscheinlichkeit ist jedoch um zwei bis drei Grössenordnungen tiefer als die der «Minimal Cut Sets» mit zwei Ereignissen.
- [39] Madjar, M.; Von Rohr P. R.; «Polyprojekt Risiko und Sicherheit Leitfäden», Nr. 5 (1995) «Risikoanalyse verfahrenstechnischer Anlagen», VDF Verlag, Zürich, Schweiz.
- [40] Interessant zu diesem Thema ist das Buch «Chemiepolitik: Gespräch über eine neue Kontroverse» Herausgegeben von Martin Held, VCH Verlag GmbH, Weinheim, 1988.
- [41] In die Leitsätze wurden Gedanken eingebaut, die im Aufsatz «Perspektiven und Grenzen von Risikoabschätzungen für Unfälle in der chemischen Industrie» von Hans-Nicolaus Rindfleisch ähnlich formuliert wurden (Literaturzitat 40).



## **Seit der Gründung unserer Firma im Jahr 1991 dreht sich bei uns alles um die Sicherheit von chemischen Prozessen**

Wir – SCHNYDER Sicherheit in der Chemie AG – haben uns darauf spezialisiert, thermische Gefahren und Explosionsgefahren aller Stufen von chemischen und thermischen Prozessen sichtbar zu machen.

Wir...

- sind ein unabhängiges Unternehmen und verfügen für Sie über die notwendigen Instrumentarien und das Know-how, thermische Gefahrenpotentiale aller Stufen des chemischen und thermischen Prozesses aufzuzeigen,
- untersuchen für Sie bestehende und neue Verfahren mit dem Ziel, die den Prozessstufen inhärenten Gefahren aufzuzeigen, und zwar mit Bezug auf die sicherheitstechnische Bewertung der Prozessstufen beim Normalbetrieb einerseits und die sicherheitstechnische Bewertung der Prozessstufen bei Abweichungen vom Normalbetrieb andererseits.
- entwickeln für Sie – auf den Kenntnissen der thermischen Gefahrenpotentiale – auf Ihre Mehrproduktanlage massgeschneiderte neue wirtschaftliche Verfahren,
- ermitteln alle Basisdaten in unseren nach neuestem Stand der Technik ausgerüsteten Laboratorien.

Mit einem motivierten und qualifizierten Team untersuchen wir Chemische Reaktionen betriebsnah in Reaktionskalorimetern (RC1) in Kombination mit Fourier-Transformation-Infrarot-On-Line-Messungen (Reakt-IR). Die thermischen Gefahren der Stoffe und der Reaktionsmassen beurteilen wir auf der Basis von Mikrothermoanalyse (DSC, TGA), Makrothermoanalyse (RADEX-, SEDEX- und SIKAREX-Thermoanalyzesystem), adiabatischer Kalorimetrie sowie Gasentwicklungs- und Druckentwicklungsexperimenten.

### **SCHNYDER Sicherheit in der Chemie AG**

#### **Hauptsitz**

Gewerbehau Oederlin  
Landstrasse 2B  
CH-5415 Rieden-Nussbaumen  
Switzerland  
Tel. +41 (0)56 282 29 39  
Fax +41 (0)56 282 28 52  
Office@schnyderchemsafety.com  
www.schnyderchemsafety.com

