Methodenentwicklung zur Verknüpfung von Sicherheitsuntersuchungen und CAD

Dissertation

zur Erlangung des akademischen Grades

Doktoringenieur

(Dr.-Ing.)

von Dipl.-Ing. Marcus Marx

geb. am 31. Juli 1970 in Paderborn

genehmigt durch die Fakultät für Verfahrens- und Systemtechnik

der Otto-von-Guericke-Universität Magdeburg

Gutachter:	Prof. Dr.-Ing. habil. Ulrich Hauptmanns
	Prof. Dr.-Ing. habil. Henner Schmidt-Traub
	Dr.-Ing. Sigmar Rützel

Eingereicht am	03. Februar 2003
Promotionskolloquium am	19. Juni 2003

Zusammenfassung

Die Grundlagen für die Sicherheit einer Anlage werden bereits während der Entwurfsphase gelegt. Da in der heutigen Zeit der Entwurf von Chemieanlagen in der Regel mit CAD-Systemen erfolgt, ist eine Verbindung von Sicherheitsaspekten mit CAD erstrebenswert.

Es wurden zahlreiche R&I-Fließbilder bestehender verfahrenstechnischer Anlagen zur Identifizierung wiederkehrender Konfigurationen bei der Auslegung verschiedener Teilsysteme (wie z.B. Reaktorkühlung und -heizung, Druckregelungen, Verriegelungen, Notabschaltungen etc.) untersucht. Die Ausführungen der jeweiligen Teilsysteme sind dabei in Abhängigkeit vom Gefahrenpotential der Anlagen bzgl. Redundanz und Diversität unterschiedlich gestaltet.

Unter Nutzung dieser Ergebnisse wurde ein Expertensystem entwickelt, in dem die notwendigen Sicherheitssysteme identifiziert werden und eine Auslegung entsprechend dem ermittelten Gefahrenpotential angeboten wird.

Das der Anlage innewohnende Gefahrenpotential wird mittels des Fire & Explosion Index (F&EI) nach DOW Chemical abgeschätzt. Hierzu werden bestimmte sicherheitsrelevante Verfahrensbedingungen in vorgegebener Weise durch Zuordnung von Strafpunkten bewertet und durch Addition und Multiplikation zum F&EI zusammengefaßt.

Daran anschließend werden über einen an die PAAG-Vorgehensweise angelehnten Dialog mit dem Benutzer mögliche Störfallabläufe für das gewählte Teilsystem bestimmt. Zur Beherrschung dieser Störfallabläufe werden vom Expertensystem betriebliche und sicherheitstechnische Systeme vorgeschlagen. Die im Programm hinterlegten Teilssysteme wurden mittels probabilistischer Untersuchungen quantitativ ausgeglichen gestaltet. Der Redundanz- und Diversitätsgrad der vorgeschlagenen Systeme richtet sich dabei nach dem evaluierten Gefahrenpotential.

Die vom Anwender getroffenen Entscheidungen werden anschließend in eine CAD-Zeichnung umgesetzt. Die Zeichnung kann vom Anwender weiter bearbeitet werden.

Alle gewählten Entscheidungen werden dokumentiert und sind so jederzeit nachvollziehbar.

Abschließend wird an zwei Beispiele gezeigt, daß eine Verbindung von Sicherheitsüberlegungen und CAD möglich ist. So wird eine sichere Auslegung angeboten die kostspielige Nachrüstungsaktionen zu vermeiden hilft. Die modulare Struktur des Verfahrens ermöglicht es, betriebliche Auslegungsvorschriften und Änderungen der geltenden Gesetzgebung leicht zu integrieren.

Danksagung

Die vorliegende Arbeit entstand in der Abteilung „Anlagentechnik und Anlagensicherheit“ der Fakultät für Verfahrens- und Systemtechnik der Otto-von-Guericke-Universität Magdeburg.

Mein besonderer Dank gilt meinem Betreuer **Prof. Dr.-Ing. U. Hauptmanns** für die interessante Themenstellung, die jederzeit gewährte freundliche Unterstützung und für die wertvollen Hinweise in zahlreichen Diskussionen.

Weiterhin danke ich **Prof. Dr.-Ing. Henner Schmidt-Traub und Dr.-Ing. Sigmar Rützel** für ihr Interesse sowie die Bereitschaft zur Übernahme der Koreferate.

Herr Dipl.-Ing. Wolfgang Dörr von der BASF Schwarzheide hat mir durch seine Erfahrung und Diskussionsbereitschaft bei der Lösung vieler auftretender Probleme immer hilfreich zur Seite gestanden. Dafür danke ich ihm im Besonderen.

Prof. Dr.-Ing. habil. Siegfried Bussenius danke ich für sein fortwährendes Interesse und die vielen Hinweise und Anregungen bei der Anfertigung meiner Arbeit.

Danken möchte ich allen **Mitarbeitern** des Lehrstuhls, die mich bei der Durchführung und Anfertigung der Arbeit unterstützt haben.

Für die Unterstützung bei der programmtechnischen Umsetzung danke ich der Mannschaft von **ACPlant Consult SD GmbH**.

Inhaltsverzeichnis

BILDVERZEICHNIS

TABELLENVERZEICHNIS

SYMBOLVERZEICHNIS

c	mol/l	Konzentration
c_p	J/mol K	spezifische Wärmekapazität
E	J/mol	Aktivierungsenergie
E		Erwartungswert
F	m^2	Wärmeübertragungsfläche
h	J/mol	Enthalpie
H	1/s	Häufigkeit
$\vec{j}$	mol/s m^2	Stoffstromdichte
k_w	W/m^2 K	Wärmedurchgangskoeffizient
k	$(m^3/mol)^{Ord-1}/s$	Reaktionsgeschwindigkeitskonstante
MTSR	K	maximale Temperatur unter adiabaten Bedingungen
M_r	kg	Reaktionsmasse
N		Anzahl
Ord		Reaktionsordnung
$\dot{Q}$	J/(s mol)	molarer Wärmestrom
r	mol/(l s)	Reaktionsgeschwindigkeit
R	J/(mol K)	allgemeine Gaskonstante
t	s	Zeit
T	K	Temperatur
ΔT_{ad}	K	adiabatische Temperaturerhöhung
$\bar{u}$		zeitlich gemittelte Nichtverfügbarkeit
V	m^3	Volumen
$\dot{V}$	m^3/s	Volumenstrom
X		Umsatz

Indices, tiefgestellt

0	Anfangs- bzw. Eingangsbedingung
A	Komponente
ab	abgeführt
chem	chemisch
f	nach der Reaktion
i	Komponente
i	Laufindex
K	Kühlmittel
R	Reaktion
r	Reaktion
st	stöchiometrisch
W	Wand

Griechisch

κ		Minimalschnitt durch Anzeigevariable dargestellt
λ	1/s	Ausfallrate
ν		stöchiometrischer Koeffizient
Ψ		Strukturfunktion
ρ	kg/ m^3	Dichte
θ	h	Funktionsprüfungsintervall

1 Einleitung

1.1 Motivation der Arbeit

Im Bereich der Technik gibt es zahlreiche Gesetze, Regeln, Richtlinien, Vorschriften und Verordnungen, die dazu dienen, die zweckmäßige Beschaffenheit und funktionelle Sicherheit technischer Systeme zu garantieren. Darüber hinaus sollen sie den Schutz von Mensch, Umwelt und wertvollen Sachgütern im bestimmungsgemäßen Betrieb, aber auch bei Versagen, gewährleisten. Von besonderer Bedeutung für Chemieanlagen sind in diesem Zusammenhang das Bundesimmissionsschutzgesetz /Gese/ mit seinen Verordnungen /Vero00/ und /Stör00/.

Die Gefahren chemischer Anlagen bestehen im wesentlichen darin, daß vielfach Stoffe gehandhabt werden, die explosibel, giftig oder leicht entzündbar sind oder solche Eigenschaften als Folge von Reaktionen mit anderen Stoffen, die im Prozeß selbst (Öle, Kühlmittel etc.) oder in der Umgebung (z.B. Reaktionen mit der Luftfeuchtigkeit nach einer Freisetzung) vorhanden sind, entwickeln können. Außerdem kann es bei Abweichungen der Prozeßparameter (Druck, Temperatur etc.) von ihren Nominalwerten zu unerwünschten Nebenreaktionen kommen, die unter Umständen zur Bildung gefährlicher Stoffe führen, wie dies beispielsweise in Seveso /Orsi77/, /Lees96_3/ der Fall war. Diese Möglichkeit ist auch gemäß Störfallverordnung zu erörtern.

Daraus läßt sich die Aufgabe der Sicherheit von Chemieanlagen ableiten. Es ist das Ziel, gefährliche Stoffe zu vermeiden, und da dies in der Regel nicht oder nicht vollständig möglich ist, diese sicher einzuschließen.

Dies erfolgt durch passive Barrieren, z.B. Rohrleitungen, Apparategehäuse und Behälter, die vor übermäßigen Belastungen, wie sie infolge von Störungen denkbar wären, durch aktive Systeme wie z.B. Sicherheitsventile oder Notabschaltungen geschützt werden sollen.

Grundlegend für die Erfüllung dieser Aufgabe ist eine hohe Qualität der Komponenten der Anlage. Damit sind vor allem Festigkeit und Lebensdauer gemeint. Dies wird weitgehend durch die Beachtung der Vorschriften des Regelwerkes sichergestellt

/Schr02/. Dabei handelt es sich um die Kodifizierung langjähriger Erfahrung. Zu nennen wären stellvertretend die

- Betriebssicherheitsverordnung /Betr02/,
- Druckbehälter-Verordnung /Tech00/ (ersetzt durch die Betriebssicherheitsverordnung /Betr02/),
- AD-Merkblätter für Druckbehälter (z.B. /AD-Merkblatt A2/, /AD-Merkblatt A1/) oder Technischen Regeln und Sicherheitsrichtlinien für Dampfkessel (TRD/SR),
- DIN-Normen, Technische Regeln,
- Richtlinien und Merkblättern der Berufsgenossenschaften, wie z.B. die BG-Vorschriften (BGV),
- Vorschriften, Bestimmungen, Richtlinien, Merkblätter, Leitsätzen und Druckschriften von Sachverständigen-Gremien wie VDI, VDE, DVGW, VDMA und AWF.

Diese beinhalten neben Berechnungsgrundlagen auch Vorgaben für Sicherheitsbeiwerte. Diese sind aus mehreren Gründen erforderlich. Zum einen sind die Berechnungsmodelle nur Annäherungen an die Realität und die notwendigen Eingabedaten sind in der Regel mit Unsicherheiten behaftet. Zum anderen lassen sich weder die Belastbarkeit noch die auftretenden Belastungen in der realen Anlage genau vorherbestimmen. Die Verwendung von Sicherheitsbeiwerten führt in der Regel zu einer Überdimensionierung. Dennoch ist ein Komponentenversagen nicht ausgeschlossen, da immer noch eine –wenn auch in der Regel sehr kleine- Wahrscheinlichkeit dafür verbleibt, daß die Belastung die Belastbarkeit überschreitet. Dies kann durch verminderte Belastbarkeit z.B. durch Alterung, vergrößerte Belastung oder beides geschehen.

Vergrößerte Belastungen sind vor allem infolge Versagens betrieblicher Komponenten der Anlage oder spontaner chemischer Vorgänge wie Polymerisation oder Zerfall von Stoffen zu erwarten. Dieser Möglichkeit trägt die Störfallverordnung /Stör00/ Rechnung, indem sie eine Reihe von Forderungen für die Beschaffenheit der Komponenten, aber auch des technischen Systems Chemieanlage aufstellt.

Beispielsweise muß „die Auslegung, die Errichtung sowie der Betrieb und die Wartung (...) ausreichend sicher und zuverlässig“ (§ 9 Abs. 1 Satz 3) sein (...), um in Zu-

kunft Unfälle wie beispielsweise das Seveso-Unglück von 1974 /Orsi77/ zu vermeiden. Weiterhin sind „die Anlagen des Betriebsbereichs mit *zuverlässigen* Meßeinrichtungen und Steuer- oder Regeleinrichtungen auszustatten, die, soweit dies sicherheitstechnisch geboten ist, jeweils mehrfach vorhanden, verschiedenartig und voneinander unabhängig sind." (§ 4 Abs. 3)

Damit werden unter anderem Anforderungen an die Konfiguration von Systemen gestellt, die auch unter der Bezeichnung redundant und diversitär bekannt sind.

Die unbestimmten Rechtsbegriffe, mit denen die Ziele der sicherheitstechnischen Auslegung in der Störfallverordnung /Stör00/ beschrieben werden, nämlich die Verhinderung (§ 3 Abs. 1) bzw. die Minderung (§ 3 Abs. 3) der Auswirkungen von Störfällen, haben in der Praxis zu einem Anlagenkonzept geführt, das aus folgenden vier Ebenen besteht:

- Ebene 1: Betriebliche Ebene (umfaßt produktionsrelevante Aufgaben wie Messen, Steuern und Regeln, um den betrieblichen Ablauf und die Qualitätsanforderungen an das Produkt zu gewährleisten),
- Ebene 2: Störungsbeherrschung mit Alarmierungen und Abschaltungen,
- Ebene 3: Schadensvermeidung mit Noteingriffen und Schnellabschaltungen zur Vermeidung des Verlassens des bestimmungsgemäßen Betriebs und
- Ebene 4: Gefahrenabwehr mit Maßnahmen der Schadensbegrenzung.

Dabei gilt, daß bei Versagen einer Ebene die Ausweitung der Störung durch die jeweils nächste verhindert werden soll. Dies wird am Schema des Bildes 1-1 deutlich:

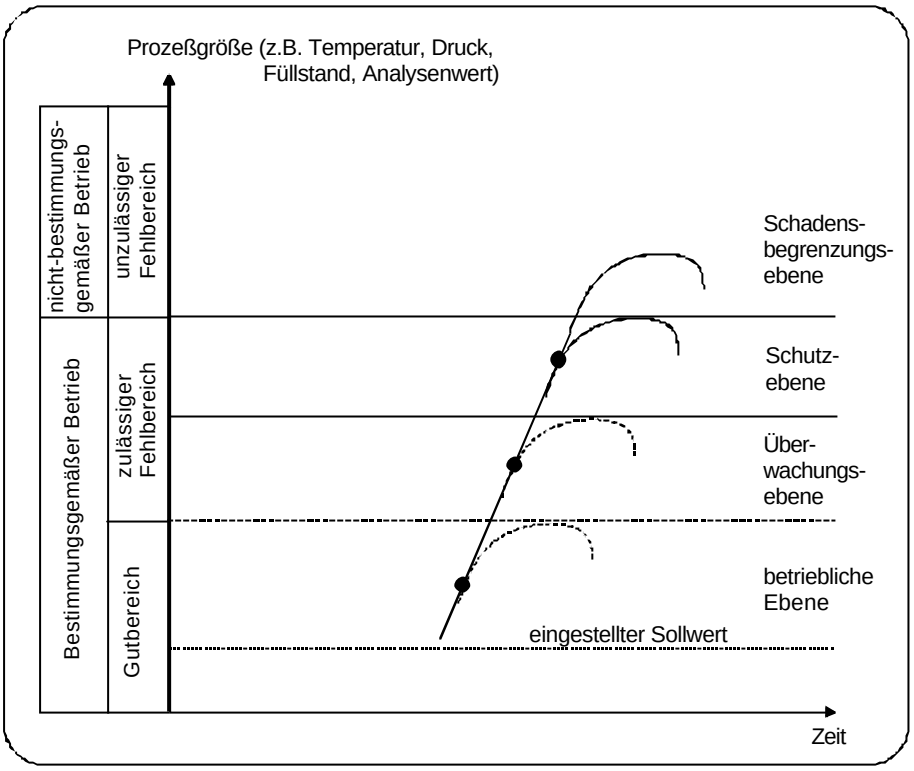


Bild 1-1: Die vier Ebenen der Sicherheit von Chemieanlagen

Das Versagen der einzelnen Ebenen kann Folge des spontanen Versagens von Komponenten oder von Reaktionen sein, die mit Überbeanspruchungen verbunden sind. In beiden Fällen handelt es sich um stochastische Ereignisse, d.h. der Zeitpunkt ihres Eintritts läßt sich nicht vorhersagen. Wohl aber läßt sich eine Wahrscheinlichkeit angeben, die im nachhinein bei entsprechenden Aufschreibungen im Prinzip empirisch ermittelt werden könnte, wegen der Seltenheit der Ereignisse aber in der Regel nur durch analytische Methoden mit Hilfe probabilistischer Sicherheitsuntersuchungen berechnet werden kann.

Das Ergebnis einer probabilistischen Sicherheitsuntersuchung wird am Bild 1-2 schamatisch deutlich.

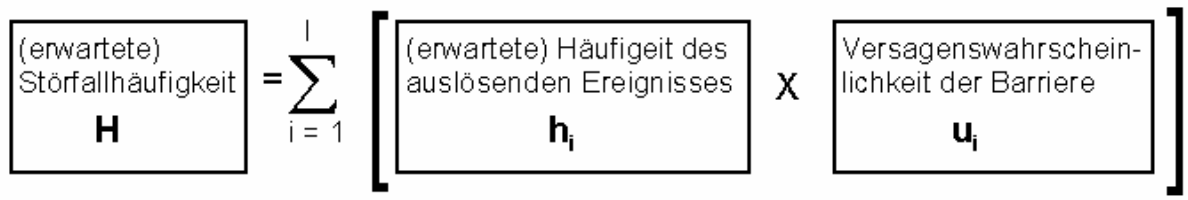


Bild 1-2: Veranschaulichung des Sicherheitskonzepts technischer Anlagen /www.uni-/

Ausfälle betrieblicher Komponenten oder spontane chemische Reaktionen sind, sofern sie Störungen einleiten[1], sogenannte auslösende Ereignisse. Sie treten mit einer gewissen (aus der Betriebserfahrung ermittelbaren) erwarteten Häufigkeit auf. Zu ihrer Beherrschung weist die Anlage Barrieren auf, die –wie bereits erwähnt- aus passiven und aktiven Elementen bestehen. Diese versagen mit einer bestimmten Wahrscheinlichkeit, so daß der Störfall mit einer erwarteten Häufigkeit auftritt, die als Produkt aus der erwarteten Häufigkeit und der Barrierenversagenswahrscheinlichkeit ermittelt wird. Da es in der Regel mehrere auslösende Ereignisse gibt, für die im übrigen unterschiedlich viele Barrieren zur Verfügung stehen, ist die Summe über alle erwarteten Häufigkeiten zu bilden. Bild 1-2 zeigt, daß eine Erhöhung der Sicherheit durch eine Herabsetzung der Größen h_i, u_i oder beider erreicht werden kann.

Die Anforderungen der Störfallverordnung beinhalten, daß durch ausreichende Zuverlässigkeit der Komponenten sowie eine redundante und diversitäre Systemauslegung die Häufigkeit der auslösenden Ereignisse und die Wahrscheinlichkeit des Barrierenversagens reduziert wird. Dies wird allerdings nicht explizit ausgeführt und auch nicht mit quantitativen Anforderungen belegt. Verbindliche Regeln für Systeme in Form von Gesetzen und Regeln gibt es nicht. Konventionen für Systeme sind höchstens innerbetrieblicher Natur, so daß dem Planer hier eine gewisse Gestaltungsfreiheit eingeräumt wird. Die hier vorgestellte Vorgehensweise stellt eine Konvention dar, die eine Möglichkeit aufzeigt, den Redundanz- und Diversitätsgrad der Systeme in Abhängigkeit vom Gefahrenpotential der Anlage festzulegen.

Aus dem Gesagten wird deutlich, daß die Sicherheit von Anlagen nicht allein durch die Qualität der einzelnen Komponenten bestimmt wird, sondern ebenso durch deren Zusammenspiel. Dabei sind natürlich auch notwendige und möglicherweise auch ungeplante menschliche Eingriffe einzubeziehen.

In der Störfallverordnung wird der Nachweis der genannten technischen Eigenschaften der Anlagen gefordert. Dazu stehen eine Reihe qualitativer und quantitativer Analyseverfahren zur Verfügung, wie z.B.

[1] Es gibt beispielsweise auch betriebliche Ausfälle, die zur Unterbrechung des Prozesses führen, nicht aber zu einer Störung, die sich zum Störfall ausweiten kann.

- „What-if“ – Methode /Guid92/,
- PAAG-Verfahren (HAZOP) /Lawl70/, /Der 80/,
- Failure Modes, Effects and Criticality Analysis (FMCA) /Guid92/,
- Fehlerbaummethode /DIN 25424/,
- Ausfalleffektanalyse /DIN 25448/,
- Ereignisablaufanalyse /DIN 25419/,
- Hoechst-Methode /Stei98/ und
- Zürich Hazard Analysis /Zogg87/.

Eine vergleichende Bewertung der Methoden findet sich in /Pilz87/. Da die sichere Gestaltung einer Anlage Teil der Entwicklungsphase ist, liegt es nahe, die Ergebnisse von Sicherheitsanalysen bereits in den Auslegungsprozeß, soweit möglich, zu integrieren. Dies ist deshalb möglich, da die Anlagen der chemischen Industrie trotz ihrer Vielfalt auf zahlreiche immer wieder anzutreffende Teilsysteme zurückgreifen. Dabei wäre zum Beispiel an Temperaturregelungen von Reaktoren, Füllstandsüberwachung bei Behältern oder Notabschaltung durch Abzug des Reaktorinhaltes zu denken.

Diese lassen sich in qualitativ verschiedenen Ausführungen, begründet durch Unterschiede in Redundanz- und Diversitätsgrad, im voraus probabilistisch bewerten und als fertige Teilsysteme in einer Datenbank abspeichern. Dazu bietet sich eine Verbindung mit einem CAD-Programm an, da der Entwurf von Chemieanlagen in der Regel mit CAD erfolgt. Neu ist dabei, daß dem Entwurfsingenieur anstelle einer Komponente ein Teilsystem für eine bestimmte Funktion zur Verwendung in seiner Anlagenauslegung angeboten wird.

1.2 Gliederung der Arbeit

Nachdem in Kapitel 2 Möglichkeiten und Grenzen des entwickelten Expertensystems aufgezeigt werden, beschreibt Kapitel 3 Expertensysteme in ihren Grundzügen und den Stand von Forschung und Technik computergestützter, sicherheitsorientierter Systeme. Im Anschluß daran wird der Aufbau einer Chemieanlage erläutert. In Kapitel 5 werden grundlegende Überlegungen zur sicheren Gestaltung von Chemieanlagen beschrieben. Danach erfolgt eine kurze Übersicht der Anforderungen an moderne Prozessleittechnik (PLT) in der Anlagensicherheit. Kapitel 7 beschreibt die Vorge-

hensweise zur Ermittlung des Gefahrenpotentials, Dow's Fire & Explosion Index, sowie die darauf aufbauende Methode zur Festlegung des Redundanzgrades betrieblicher und sicherheitsgerichteter Ausrüstungen. Daß neben dem Redundanzgrad der Ausrüstung auch die sicherheitstechnische Ausgewogenheit innerhalb einer Meßkette beachtet werden muß, beschreibt Kapitel 8. Daran schließt sich die Vorstellung des Expertensystems in Kapitel 9 an. Abschließend werden die Ergebnisse kurz zusammengefaßt und ein Ausblick gegeben.

2 Vorgehensweise und Abgrenzung

Zur Integration von Sicherheitsüberlegungen in CAD bedarf es einer Reihe von Schritten, die im Programmsystem SafeCAD /Marx01/, /Marx02/ umgesetzt sind.

Zunächst ist das Gefahrenpotential der auszulegenden Teilanlage abzuschätzen. Dazu stehen im Grundsatz eine Reihe von Methoden zur Verfügung, z.B.

- DOW's Fire&Explosion (F&E) Index /Fire94/,
- DOW's Chemical Exposure Index /Chem94/,
- DOW's Mond-Index /Impe85/,
- van der Brandt – Index /Inte93/ und
- TÜV-Rheinland-Methode /Kühn97/.

Gewählt wurde DOW's F&E Index, da er langjährig erprobt ist, periodisch auf den neuesten Stand gebracht wird und übersichtlich in der Handhabung ist. Die Methode ist nicht zeitaufwendig, da viele Faktoren und Stoffdaten in Tabellen zusammengefaßt und in der Anleitung Entscheidungshilfen vorhanden sind.

Das durch den DOW Index eingestufte Gefahrenpotential der Anlage ist die Grundlage für die Festlegung des Redundanzgrades und der Diversitätsanforderungen für Teilsysteme auf den Ebenen eins bis drei des Bildes 1-1.

Zur Ermittlung, welche konkreten Gefährdungen mit der Teilanlage verbunden sind, d.h. wie das ihr innewohnende Gefahrenpotential wirksam werden kann, müssen diese in systematischer Weise identifiziert werden. Als Grundlage dafür bietet sich das PAAG-Verfahren /Der 80/ an, das die deutsche Version des langjährig erprobten und speziell für Chemieanlagen entwickelten HAZOP /Lawl70/ Verfahrens ist. Dieses wurde –wie später im Einzelnen ausgeführt– an den vorliegenden Zweck angepaßt.

Neben der Ermittlung der Gefährdung zeigt diese Analyse auch, welche Teilsysteme zur Beherrschung der Gefährdungen erforderlich sind, d.h. welche Teilsysteme für die zu entwerfende Teilanlage im CAD-System anzubieten sind. Auf diese werden

dann die Anforderungen bezüglich Redundanz und Diversität aus dem ersten Schritt angewandt.

Das PAAG-Verfahrens wird sinnvollerweise in Form eines rechnergestützten Dialogs angewandt.

Die Verbindung der Elemente (F&E-Index, Gefährdungsermittlung, CAD) führt auf ein Expertensystem, wie in Kapitel 9 erläutert wird.

Das Expertensystem beinhaltet darüber hinaus Hilfen für den Benutzer, in dem unter anderem Hinweise aus den Regelwerken enthalten sind. Bild 2-1 gibt einen Überblick über den Ablauf einer Auslegung.

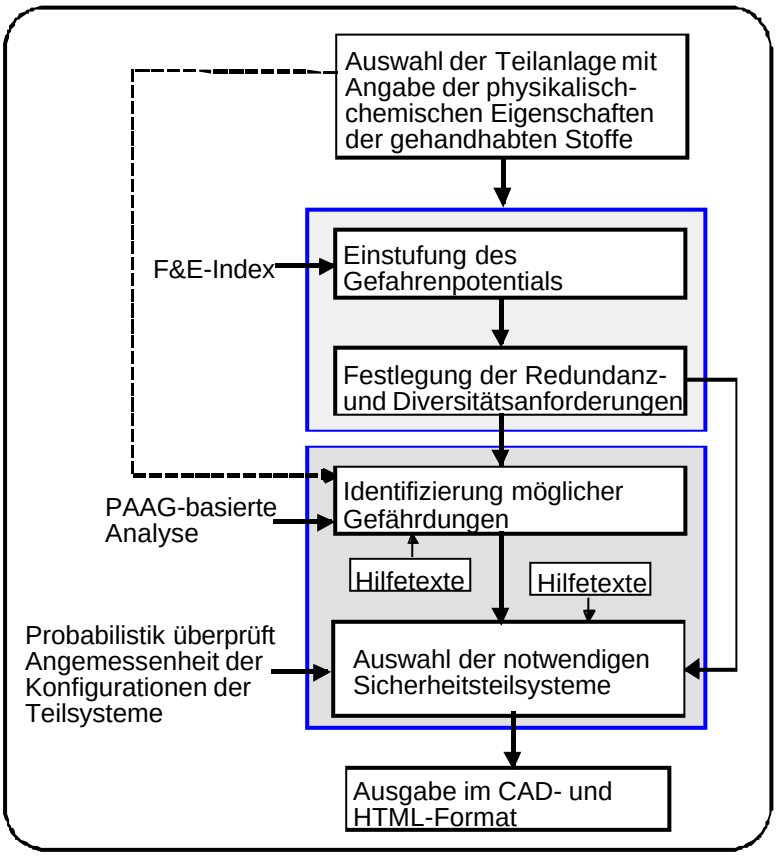


Bild 2-1: Bestandteile des Expertensystems SafeCAD

Der Nachweis der Wirksamkeit dieser Methode erfolgte über die Anwendung von Fehlerbäumen für die Alternativen unterschiedlicher Gefahrenpotentiale. So kann festgestellt werden, ob die jeweiligen Alternativen den Gefahrenpotentialen entsprechen und somit, auch aus wirtschaftlicher Sicht, eine übermäßige sicherheitstechni-

sche Ausrüstung vermieden werden kann. Dies ist auch aus sicherheitstechnischer Perspektive zu begrüßen, da ein Mehr an Sicherheitssystemen nicht unmittelbar einen Gewinn an Sicherheit bedeuten muß.

Denkbar ist auch ein Einsatz der Vorgehensweise zu Schulungs- und Einarbeitungszwecken, indem fiktive Anlagen von einem Team unter Zuhilfenahme des Systems ausgelegt werden. Am besten geschieht dies anhand einer einfachen, schon innerhalb des Betriebsbereiches bestehenden Anlage, so daß im Anschluß leichter verglichen werden kann. Darüber hinaus besteht so zusätzlich die Möglichkeit, Schwachstellen innerhalb der Anlage aufzudecken und auf andere Anlagenbereiche zu übertragen, wodurch der kontinuierliche Verbesserungsprozeß des Betriebs unterstützt werden kann.

Die hardwareseitige Auslegung von PLT-Schutzeinrichtungen wird ausführlich in der DIN 19250 /DIN V 19250/, DIN EN 2180 /DIN/VDE2180_2/ und der NAMUR-Richtlinie NE 31 /NAMU93/ beschrieben. Die Festlegung, wann eine Sicherheitsschaltung der Kategorie A (Z-Schaltung[2]) und wann eine Sicherheitsschaltung der Kategorie B (S-Schaltung[3]) vorzusehen ist, wird derzeit nicht vom Expertensystem vorgenommen. Die in der DIN 19250 beschriebene Matrixmethode kann aber in das System integriert werden.

Des weiteren erfolgt keine Prozeßauswahl etwa unter dem Hinblick auf ein möglichst geringes Schadstoffinventar. Diese muß von den Entwicklungsingenieuren bei Festlegung des Verfahrens und des Anlagentyps in Zusammenarbeit mit den Laborexperten und Fachleuten verschiedener Ausrichtungen vorgenommen werden.

Ziel dieser Arbeit ist es mithin, ein Verfahren zu entwickeln, daß das Gefahrenpotential einer Anlage richtig einschätzt sowie den Planer bei der Evaluierung möglicher betrieblicher Abweichungen unterstützt und Lösungsvorschläge anbietet, die aufgrund ihres Redundanzgrades und ihrer Diversität eine Ausfallhäufigkeit aufweisen,

---

[2] Z-Schaltungen sind "PLT-Schutzeinrichtungen (...) zur Vermeidung von Personen- oder größeren Umweltschäden sowie Sachschäden, die im Sinne der Störfallverordnung als "ernste Gefahr" anzusehen sind." /NAMU93/.

[3] S-Schaltungen sind "PLT-Schutzeinrichtungen (...) zur Vermeidung größerer Sachschäden, die im unternehmerischen Eigeninteresse betrachtet werden und bei denen Personenschäden und größere Umweltschäden ausgeschlossen werden können." /NAMU93/.

die im Hinblick auf das Gefahrenpotential der Anlage entsprechend gering ist. Es sei betont, daß es nicht Ziel ist, eine rechnergestützte Methode zu entwickeln, die herkömmliche Sicherheitsanalysen ersetzten soll. Dies kann und darf auch nicht Ziel zukünftiger Entwicklungen auf dem Gebiet der Sicherheit sein, da das abstrakte Denk- und Kombinationsvermögen von Experten nicht durch computergestützte Systeme ersetzt werden kann.

3 Stand der Forschung zu Expertensystemen

In diesem Kapitel werden die Grundlagen von Expertensystemen kurz aufgezeigt. Darauf aufbauend wird in Kapitel 9 die Entwicklung von SafeCAD vorgestellt. Neben ausgewählten Beispielen von Expertensystemen, die sich mit der Sicherheit von Chemieanlagen befassen, werden darüber hinaus die Grenzen heutiger Systeme und weitere Entwicklungsmöglichkeiten dargestellt.

3.1 Einführung

Expertensysteme sind derzeit das erfolgreichste Anwendungsgebiet der künstlichen Intelligenz /Wach95/. Beierle /Beie00/ definiert ein Expertensystem wie folgt:

> *„Ein Expertensystem ist ein Computersystem (Hardware und Software), das in einem gegebenen Spezialisierungsbereich menschliche Experten in Bezug auf ihr Wissen und ihre Schlußfolgerungsfähigkeit nachbildet."*

Es handelt sich somit um ein Programmsystem, das „Wissen“ über ein Spezialgebiet speichert, daraus Schlußfolgerungen ziehen kann und zu konkreten Fragen dieses Fachgebietes Lösungen anbietet. Damit wird Expertenwissen in Form eines Algorithmus für bestimmte Gebiete strukturiert angeboten. Dabei sind die Schritte eines Algorithmus im einzelnen:

1. Problembeschreibung,
2. Kriterien zur Entscheidung, ob eine Lösung gefunden wurde,
3. Folge von Einzelanweisungen, die für die Maschine (in der Regel ein Computer) ausführbar sein müssen und
4. Vorschrift, in welcher Folge die Anweisungen abzuarbeiten sind.

Der Algorithmus muß dabei so konzipiert sein, daß er in endlicher Zeit eine eindeutige Lösung für das beschriebene Problem erzeugt. Zur Erreichung des Ziels der Speicherung, Abbildung und des Transports von Expertenwissen sind verschiedene Eigenschaften erforderlich /Frie90/, /Beie00/:

- Integration des Wissens eines oder mehrerer Experten zur Lösung von Problemen in einem bestimmten Anwendungsbereich,

- explizite, möglichst deklarative Darstellung des Expertenwissens,
- Unterstützung des Wissenstransfers vom Experten zum System,
- leichte Wartbarkeit und Erweiterbarkeit des im System enthaltenen Wissens,
- Darstellung des Wissens in einer leicht lesbaren Form,
- Verwendung unsicheren Wissens (sowohl Expertenwissen als auch Wissen über einen gegebenen Fall ist oft mit Unsicherheiten verbunden),
- möglichst natürliche und anschauliche Benutzerschnittstelle sowie
- Begründung und Erklärung der Ergebnisse,
- klare Trennung von Faktenwissen und Problemlösungsheuristiken und
- Wiederverwendbarkeit einmal erworbenen Wissens in verwandten Problembereichen.

Bild 3-1: Qualitätsmerkmale eines Expertensystems

Derzeitige Expertensysteme erfüllen die Anforderungen des Bild 3-1 nur teilweise /Frie90/. Ihre Qualität läßt sich anhand des Erfüllungsgrades der einzelnen Punkte messen. In Kapitel 9 wird die Erfüllung der in Bild 3-1 genannten Anforderungen durch SafeCAD diskutiert.

Ziel bei der Entwicklung von Expertensystemen ist es, das Spezialwissen und die Schlußfolgerungsfähigkeit von Experten auf Spezialgebieten nachzubilden. Dazu werden detaillierte Einzelkenntnisse über das Aufgabengebiet und Problemlösungsstrategien benötigt. Zur Erhöhung der Transparenz und Änderungs- sowie Erweiterungsfreundlichkeit von Expertensystemen ist eine klare Trennung zwischen Wissen und Strategie erforderlich. Der Unterschied zu konventionellen Programmen besteht somit im Programmierstil. Während bei den gewöhnlichen Programmen der anweisungsbasierte Programmierstil durch Sequenzen von Befehlen und Abfragen genau festlegt, was in welcher Reihenfolge getan wird, ermöglicht der regelbasierte Programmierstil durch die Vorgabe von Regeln und deren Interpretierer dem Experten festzulegen, was getan wird. Die Reihenfolge bestimmt hierbei der Regelinterpretierer. Weiterhin sollte ein Expertensystem über eine Erklärungskomponente verfügen, die den Lösungsvorschlag des Systems für den Anwender transparenter macht.

Diese Eigenschaften erfüllte erstmals das Expertensystem MYCIN /Buch84/ zur Diagnose und Therapie von bakteriellen Infektionskrankheiten des Blutes und Meningi-

tis. Bei der Entwicklung von MYCIN wurden folgende Punkte berücksichtigt bzw. umgesetzt:

- Implementierung eines interaktiven, entscheidungsunterstützenden Frage-Antwort- Dialogs zur Kommunikation zwischen Benutzer und System,
- Möglichkeit der Verarbeitung von Labordaten,
- Erklärungskomponente,
- Möglichkeit zur Erweiterung der Wissensbasis und
- eine modulare Wissensrepräsentationsform.

Der letzte Punkt hängt mit der Erweiterung der Wissensbasis zusammen. Ohne einen modularen Aufbau müßte die Wissensbasis nach jeder Bearbeitung umstrukturiert werden. Dies würde zum einen einen enormen Arbeitsaufwand erfordern und zum anderen die Fehlerwahrscheinlichkeit erhöhen. MYCIN diente somit als Vorbild für weitere Entwicklungen. Als Beispiel sind hier zu nennen:

- Prospektor /Pupp91/
  Dieses Expertensystem verarbeitet unsicheres Wissen auf dem Gebiet der Geologie unter Verwendung von Wahrscheinlichkeiten.
- HEARSAY II /Erma80/
  Es ermöglichte erstmals das Verstehen gesprochener Sprache und wandelte diese in computerverständliche Befehle um.

Die Vielzahl der heute gebräuchlichen Expertensysteme gestaltet eine Auflistung der neueren Systeme schwierig. Einen Überblick vermittelt z.B. /Rodg95/, /Mert93/. Im folgenden werden auszugsweise Systeme kurz vorgestellt, die sich mit einem oder mehreren der Punkte

- R&I-Fließbilder verfahrenstechnischer Anlagen /DIN28004_1/,
- PAAG-Verfahren,
- Komponenten verfahrenstechnischer Anlagen oder
- der Sicherheit verfahrenstechnischer Anlagen

befassen.

Frühe Systeme zur automatisierten Sicherheitsbetrachtung bieten meist nur standardisierte Formblätter zur Unterstützung von PAAG Analysen an. Als Beispiel sei hier SAnDOC genannt /SanD89/. Der Nachteil ist, daß keine Analyse der betrachteten Anlage auf diese Weise möglich ist. Ebenso wenig werden Maßnahmen angeboten, um die im Rahmen der manuellen Analyse aufgedeckten Gefährdungen entsprechend vermeiden bzw. beherrschen zu können. Allerdings darf der Vorteil der automatischen Erstellung einer Dokumentation nicht außer Acht gelassen werden.

Sonnenschein /Sonn95/ entwickelte ein wissensbasiertes System, das auf der Grundlage von Verfahrensfließbildern die Instrumentierung auf der betrieblichen Ebene über einen Frage-Antwort Dialog mit dem Anwender vornimmt. Dazu werden Baumstrukturen über die Programmiersprache Prolog zur Wissensverarbeitung genutzt. Zur Visualisierung der Ergebnisse wird ein CAD-System genutzt. Sicherheitstechnische Untersuchungen sind nicht Gegenstand der Arbeit.

Göring /Göri93/ hingegen hat auf der Grundlage des PAAG-Verfahrens und seiner praktischen Anwendung das Expertensystem HAZEXPERT (Hazard Identification Expert System) erarbeitet. Dazu wird ein Verfahrensfließbild erstellt und dessen topologische Struktur über ein Programm in objektorientierter Form abgeleitet. Darauf aufbauend findet die sicherheitstechnische Überprüfung mittels HAZEXPERT statt. Im Rahmen einer zielgerichteten Suche entlang von Fließlinien werden die möglichen Auswirkungen von Gefährdungen wie verstärkter Massenzustrom oder verringerter Energieabstrom auf die Komponenten untersucht. Aus einer Vorschlagsliste können dann Gegenmaßnahmen ausgewählt werden.

HAZEXPERT ermöglicht jedoch derzeit eine vollständige Analyse von Chemieanlagen auf der Grundlage ihrer Verfahrensfließbilder lediglich im Hinblick auf die Gefährdung einer Anlage durch „Überdruck“. Hier ist eine Ausweitung auf andere Gefährdungen nötig. Eine Berücksichtigung des Redundanz- und Diversitätsgrades bei der Auswahl der Gegenmaßnahmen ist nicht vorgesehen.

Der modellbasierte Ansatz von *Graf* /Graf00/ stützt sich ebenfalls auf das PAAG-Verfahren. Um instationäre Vorgänge zu berücksichtigen, wird das PAAG-Verfahren

durch ein Anlagenmodell ergänzt, bei dem die zeitlichen Änderungen von Prozeßgrößen durch eine Reihe qualitativer diskreter Zustände simuliert werden. Die Änderungen werden durch nicht zeitbewertete Zustandsübergänge beschrieben. Bezogen auf den Zustand „Ventil öffnet bei Behälter voll“ werden die Zustandsübergänge „Behälter fast voll“, „Behälter teilweise voll“, „Behälter fast leer“ und schließlich „Behälter leer“ generiert. Zur Umsetzung im Programm wurde das Verfahren der „state charts“ aus der Informatik verwendet. Diese dienen der Widerspiegelung der Anlagentopologie.

Vorteile der Methode sind die Visualisierung von Gefahren und deren Auswirkungen, die Untersuchung von Fehlerfortpflanzung in der Gesamtanlage und bezüglich der Vollständigkeit und Nachvollziehbarkeit der Dokumentation. Zur Anwendung ist auch hier die Vorgabe des Verfahrensfließbildes nötig.

Die vorgestellten Modelle zeigen, daß auf dem Gebiet der rechnergestützten Sicherheitsbetrachtung in den letzten Jahren Fortschritte erzielt werden konnten. Oftmals lagen Probleme bei der Umsetzung an der Qualität der Hardware. Die Entwicklungen der jüngsten Zeit auf diesem Gebiet haben dafür gesorgt, die Einflüsse dieses Problems zu mindern.

3.2 Entwicklungsschritte

Ein Expertensystem darf kein starres, einmal eingerichtetes Werkzeug sein. Vielmehr muß es sich leicht an Änderungen und Weiterentwicklungen anpassen lassen. Ein ständiger Dialog zwischen Nutzern, Experten und Entwicklern kann dies am leichtesten realisieren. Bild 3-2 veranschaulicht die Zusammenhänge.

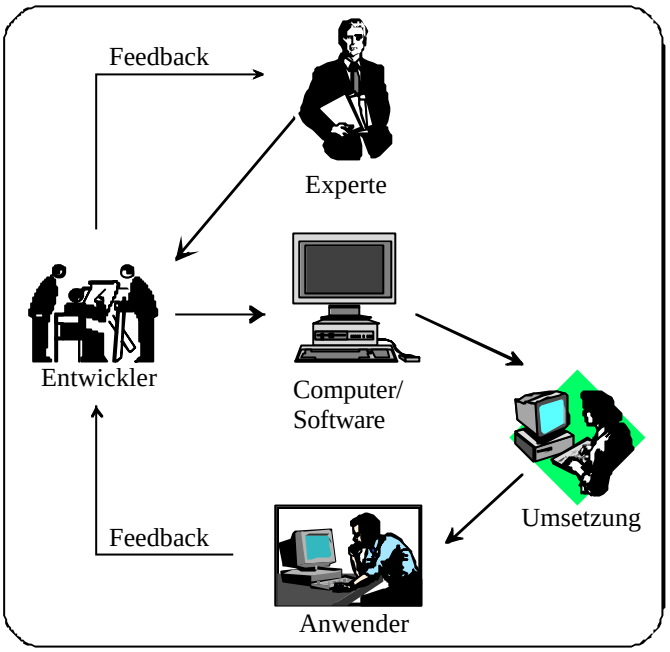


Bild 3-2: Das dynamische Expertensystem /Rodg95/

Die Entwicklung von Expertensystemen erfolgt in mehreren Schritten. In /Rodg95/ werden sechs Schritte angeführt, *Castillo et al.* hingegen schlagen in Erweiterung acht Schritte gemäß Tabelle 3-1 vor /Cast97/. In der rechten Spalte der Tabelle wird angeführt, wie die einzelnen Punkte in SafeCAD verarbeitet wurden. Die genaue Beschreibung der Punkte erfolgt im weiteren Verlauf der Arbeit.

Castillo et al.	**Umsetzung im Programm**
1. Problembeschreibung	Auslegung technischer Systeme, Kapitel 2.
2. Wissensquellen	Auswertung von R&I, PAAG-Analysen, Gespräche mit Fachleuten aus der Industrie, F&EI, Literaturrecherche, Kapitel 3.
3. Design	Darstellung der Lösung als HTML-Datei und als Zeichnung im dwg-Format; Oberflächendesign der Anwenderschnittstelle, Abschnitt 9.2.3 und 9.3.
4. Entwicklungswerkzeug	Editor, Analyzer, HTML, C++, Python, Kapitel 9.
5. Entwicklung eines Prototypen	SafeCAD wurde im rapid-prototyping-Verfahren entwickelt, Kapitel 9.
6. Testen des Prototyps	
7. Verfeinerung und Generalisierung	
8. Wartung und Pflege	Modularisierung der Wissensbasis erleichtert Wartung und Pflege, Kapitel 9.

Tabelle 3-1: Entwicklungsschritte eines Expertensystems

Zwischen den Punkten bestehen Wechselbeziehungen, so daß sie nicht der Reihe nach abgearbeitet werden können. Eine detaillierte Erläuterung der einzelnen Punkte findet man in /Frie90/.

Zu deren Umsetzung werden im groben folgende Schritte in der angegebenen Reihenfolge durchlaufen:

1. Das Expertenwissen wird in geeigneter Form im System gespeichert.
2. Der Anwender formuliert das Problem.
3. Ein Wissensinterpreter sucht in der Wissensbasis die Lösung des Problems.

Die Qualität des ersten Schrittes mißt sich dabei an dem Erfolg des dritten Schrittes. D.h., das Wissen liegt dann in „geeigneter Form“ vor, wenn der Wissensinterpreter das Problem bewerten kann und in der Lösungsmenge derart navigieren kann, daß die Suche zu einer gültigen Lösung führt. Es muß für die Implementierung beider Punkte eine geeignete Form der Wissensdarstellung und eine geeignete Suchstrategie gefunden werden. Dabei spielt die Verknüpfung zwischen Wissensbasis und Wissensverarbeitung eine übergeordnete Rolle. Die Wissensrepräsentation hängt entscheidend von der Gestaltung der Wissensbasis ab. Die Schwierigkeit besteht darin, menschliches Wissen durch eine formale symbolische Notation darzustellen. Als Mittel zur Wissensdarstellung sind folgende Formen einsetzbar:

- **Produktionsregeln:** verknüpfen eine Bedingung mit einer Aktion.
- **Frames:** stellen Rahmensituationen dar, die an mehreren Stellen wiederverwandt werden können. Diese können durch Parametrisierung angepaßt werden. Die Parameter werden als Slots bezeichnet,
- **Prädikate:** sind logische Ausdrücke, also Operatoren oder Funktionen, die Operatoren bzw. Parameter verarbeiten und einen logischen Wert liefern.
- **Semantische Netze:** sind gerichtete Graphen, deren Knoten Lösungen oder Zwischenlösungen entsprechen. Die Kanten des Graphen werden durch Regeln gebildet, mittels derer der Lösungsalgorithmus (Regelinterpreter) zu den verschiedenen Zwischenlösungen navigiert.

- **Topics („Gegenstandsbeschreibungen“):** ähneln in ihrer Funktionsweise den Frames. Obwohl sie lediglich auf eine bestimmte Situation anwendbar sind, erlauben sie eine Parametrisierung über Variable und Ausgangsparameter.

Die in SafeCAD angewendete Form der Wissensrepräsentation wird in Kapitel 9 beschrieben.

3.3 Grenzen

Puppe /Pupp91/ beschreibt, wie ein Experte bei der Lösung eines Problems vorgeht. Er muß

1. das Problem verstehen,
2. eine Lösung anbieten,
3. diese erklären,
4. Randgebiete überblicken,
5. seine Kompetenz bei der Problemlösung einschätzen und
6. neues Wissen erwerben und strukturieren.

In Expertensystemen hingegen läßt sich nur der zweite und dritte Punkt verwirklichen. Aber gerade die Verbreiterung der Wissensbasis durch logische Verknüpfung von Teilen des Allgemeinwissens (vgl. Bild 3-3) mit einem Problem führen oftmals zu gänzlich neuen Lösungen. Eine solche Lernfunktion besitzen Expertensysteme dieser Art nicht. Dies würde voraussetzen, daß das Expertensystem das Problem versteht (vgl. Bild 3-4).

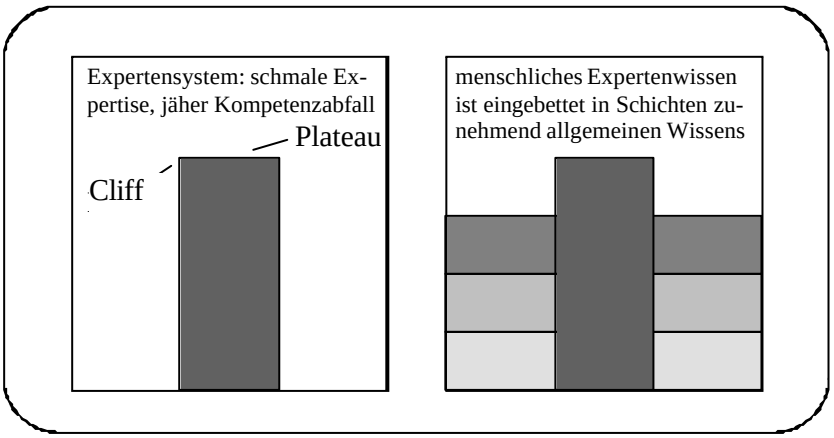


Bild 3-3: Cliff-Plateau-Effekt /Wach95/

Somit sorgt der scharfe Kompetenzabbruch der Systeme dafür, daß nur für klar spezifizierte Anforderungen vom System geeignete Lösungen angeboten werden können.

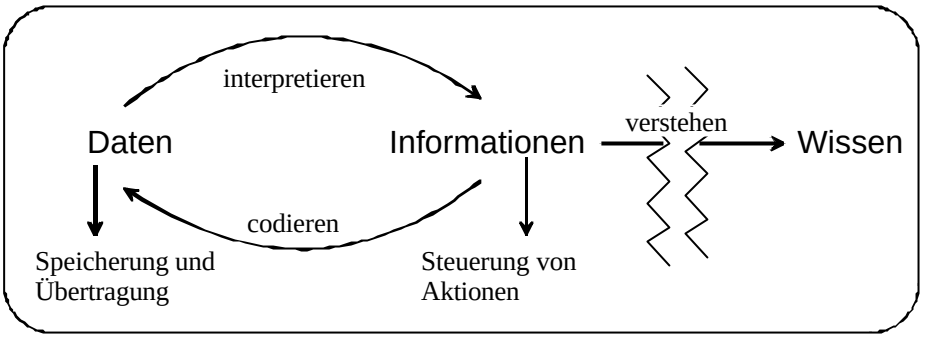


Bild 3-4: Grenzen des Expertensystems

Diese Aufgabe mittels symbolverarbeitender künstlicher Intelligenz zu erfüllen, ist durch Verarbeitung enormer Wissensmengen und damit einer Verbreiterung des Plateaus gemäß Bild 3-3 vorstellbar /Wach95/. Derzeit werden auch Überlegungen angestellt, durch Integration adaptiver subsymbolischer Ansätze -wie etwa Evolutionärer Algorithmen (EA)- mit der symbolverarbeitenden Wissensrepräsentation regelbasierter Expertensysteme zu optimieren. Hauptunterschied der Evolutionären Algorithmen zur klassischen KI ist dabei das Vorgehen im Lösungsraum. KI-Systeme bewegen sich explizit, also regelbasiert im Lösungsraum, während EA sich stochastisch im Lösungsraum bewegen. Dabei werden durch integrierte evolutionäre Operatoren immer neue Lösungsstrukturen erzeugt. Die Bewertung der neuen Strukturen sorgt dafür, daß nur gute Lösungen vererbt werden und somit die Population als Ausdruck für die Anzahl an Lösungen beständig steigt. Eine Einführung in EA wird u.a. in /Niss97/ und /Pohl00/ gegeben. Die Verknüpfung mit EA ist im Rahmen dieser Arbeit nicht vorgesehen und auch nicht nötig, da nur industriell erprobte Lösungen angeboten werden sollen und somit jeder Anforderung eine bestimmte Lösungsmenge zugeordnet werden kann.

4 Aufbau einer Chemieanlage

Chemieanlagen setzen sich im allgemeinen aus den drei Stufen

- Aufbereiten/Vorhalten,
- Reaktion und
- Aufbereitung

zusammen /Onke96/. Bild 4-1 verdeutlicht die Grundstruktur einer Chemieanlage:

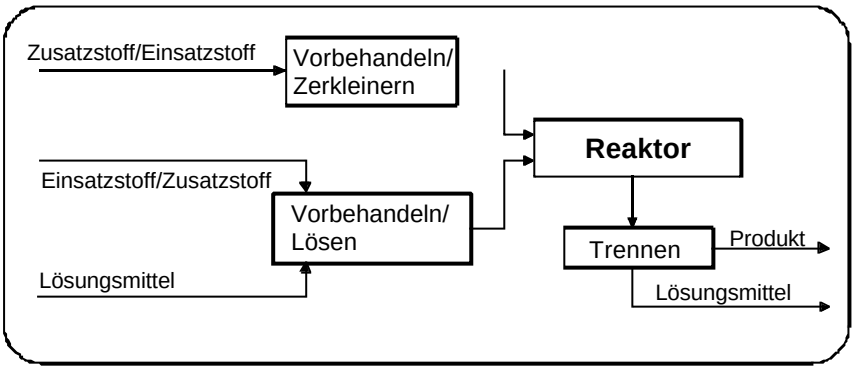


Bild 4-1: Grundstruktur einer Chemieanlage

Diese Abschnitte bestehen im wesentlichen aus einer Hauptanlage der chemischen oder thermischen Stoffumwandlung zur Erzeugung des gewünschten Produktes und einer Vielzahl von Nebenanlagen. Dabei besteht die Hauptanlage aus einem Prozeß der chemischen Stoffumwandlung (unit processes) wie /Satt00_1/

- Oxidation
- Reduktion
- Hydrierung
- etc.

oder der physikalischen Stoffumwandlung (unit operations) wie

- Trennen
- Vereinigen
- Formgeben
- Wärmeaustauschen

- etc.

Die Nebenanlagen dienen /Satt00_1/

- der Versorgung der Hauptanlagen mit Energien,
- dem Heranführen der Roh- und Hilfsstoffe und zum Abtransport der Produkte,
- dem Lagern der Roh- und Hilfsstoffe, der Produkte, der Ersatzteile, der Reparatur- und Wartungsmaterialien,
- der Bereitstellung von Hilfsstoffen wie Wärmeträgern, Katalysatoren, Lösungsmitteln, Inerten,
- der Entsorgung,
- der Regelung und Steuerung der Hauptanlage,
- der elektrotechnischen und nachrichtentechnischen Ausrüstung,
- der heizungs-, lüftungs- und klimatechnischen Versorgung von Produktionsräumen, Meßwarten usw. und
- den Einrichtungen für das Betriebspersonal.

Den allgemeinen Aufbau einer Hauptanlage zeigt Bild 4-2. Dabei ist die durch das Produkt vorgegebene Kombination der verschiedenen Teilanlagen charakteristisch für die jeweilige Anlage. Mit Teilanlage ist der Teil einer Anlage gemeint, der zumindest zeitweise selbständig betrieben werden kann. Die hierarchische Gliederung einer Chemieanlage verdeutlicht Bild 4-3.

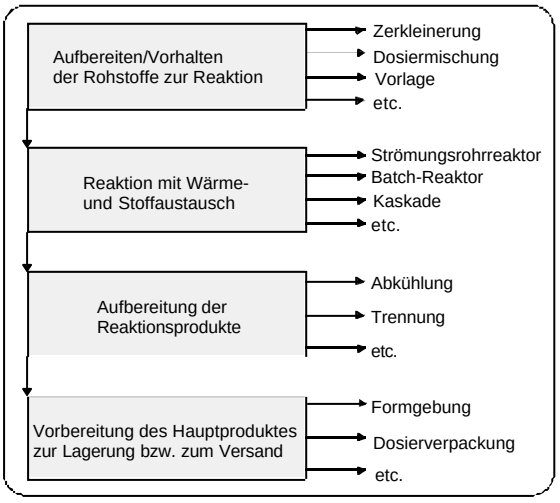


Bild 4-2: Aufbau einer Hauptanlage der chemischen Industrie (nach /Satt00_1/)

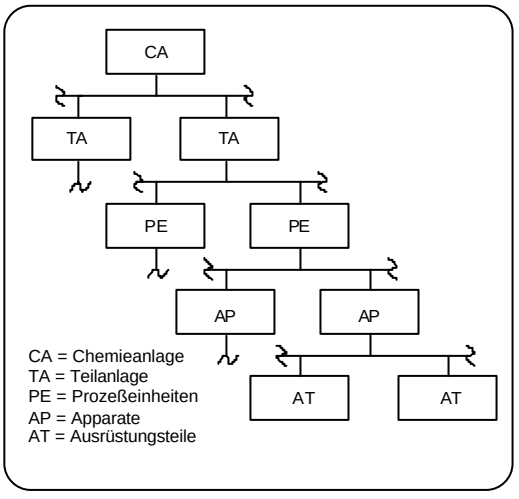


Bild 4-3: Gliederung einer Chemieanlage

Der chemische Reaktor bildet dabei das Kernstück der Anlage. Bei der Wahl des geeignetsten Reaktors müssen die Punkte

- allgemeine Überlegungen,
- Inventar,
- Kinetik und Wärmeentwicklung der Reaktion,
- Stabilität der Reaktion und
- Kontrolle der Reaktion

berücksichtigt werden /Lees96_1/. Besondere Bedeutung hat dabei die Reaktion. Die Reaktion kann in der Gas-, Flüssig- oder Feststoffphase ablaufen, sie kann katalytisch oder nicht-katalytisch sein. Die Reaktionskinetik kann erster oder höherer Ordnung, die Reaktion reversibel oder irreversibel mit unterschiedlichen Umsetzungsraten sein. Ebenso spielt die Art der Reaktion hinsichtlich ihrer Wärmeentwicklung (endotherm, exotherm) eine entscheidende Rolle.

Ein weiterer wichtiger Punkt bei der Reaktorwahl ist die Entscheidung für einen Batchreaktor oder kontinuierlichen Reaktor, für einen ideal durchmischten oder plug-flow Reaktor. Der Einfluß der Wahl des Reaktortyps auf das Gefahrenpotential wird in Kapitel 5 näher beschrieben (Tabelle 5-1).

Neben dem Aufbau der Anlage spielt bei ihrer Planung auch die Struktur des Verfahrens beziehungsweise des Prozesses eine wichtige Rolle. Nach /DIN EN 61512-1/ kann ein Prozeß in Prozeßabschnitte, Prozeßoperationen und Prozeßschritte zerlegt werden. Die Strukturierung des Prozesses ist von Bedeutung für die richtige Rezeptfahrweise der Anlage; sie ist nicht Gegenstand dieser Arbeit.

Im Rahmen der neuen Vorgehensweise wurden im Expertensystem SafeCAD aus den Bereichen gemäß Bild 4-2 die Teilanlagen Vorlagebehälter, Reaktor (semi-batch) und Absorptionskolonne implementiert.

5 Sichere Auslegung von Chemieanlagen

Die nachfolgenden Betrachtungen zeigen die übliche Vorgehensweise zur sicheren Auslegung von Chemieanlagen auf. Sie dienen dem Programm SafeCAD als Grundlage und sind im Programm an den entsprechenden Stellen zum Teil als Orientierung in der Hilfefunktion (siehe Kapitel 9) abgelegt.

5.1 Gefahrenpotential chemischer Prozesse/Reaktionen

Das Gefahrenpotential einer Chemieanlage setzt sich in erster Linie aus den energetischen und toxikologischen Potentialen der gehandhabten Stoffe sowie deren Quantitäten zusammen. Prozesse, die hinsichtlich der Reaktion besonders gefährlich sind, beinhalten in der Regel /Lees96_2/:

- hoch reaktive Substanzen,
- hohe Exothermien,
- unstabile Substanzen,
- thermisch empfindliche Substanzen oder
- Substanzen, die empfindlich auf Verunreinigungen oder
- hohe Drücke sowie hohe Temperaturen reagieren.

Für die sichere Fahrweise eines chemischen Reaktors bei exothermen Bedingungen ist jedoch in den meisten Fällen die Beherrschung der durch die Reaktion entstehenden Wärmemenge entscheidend /TAA-GS-05/. Diese läßt sich über die Stoff- und Energiebilanz bestimmen, wenn die Reaktionsgeschwindigkeiten für die entsprechenden Reaktionen bekannt sind. Unter den Voraussetzungen

- Homogenität,
- exotherme Reaktion,
- ideale Durchmischung sowie
- Vernachlässigung anderer Wärmequellen (z.B. durch einen Rührer) gegenüber der Wärmeproduktion durch Reaktion und
- kontinuierlich betriebener Rührkessel

ergibt sich die Stoffbilanz aus der allgemeinen Bilanz für den Stoffumsatz /Hugo94/

$$\frac{\partial c_i}{\partial t} = -div\vec{j}_i + n_i \cdot r(c,T) \qquad (5\text{-}1)$$

unter der Annahme eines Reaktanden zu:

$$V\frac{dc}{dt} = -q\cdot(c-c_0) - V\cdot r(c,T) \qquad (5\text{-}2)$$

Und die Wärmebilanz ergibt sich aus der differentiellen Bilanz /Hugo94/

$$\frac{\partial}{\partial t}\cdot\left(r\cdot c_p\cdot T\right) = -div\vec{q} + \left(-\Delta H\right)\cdot r(c,T) \qquad (5\text{-}3)$$

zu:

$$V_R\, r\, c_p\frac{dT}{dt} = V_R\cdot(-\Delta H)\cdot r(c,T) - r\, c_p\dot{V}(T-T_0) - k_w F_w(T-T_K) \qquad (5\text{-}4)$$

Für andere Reaktoren ergeben sich die Gleichungen entsprechend. Für einen diskontinuierlich betriebenen Rührkessel beispielsweise müssen nur die Einflüsse durch den Zu- bzw. Ablauf vernachlässigt werden. *Hugo* beschreibt in /Hugo80/ anschaulich die Herleitung der Stoff- und Energiebilanzen für einen Batch-Prozeß.

Die Reaktionsgeschwindigkeit *r* wird über einen konzentrationsabhängigen Faktor, gegebenenfalls unter Berücksichtigung von Katalysatoren und dem Arrhenius-Ansatz als Maß für die exponentielle Abhängigkeit der Reaktionsgeschwindigkeit von der Temperatur beschrieben:

$$r(c,T,Katalysator) = f(c)\cdot k(T), \qquad mit k(T) = k_\infty e^{-\frac{E}{RT}} \qquad (5\text{-}5)$$

Dabei ist *E* die Aktivierungsenergie der Reaktion. Der Stoßfaktor k_∞ kann näherungsweise als von der Temperatur unabhängig angesehen werden. Diese Vereinfachung gilt nicht beliebig; bei Gasphasenreaktionen z.B. spielen noch Einflüsse durch Chemiesorption eine Rolle.

Die durch Reaktion entstehende Wärme heizt zum einen den in den Reaktor strömenden Zulauf auf (kontinuierliche Betriebsweise), zum anderen wird die Wärme

über die Kühlung abgeführt. Stehen diese beiden Größen mit der Wärmeproduktion im Gleichgewicht, lautet Gleichung (5-4)

$$0 = V \cdot (-\Delta H) \cdot r(c,T) - rc_p q(T - T_0) - k_w F(T - T_K), \qquad (5\text{-}6)$$

so liegt der stationäre Betriebszustand vor. Der Reaktor arbeitet stabil, wenn gilt:

$$\frac{d\dot{Q}_{ab}}{dT} > \frac{d\dot{Q}_{chem}}{dT} \qquad (5\text{-}7)$$

Da der abgeführte Wärmestrom linear von der Temperatur abhängt, erscheint dieser in Bild 5-1 als Gerade, der entstehende Wärmestrom hingegen als S-Kurve. Dies liegt daran, daß die Wärmeproduktion sich zunächst exponentiell aufgrund der Abhängigkeit der Reaktionsgeschwindigkeit von der Temperatur gemäß Gleichung (5-3) entwickelt und sich dann asymptotisch wegen des Reaktandenverbrauchs einem durch den vollständigen Umsatz vorgegebenem Grenzwert annähert. Dies gilt in erster Linie für den Batchreaktor. Werden dem Reaktor weiterhin Edukte zugeführt, so verschiebt sich der Grenzwert der Wärmeproduktion entsprechend der gestrichelten Linie auf ein höheres Temperaturniveau.

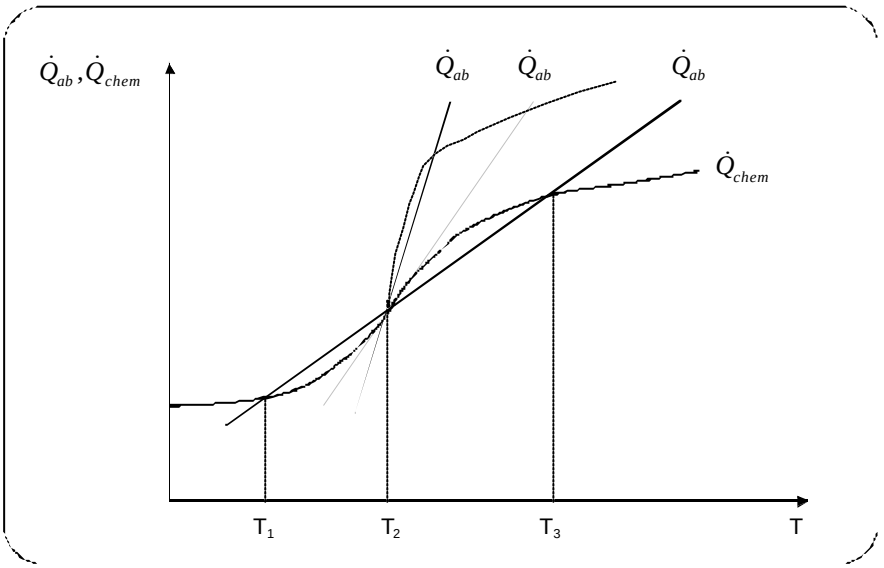


Bild 5-1: Stabilitätsdiagramm für eine exotherme Reaktion

Die Steigung der Wärmeabfuhrgeraden hängt vom Verhältnis der Wärmeübertragungsfläche zum Reaktorvolumen gemäß Gleichung (5-8) ab und sinkt damit mit zunehmender Größe des Reaktors. Dem kann durch zusätzliche innenliegende Kühlschlangen entgegengewirkt werden.

$$\frac{d\dot{Q}_{ab}}{dT} \cong \frac{F}{V_R} \qquad (5\text{-}8)$$

Je nach Steigung der Wärmeabfuhrgeraden ergeben sich zwischen dieser und der Wärmeerzeugungskurve ein oder drei Schnittpunkte, die die stationären Betriebspunkte der Reaktion beschreiben. In diesen Punkten ist die erzeugte gleich der abgeführten Wärme. Im Falle der in Bild 5-1 dick markierten, flachen Geraden mit drei Schnittpunkten erfüllt der mittlere Schnittpunkt zwar die Voraussetzungen für Stationärität nach Gleichung (5-6), jedoch wird das Stabilitätskriterium nach Gleichung (5-7) nicht erfüllt, da die Steigung der Wärmeerzeugungskurve in diesem Punkt größer ist als die der Wärmeabfuhrgeraden. Eine kleine Erhöhung der Reaktionswärmeerzeugung, z.B. durch einen Konzentrationssprung, könnte somit zu einem Durchgehen der Reaktion führen /Heng81/. Hier sind der obere und untere Schnittpunkt stabile Betriebspunkte, an denen der Reaktor sicher betrieben werden kann. Die beste Ausbeute läßt sich aber oft nur bei mittlerem Schnittpunkt erreichen, so daß Reaktoren oft hier gefahren werden. Eine Fahrweise bei mittlerem Schnittpunkt kann durch regelungstechnische Maßnahmen stabilisiert werden. Ein Beispiel anhand eines P-Reglers wird in /Heng81/ erläutert.

Um eine Reaktion sicher beherrschen zu können, muß die Temperaturentwicklung über der Zeit sowie die höchstens zu erwartende Temperatur bei vollständigem Umsatz bekannt sein. Zur Feststellung der maximal möglichen Temperatur wird gewöhnlich die adiabate Temperaturerhöhung ΔT_{ad} herangezogen. Sie beschreibt für einen kontinuierlich betriebenen Rührkesselreaktor die bei gegebener Konzentration und vollständigem Umsatz entstehende Reaktionswärme im Reaktorsystem ohne Stoff- und Wärmeaustausch mit der Umgebung.

$$\Delta T_{ad} = \frac{(-\Delta H_R \cdot c_{A_0})}{(-n \cdot r \cdot c_p)} \qquad (5\text{-}9)$$

In /TAA-GS-05/ wird davon ausgegangen, daß eine Reaktion, bei der ΔT_{ad} im Normalbetrieb unter 50 K und bei der nicht von thermischen Instabilitäten der Einsatz-, Zwischen- sowie Endstoffen auszugehen ist beziehungsweise deren Einfluß auf die Wärmeentwicklung mit ΔT_{ad} zusammen nicht mehr als 50 K ergeben, sicher beherrscht werden kann. Nachteil der Methode ist, daß zur Bestimmung von ΔT_{ad} die

Bildungsenthalpie ΔH_{fi} der einzelnen Reaktanden bekannt sein sowie eine Reaktion zur Bestimmung der Reaktionsenthalpie vorgegeben werden muß. Unter der molaren Bildungsenthalpie ΔH_{fi} einer Verbindung versteht man die Enthalpie der Reaktion, bei der ein Mol der Verbindung aus den Elementen im Normzustand gebildet wird. Für viele Verbindungen sind die Bildungsenthalpien tabelliert. Sie können aber auch aus Inkrementen der einzelnen Atomgruppen abgeschätzt werden /Zach81/. Sind die Bildungsenthalpien der Reaktanden bekannt, so läßt sich darüber die Reaktionsenthalpie als Maß für den Wärmeumsatz berechnen:

$$\Delta H_R = \sum_{i=1}^{N} n_i \cdot \Delta H_{fi} \qquad (5\text{-}10)$$

Verlaufen zusätzlich noch Nebenreaktionen bzw. können diese nicht sicher ausgeschlossen werden, können diese genauso schwer berücksichtigt werden wie beispielsweise der Wärmeeintrag durch einen Rührer. Besser ist hier, die gesamte Reaktionswärme mit einem Reaktionskalorimeter zu bestimmen. Können Zwischen- und Nebenreaktionen ausgeschlossen werden bzw. ist deren Einfluß auf die Reaktionswärme bekannt, kann die oben genannte Berechnungsmethode angewandt werden. Darüber hinaus ist genauso die maximale Gasentwicklung als Maß für den Druckaufbau sowohl für den Normalbetrieb als auch für den Betrieb unter erschwerten Umständen bei der Auslegung der Anlage zu beachten, soweit das Produkt gasförmig ist bzw. mit Gasentwicklung zu rechnen ist.

Liegt ΔT_{ad} einschließlich möglicher stofflich-thermischer Instabilitäten über 50 K, so ist nach /TAA-GS-05/ und /Merk95/ der zeitliche Verlauf der Wärmeproduktionsgeschwindigkeit zur Abschätzung des Prozesses heranzuziehen.

Oftmals sind Temperaturen oberhalb des Wendepunktes der Wärmeerzeugungskurve aus Bild 5-1 bereits zu hoch und müssen vermieden werden, so daß im Rahmen der Sicherheitsuntersuchungen für solche Reaktionen nur der erste Schnittpunkt betrachtet wird. Erhöht sich die Temperatur des Kühlsystems infolge einer Reduzierung des Kühlmittelzuflusses oder erhöhter Reaktion, kann sich die Wärmeabfuhrgerade bis in einen Tangentenpunkt verschieben, wie Bild 5-2 zeigt. Die Reaktion verläuft in diesem Punkt kritisch. Eine kleine Erhöhung der Reaktionstemperatur würde so zum

Runaway der Reaktion führen. Nur der Schnittpunkt bei T_1 erfüllt das Stabilitätskriterium von Gleichung (5-7), so daß die Reaktion hier sicher beherrscht werden kann.

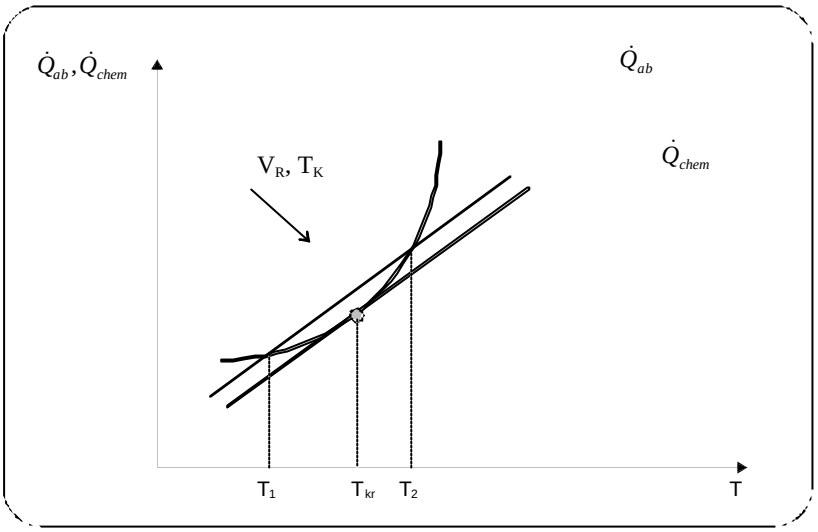


Bild 5-2: Wärmebilanz für einen Rührkessel

Die Folge eines Runaways ist meist neben der rasant steigenden Temperatur infolge erhöhter Reaktivität ein aufgrund

- der Zunahme des Dampfdruckes,
- der Entwicklung nicht zu kondensierender Zersetzungsgase sowie
- der Wärmeausdehnung der flüssigen Phase

resultierender Druckanstieg. In Verbindung mit der hohen Temperatur können hier schnell die Auslegungsgrenzen der Anlage überschritten werden.

5.1.1 Fouling

Zum Runaway einer Reaktion kann es ebenso durch Fouling auf den wärmeübertragenden Oberflächen kommen /Guid95/. Dies geschieht schleichend über einen langen Zeitraum. Am Anfang wird es in der Regel automatisch vom Prozeßleitsystem durch Erhöhung der Kühlflüssigkeitsmenge ausgeglichen. Dem sind aber physikalische Grenzen gesetzt, so daß es auch in diesem Fall zu einer Verringerung der Wärmeabfuhr kommen kann und so das Kühlsystem die Reaktionswärme nicht mehr ausreichend abführen kann. Grafisch zeigt sich dieses durch eine Minderung in der Steigung der Wärmeabfuhrgeraden.

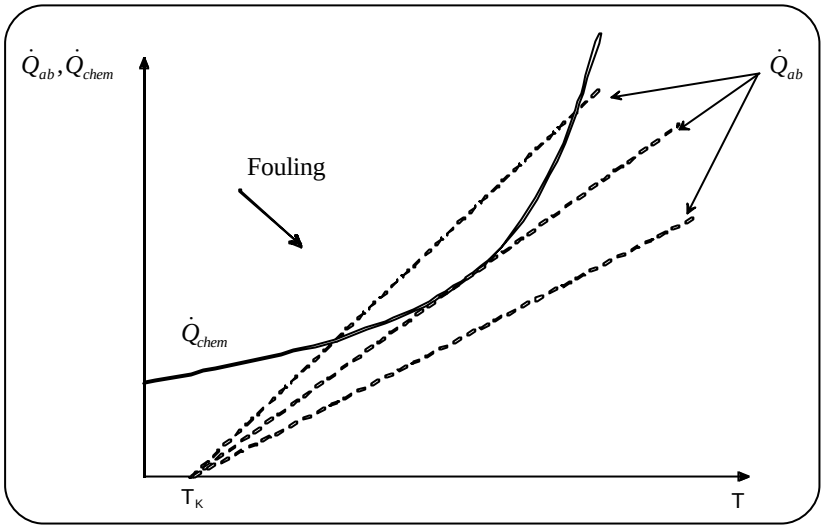


Bild 5-3: Fouling

Gegen Fouling hilft eine regelmäßige Wartung der Kühlaggregate und Kontrolle der Kühlleistung im Verhältnis zum Kühlmittelstrom.

5.1.2 Sekundärreaktion

Wird nicht genügend Wärme abgeführt, kann neben der Gefahr des Runaways der Primärreaktion zusätzlich noch die Gefahr der Initiierung einer exothermen Sekundärreaktion bestehen. Einen möglichen Ereignisverlauf, der zu einer Wärmeexplosion in Folge einer durchgehenden Reaktion führt, veranschaulicht Bild 5-4.

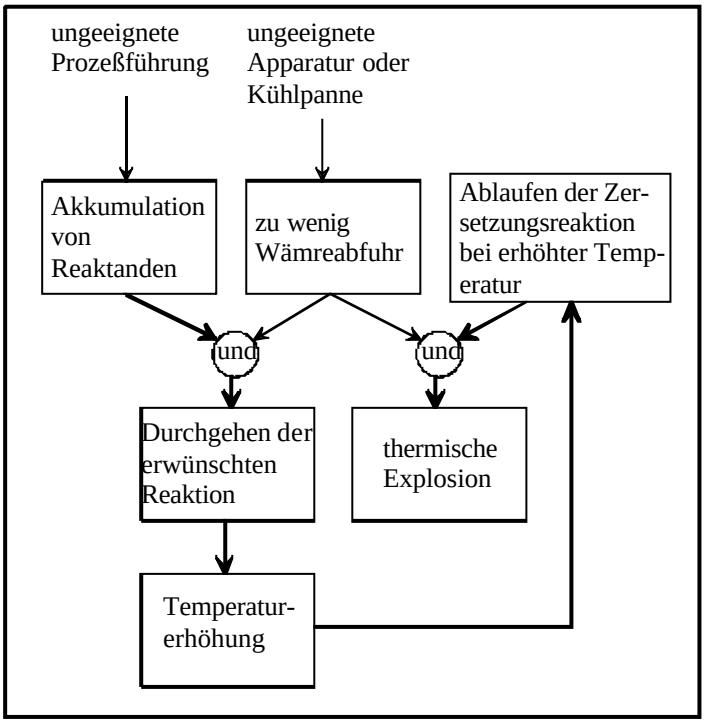


Bild 5-4: Möglicher Ereignisverlauf einer durchgehenden Reaktion

Bild 5-5 zeigt ein für den Temperaturverlauf mögliches Szenario einer durchgehenden Primärreaktion mit anschließendem Starten einer Sekundärreaktion infolge eines Kühlmittelausfalls nach /Geik90-96/. Hier wird deutlich, daß die bloße Kenntnis der maximalen Temperaturerhöhung der gewünschten Primärreaktion nicht ausreicht, sondern vielmehr auch mögliche Nebenreaktionen bezüglich ihrer Startbedingungen untersucht werden müssen.

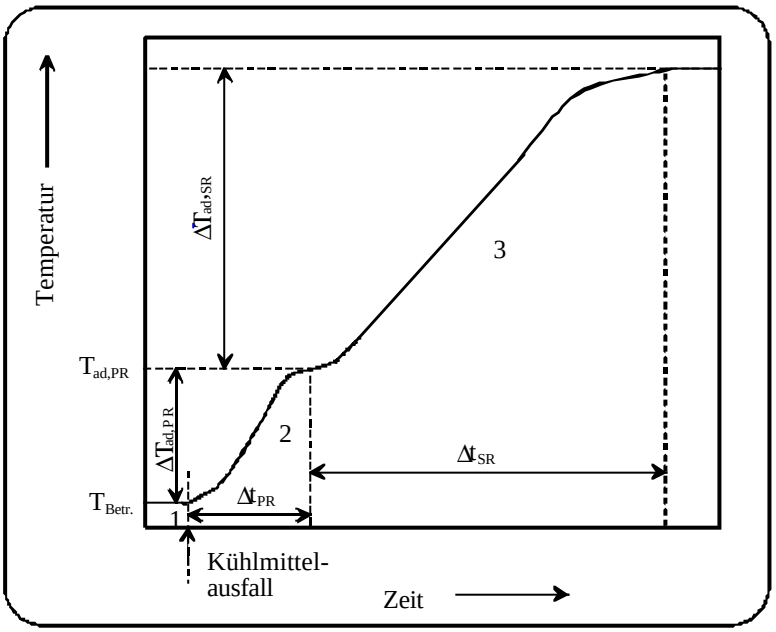


Bild 5-5: Möglicher Temperaturverlauf beim Durchgehen einer Reaktion /Geik90-96/

Aus sicherheitstechnischer Sicht sollte die Differenz zwischen der Starttemperatur der Sekundärreaktion und der Summe aus Betriebstemperatur $T_{Betr.}$ und adiabater Temperaturerhöhung $?T_{ad,PR}$ der Primärreaktion sehr groß sein. Ist dies nicht der Fall, so muß durch entsprechende sicherheitstechnische Instrumentierung das Gefahrenpotential der Reaktion beherrscht werden können. Hierzu sind Angaben über die Reaktionskinetik hilfreich. Da dies aufgrund der Komplexität der möglichen unterschiedlichen Reaktionen bei Mehrstoffgemischen nahezu unmöglich ist, müssen zumindest grundlegende Eigenschaften und Näherungsdaten ermittelt werden. Dabei sollten die das Durchgehen einer Reaktion charakterisierenden Größen durch Beantwortung folgender Fragen abgeschätzt werden /Geik96/, /Stoe93/, /Joch00/:

- Wie groß ist die Wärmeproduktion des laufenden Verfahrens zu jedem Zeitpunkt, der die Apparate gewachsen sein müssen?

- Kann die Prozeßtemperatur durch das gewählte Kühlsystem beherrscht werden?
- Welche Temperatur kann erreicht werden, wenn beim Versagen der Kühlung adiabatische Bedingungen angenommen werden? In welcher Zeit wird die maximale Temperatur erreicht?
- Welches ist der kritischste Zeitpunkt für ein Versagen der Kühlung?
- Welche Neben-, Folge- oder Zersetzungsreaktionen laufen in welchen Zeiträumen ab – bei der normalen Betriebstemperatur bzw. bei adiabatischer Höchsttemperatur beim Durchgehen der Hauptreaktion?
- Welches ist die Größenordnung eines adiabatischen Temperaturanstiegs, der durch das Durchgehen sekundärer Reaktionen verursacht wird, und was sind die Konsequenzen?
- Welchen Einfluß können Phasenverhältnisse, Durchmischung, Katalysatoren, Spurenkomponenten und andere Faktoren ausüben?

In /Guid95/ und /Guid99/ werden die die Sicherheit einer Reaktion betreffenden notwendigen Fragen zusammen mit den dafür benötigten Daten/Parametern und den Methoden, diese zu ermitteln, übersichtlich aufgelistet:

Grundlegende Fragen der Sicherheit für chemische Reaktionen		
Frage	**Benötigte Daten**	**Ausgewählte Methoden zur Ermittlung der Daten**
1. Wie hoch ist die mögliche Temperatur bei der gewünschten Reaktion? Wie schnell ist der maximale Temperaturanstieg? Welche Konsequenzen folgen daraus? Wie hoch ist der maximal zu erwartende Druck?	• Enthalpie der erwünschten Reaktion • Spezifische Wärmekapazität • Dampfdruck des Lösungsmittels als Funktion der Temperatur • Gasentwicklung	• Datentabellen • Thermodynamische Daten • Rechnungen; Einschätzungen • DTA/DSC • Dewar flask Experimente • Reaktionskalorimetrische Untersuchungen • Thermometrie/Manometrie • ARC/RSST/VSP
2. Wie hoch ist der maximale Temperaturanstieg bei unerwünschten Reaktionen, z.B. infolge Kontamination oder Verunreinigungen? Welche Konsequenzen sind zu erwarten? Wie hoch ist der maximal zu erwartende Druck?	• Daten von Nr. 1 • Enthalpie der unerwünschten Reaktion • Reaktionsrate der unerwünschten Reaktion als Funktion der Temperatur	• Siehe Nr. 1
3. Ist Akkumulation möglich? Welche Konsequenzen sind zu erwarten?	• Konzentrationsmessungen • Kinetische Daten • Daten von Nr. 1 und 2	• Reaktionskalometrie • Potentielle Energie durch DSC/DTA • RSST/VSP
4. Wie hoch ist der Temperaturanstieg infolge der physi-	• Wärmeübertragungsdaten • Wärmeeintrag durch Rührer	• Auslegungsdaten

Grundlegende Fragen der Sicherheit für chemische Reaktionen		
Frage	**Benötigte Daten**	**Ausgewählte Methoden zur Ermittlung der Daten**
kalischen Gegebenheiten des Prozesses?	• Wärmeeintrag durch Pumpen • Wärmeeintrag durch Strahlung	

Bild 5-6: Sicherheitsaspekte chemischer Reaktionen

Eine ausführliche Beschreibung der Methoden findet sich unter anderem in /TAA-GS-05/, /Stoe95/, /Stoe93/, /Ratg98/, /Guid95/. Aufgrund denkbarer Gefährdungen sollten die Daten, wenn möglich, im Labormaßstab oder im Technikum und nicht in der Produktionsanlage ermittelt werden. Ingenieurmäßige Einschätzungen können bei weniger gefährlichen Reaktionen und hohem Erfahrungsschatz des Prozeß-Ingenieurs hier auch ausreichend sein. Es gilt jedoch zu beachten, daß im Labormaßstab ermittelte Wärmeabfuhrleistungen nicht linear auf die Produktionsanlage übertragen werden können, da sich die Wärmebilanz bei Maßstabsvergrößerungen oft nicht unerheblich zugunsten der Wämeproduktion verschiebt /Gyga88/, /Guid95/, /Ratg98/.

Die Wärmeübertragungssysteme spielen bei der Sicherheit einer Chemieanlage eine entscheidende Rolle. Meist gehen Reaktionen durch, weil Kühlsysteme versagen oder falsch ausgelegt wurden /Hugo94/. Generell sollte ein stabiler Arbeitspunkt bei niedrigen Temperaturen angestrebt werden, um die Gefahr des Durchgehens einer Reaktion von vornherein zu minimieren. Weiterhin muß die Wärmeübertragungsfläche ausreichend groß gewählt werden und die Temperaturdifferenz zwischen zu kühlendem und kühlendem Medium sollte möglichst klein sein, so daß ausreichend Reserven vorhanden sind, falls im Falle z.B. zu hoher Dosierung oder plötzlichem Akkumulationsabbaus die Reaktionsstemperatur zwischenzeitlich ansteigt. Dies hat darüber hinaus den Vorteil, daß ein Reglerausfall eher kompensiert werden kann als bei der Wahl einer kleineren Übertragungsfläche.

Um die Reaktion möglichst sicher beherrschen zu können, muß die Reaktionsgeschwindigkeit jederzeit beeinflußbar sein, ein vorzugsweise selektiv wirkender Katalysator sowie ein zuverlässiges Wärmeübertragungssystem gewählt werden. Bei gefährlichen Stoffgemischen sind Flüssigkeitssysteme mit Zwangsumlauf anderen Systemen wie z.B. elektrischen oder dampfbetriebenen vorzuziehen /Geik96/. Ebenso

sollte ein Puffer auf der Wärmeüberträgerseite und ein minimales Wärmepotential auf der Reaktionsseite vorhanden sein /Geik90-96/.

5.2 Sichere Betriebsführung

Oberstes Ziel der sicheren Auslegung von Chemieanlagen ist es, Prozeßgefährdungen zu vermeiden statt diese durch zusätzliche Maßnahmen beherrschen zu wollen /Lees96_2/. Voraussetzung für eine sichere Betriebsführung ist die optimale Auslegung auf der betrieblichen Seite, so daß die Häufigkeit des Ansprechens der Schutzfunktionen minimiert wird (vgl. Bild 1-1). Hierzu dienen in der Regel entsprechende Schalt- und Verriegelungsfunktionen, die in Abhängigkeit von Prozeßparametern wie Druck und Temperatur prozeßabhängig bestimmt werden müssen. Daher ist entscheidend, daß der zulässige Betriebsbereich (vgl. Bild 6-5) genau festgelegt wird und durch die richtige Auswahl und Anordnung der Ausrüstungen /Mäde90/

- Druckmessung und –anzeige
- Temperaturmessung und –anzeige
- Überfüllsicherung
- Leckanzeigegeräte
- Füllstandssteuerung
- etc.

auch eingehalten wird. Dazu zählt desgleichen, daß das Kontroll-System fehlertolerant gestaltet ist, um nicht unnötige oder falsche Funktionen auszulösen. Ändern sich beispielsweise Prozeßvariable auf den Anzeigetafeln in der Prozeßleitwarte schneller, als dies physikalisch möglich ist, so sollte dies ebenso angezeigt werden wie Meßwerte, die sich außerhalb einer festgelegten Wertespanne befinden. Zittersignale können gleichermaßen ein Signal für einen Fehler im Kontroll-System sein und sollten dementsprechend untersucht werden /Engl92/.

Die genaue Einhaltung von Rezepturen sowie der stofflichen Reihenfolge bei chemischen Prozessen und eine exakte Dosierung sind wesentliche Bestandteile der sicheren Betriebsführung.

Werden Rezepturen nicht streng eingehalten, können sich Veränderungen im Wärmestromverlauf ergeben (die Erhöhung des Methacrylsäureanteils bei einer Copolymerisation von Methacrylsäure mit Styrol um fünf Prozent führte zu einer Verdopplung der Wärmestromdichte /Mori95/). Die Auslegungsgrenzen einer Anlage beziehungsweise ihres Wärmeübertragungssystems können so schnell erreicht werden.

Werden in einem semi-batch Verfahren zuerst die Edukte vorgelegt und dann der Katalysator zugeführt, kann es bei entsprechend exothermen Reaktionen zu einer spontanen Abreaktion des gesamten Behälterinhalts kommen. Die Akkumulation der Reaktanden muß unbedingt verhindert werden. Das heißt nicht nur, daß eine Dosierung nur in einem bestimmten Temperaturfenster durchgeführt werden darf, sondern auch, daß der Katalysator vor der reaktiven Komponente in den Behälter eingebracht werden muß.

Die Dosierung spielt im Zusammenhang mit möglichen Pannen wie etwa dem Kühlungsausfall eine wichtige Rolle. In diesem Fall muß die Zufuhr so zeitig unterbrochen werden, daß die Auslegungsparameter bezüglich Druck und Temperatur infolge der fehlenden Wärmeabfuhr nicht überschritten werden. Durch so genannte Verriegelungen kann dies gewährleistet werden, das heißt, die Dosierung kann beispielsweise nur

- bei laufendem Rührer,
- innerhalb eines festgelegten Temperaturbereichs,
- bei einem Mindestfüllstand etc.

oder Kombinationen der Maßnahmen erfolgen. Andernfalls kann die Dosierung nicht gestartet werden.

Sollte es dennoch möglich sein, die Grenzen des zulässigen Betriebsbereichs zu überschreiten, so sind bei der Auslegung einer verfahrenstechnischen Anlage Maßnahmen vorzusehen, die die Anlage wieder in den bestimmungsgemäßen Betrieb überführen (z.B. durch entsprechende regelungstechnische Schaltungen) oder durch deren Ansprechen ein weiteres Ansteigen der Prozeßparameter der Anlage dauerhaft verhindert wird (z.B. Berstsicherung, Reaktionsstopper). Im wesentlichen greifen

hier die aktiven Maßnahmen, die entweder automatisch oder manuell aktiviert werden. Eine genauere Beschreibung erfolgt in Abschnitt 5.3.

Neben der technischen Ausrüstung spielt die „Mensch-Maschine-Beziehung" einschließlich der Meßwartenkonzeption und des Verhaltenstrainings im „Nichtbestimmungsgemäßen Betrieb" eine wichtige Rolle /Geik90-96/, ein Verfahren sicher innerhalb der Grenzen zu halten. Der Aufgabenbereich des Anlagenpersonals muß genau festgelegt sein; er darf das Personal weder über- noch unterfordern. Die zur Verfügung stehenden Informationen über einen Prozeß sind auf das Wesentliche zu beschränken, um einen „Informationsüberfluß" zu vermeiden. Außerdem verleitet eine zu wenig fordernde Arbeit infolge einer zu stark automatisierten Anlage zur Unaufmerksamkeit.

5.3 Sichere Verfahren

Die Sicherheit einer Anlage beziehungsweise der in dieser durchgeführten Prozesse stützt sich zum Schutz vor gefährlichen Ereignissen auf verschiedene Sicherheitsebenen. Die Ebenen sind im einzelnen:

- grundlegende Prozeßauslegung,
- Kontrollsysteme,
- Alarme und Verriegelungen,
- Sicherheitsabschaltungen,
- auswirkungsverringernde Maßnahmen und
- Gefahrenabwehrpläne.

Graphisch wird dies im folgenden Bild dargestellt.

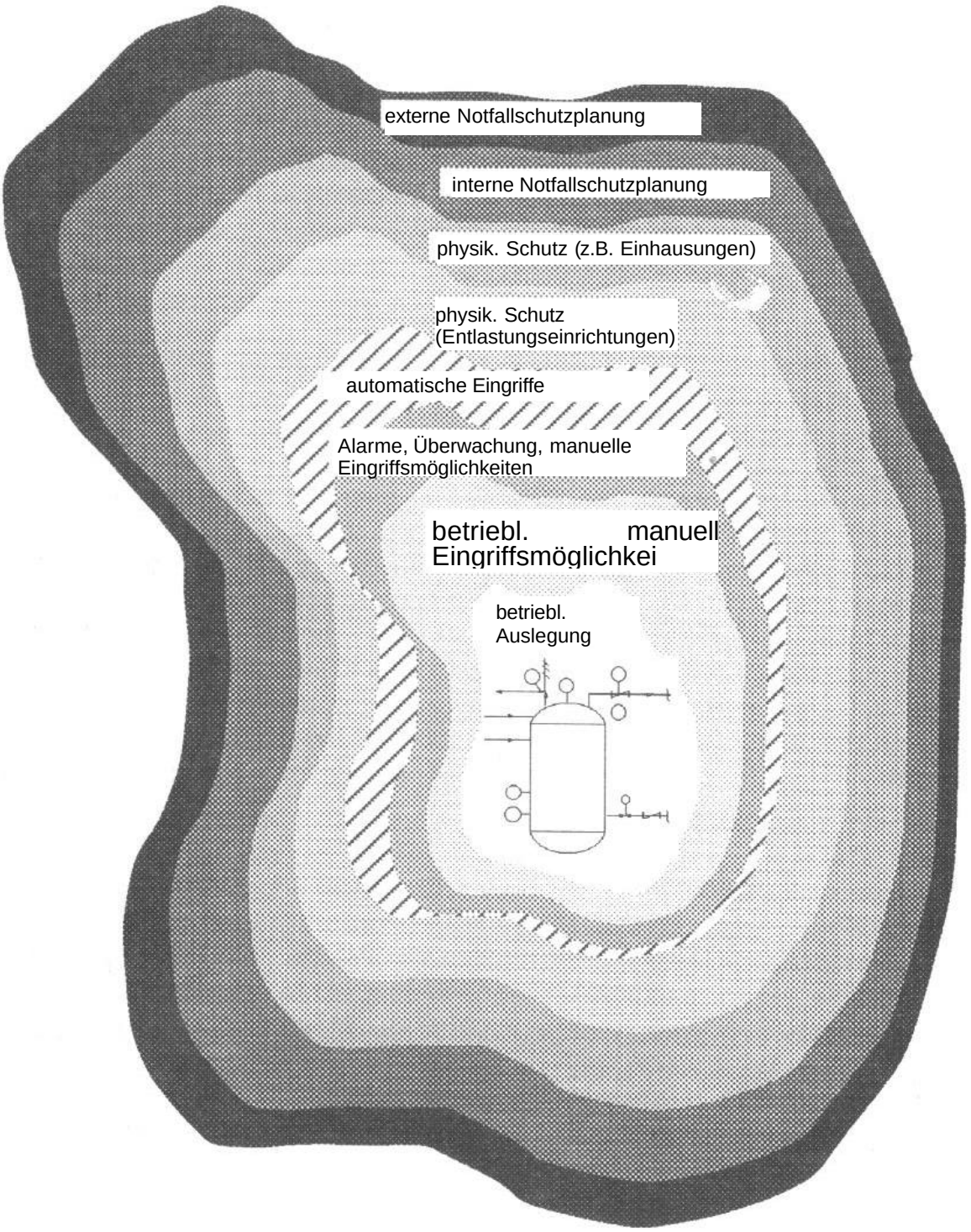


Bild 5-7: Sicherheitsebenen einer Chemieanlage /Guid93b/

Das Risiko einer Anlage setzt sich, wie in Kapitel 1 beschrieben, aus der erwarteten Häufigkeit des Eintritts eines unerwünschten Ereignisses und dessen zu erwartenden Auswirkungen zusammen. Bezogen auf die Reduzierung der Auswirkungen haben sich dafür Maßnahmen durchgesetzt, die sich den folgenden Kategorien zuordnen lassen /Guid93a/:

- Inhärente Maßnahmen,
- passive Maßnahmen,
- aktive Maßnahmen,
- organisatorische Maßnahmen und
- auswirkungsverringernde Maßnahmen.

Die Kategorien und ihr Einfluß auf die Sicherheit einer Anlage werden in den nächsten Abschnitten näher erläutert.

5.3.1 Passive Maßnahmen

Der Begriff der inhärenten Sicherheit (= „Eigensicherheit“) kommt aus der Kerntechnik und findet immer häufiger Anwendung in der chemischen Industrie, insbesondere nach den Vorfällen in Seveso /Orsi77/, Flixborough /Park75/ und Bhopal /Badh84/.

Kletz /Klet98/ unterscheidet zwischen inhärenten und passiven Maßnahmen. Im Vergleich zu den passiven Maßnahmen verhindern inhärente Maßnahmen die Entstehung der Gefährdung /Boll96/. Am Beispiel einer durchgehenden Reaktion ergeben sich für die verschiedenen Maßnahmentypen im einzelnen folgende Möglichkeiten:

- ***Inhärent*:** Nutzung eines anderen Verfahrens oder anderer Einsatzstoffe, so daß ein Durchgehen der Reaktion ausgeschlossen werden kann (z.B. Selbststabilisierung infolge Blasenbildung).
- ***Passiv*:** Auslegung des Reaktors derart, daß er der maximal zu erwartenden Temperatur oder dem maximal zu erwartenden Druck standhält.
- ***Aktiv*:** Automatische Aktivierung einer Notkühlung, Verriegelung der Zuführungsleitung über Druck und Temperatur, Notablaß über ein Sicherheitsventil oder eine Berstscheibe.
- ***Organisatorisch*:** Anweisungen an das Bedienpersonal, festgelegte Handlungen durchzuführen, zum Beispiel manuelle Abschaltung der Reaktandenzuführung, manuelle Auslösung einer Notkühlung etc..

Da inhärente und passive Maßnahmen oft nur schwer unterschieden werden können /Guid98/, werden sie im weiteren Verlauf dieser Arbeit unter dem Begriff *passive Maßnahmen* zusammengefaßt.

Trevor Kletz /Klet78/ hat erstmals systematisch die Grundzüge zur Erreichung eigensicherer Chemieanlagen aufgezeigt. Die vier Grundprinzipien sind dabei /Klet98/:

1. Intensivierung von Prozessen

   Während der Entwicklung eines chemischen Prozesses muß auch die Entscheidung über den geeignetsten Reaktortyp getroffen werden. Dabei hat die Wahl neben verfahrenstechnischen Gesichtspunkten auch einen Einfluß auf die Sicherheit des Prozesses. So werden in einem Batch-Prozeß die Reaktanden vorgelegt und somit ist hier im Gegensatz zum kontinuierlichen Prozeß das Volumen der Stoffe meist erheblich höher, wodurch das Gefahrenpotential ansteigt. Die Auswahl des Reaktortyps ist nicht beliebig, sondern richtet sich nicht zuletzt nach dem Prozeß bzw. dem gewünschten Produkt. Folgende Tabelle zeigt einen Überblick über die Vor- und Nachteile der unterschiedlichen Reaktoren hinsichtlich ihrer Gefahrenpotentiale /Guid95/.

Vergleich verschiedener Reaktortypen unter sicherheitstechnischen Gesichtspunkten			
PFTR[4]	CSTR[5]	BATCH	SEMI-BATCH
Vorteile			
• wenig Ausrüstung • stationäre Bedingungen	• stationäre Bedingungen • durch das Rührwerk wird ein Sicherheitsinstrument bereitgestellt (Notverdünnung, Reaktionsstopper) • zur Verlangsamung der Reaktion können die Stoffströme verdünnt werden	• durch das Rührwerk wird ein Sicherheitsinstrument bereitgestellt (Notverdünnung, Reaktionsstopper)	• kontrollierbare Zugaberate • durch das Rührwerk wird ein Sicherheitsinstrument bereitgestellt (Notverdünnung, Reaktionsstopper) • stark exotherme Reaktionen sind kontrollierbar
Nachteile			
• Potential für hot spots • schwierig auszulegen	• viel Ausrüstung • Schwierigkeit, große Massen zu kühlen • schwierige An- und Abfahrbedingungen • Probleme mit Ablagerungen • geringe Durchsatzrate	• stark exotherme Reaktionen sind schwierig zu kontrollieren • viel Ausrüstung • alle Reaktionsstoffe sind gleichzeitig an der Reaktion beteiligt	• Starttemperatur ist kritisch (bei zu geringer Starttemperatur Gefahr der Akkumulation) • Probleme mit Ablagerungen

Tabelle 5-1: Vor- und Nachteile verschiedener Reaktortypen

[4] Ideales Ströhmungsrohr, Vereinfachungen bzw. Annahmen siehe /Hugo94/

[5] Idealer Durchflußrührkessel, Vereinfachungen bzw. Annahmen siehe /Hugo94/

Im Hinblick auf die Intensivierung von Prozessen sollte, wenn möglich, immer ein kontinuierlicher Prozeß gewählt werden, da hier das Inventar reaktiver Stoffe im Vergleich zum Batch-Prozeß geringer sind. Ist dies nicht möglich, besteht durch Minimierung der Masse an Einsatzstoffen die Möglichkeit, das Gefahrenpotential zu reduzieren /Hend00/. Hierbei sollte nach Möglichkeit bei der Verfahrensplanung auf unnötige Puffergefäße durch sinnvolle betriebliche Verschaltung der Teilanlagen und geeignete Ablaufsteuerung verzichtet werden.

2. Ersatzstoffe oder Ersatzsysteme
   Lassen sich Substanzen mit gefährlichen Eigenschaften nicht durch Wahl eines anderen Verfahrens vermeiden, so sollte versucht werden, diese durch weniger gefährliche zu ersetzen. Dies bezieht sich sowohl auf die Ausgangs- und Endprodukte sowie auf mögliche Zwischenprodukte.
3. Verminderung der Reaktionsfähigkeit
   Die Moderation gefährlicher Stoffe führt gleichermaßen zu einer Erniedrigung ihrer Reaktionsfähigkeit. Moderation bedeutet in diesem Zusammenhang, daß Materialien unter weniger gefährlichen Bedingungen eingesetzt werden. Hier bieten sich verschiedene Möglichkeiten an. Zum einen kann die Form des Stoffes die Sicherheit erhöhen, indem statt staubförmiger Einsatzstoffe pastöse Gemische verwendet werden /Merk96/ und somit die aktive Oberfläche reduziert wird, zum anderen können die Reaktionsparameter Druck, Temperatur sowie Konzentration durch Wahl eines geeigneten Katalysators, falls ein Einsatz möglich ist, erniedrigt werden.
4. Begrenzung von Auswirkungen
   Technisch erreichbar ist dieses Ziel durch die Einhausung von besonders gefährdeten Anlagenteilen oder Teilen, in denen toxische oder brennbare Stoffe behandelt beziehungsweise erzeugt werden. Somit wird im Falle einer Freisetzung das kontaminierte Gebiet eingegrenzt. Abzugsanlagen oder so genannte Wasserschleier verhindern ebenso die großflächige Ausbreitung freigesetzter Gefahrstoffe.

Inhärente und passive Maßnahmen zur Erhöhung der Sicherheit können Teil verschiedener Sicherheitsebenen sein. Zum Beispiel optimal dimensionierte Eindämmungen können die Verdampfung freigesetzter Stoffe auf der Ebene der auswirkungsverringernden Maßnahmen minimieren. Am besten greifen inhärente Maß-

nahmen aber in der ersten Ebene, der Prozeßauslegung. Die beste Sicherheit ist die, ein Verfahren so zu gestalten, daß gefährliche Zustände prozeßbedingt gar nicht entstehen können.

Der Vorteil der Erhöhung der passiven Sicherheit einer Anlage liegt darin, daß ihr Wirken unabhängig von der Wirksamkeit von Regelsystemen und Schutzvorkehrungen ist.

Den bereits angesprochenen Möglichkeiten zur Erhöhung der passiven Sicherheit durch die druckfeste Auslegung des Reaktionsbehälters einschließlich der zugehörigen Anlagenteile sind jedoch Grenzen gesetzt. Die druckfeste Bauweise für eine Nitrierreaktion beispielsweise würde aufgrund des konstruktiven und finanziellen Aufwandes die Anlage betriebswirtschaftlich uninteressant werden lassen. Darüber hinaus verschlechtert sich mit zunehmender Wanddicke der Wärmedurchgang. Gerade im Falle stark exothermer Reaktionen sollte dieser besonders gut sein. Weiterhin muß ausgeschlossen werden können, daß es im Falle einer durchgehenden Reaktion nicht zur Gasbildung und somit zum weiteren Druckaufbau im Verlauf einer anschließenden Folgereaktion kommt. Somit eignet sich die druckfeste Bauweise in erster Linie für schwach exotherme Reaktionen ohne Gasfreisetzung. Im Falle der Nitrierreaktion ist dies keine geeignete Maßnahme; hier ist eine Reduzierung der Dosiergeschwindigkeit durch konstruktive Maßnahmen (z.B. Lochblende in der Dosierleitung, Durchmesser der Rohrleitung, Pumpenleistung) sinnvoller.

Die sich aus den Verfahrensbedingungen hinsichtlich des bestimmungsgemäßen Betriebs ergebenden Anforderungen (Druck, Temperatur etc.) an die Apparate müssen jedoch passiv abgesichert werden können. Dies bezieht sich insbesondere auch auf die konstruktiven Sicherheitszuschläge bei der Festigkeitsberechnung der bei der Auslegung der Apparate zu verwendenden Materialien. Dies ist jedoch nicht Gegenstand dieser Arbeit und wird von SafeCAD nicht unterstützt. Die Anbindung eines entsprechenden Programmtools ist aber möglich.

5.3.2 Aktive Maßnahmen

Trotz passiver Maßnahmen kann es zu Störungen im Betrieb kommen. Diese können im allgemeinen durch aktive Maßnahmen begrenzt werden. Sie sorgen dafür, daß

der Prozeß nicht den bestimmungsgemäßen Betriebsbereich verläßt. Beispiele aktiver Maßnahmen sind /AD-Merkblatt A6/:

- Abschalten der Reaktandenzufuhr
  Die Abschaltkriterien müssen bekannt sein, d.h. es muß bekannt sein, welche Energie nach der Abschaltung noch frei werden kann, ohne daß die Auslegungsparameter des Reaktors überschritten werden. Aus diesem Grund sollte man bei stark exothermen Reaktionen nie beide Reaktanden gleichzeitig vorlegen.
- Einschalten einer Notkühlung /Ratg98/
  Insbesondere bei Reaktionen, die nicht kontinuierlich oder in semi-batch-Fahrweise durchgeführt werden können, kann die Temperatur unter adiabaten Bedingungen bis an die Zersetzungsgrenze der Substanzen steigen. Hier ist es oftmals erforderlich, ein zweites Kühlsystem mit unabhängiger Energieversorgung vorzusehen. Dies ist zwar eine aufwendige Lösung, da das Kühlmedium bevorratet werden muß, dafür aber eine sehr sichere Maßnahme, wenn die Einschaltkriterien für die Notkühlung genau festgelegt werden können. Eine bestimmte Grenztemperatur, der Ausfall der Hauptkühlung oder der Energieversorgung können hierfür herangezogen werden. Um die Kühlmittelbevorratung auslegen zu können, muß das Reaktionspotential bekannt sein. Wichtig ist neben einer ausreichenden Kühlung auch, nicht zu viel zu kühlen, da es sonst zu einem Abklingen der Reaktion und dadurch zu einer Akkumulation kommen kann. Falls dabei die Erstarrungstemperatur der beteiligten Stoffe erreicht wird, kann sich der Wärmedurchgang verringern und der Reaktorausgang verstopfen.
- Einschalten einer Notdurchmischung
  Fällt der Rührer aus, kann es zu einer lokalen Akkumulation des Reaktionsgemisches kommen. Die Auswirkungen bei erneutem Einschalten des Rührers können verheerend sein, wenn die Reaktion plötzlich wieder anläuft und größere Massen auf einmal abreagieren. Hier besteht die Möglichkeit, durch gezielte Eindüsung z.B. von Stickstoff eine Notumrührung zu erreichen. Kombinationen mit einem Inhibitor oder Reaktionsstopper sind ebenso denkbar. In Ausnahmefällen kann aber auch die Gasentwicklung während der Reaktion oder thermische Konvektion in homogener Phase zu einer ausreichenden Durchmischung führen /Ratg98/.
- Einschalten einer Notverdünnung/Einleiten eines Inhibitors

Diese Maßnahme kann nur bei langsameren Reaktionen eingesetzt werden. Sie setzt voraus, daß man noch in der Lage ist, den Inhibitor im Reaktor zu verteilen. Wenn durch Viskositätserhöhung des Reaktormediums bei einer Durchgehreaktion der Rührer ausfällt, gelingt das meist nicht mehr.

- Einbringen eines Reaktionsstoppers
  Entscheidend ist auch hierbei, daß der Stopper schnell genug im gesamten Reaktor verteilt werden kann. Bei gleichzeitigem Ausfall des Rührers muß dies genau wie bei der Notverdünnung nicht der Fall sein. Für dieses Szenario muß dann eine andere Maßnahme gefunden werden bzw. mit einer weiteren (s.o.) kombiniert werden.
- Entspannungseinrichtungen
  Die Druckentlastung ist die letzte Barriere zur Beherrschung durchgehender Reaktionen. Haben vorher andere Maßnahmen nicht oder nicht ausreichend angesprochen, kann durch gezielte Abführung bestimmter Mengen des Produktes ein Bersten des Reaktors verhindert werden. Voraussetzung für eine sichere Druckentlastung neben der Rückhaltung freigesetzter, gefährlicher Stoffe /TAA 94/ ist dabei /Ratg98/:

  1. das chemische System muß für eine Druckentlastung geeignet sein,
  2. Kenntnis des richtigen Ansprechdrucks,
  3. richtige Dimensionierung des Druckentlastungsquerschnittes und
  4. die Randbedingungen der Auslegung müssen sichergestellt sein (Produktabführung, Entsorgung)

Als Entspannungseinrichtungen bieten sich Sicherheitsventile und Berstsicherungen an. Hierbei ist, wenn möglich, das Sicherheitsventil vorzuziehen, da beim Ansprechen des Ventils im Gegensatz zur Berstsicherung der Betrieb fortgeführt werden kann. Im Unterschied zur Berstsicherung schließt die Öffnung selbsttätig wieder, wenn der Druck weit genug abgesunken ist. Berstsicherungen erhalten den Vorzug /AD-Merkblatt A1/, wenn

- mit einem schnellen Druckanstieg gerechnet werden muß,

- die Betriebsbedingungen zu Ablagerungen und Verklebungen führen können, die die Funktion anderer Sicherheitseinrichtungen gegen Drucküberschreitung beeinträchtigen würden,
- erhöhte Anforderungen an die Dichtheit gestellt werden und
- große Entlastungsquerschnitte erforderlich sind.

Bei polymerisierenden Medien kann eine Berstsicherung auch einem Sicherheitsventil vorgeschaltet werden, um ein Verkleben des Ventils zu vermeiden. In jedem Fall müssen Sicherheitsventile und Berstsicherungen den Anforderungen der Druckbehälterverordnung /Tech00/ bzw. der Betriebssicherheitsverordnung /Betr02/ und der AD-Merkblätter A1 /AD-Merkblatt A1/ und A2 /AD-Merkblatt A2/ genügen.

Problematisch bei einer Notentlastung ist, wenn der Reaktorinhalt am Auslaß ausreagiert ist (Verklebungs- bzw. Verstopfungsgefahr) oder der Inhalt giftig bzw. brennbar ist. Meist wird versucht, solche Maßnahmen zu wählen, die ein sicheres Verbleiben der Reaktionsstoffe im Reaktionsbehälter gewährleisten, da so eine gefahrlose Beseitigung eher möglich ist, als wenn der Reaktorinhalt abgeführt wurde. Zusätzlich zu Z-Schaltungen (siehe Kapitel 2) angebrachte Berstscheiben oder Sicherheitsventile dienen oftmals dem Ableiten der Anteile, die durch Druckerhöhungen beispielsweise infolge eines Umgebungsbrandes die Auslegungsgrenzen der Anlage überschreiten könnten. Hier nimmt man das Freisetzen geringer, mitunter sehr gefährlicher Stoffe trotz Ansprechens einer Z-Schaltung eher in Kauf, bevor durch weitere Drucksteigerung die gesamte Anlage gefährdet wird /Pers/. Anfallende Mengen können über den Tassenboden abgeführt werden, umfangreiche Abführungssysteme werden für diesen Fall in der Regel nicht vorgesehen.

Bei einigen Reaktionstypen gibt es keine Alternative zu einem Notablaß als letzte störfallverhindernde Maßnahme. Als Beispiel kann hier eine Nitrierreaktion genannt werden, die in /Haup85a/ als Teil einer Hexogen-Anlage näher erläutert wird.

5.3.3 Organisatorische Maßnahmen

Neben aktiven Maßnahmen gibt es noch eine Reihe organisatorischer Maßnahmen. Im wesentlichen sind diese vergleichbar mit den aktiven Maßnahmen. Deren Auslösung wird nach Alarmierung jedoch nicht automatisch, sondern vom Anlagenpersonal eingeleitet.

Entscheidend bei der Wahl organisatorischer Maßnahmen ist die genaue Zeitermittlung für die Durchführung und das Wirksamwerden der Maßnahmen.

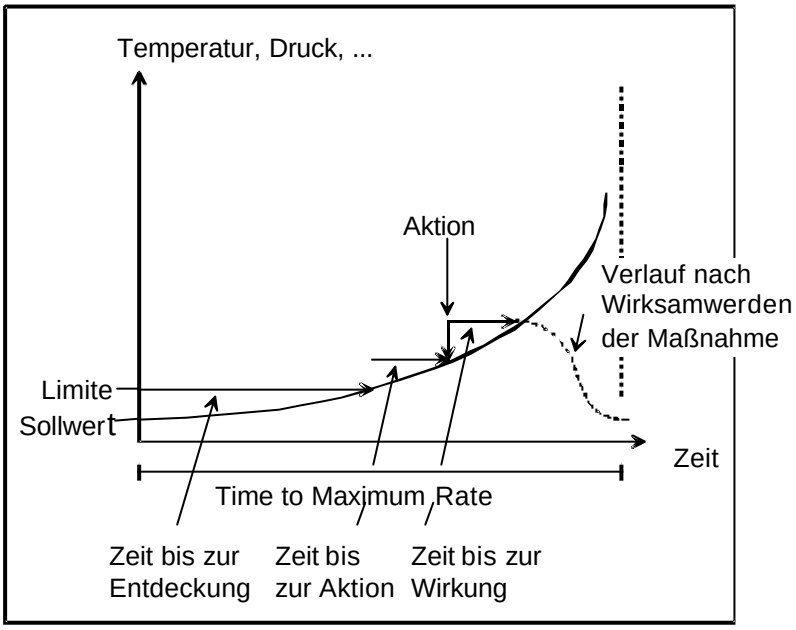


Bild 5-8: Zeitlicher Maßnahmenverlauf /Gyga88/

Diese Zeit muß geringer sein als die Zeit zwischen Erkennen der Abweichung und Erreichen des unzulässigen Fehlbereichs durch den Prozeß. Darüber hinaus sollte hier noch ein Zeitpuffer als „Sicherheitspolster“ mit vorgesehen werden. Bild 5-8 zeigt den Verlauf einer Prozeßgröße nach einer Störung bis zum Greifen der Sicherheitsmaßnahmen. Für die automatische Auslösung der aktiven Maßnahmen gilt dies ebenso (siehe auch Kapitel 6.2). Weitere Anforderungen an die Durchführbarkeit organisatorischer Maßnahmen sind /Merk96/:

- Der Grund für die Abweichung des Prozesses muß eindeutig in Bezug auf die Gegenmaßnahme sein.
  Ist dies nicht der Fall, kann unter Umständen auf eine Abweichung mit einer Maßnahme reagiert werden, die nicht unmittelbar die geeignetste zu ihrer Behe-

bung ist. Fällt zum Beispiel der Rührer aus, und steigt infolge dessen die Temperatur im Reaktor, so reicht die Erhöhung der Kühlmittelzufuhr allein nicht aus. Vielmehr muß gleichzeitig die Zufuhr der Reaktanden unterbrochen werden, um eine mögliche, durch erhöhte Temperatur steigende Reaktionsrate zu vermeiden. Dies gilt insbesondere im Hinblick auf einen spontanen Akkumulationsabbau, der sich aufgrund des Rührerausfalls lokal bilden kann.

- Das Anlagen-Personal muß ausreichend geschult sein.
  Da organisatorische Schutzmaßnahmen in der Regel selten durchgeführt werden müssen, sinkt mit fortschreitender Zeit der Vertrautheitsgrad des Personals. Daher muß regelmäßig die Einhaltung der Reihenfolge sowie der sachgemäßen Durchführung der einzelnen Maßnahmen in Schulungen geübt werden.
- Bei der Umsetzung der Maßnahmen darf niemand gefährdet werden.
  Im Fall einer Alarmierung wird das Anlagen-Personal einer Streßsituation ausgesetzt. Handlungen können daher unter Umständen anders ablaufen als unter Normalbedingungen. Somit müssen alle Einrichtungen bei der Durchführung der Maßnahmen leicht bedienbar sowie gut erreichbar und eindeutig identifizierbar sein, um die Gefahr von Fehlbedienungen zu minimieren.
- Die Anzahl der durchzuführenden Maßnahmen muß jederzeit umsetzbar sein.
  Hier muß die Anzahl der im Extremfall gleichzeitig durchzuführenden organisatorischen Maßnahmen zugrundegelegt werden. Die Anzahl sollte angemessen niedrig sein. Darüber hinaus muß sichergestellt sein, daß zu jeder Zeit ausreichend Personal anwesend ist und dieses auch entsprechend geschult ist. Somit kann auch im Zusammenspiel mit einer eindeutigen Kennzeichnung gewährleistet werden, daß die Maßnahmen in der richtigen Reihenfolge ausgeführt werden.

Vorstellbare Ursachen für Abweichungen vom Normalbetrieb werden unter anderem in /Merk95/ genannt. Welche Abweichungen möglich sind und welche Maßnahmen nun im einzelnen zur Vermeidung bzw. Beherrschung dieser Fehlzustände zu wählen sind, wird gewöhnlich im Rahmen eines Sicherheitsgespräches /Grei91/ unter Experten der verschiedenen Fachgruppen (Forschung, Verfahrenstechnik, Anlagenbau, Betrieb, Bauabteilung, PLT, Instandhaltung, Werks- und Betriebstechnik, Anlagensicherheit, Umwelt- und Arbeitsschutz, Qualitätssicherung, Ergonomie und Psychologie) /Ratg98/ entschieden. Im Rahmen eines solchen Gesprächs wird weiterhin entschieden, ob die Anlage bzw. die Teilanlage einer genaueren sicherheitstechni-

schen Überprüfung bedarf. In der Industrie haben sich hierfür Methoden wie z.B. das PAAG-Verfahren (siehe Kapitel 3) bewährt. Gewöhnlich werden mehrere Maßnahmen in Abhängigkeit der evaluierten potentiellen Abweichungen ausgewählt, um über Redundanz und Diversität das Halten der Prozeßparameter im bestimmungsgemäßen Betriebsbereich wahrscheinlicher zu machen.

5.3.4 Verringernde Maßnahmen

Kommt es trotz aller Vorkehrungen dennoch zum Störfall oder zur Stofffreisetzung beispielsweise infolge einer Leckage, können Maßnahmen wie

- Schutzstreifen und Schutzzonen,
- Auffangräume,
- Gaswarneinrichtungen,
- Gasvernichtungsanlagen,
- persönliche Schutzausrüstung und
- Notfallplanung

die Auswirkungen der Ereignisse lindern beziehungsweise reduzieren. Schutzstreifen und Schutzzonen sollen im Störfall ein Übergreifen auf benachbarte Anlagen vermeiden, so daß der Domino-Effekt unwahrscheinlicher wird, der in der neuen Störfallverordnung /Stör00/ als Umsetzung der Seveso-II-Richtlinie /Seve96/ im § 15 entsprechende gesetzliche Anerkennung findet:

> *(...) bei welchen Betriebsbereichen (...) auf Grund ihres Standortes, ihres gegenseitigen Abstandes (...) eine erhöhte Wahrscheinlichkeit oder Möglichkeit von Störfällen bestehen kann (...).*

Weitere gesetzliche Vorgaben sind in der TRbF 30 /TRbF30/ und der Reihen 600 /TRbF600/ zu finden. Falls nicht ausreichend Platz auf dem Gelände vorhanden ist, können durch bautechnische Begrenzungsmaßnahmen (z.B. Mauern, Erdwälle, Einhausungen etc.) die gesetzlichen Mindestabstände unterschritten werden, wobei die Sicherheit nicht geringer werden darf.

Auffangräume sollen ein sicheres Aufnehmen von Leckageflüssigkeit zum Schutz vor Brand und Explosion sowie Umwelt- und Personengefährdung infolge Toxizität des Lagerstoffes garantieren. Darüber hinaus können sie bei entsprechender Dimensionierung zusätzlich Niederschlagswasser und im Störfall auch Löschwasser aufnehmen, so daß dieses vor weiterer Einleitung auf toxische Rückstände hin untersucht werden kann.

Dazu ist es erforderlich, die Auffangräume und Rückhaltebecken entsprechend dicht zu gestalten, damit sie für einen vorgegebenen Zeitraum die Flüssigkeit verlustfrei aufhalten können. Das Prüfzeichen des Institus für Bautechnik in Berlin (IfBt) garantiert die Anwendbarkeit des Abdichtungssystems (Beschichtungsstoff, Keramik, Zement, Stahlblech) für den jeweiligen Einsatzzweck.

Gaswarneinrichtungen sollten immer dann eingesetzt werden, wenn das Gas oder die Dämpfe geruchlos sowie toxisch oder explosions- bzw. brandgefährlich sind oder eine hohe Geruchsschwelle besitzen. Ist das Gas weniger gefährlich und hat es eine geringe Geruchsschwelle, so kann bei ständig besetzter Anlage auch die Wahrnehmung durch das Personal ausreichen. Hierbei ist jedoch zu bedenken, daß gefährliche Gase oder Dämpfe bei sonst gleicher Konzentration durch Geruchsüberlagerungen weniger gut wahrgenommen werden können. Ebenso können einige Gase oder Dämpfe die Empfindlichkeit der Geruchsnerven negativ beeinflussen, so daß eine Perzeption nicht mehr rechzeitig möglich ist /Satt00_1/. Man erkennt, daß die Wahl einer Gaswarneinrichtung keinen allgemein gültigen physikalischen Gesetzen unterliegt und somit von Fall zu Fall zu entscheiden ist. Letztendlich spielt bei der Auswahl geeigneter Einrichtungen die Zulassungsbehörde u.U. die ausschlaggebende Rolle.

In Abhängigkeit der denkbaren Gefährdungen insbesondere im Hinblick auf die Toxizität der gehandhabten Stoffe kann eine geeignete Schutzausrüstung das direkt betroffene Personal innerhalb der Anlage schützen. Die genaue Auswahl der Ausrüstung ist stoffabhängig und muß daher individuell –unter Beachtung geltender Gesetze und Vorschriften– betrachtet werden. Entscheidend ist der Zeitpunkt der Alarmierung, so daß die Schutzausrüstung noch rechtzeitig angelegt werden kann. In Alarmplänen sowie Betriebsvorschriften müssen die genauen Abläufe festgelegt

sein. Regelmäßig durchgeführte Übungen zum Verhalten im Notfall sorgen dafür, daß das Personal in einer Notsituation nicht völlig unvorbereitet handelt.

Damit die Prozeßparameter nicht den bestimmungsgemäßen Betriebsbereich verlassen beziehungsweise mögliche Auswirkungen begrenzt werden, sind für gewöhnlich Barrieren vorgesehen. Diese zeigt im Überblick Bild 5-9.

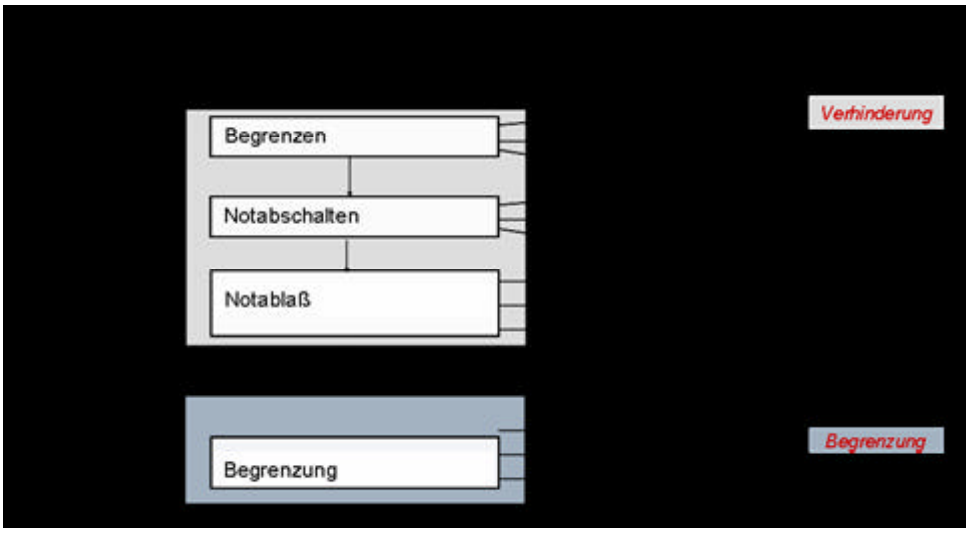


Bild 5-9: Mögliche Aktionsparameter zur Sicherung des Prozesses

Insgesamt läßt sich die sicherheitstechnische Auslegung einer Anlage wie folgt gliedern:

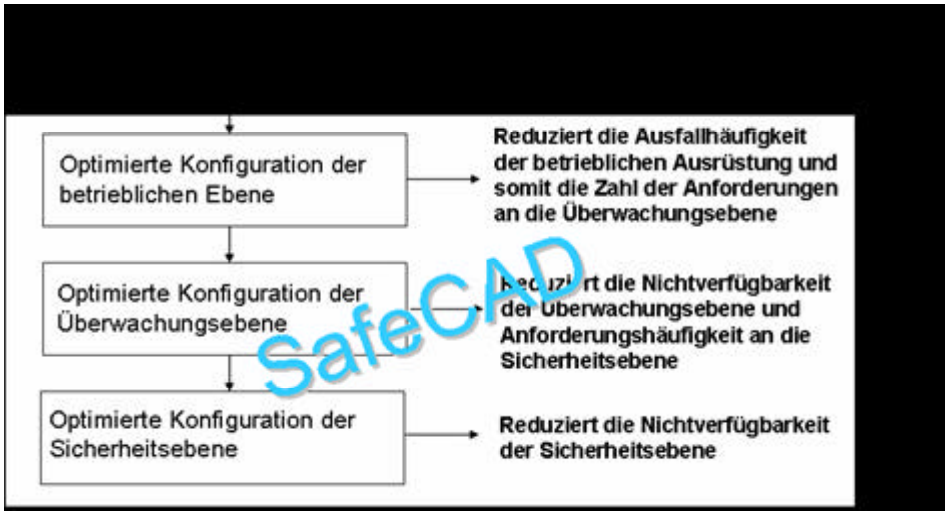


Bild 5-10: Maßnahmenverlauf

Die richtige Dimensionierung auf der Ausrüstungsseite garantiert dabei eine minimale Versagenswahrscheinlichkeit der Komponenten. Ausfälle infolge zu geringer Di-

mensionierung (z.B. zu dünne Wandungen bei einem Behälter) können so verhindert werden. Die korrekte Auslegung auf der betrieblichen Ebene erhöht die Wahrscheinlichkeit des Verbleibs der Prozeßparameter im Bereich des bestimmungsgemäßen Betriebes und reduziert gleichzeitig die Ausfallhäufigkeit dieser. Die geeignete Konfiguration der Überwachungsebene vermindert die Anforderungshäufigkeit der Sicherheitssysteme, indem rechtzeitig auf den Prozeß eingewirkt wird, damit die Prozeßparameter nicht den bestimmungsgemäßen Bereich verlassen oder indem das Anlagenpersonal alarmiert wird. Sollten dennoch die Grenzen des bestimmungsgemäßen Betriebs überschritten werden, so sorgt die richtige Auslegung der Sicherheitssysteme für eine Reduzierung ihrer Nichtverfügbarkeit.

Die vorgestellte neue Methode behandelt dabei die in Bild 5-10 markierten Bereiche

- richtige Konfiguration der betriebl. Ebene,
- richtige Konfiguration der Überwachungsebene und
- richtige Konfiguration der Sicherheitssysteme.

Die Anordnung der Anlagen und Teilanlagen im Betriebsbereich sowie die Dimensionierung der Aggregate wird nicht von der neuen Methode behandelt und muß nach wie vor von den Experten der entsprechenden Bereiche aufgrund der physikalischen, chemischen umd technischen Anforderungen vorgenommen werden.

Eine besonders große Rolle für die Sicherheit von Anlagen spielt die Prozeßleittechnik, da die meisten Sicherheitssysteme aktive Systeme sind. Es gibt zwar Bemühungen, vermehrt passive Systeme zur Sicherung von Anlagen einzusetzen, jedoch ist dies bei bestimmten Anlagentypen nur begrenzt möglich. Im nächsten Kapitel wird daher der Einsatz der PLT bei der Anlagensicherheit näher beschrieben.

5.3.5 Beispiele zur sicheren Gestaltung von Chemieanlagen

In diesem Abschnitt wird an vier Beispielen skizziert, wie

- in der Industrie der Redundanz- und Diversitätsgrad festgelegt wird,
- man aus der Analyse des Prozeßverhaltens auf die notwendigen Sicherheitssysteme schließen kann,

- man Gefährdungen bewertet und kontrolliert und
- die Absicherung einer exothermen Reaktion im semi-batch Betrieb vorgenommen wird.

Englund und *Grinwins* /Engl92/ von DOW Chemical entwickelten eine qualitative Gefahren-Instabilitäts-Matrix, um in Abhängigkeit sowohl vom Gefahrenpotential als auch von der Prozeß-Instabilität ein geeignetes Maß an Redundanz und Diversität zu erhalten. Bild 5-11 zeigt die Matrix mit den zugehörigen Redundanz-Graden.

<table>
<tr><th>hohes Gefahrenpotential, geringe Prozeß-Instabilität</th><th>hohes Gefahrenpotential, hohe Prozeß-Instabilität</th></tr>
<tr><td>• Zwei oder mehr Meßeinrichtungen
• Zwei oder mehr Eingänge für die Auslösung eines Alarms
• "1 von 2" – Logik für die Auslösung eines Alarms
• Sowohl einfacher als auch redundanter Eingang für die Prozeß-Kontrolle

Anlagen-Strategie:
Anlagenpersonal entscheidet über Abschaltung; unnötige Abschaltungen sind möglich.

Beispiele:
• Chlortankwagenumfüllstation
• Teile eines Tankparks für brennbare Flüssigkeiten</td><td>• Dreifach redundante Meßeinrichtungen
• "2 von 3" – Logik für die Auslösung eines Alarms
• Mehr als ein Eingang für die Prozeß-Kontrolle
• Kontroll-System entscheidet über Alarmbedingungen
• Alarmierung bei unterschiedlichem redundantem Eingangssignal
• Bedienpersonal veranlaßt die Reparatur

Anlagen-Strategie:
Minimierung falscher Abschaltungen; Fehler in der Regelung/Messung können zu Sicherheitsproblemen und wirtschaftlichen Verlusten führen

Beispiele:
• Teile einer Ethylen-Anlage
• Teile einer Ethylenoxid-Anlage</td></tr>
<tr><th>geringes Gefahrenpotential, geringe Prozeß-Instabilität</th><th>geringes Gefahrenpotential, hohe Prozeß-Instabilität</th></tr>
<tr><td>• Eine Meßeinrichtung
• Ein Eingang für die Auslösung eines Alarms
• "1 von 1" – Logik für die Auslösung eines Alarms
• Einfacher Eingang für die Prozeß-Kontrolle
• Keine Reserveausrüstung

Anlagen-Strategie:
• Falsche Abschaltung stellt keine Probleme dar, außer der Stillstandszeiten und kleiner Produktverluste

Beipiele:
• Calciumchlorid – Trockner
• Plastik Granualt Extruder- und Verpackungslinie
• Wasseraufbereitungsanlage (soweit nicht nachgelagerte Anlagen betroffen werden)</td><td>• Zwei Meßeinrichtungen
• Zwei Eingänge für die Auslösung eines Alarms
• "2 von 2" – Logik für die Auslösung eines Alarms
• Mehr als ein Eingang für die Prozeß-Kontrolle
• Alarmierung bei unterschiedlichem redundanten Eingangssignal
• Bedienpersonal veranlaßt die Reparatur und/oder Abschaltung bei unterschiedlichen Eingangssignalen

Anlagen-Strategie:
• Minimierung falscher Abschaltungen; Fehler in der Regelung/Messung können zu geringen Sicherheitsproblemen und hohen wirtschaftlichen Verlusten führen
• Zur Entscheidungsfindung bleibt dem Anlagenpersonal ausreichend Zeit
• Anlagenpersonal kann falsche Entscheidungen treffen

Beipiele:
• Kalkbrennofen
• Hochofen</td></tr>
</table>

Bild 5-11: Redundanzgrad in Abhängigkeit vom Gefahrenpotential und der Prozeß-Instabilität

Die Prozeß-Instabilität spielt hier eine Rolle, da im Sinne der Sicherheit ausgelegte Bewertungsschaltungen unter dem Blickwinkel der Anlagen-Verfügbarkeit in der Regel gegenläufig sind (vergleiche Kapitel 6.3). Hier wurde ein Kompromiß gefunden, der nicht auf Kosten der Sicherheit geht.

Stoessel /Stoe95/ beschreibt eine Methode, wie aus der quantitativen Analyse des Prozeßverhaltens ermittelt werden kann, welche Sicherheitssysteme notwendig sind, am Beispiel eines exothermen semi-batch Reaktors in vier Schritten:

1. Prüfung, ob der Prozeß isotherm gefahren werden kann.
   Hier werden die Wärmefreisetzungsrate q_{rx} und der Energieeintrag des Zustromes q_{fd} addiert, um die Kapazitäten der Kühlung zu ermitteln. Des weiteren werden dabei ebenso die Einflüsse der Rührer- sowie Zulaufgeschwindigkeit und der Temperatur auf die Wärmefreisetzungsrate berücksichtigt. Dies entspricht den Betrachtungen gemäß Gleichung (5-6).
2. Bestimmung der maximal tolerierbaren akkumulierten Menge an Reaktanden.
   Dieser Schritt ist der wichtigste bei der Untersuchung eines Prozesses, da die Ergebnisse die Auslegung des Reaktors sowie des Kühlsystems maßgeblich beeinflussen. *Stoessel* errechnet die maximal mögliche Temperatur bei Ausfall der Kühlung mit Hilfe von

$$MTSR = T_r + (1 - X_{st}) \cdot \Delta T_{ad} \cdot \frac{M_{r,f}}{M_{r,st}} \qquad (5\text{-}11)$$

   und berücksichtigt somit den Grad des Umsatzes X_{st} bei der Berechnung der Maximaltemperatur.
3. Anpassung des Prozesses an die Vorgaben.
   Hier wird überprüft, ob die maximal mögliche Temperatur nach Gleichung (5-11) vom gewählten Betriebs- und Sicherheitssystem beherrscht werden kann oder ob Veränderungen oder Ertüchtigungen z.B. des Kühlsystems nötig sind.
4. Kontrolle der Zufluß- und Reaktionsraten.
   Die Wärmeentwicklung hängt im wesentlichen von der Reaktionsrate und der zugeführten Produktmasse ab. Daher schlägt *Stoessel* entsprechende Kontroll- und Sicherheitsmechanismen vor:

1. Begrenzung der Zuflußrate durch Verwendung einer Volumenpumpe.
2. Verriegelung des Zuflusses bei zu hoher oder zu niedriger Reaktortemperatur. Bei zu hoher Temperatur besteht die Gefahr des Durchgehens der Reaktion und bei zu niedriger Temperatur die Gefahr des Einschlafens der Reaktion. Dies kann zur Akkumulierung der Reaktanden und zu heftiger Reaktion bei Rückführung der Temperatur auf ihren Nominalwert führen.
3. Messung und Kontrolle der Zuflußtemperatur zur Vermeidung von zu hoher Aufheizung des Reaktorinhaltes oder zur Vermeidung von Akkumulation bei zu niedriger Zulauftemperatur.
4. Verriegelung des Zuflusses über den Rührer zur Vermeidung von Stoffanreicherung bei ungenügender Durchmischung.

Bei Beachtung dieser Punkte kann der Prozeß nach *Stoessel* auch im Falle von Störungen ausreichend sicher beherrscht werden. Diese Methode der „formelgestützten Experteneinschätzung“ läßt sich mit der HAZOP-Methode kombinieren, bei der man ähnlich vorgeht, allerdings in Form von Gedankenexperimenten. Diese sagen das Prozessverhalten tendenziell vorher, aber nicht die genauen Werte, die für eine Dimensionierung notwendig sind.

Gibson et al. /Gibs87/ schlägt erstmals eine übergreifende Strategie in vier Schritten vor:

1. Definition der Prozeßbedingungen.
2. Charakterisierung der chemischen Reaktion und ihrer Gefährdung.
3. Auswahl und Spezifikation der sicherheitstechnischen Messungen/Maßnahmen.
4. Implementierung und Wartung der sicherheitstechnischen Messungen/Maßnahmen.

Auf die quantitative Bewertung der Prozeßbedingungen folgt die Festlegung der Sicherheitsmaßnahmen und deren qualitativen Einschätzung. Die einzelnen Schritte zur Bewertung und Beherrschung der Gefährdungen zeigen die folgenden Bilder:

Bild 5-12: Schritte zur Kontrolle von Gefährdungen bei chemischen Reaktionen

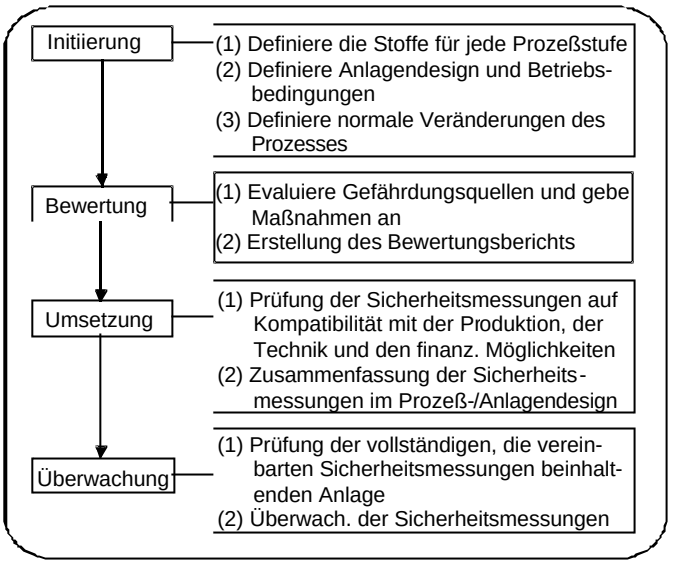


Bild 5-13: Strategie zur Kontrolle von Gefährdungen bei chemischen Reaktionen

Eine sichere Prozeßführung im semi-batch Betrieb wird durch eine dosierkontrollierte Reaktionsführung /Ratg98/ erreicht. Dazu wird im Reaktionsbehälter ein Edukt vorgelegt und das andere hinzudosiert. Dies hat den Vorteil, daß es in der Regel prompt zur Abreaktion und somit nicht zur Akkumulation kommen kann. Bedingung hierfür ist die Dosierung innerhalb eines festgelegten Temperaturfensters. Außerhalb seiner Grenzen ist die Zufuhr verriegelt. Voraussetzung für die Zufuhr ist die Funktion des Rührers sowie ein Mindestfüllstand des Reaktionspartners. Ohne eine Durchmischung kann die sofortige Abreaktion jedoch nicht gewährleistet und eine Akkumulation nicht ausgeschlossen werden. Ist der Reaktionspartner nicht in ausreichender Menge vorgelegt, kann dies ebenso zu einer übermäßigen Wärmeproduktion nach anschließender Auffüllung führen /Ratg98/.

Kommt es dennoch zu Abweichungen, so greift beispielsweise bei der BASF /Pers/ das folgende Barrierenkonzept:

1. Zufuhr der Reaktanden reduzieren.
2. Kühlmittelzufuhr erhöhen.
3. Abschaltung der Reaktanden über Schutzschaltungen (z.B. TZ+ oder PZ+).

Dies setzt voraus, daß die Abschaltkriterien bekannt sind, d.h. es muß bekannt sein, welche Energie nach Abschaltung noch frei werden kann, ohne daß die Auslegungsparameter des Reaktors überschritten werden.

Notentlastungseinrichtungen werden aus den in Abschnitt 5.3.2 genannten Gründen ungern eingesetzt.

6 PLT in der Anlagensicherheit

Der Begriff der Prozeßleittechnik leitete sich aus dem früher gebräuchlichen Begriff der MSR –Technik (Messen, Steuern, Regeln) ab. Dabei umfaßt die PLT sowohl die Anregeebene (z.B. Sensoren) als auch die Ausführungsebene (z.B. Ventile).

6.1 Prozeßleittechnik

Die Prozeßleittechnik erlaubt die Realisierung hoher Ansprüche der Automatisierung auf der Betriebs-, Überwachungs- und Schutzebene der Anlage. Die Aufgaben der PLT bestehen nach *Schuler* /Schu95/ in:

- Realisierung der erforderlichen Verarbeitungsfunktionen zur Beeinflussung des Prozesses durch binäre und kontinuierliche Verstellung von Aktoren,
- Visualisierung binärer und kontinuierlicher Meßsignale,
- Meldung und Alarmierung von Zuständen und Ereignissen,
- Realisierung von Überwachungs- und Schaltfunktionen, die ereignisgesteuert selbsttätig den Prozeß beeinflussen oder Bedienungen zustandsabhängig verbieten,
- Auswertung und Protokollierung von Ereignissen und Zuständen (chargen-, zeit- oder ereignisabhängig),
- Datenarchivierung (Meldungen, Alarme, Meßwerte, Zustände).

Bild 6-1: Funktionen der PLT

Da es sich bei der PLT um ein System verschiedener Apparate, Regler und Rechner handelt, spricht man im Zusammenhang mit der Prozeßführung verfahrenstechnischer Anlagen auch von Prozeßleitsystemen (PLS). Der Vorteil der PLS liegt in der simultanen Verarbeitung mehrerer Signale und der gleichzeitigen Entscheidungsfindung. Ein solches System besteht dann mindestens aus den drei Komponenten /Polk94/:

1. Prozeßnahe Komponenten (z.B. Regler),
2. Systembus und
3. Signalverarbeitung.

Bild 6-2: Komponenten der PLS

Die PLT-Einrichtungen unterliegen im Rahmen der PLS mehreren Einflußgrößen /Kess89/:

- Zweck und Art der verfahrenstechnischen Anlage,
- betriebliche Anforderungen (Verfügbarkeit, Flexibilität, Produktqualität, Prozeß-Anzeige und -Bedienung),
- verfahrenstechnische Gesichtspunkte (Entwicklungsstand des Verfahrens, Verfahrensvorschriften),
- spezifische Randbedingungen des Umfeldes.

Deutlich wird dies auch an folgender Darstellung:

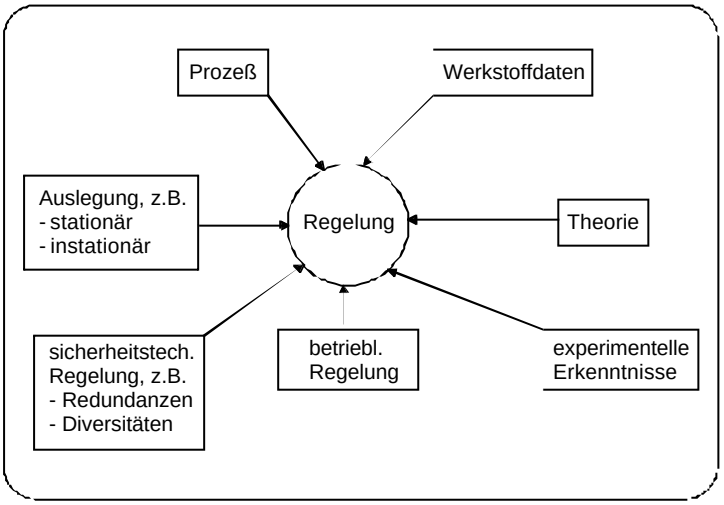


Bild 6-3: Einflußfaktoren auf die Auslegung einer Regelung

So gilt es im Rahmen der Planung, die verfahrens- und prozeßleittechnischen Ausrüstungen der Anlage unter Berücksichtigung der jeweiligen Einflußgrößen ausgewogen zu gestalten.

6.2 Anlagensicherheit mit Hilfe der Prozeßleittechnik

In den letzten Jahren hat die Prozeßleittechnik nicht zuletzt auch durch die gestiegene Komplexität der Anlagen erhöhte Aufmerksamkeit im Rahmen der Anlagensicherheit erfahren, z.B. /Nett93/, /DeHa86/, /Brus88/, /Weid96/, /Müll90/, /Grei91/. Neuere Systeme regeln nicht mehr nur den bestimmungsgemäßen Betrieb, sondern kontrollieren ebenso die Sicherheit einer Anlage (siehe Bild 6-4). Diesem Umstand wurde u.a. durch die NAMUR in Form ihrer Empfehlung NE 31 /NAMU93/ und der DIN/VDE 2180, Blatt 1-4 /DIN/VDE2180_2/, /DIN/VDE2180_1/, /DIN/VDE2180_3/,

/DIN/VDE2180_4/ sowie dem Merkblatt des VdS /Merk00/ Rechnung getragen. Ziel der Anlagensicherheit ist es, das Risiko soweit zu verringern, bis das verbleibende Risiko kleiner als das Grenzrisiko ist /Stro78/. Nach wie vor sollten dabei aber vorzugsweise Nicht-PLT-Einrichtungen (z.B. Berstscheibe) zum Einsatz kommen /DIN/VDE2180_2/. Anlagensicherungen der PLT-Technik sind vorzuziehen, wenn andere Maßnahmen nicht ausreichend oder nicht anwendbar sind bzw. die Wirtschaftlichkeit bei gleicher Sicherheit und Zuverlässigkeit höher ist.

Aufgrund der unterschiedlichen Funktionen der PLT-Einrichtungen im Hinblick auf den Betrieb und die Sicherheit einer Anlage werden diese in vier Klassen eingeteilt /DIN/VDE2180_2/, /NAMU93/:

1. PLT-Betriebseinrichtungen
2. PLT-Überwachungseinrichtungen
3. PLT-Schutzeinrichtungen
4. PLT-Schadensbegrenzungseinrichtungen

Bild 6-4: Klassen der PLT

So können die einzelnen PLT-Klassen aufgabengerecht ausgelegt werden, was gerade im Hinblick auf die Unabhängigkeit der Klassen hilfreich ist. Eine Entmaschung von Schutzeinrichtung und betrieblicher Regelung ist nicht erforderlich. Wird beispielsweise ein Stellgerät für beide PLT-Klassen genutzt, so muß es einer ständigen betrieblichen Überwachung unterliegen. In diesem Fall muß gewährleistet sein, daß die Funktionen der Schutzeinrichtungen immer vorrangig ausgeführt werden und die Qualität der Auslegung der für die Schutzeinrichtung geforderten entspricht /DIN/VDE2180_2/, /NAMU93/.

Die Aufgaben der PLT-Klassen aus Bild 6-4 werden in /DIN/VDE2180_2/, /NAMU93/, /Polk94/, /Kess89/, /DIN/VDE2180_1/, /DIN/VDE2180_3/, /DIN/VDE2180_4/, /Stro78/, /Nett93/, /Eute95/, /Grei91/ und /Grei87/ ausführlich vorgestellt. Daher werden sie hier nur kurz skizziert.

Der Betriebsbereich einer Anlage läßt sich in den bestimmungsgemäßen und den nicht-bestimmungsgemäßen Bereich unterteilen, wobei sich der bestimmungsgemäße Bereich noch in den Gutbereich und den zulässigen Fehlbereich gliedert. Die

PLT-Betriebseinrichtungen regeln den bestimmungsgemäßen Betrieb einer Anlage vorrangig in ihrem Gutbereich. Das beinhaltet alle für den Betrieb wichtigen MSR-Prozesse sowie die Registrierung und Protokollierung. Verlassen eine oder mehrere Prozeßgrößen den Gutbereich, spricht an der Grenze zum zulässigen Fehlbereich die PLT-Überwachungseinrichtung an. So wird das Anlagenpersonal über den veränderten Zustand informiert und somit dessen Aufmerksamkeit erhöht. Im zulässigen Fehlbereich besteht aus sicherheitstechnischer Sicht noch keine Gefahr, daher muß die Anlage nicht heruntergefahren bzw. Gegenmaßnahmen eingeleitet werden. Läßt sich die Anlage nicht mehr in den Gutbereich zurückführen, da die Prozeßgröße weiter steigt oder sinkt, spricht an einem bestimmten Grenzwert die Schutzeinrichtung an.

Aufgabe der Schutzeinrichtung ist die Vermeidung von nicht-bestimmungsgemäßen Betriebszuständen. Typische Funktionen dieser Einrichtungen sind /Grei91/:

- Automatische Einleitung von Schaltvorgängen und
- Alarmierung des anwesenden Personals zur Durchführung notwendiger Maßnahmen.

Dabei ist entscheidend, daß die Grenzwerte beim Übergang vom Gutbereich in den unzulässigen Fehlbereich und weiter zum nicht-bestimmungsgemäßen Betrieb so gewählt werden, daß die theoretisch verbleibende Zeit bis zum Eintritt des unerwünschten Ereignisses ausreicht, die Anlage wieder in den Gutbereich zu führen bzw. andere Maßnahmen einzuleiten. Die Grenzwerte sind von verschiedenen Faktoren abhängig und müssen daher individuell für jede Anlage beziehungsweise jeden Prozeß bestimmt werden.

Die PLT-Betriebseinrichtungen unterliegen einer ständigen Plausibilitätskontrolle hinsichtlich der Bandbreite der zu regelnden Prozeßparameter durch das Personal. Dies ist bei den sehr selten ansprechenden Schutzeinrichtungen nicht der Fall. So kann es sinnvoll sein, Komponenten sowohl für Betriebseinrichtungen als auch für Schutzeinrichtungen nutzen zu lassen, um so die Verfügbarkeit der Schutzeinrichtung zu erhöhen. Da die Anforderungen an Komponenten der PLT-Betriebseinrichtungen und die PLT-Schutzeinrichtungen nicht gleich sein müssen, sind in diesem Fall die Anfor-

derungen der Schutzeinrichtungen zu erfüllen. Bild 6-5 /NAMU93/ stellt in Erweiterung von Bild 1-1 die Wirkungsweise der PLT-Klassen eins bis drei gemäß Bild 6-4 dar.

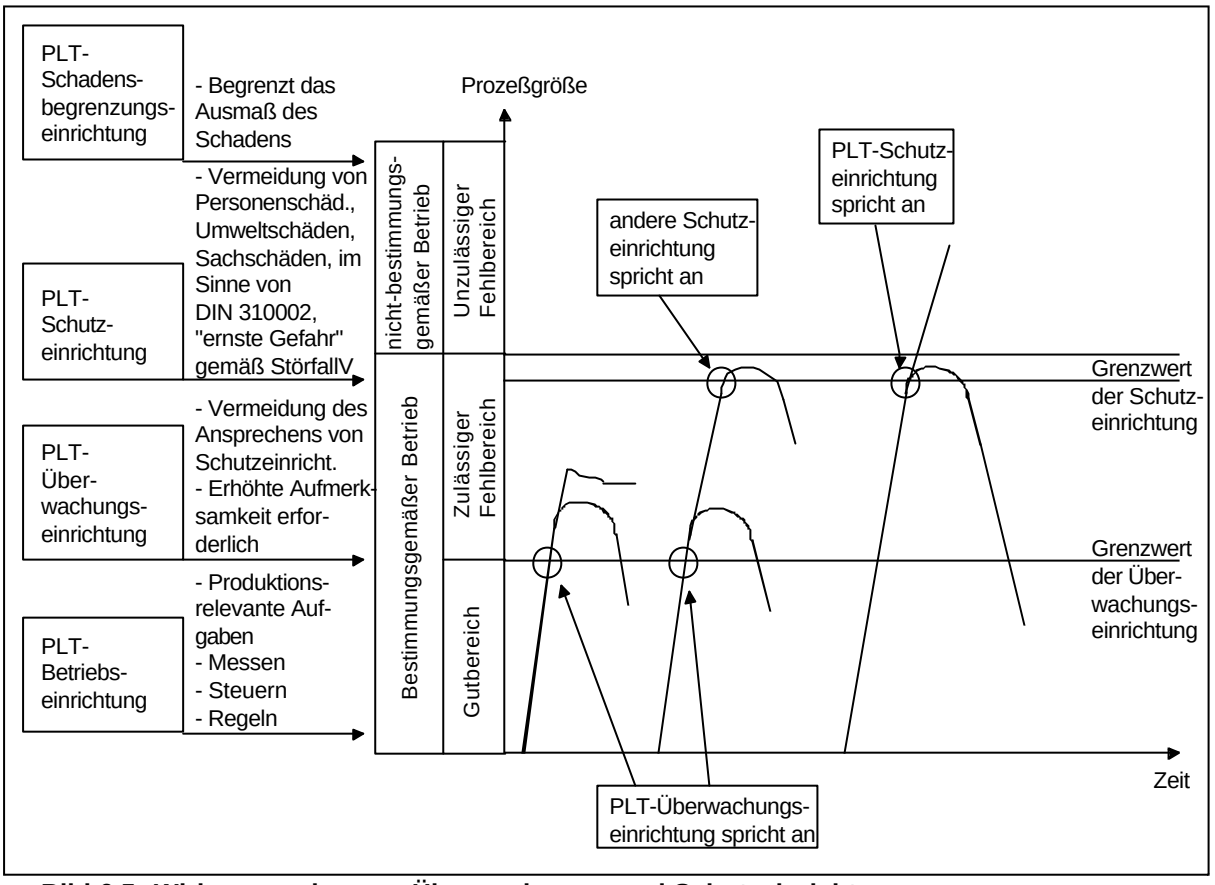


Bild 6-5: Wirkungsweise von Überwachungs- und Schutzeinrichtungen

Bild 6-6 zeigt noch mal eine Gegenüberstellung der ersten drei Klassen, woraus die Funktionen und Anforderungen der PLT-Einrichtungen deutlich werden /Grei87/.

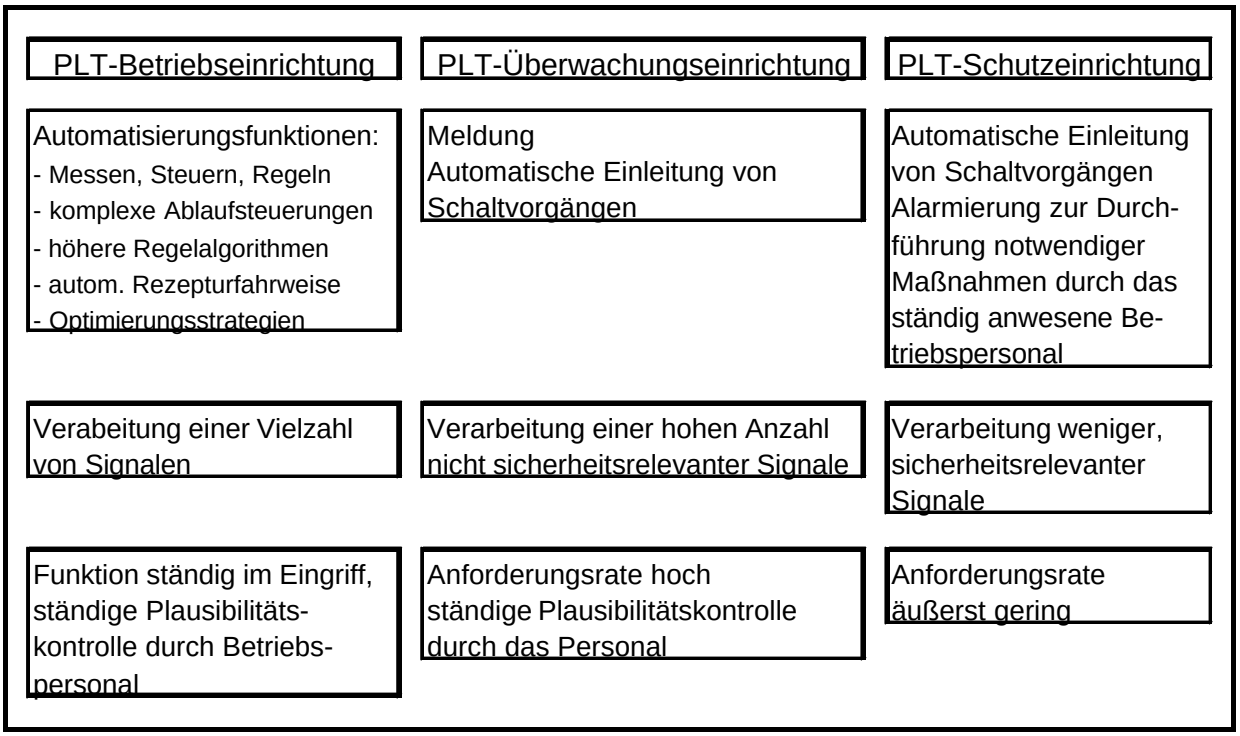


Bild 6-6:Gegenüberstellung der PLT-Klassen

Neben PLT-Schutzeinrichtungen gibt es eine Reihe anderer, unmittelbar wirksamer Schutzeinrichtungen (z.B. Sicherheitsventile), denen PLT-Schutzeinrichtungen vorgelagert sein können, um die Auslösehäufigkeit dieser Einrichtungen zu mindern. Diese Schutzeinrichtungen werden dann nach /DIN/VDE2180_2/ und /NAMU93/ als Überwachungseinrichtungen klassifiziert. Gemäß Störfallverordnung /Stör00/ sind neben Vorkehrungen zur Verhinderung von Störfällen auch vorbeugende Maßnahmen zu treffen, um im Störfall dessen Auswirkungen so gering wie möglich zu halten. Demnach lassen sich auch die Nicht-PLT-Schutzeinrichtungen unterscheiden. Störfallverhindernd wirken u.a. /Grei91/:

- Sicherheitsventile,
- Berstscheiben,
- Explosionsklappen und
- Schnellschlußventile und –schieber.

Auswirkungsbegrenzend wirken z.B.:

- sprengkapselbetätigte Löschmittelsperren,
- Auffangräume,

- Abmauerungen.

Die Begrenzung der Störfallauswirkungen ist nicht Gegenstand dieser Arbeit und wird daher im weiteren nicht näher betrachtet.

In der ursprünglichen DIN/VDE 2180 erfolgte die Unterteilung der PLT-Einrichtungen in die ersten drei Klassen gemäß Bild 6-4. Die Empfehlung der NAMUR /NAMU93/ führte dazu noch die vierte Klasse der Schadensbegrenzungseinrichtungen ein, die dann 1998 ebenfalls in die überarbeitete DIN/VDE 2180 /DIN/VDE2180_2/ aufgenommen wurde. Hierbei handelt es sich um auswirkungsverringernde Maßnahmen für den Fall, daß die Grenzen des nicht-bestimmungsgemäßen Betriebes überschritten wurden und ein unerwünschtes Ereignis eingetreten ist.

6.3 PLT-Fehler

Ziel aller Sicherheitsüberlegungen ist es, die Eintrittshäufigkeit und das Ausmaß eines Schadens so weit wie möglich zu reduzieren. Für die Prozeßleittechnik bedeutet dies, die PLT-Ausrüstungen entsprechend zuverlässig und fehlerfrei zu konzipieren.

Dabei richtet sich der Aufwand zur Erreichung einer bestimmten Zuverlässigkeit bzw. Sicherheit nach den Schutzzielen und dem Gefährdungspotential der zu konzipierenden Anlage /Eute95/.

Die Fehlerquellen und –arten der PLT lassen sich in physikalisch-chemische und menschliche Fehler unterteilen. Eine Übersicht über die häufigsten Fehler dieser Art zeigt Bild 6-7 /Laub89/:

<u>physikalisch-chemische Fehler</u>

- Komponenten-Ausfälle
- Software-Verfälschung durch sporadische Hardwareausfälle
- elektromagnetische Störungen

menschliche Fehler

- Spezifikationsfehler im Pflichtenheft
- Software-Entwurfsfehler
- Codierfehler
- Hardware-Entwurfsfehler
- Schaltungs- und Verdrahtungsfehler
- Eingabe- und Bedienfehler
- Wartungsfehler
- Dokumentationsfehler
- Vandalismus oder Sabotage

Bild 6-7: Mögliche Fehler in PLT-Systemen

Oftmals werden die Grundlagen für Fehler bereits bei der Planung von PLT-Einrichtungen gelegt /Müll90/. Oberstes Ziel bei der Auslegung von verfahrenstechnischen Anlagen ist die Fehlervermeidung. Bezogen auf die Auslegung bedeutet dies /Köni87/, /Merk96/:

- Einsatz bewährter Geräte und bewährter Installationstechnik
- Überdimensionierung
- Fehlerfortpflanzungssperren
- Ausschaltung schädlicher Umgebungseinflüsse
- Einfacher, übersichtlicher Aufbau und wartungsfreundliche Installation der Schutzeinrichtungen. Möglichst ohne längeren Funktionsausfall prüfbar.

Eine genaue Beschreibung der einzelnen Maßnahmen findet sich in /Eute95/. Weitere Maßnahmen sind kurze Fehlererkennungszeiten durch häufige Plausibilitätsprüfungen sowie regelmäßige Inspektion und Wartung der Schutzeinrichtungen mit Sichtkontrolle, Funktionsprüfung sowie der Einsatz von qualifiziertem Personal in Betrieb und Instandhaltung /Merk96/.

Neben der Fehlervermeidung müssen im Rahmen der Planung von PLT-Einrichtungen ebenso die Prinzipien der Fehlerbeherrschung berücksichtigt werden. Bild 6-8 /Grei87/ zeigt die Maßnamen der Fehlervermeidung und -beherrschung im Überblick.

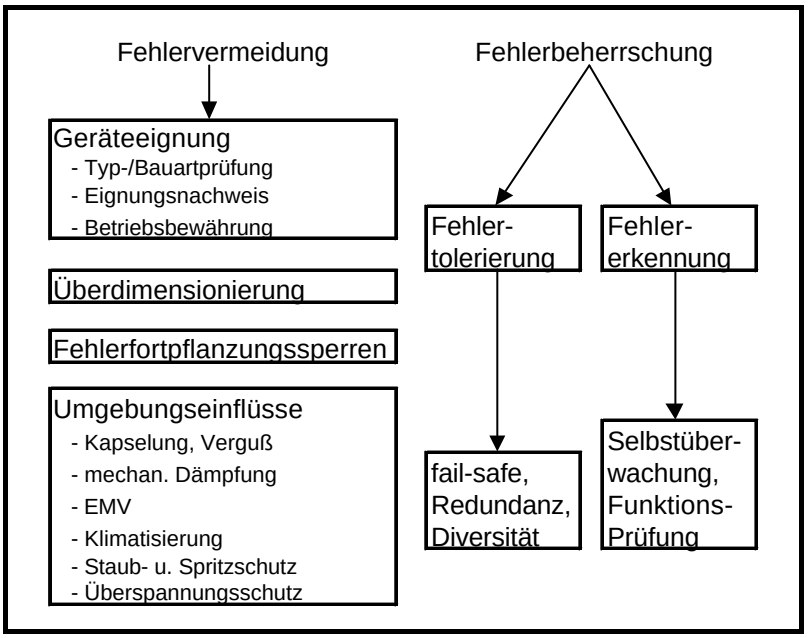


Bild 6-8: Maßnahmen der Fehlervermeidung und -beherrschung

Bei der Beherrschung von Fehlern unterscheidet man zwischen Fehlertolerierung und Fehlererkennung. Die Tolerierung umfaßt die Maßnahmen /Eute95/, /Grei87/:

- Fail-Safe
- Redundanz
- Diversität
- Bewertungsschaltungen

Unter der Voraussetzung, daß ein sog. ‚sicherer Zustand' für ein technisches System besteht, sollten Sicherheitssysteme immer ‚fail-safe' ausgelegt sein, d.h. eine Sicherungseinrichtung geht unter bestimmten, fest vorgegebenen Bedingungen, zum Beispiel Energieausfall, in einen sicheren Zustand über /VDI/VDE 3542/. Für ein Ventil kann dies etwa bedeutet, daß es prozeßgrößenabhängig im Ansprechfall voll geöffnet (z.B. Notablaß) oder geschlossen (z.B. Schnellschluß im Zulauf eines den Prozeßzustand weiter verschlechternden Reaktanden) wird.

Redundanz besagt, daß mehr technische Mittel zur Ausführung einer vorgegebenen Funktion zur Verfügung stehen, als dafür mindestens notwendig sind. Dabei unterscheidet man zwischen ‚kalter' und ‚heißer' bzw. ‚warmer' Redundanz /Biro97/. Für eine Pumpe bedeutet ‚kalte' Redundanz, daß eine zweite Pumpe erst angefordert

wird, wenn die erste ausfällt. Bei der ‚heißen' Redundanz ist die zweite Pumpe in Betrieb und übernimmt einen Teil der vorgegebenen Funktion. Für den Fall eines Ausfalls einer der beiden Pumpen erfüllt die andere dann die Funktion zu 100 Prozent.

Bei der Auslegung von Anlagen ist darauf zu achten, daß die Verfügbarkeit (der Schutzeinrichtungen) bzw. die Ausfallwahrscheinlichkeit (betriebliche Regelung) der Anregeebene (PLT-Technik) der der Ausführungsebene (Stellglieder) entspricht (siehe Abschnitt 8.2). Dies ist über den Redundanzgrad der PLT-Technik und der Verfahrenstechnik erreichbar. Bezogen auf die PLT-Technik ist die Ausgabe analoger oder binärer Signale über mehrere Kanäle oder die Verwendung zweier oder mehr Sensoren ein Beispiel für Redundanz. Im Falle der Verfahrenstechnik bietet sich beispielsweise die Verwendung eines zweiten Ventils an. Eine Erhöhung der Zuverlässigkeit ist ebenso über die Wahl qualitativ höherwertiger Ausrüstungen bzw. durch die Reduzierung der Funktionsprüfungsintervalle für die Schutzeinrichtungen (vgl. Gleichung (8-12)) erreichbar.

Um die Auswirkungen verborgener Konstruktionsfehler zu vermeiden, bietet sich die diversitäre Redundanz an /DIN/VDE2180_2/. Im Falle der o.g. heißen Redundanz des Pumpensystems sind die Pumpen dann verschiedenen Typs bzw. von verschiedenen Herstellern. Bezogen auf die PLT-Technik kann man Diversität in drei Kategorien gliedern /Eute95/:

1. physikalische Diversität,
2. meßtechnische Diversität,
3. Herstellerdiversität.

Zur Vermeidung der Gegenläufigkeit der sicherheitsbezogenen Verfügbarkeit und der Anlagenverfügbarkeit müssen zwei Forderungen erfüllt werden:

1. Steigerung der Verfügbarkeit der Sicherheitseinrichtungen zur Reduzierung der Nichtverfügbarkeit der Schutzeinrichtungen im Anforderungsfall.
2. Steigerung der Anlagenverfügbarkeit durch Vermeidung von Fehlanregungen der Schutzeinrichtungen.

Als Mittel hierzu eignen sich Bewertungsschaltungen (Majoritätsredundanz) /Biro97/. Bei einer m-von-n Bewertungsschaltung spricht die Sicherheitseinrichtung erst an, wenn mindestens m-Einrichtungen das Signal dafür geben. Bezogen auf die Vermeidung von Fehlalarmen und Fehlabschaltungen einer Anlage wird aus einer m-von-n Sicherheitsschaltung eine (n-m+1)-von-n Schaltung /Grei87/. Für den Fall einer 1-von-2 Schaltung folgt daraus für die Verfügbarkeit eine 2-von-2 Schaltung, also beide Kanäle dürfen kein Signal zum Abschalten geben, damit die Anlage läuft. Sicherheitstechnisch ist dies unbedenklich. Aus Sicht der Anlagenverfügbarkeit verhält es sich vice versa. Hier spielt nun neben gesetzlichen Anforderungen das Gefahrenpotential einer Anlage eine entscheidende Rolle. Bei Anlagen, die prozeßbedingt den unzulässigen Fehlbereich nach Bild 6-5 nicht erreichen können, kann es sinnvoll sein, die Schaltung in Bezug auf die Zuverlässigkeit auszulegen. Hier haben nicht zuletzt auch betriebswirtschaftliche Gesichtspunkte einen Einfluß. Darüber hinaus kann man über

$$m = \frac{n+1}{2} \qquad (6\text{-}1)$$

auch eine Gleichbehandlung von Sicherheit und Betriebsverfügbarkeit erreichen. Die voranstehenden Überlegungen setzen voraus, daß die Wahrscheinlichkeit für den Ausfall der gewünschten Funktion und die Wahrscheinlichkeit für ein fälschliches Ansprechen der Schutzfunktion in etwa gleich groß sind. Hierbei muß berücksichtigt werden, daß nicht jeder Fehlalarm zum Abschalten der Anlage führen muß. Von Bedeutung in diesem Zusammenhang sind somit nur Fehlalarme, die die Produktion der Anlage unterbrechen. Das niedrigste redundante Schaltungsbeispiel für eine Gleichbehandlung ist die 2-von-3 Schaltung. Wendet man (n-m+1)-von-n auf die 2-von-3 Schaltung an, so ergibt sich, daß sowohl für die Sicherheit als auch für die Verfügbarkeit einer Anlage die Wahrscheinlichkeiten den gleichen Wert besitzen.

Es ist aber durchaus möglich, daß eine erhöhte sicherheitstechnische Auslegung einer Teil- oder Gesamtanlage ebenfalls zur Erhöhung der Betriebsverfügbarkeit führt. So kann zwar durch vermehrtes zufälliges Ansprechen der Sicherungseinrichtungen die Anlage häufiger kurzzeitig abgefahren werden, was aber in keinem Verhältnis zur zeitlichen Nicht-Verfügbarkeit einer Anlage infolge eines Störfalles aufgrund eingesparter Sicherheitseinrichtungen steht.

Andererseits beanspruchen häufiges Ab- und Anfahren die Komponenten einer Anlage mehr als der bestimmungsgemäße Betrieb. Somit muß für jede Anlage individuell in Abhängigkeit des ihr innewohnenden Gefahrenpotentials abgewogen werden, welche Bewertungsschaltung zum Einsatz kommen soll.

Ziel dieser Arbeit ist nicht, den Zusammenhang zwischen Sicherheit und betrieblicher Verfügbarkeit verschiedener Anlagentypen aufzuzeigen, sondern vielmehr soll durch geeignete Wahl der Sicherheitseinrichtungen eine dem Gefahrenpotential der Anlage entsprechende Auslegung ermöglicht werden (vgl. Abschnitt 1.1 und 7.2).

Die Fehlererkennung gliedert sich in Selbstüberwachung und organisatorische Maßnahmen. Prinzipien der Selbstüberwachung sind:

- Ruhestromprinzip
- life-zero-Verfahren
- Antivalenzüberwachung
- Vergleich redundanter Kanäle
- Stellungsüberwachung
- gepulste Überwachung
- Kartenziehschleife
- Türkontaktüberwachung

Bild 6-9: Prinzipien der Selbstüberwachung

Eine genaue Erläuterung der Maßnahmen kann in /Eute95/ nachvollzogen werden. Die Wahl der Selbstüberwachungseinrichtungen ergibt sich zum einen aus dem im Rahmen der Planung üblichen Sicherheitsgespräch /Grei91/ zwischen Fachleuten verschiedener, den technischen Erfordernissen entsprechenden Fachrichtungen, zum anderen ergeben sie sich zum Teil direkt aus der Konfigurierung der verfahrens- und prozeßleittechnischen Ausrüstungen.

Die organisatorischen Maßnahmen werden unterschieden in /DIN/VDE2180_2/:

- ständige Überwachung
- Inspektion

- Wartung
- Instandsetzung

Dabei ist entscheidend, daß die durchgeführten Maßnahmen dokumentiert werden, damit Entscheidungen jederzeit nachvollziehbar sind. Lassen sich aktive Fehler direkt durch Fehlauslösung einer Schutzfunktion lokalisieren, können dagegen passive Fehler nur über Funktionsprüfungen erkannt werden. Daher ist es erforderlich, daß für jede Anlage genau definierte Prüfanweisungen existieren, die neben Art und Umfang der durchzuführenden Prüfungen auch Angaben zum Sollzustand bzw. Sollverhalten einer Schutzeinrichtung sowie Angaben über Spezifikationsmerkmale wie z.B.:

- Grenzwert
- Meßbereich
- Stellzeiten
- Verzögerungszeiten

enthalten müssen. Eine genaue Festlegung der Abstände zwischen den Prüfungen ist ebenso erforderlich.

Zur Verringerung der Anzahl menschlicher Fehlhandlungen sollte der Betreiber einer Anlage für jeden Typ der Instrumentierungsausrüstung genaue Wartungs- und Reparaturanweisungen sowie entsprechende Ersatzteile bereithalten und das Wartungs- sowie das Betriebspersonal mit den jeweiligen Besonderheiten vertraut machen /Ullr96/. Weiterhin spielt die Bediensicherheit technischer Systeme eine entscheidende Rolle. Hierauf muß bereits während der Planungsphase bei der Auswahl der Instrumente für die Anlage geachtet werden.

6.4 Grenzen der Prozeßleittechnik

Die zunehmende Automatisierung in der chemischen Industrie durch die Fortschritte der Prozeßleittechnik hat zu einer Erhöhung der Sicherheit in der chemischen Industrie geführt. Dies gilt insbesondere für kontinuierliche Verfahren. Aber auch Batch-Prozesse profitieren von den Entwicklungen, da die Überwachung wichtiger Prozeßparameter und die Auslösung von Schutzfunktionen automatisiert wurden.

Schwierigkeiten bestehen weiterhin bei Mehrstoffanlagen. Neben der Wirtschaftlichkeit einer voll automatisierten Mehrstoffanlage müssen hier nicht nur organisatorische, sondern auch technische Probleme bedacht werden. Es werden bei jeder Reaktion andere Prozeßparameter eingestellt bzw. sind sogar andere Meßverfahren für deren Erfassung erforderlich.

Trotz steigender Zuverlässigkeit der technischen Systeme darf nicht außer acht gelassen werden, daß Überwachungs- und Schutzausrüstung nur gegen die bei deren Auslegung prognostizierten Störungen wirken. Somit muß bei der Evaluierung möglicher Szenarien entsprechend sorgfältig vorgegangen werden.

Bei der Schulung des Personals ist darauf zu achten, daß die Grenzen der Automatisierung dem Personal vermittelt werden. Trotz scheinbarer Sicherheit (die Prozeßparameter befinden sich in der Anzeige innerhalb ihrer Toleranzen) arbeitet kein technisches System garantiert fehlerfrei. Mögliche Abweichungen von Sollwerten infolge von z.B. Planungsfehlern oder Betriebsstörungen müssen auch weiterhin sicher vom Personal erkannt werden. Die richtigen Reaktionen des Personals auf diese Abweichungen müssen regelmäßig durch Schulungen trainiert werden.

6.5 Instrumentierungsbeispiele

Als Vorgriff auf Abschnitt 7.4 und 8.3 werden im folgenden zwei typische Instrumentierungsbeispiele aus der Industrie gezeigt. Als Beispiel für die verschieden redundante Gestaltung eines Sicherheitssystems wird hier der Schutz gegen Überfüllung bei einem Methanol-Vorlagebehälter (Bild 6-10) und einem Lagertank für Isocyanate (Bild 6-11) dargestellt.

Im Falle des Methanol-Vorlagebehälters reicht eine Sicherheitsschaltung (eingekreist) aus. Beim Lagertank hingegen wird der Füllstand redundant (eingekreist) überwacht. Der Grund hierfür liegt am höheren Gefahrenpotential des Lagertanks.

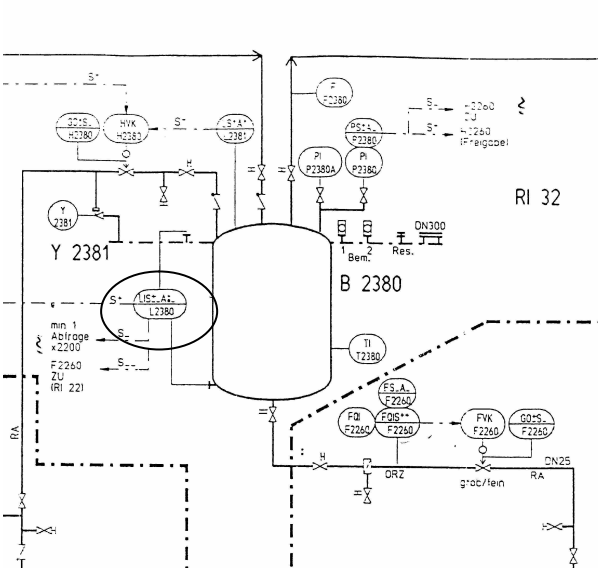


Bild 6-10: Methanol-Vorlagebehälter

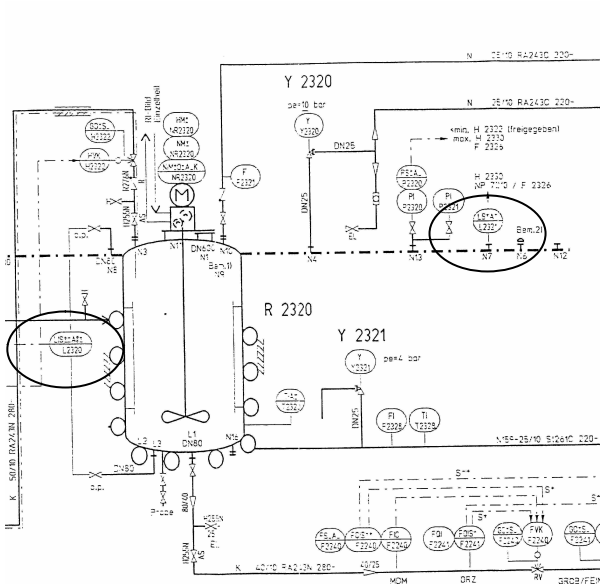


Bild 6-11: Isocyanat-Lagertank

Beispiele wie diese lassen sich zahlreich in der chemischen Industrie finden. Dabei steigt der Ausrüstungsgrad hinsichtlich Redundanz und Diversität mit zunehmendem Gefahrenpotential der Anlagen. Ein erhöhtes Gefahrenpotentials stellt somit höhere Ansprüche an die Verfügbarkeit der Sicherheitssysteme. Dies findet auch in geltender Gesetzgebung seinen Niederschlag. Hier sei noch einmal in Anlehnung an Kapitel 1 auf die Störfallverordnung /Stör00/, insbesondere auf § 4, Abs. 3 verwiesen, indem Anforderungen an die Ausstattung der Anlage mit prozeßleittechnischen Ausrüstungen gefordert wird, „die, soweit dies sicherheitstechnisch geboten ist, jeweils mehrfach vorhanden, verschiedenartig und voneinander unabhängig sind." Ziel dieser Forderung ist es, die Anlage hinsichtlich der „Auslegung, (...) Errichtung sowie (...) Betrieb und (...) Wartung (...) ausreichend sicher und zuverlässig“ (§ 9 Abs. 1 Satz 3) zu gestalten. Wie dieser Zustand im speziellen zu erreichen ist, wird jedoch nicht vorgeschrieben. Somit bleibt es den Experten der Betriebe überlassen, in Zusammenarbeit mit der genehmigenden Behörde einen geeigneten Weg zu finden.

Im Rahmen dieser Arbeit wurde ein Ansatz gewählt, der den Redundanz- und Diversitätsgrad der Betriebs- und Sicherheitssysteme in Abhängigkeit vom Gefahrenpotential der Anlage festlegt. Die Lösung SafeCAD’s wird in Kapitel 8 vorgestellt. In Abschnitt 10 wird der in Bild 6-10 gezeigte Vorlagebehälter näher erläutert und anschließend mittels SafeCAD abgebildet und mit der Industrieanlage verglichen.

7 Abschätzung des Gefahrenpotentials

Die in den Anlagen der chemischen Industrie verwendeten Stoffe und unterschiedlichen Verfahren führen, in Abhängigkeit von ihrer Gesamtmasse und den Verfahrensparametern, zu einem entsprechend unterschiedlichen Gefahrenpotential einer Chemieanlage. Daher ist es notwendig, Chemieanlagen nicht nur bezüglich ihres Gefahrenpotentials zu klassifizieren, sondern auch die möglichen Abweichungen vom Normalbetrieb zu evaluieren. Bei deren Nichtbeherrschung kann das Gefahrenpotential wirksam werden und sich durch eventuelle Nebenreaktionen erhöhen. Zusätzlich können geeignete Maßnahmen festgelegt werden, die die Beherrschung des Verfahrens auch bei Störungen zu gewährleisten vermögen.

7.1 Bestimmung des Gefahrenpotentials

Das Gefahrenpotential wird bestimmt durch die Stoffeigenschaften, ihre gehandhabten oder gelagerten Massen und ihre Reaktivität. Oftmals führen erst die Prozeßbedingungen (Druck, Temperatur) zur Reaktionsneigung der Stoffe. Dies ist gewollt, da ohne entsprechende Reaktivität keine Reaktion erfolgt und somit keine Stoffumwandlung stattfinden kann. Anlagensicherheit beinhaltet, das jeweils vorhandene Gefahrenpotential richtig abzuschätzen und geeignete Maßnahmen auszuwählen, die das Gefahrenpotential am Wirksamwerden hindern, z.B. durch einen sicheren Einschluß aller gehandhabten Stoffe.

Die Höhe des Gefahrenpotentials ist somit abhängig /Krem78/:

- von den Gefahren durch Stoffeigenschaften, wie
  - Toxizität, Brennbarkeit etc.,
  - von der Masse der vorhandenen beziehungsweise im Störfall zu erwartenden Stoffe und
  - von der Reaktivität der Stoffe,
- von den Gefahren aus dem Verfahrensablauf (hohe und niedrige Temperaturen oder Drücke).

Zur Ermittlung des Gefahrenpotentials bieten sich verschiedene Möglichkeiten an. So ist es denkbar, eine Kategorisierung anhand der in der Anlage verwendeten bzw. produzierten Stoffe vorzunehmen /Cher99/. Eine Einteilung kann auch über das Si-

cherheitsdatenblatt nach § 14 der Gefahrstoffverordnung /Vero00/ erfolgen, wobei es zu der Stoffliste gemäß § 4a der Gefahrstoffverordnung bereits eine nationale Ergänzung /Gefahr99/ gibt, die dann ebenfalls beachtet werden muß. Weiterhin ist eine Einteilung nach möglichen, gefährlichen chemischen Reaktionen /Roth90/ denkbar. Der Nachteil der genannten Wege besteht darin, daß die verwendeten Massen, sowohl bei der Herstellung als auch im Lagerbereich, nicht beachtet werden.

Des weiteren könnte eine Klassifizierung anhand von Unfallstatistiken erfolgen /Kier83/, wobei hier in der Regel die Anzahl der zugrundeliegenden Vorfälle zu gering ist, um alle relevanten Ereignisabläufe zu beobachten /Haup85a/.

Wesentlich sinnvoller ist die Anwendung einer bereits erprobten und weit verbreiteten Methode /Lees96_2/, wie dem Fire & Explosion Index des Konzerns Dow Chemical. Dieser Index wurde hier gewählt.

Bereits 1964 wurde der F&EI bei Dow Chemical eingeführt und seitdem ständig weiterentwickelt. Das Index-Verfahren wird zunehmend auch außerhalb des Konzerns angewendet und ermöglicht es, neben den Punkten /Fire94/

1. **Quantifizierung** des erwarteten Schadens aus möglichen Explosionen, Brand- und Reaktivitätsstörfällen auf realistische Weise,
2. **Identifizierung** der Anlagenteile, die mit einer gewissen Wahrscheinlichkeit zum Entstehen oder zur Ausweitung eines Störfalls beitragen und
3. **Bewußtmachen** des mit dem Index ermittelten Risikopotentials beim Management,

Aussagen über das Schadenpotential der untersuchten Prozeßeinheit zu treffen und damit die Grundlagen für seine Minderung bereitzustellen. Ursprünglich wurde die Methode zu Versicherungszwecken entwickelt. Durch die Berechnung eines Zahlenwertes, F&EI genannt, ist es möglich, das Gefahrenpotential der betrachteten Anlage abzuschätzen.

Die Vorgehensweise bei der Bestimmung des F&EI ist in Bild 7-1 dargestellt; sie läßt sich wie folgt beschreiben: Die Anlage wird zuerst in Prozeßeinheiten (z.B. Destillati-

ons- oder Absorptionskolonne, Reaktor, Pumpe, Ofen etc.) zerlegt. Danach wird unter Berücksichtigung verschiedener Einflußfaktoren wie Masse und physikalischer Eigenschaften der eingesetzten Stoffe, Betriebsbedingungen usw. die Einheit mit dem größten Gefahrenpotential für die Anlage identifiziert. Der F&EI wird dann für diese Prozeßeinheit bestimmt. Der dabei ermittelte höchste Wert wird gleichzeitig als F&EI der gesamten Anlage gesetzt.

Der F&EI wird aus einem Materialfaktor (MF für Reaktivität und Entflammbarkeit eines Stoffes), zwei Malusfaktoren (F_1 für allgemeine Prozeßgefährdungen und F_2 für spezielle Prozeßgefährdungen) und einem Faktor F_3 für Gefährdungen durch diese Prozeßeinheit, der sich aus Multiplikation von F_1 und F_2 ergibt, gebildet. Das Produkt aus Materialfaktor und F_3, also $MF \cdot F_3$, ergibt den F&EI.

Der Ablauf der Berechnung des Index wird im folgenden Bild gezeigt. Die ebenfalls im Dow-Index enthaltenen Gutschriften für die Qualität der technischen Auslegung und Sicherheitseinrichtungen (gestrichelter Bereich in Bild 7-1) werden im vorliegenden Zusammenhang nicht benötigt. Vielmehr ist die Bereitstellung einer qualitativ hochwertigen Auslegung der Betriebs- und Sicherheitssysteme Ziel des Verfahrens SafeCAD.

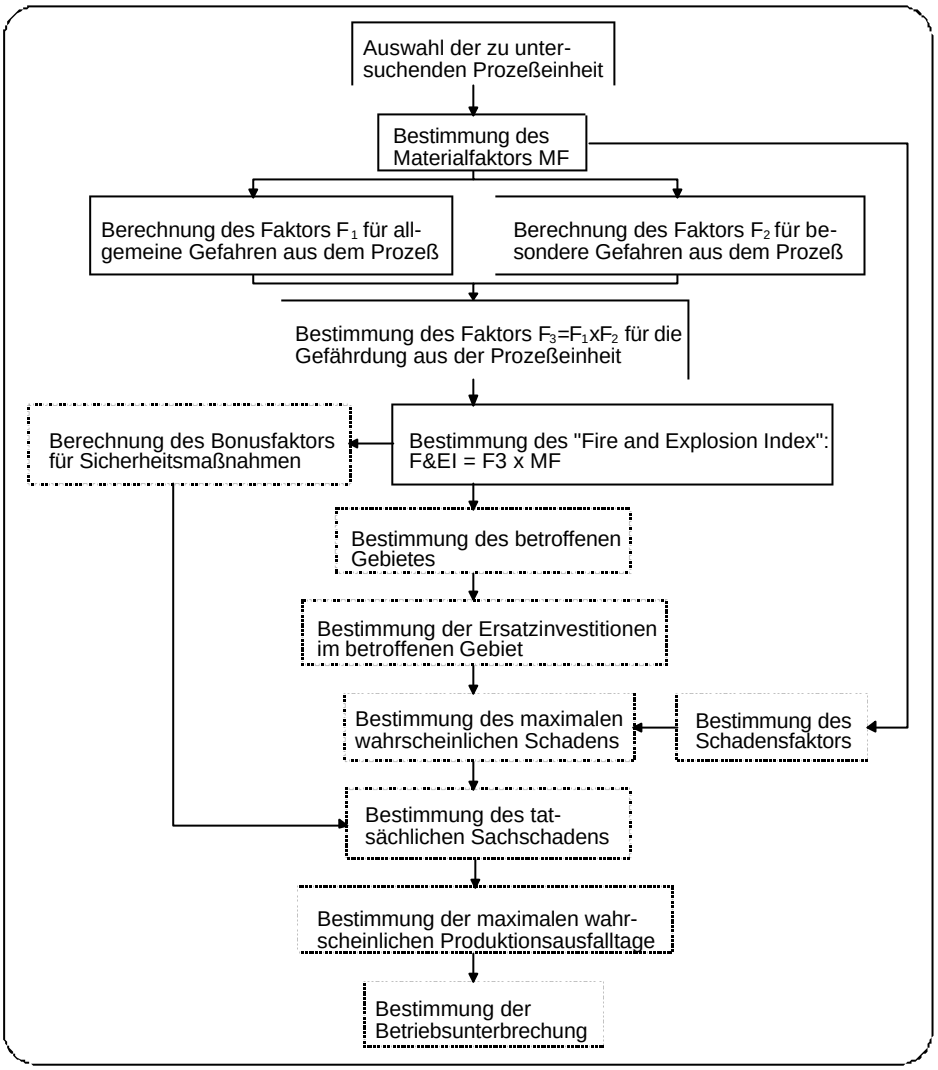


Bild 7-1: Berechnung des Fire and Explosion Index mit Verdeutlichung der genutzten Schritte

Im einzelnen bedeuten die Schritte zur Ermittlung des F&EI:

<u>Auswahl der zu untersuchenden Prozeßeinheit</u>

Bei der Auswahl der geeignetsten Prozeßeinheit sollten größere Aggregate wie z.B. Reaktor, Verdampfer etc. gewählt werden. Kriterien bei der Auswahl sind dabei:

- chemisches Energiepotential (Materialfaktor),
- Menge gefährlicher Stoffe in der Prozesseinheit,
- Prozeßdruck und –temperatur,
- etwaige frühere Probleme, die zu Bränden und Explosionen führten,
- Einheiten, die essentiell für den Anlagenbetrieb sind, z.B. thermische Oxidierung.

Materialfaktor

Dieser Faktor enthält Bewertungen, welche die Entflammbarkeit und Reaktivität (Instabilität) erfassen; seine Bestimmung erfolgt mit Hilfe von Erfahrungswerten. Die Werte beziehen sich auf Umgebungstemperatur, werden aber zur Berücksichtigung der Erhöhung des Gefahrenpotentials angepaßt, falls der Stoff bei höheren Temperaturen vorliegt. Zur Identifizierung des Faktors sind Angaben zu

- Flammpunkt,
- Siedepunkt und
- Dicke (bei brennbaren Feststoffen) oder Form (z.B. Faser, Puder, Granulat etc.)

erforderlich.

Allgemeine Prozeßgefährdungen

In diesem Zusammenhang werden folgende fünf Punkte betrachtet, die bei Störfällen in der Vergangenheit eine große Rolle gespielt haben:

- exo- und endotherme chemische Reaktionen,
- Stoffhandhabung und –transport,
- eingehauste oder in Hallen befindliche Prozesseinheiten,
- Anlagenzugang,
- Abfluß- und Leckagekontrolle der Chemikalien.

Spezielle Prozeßgefährdungen

Die speziellen Gefährdungen tragen vor allem zur Wahrscheinlichkeit eines Störfalls bei. Aufgrund der Erfahrung werden die nachstehenden speziellen Bedingungen aufgeführt, die sich als wesentliche Gründe für Brände und Explosionen erwiesen haben:

- toxische Materialien,
- Betrieb bei Unterdruck,
- Flammbereich,
- Staubexplosion,

- Betrieb bei hohen Drücken,
- tiefe Temperaturen bei gleichzeitigem Vorhandensein kohlenstoffhaltiger Stahlteile (z.B. Behälter, Rohrleitungen etc.),
- Menge entflammbarer oder instabiler Stoffe,
- Korrosion und Errosion,
- Leckagen,
- Wärmetauscher und
- rotierende Geräte.

Der Vorteil des F&EI ist, daß neben den Stoffeigenschaften auch anlagenspezifische Eigenschaften berücksichtigt werden. Zudem wurde in /Stei98/ festgestellt, daß der F&EI für die Anwendung in der Auslegungsphase einer Anlage geeignet ist. Die Art der Auslegung kann zu einer Reduzierung der Gefährdung durch die Anlage beitragen, wobei dies allerdings analog für eine Erhöhung bei entsprechend negativen Anlagenspezifikationen gilt. Ein weiterer Vorteil des F&EI ist die Möglichkeit, bei Vorhandensein mehrerer Verfahren zur Herstellung eines Produktes dasjenige mit dem geringsten Gefahrenpotential auszuwählen, so daß neben der Maximierung der Sicherheit unter Umständen auch die Kosten für eine neue Anlage schon im Vorfeld der Planung reduziert werden können.

Die Skala des F&EI reicht von 1 bis ca. 200. In /Fire94/ werden hierfür die Kategorisierungen gemäß Tabelle 7-1 bezüglich des Gefahrenpotentials vorgeschlagen:

F&EI Bereich	Gefahrenpotential-Kategorie
1 - 50	niedrig
51 - 81	moderat
82 - 107	mittel
108 - 133	hoch
> 133	sehr hoch

Tabelle 7-1: Gefahrenpotentiale nach Dow

Im nachfolgenden Abschnitt wird die Anpassung des F&EI an die neue Vorgehensweise beschrieben.

7.2 Modifizierung des Fire and Explosion Index für die Vorgehensweise

Im Rahmen dieser Arbeit wird die Kategorisierung des Gefahrenpotentials im Gegensatz zur Einteilung nach DOW (siehe Tabelle 7-1) leicht abgewandelt. Es werden jeweils die zweite und dritte sowie die vierte und fünfte Kategorie zusammengefaßt, so daß das Gefahrenpotential einer Chemieanlage abweichend vom F&EI in die drei Kategorien der Tabelle 7-2 eingeteilt wird. Grund dafür ist, daß eine dreifache Abstufung mögliche Systemauslegungen als ausreichend erachtet wird.

F&EI Bereich	Gefahrenpotential-Kategorie
1 - 50	I = niedrig
51 - 107	II = mittel
> 107	III = hoch

Tabelle 7-2: Gefahrenpotentiale der neuen Methodik

In /Stei98/ wurde beim Vergleich mehrerer Analysemethoden zur Evaluierung des Gefahrenpotentials verfahrenstechnischer Anlagen festgestellt, daß der F&EI die tatsächliche Gefährdung „*völlig überschätzt*“. Sollte sich dies im Verlauf der Anwendung von SafeCAD ebenso herausstellen, kann die Einstufung entsprechend verändert werden.

Den Gefahrenkategorien gemäß Tabelle 7-2 werden die verschiedenen, aus den R&I – Fließbildern identifizierten Teilsysteme mit entsprechendem Redundanzgrad zugeordnet.

7.3 Ermittlung möglicher Abweichungen vom bestimmungsgemäßen Betrieb

Zur Ermittlung der Möglichkeiten des Wirksamwerdens des Gefahrenpotentials, also konkreter Gefährdungen durch:

- technisches Versagen wie
  - Ausfall von Kühlung oder Rührer während einer chemischen Reaktion,
  - Störungen an Meß- und Regelgeräten, oder
- menschliches Versagen (Bedienungsfehler an der Apparatur, z.B. falsche Zugabe von Reaktionskomponenten),

bieten sich mehrere Methoden, wie in Kapitel 1 genannt, an.

In der Industrie hat sich dabei das PAAG-Verfahren etabliert. Es wurde in den siebziger Jahren bei ICI[6] in England unter dem Begriff HAZOP (Hazard and Operability Study) entwickelt und ist besonders gut für Chemieanlagen geeignet, da die Fragen nicht nur Komponentenausfälle aufdecken, sondern auch chemiespezifische Gefährdungen, wie z.B. Inkompatibilitäten von Stoffen. Neben der Identifizierung möglicher Gefahren und ihrer Ursachen werden im Rahmen einer Analyse auch geeignete Gegenmaßnahmen festgelegt.

Das Verfahren wird von Gruppen, bestehend aus Experten verschiedener Fachrichtungen, durchgeführt. Ziel ist das Aufdecken der Gründe möglicher Abweichungen der Prozeßparameter von ihren nominalen Werten beim bestimmungsgemäßen Betrieb. Um geeignete Maßnahmen zur Einhaltung des bestimmungsgemäßen Betriebes treffen zu können, müssen zuerst die Störungen und deren Auswirkungen erkannt werden. Dazu wird die Anlage in Teilbereiche zerlegt und deren Sollfunktionen charakterisiert. Die Erkennung von Störungen erfolgt durch die systematische Suche von Abweichungen von der Sollfunktion eines Teilbereichs anhand einer Leitwort-Abfragetabelle, die jeweils an die entsprechende Sollfunktion angepaßt wird. Ursprünglich wurden die Leitworte für die Anwendung auf die die Teilbereiche durchziehenden Rohrleitungen entwickelt, da Abweichungen in den Aggregaten sich im Rohr stromabwärts zeigen. Man kann diese Leitworte aber auch direkt auf Aggregate wie „Behälter" anwenden. Das Leitwort „mehr" in Verbindung mit einem zu hohen Druck im Behälter kann zum Beispiel das mögliche Durchgehen einer Reaktion in Folge falscher oder zu hoher Reaktandenzuführung aufdecken. Die sieben Leitworte des PAAG-Verfahrens werden in Tabelle 7-3 erläutert.

[6] Imperial Chemical Industries

Leitworte	Bedeutung	Kommentare
Nein oder **Nicht** (Kein oder Keine)	Verneinung der Sollfunktion	Kein Teil der Sollfunktion wird ausgeübt, aber es geschieht auch nichts anderes
Mehr	Quantitativer Anstieg	Mehr oder Weniger beziehen sich auf : – Quantitative Größen z.B. Temperatur, Druck, Mengenstrom (zu hoch, zu tief, zuviel, zu wenig, zu gering etc.) Funktionen z.B. Erwärmen, Reagieren
Weniger	Quantitative Verringerung	
Sowohl als auch	Qualitativer Anstieg	Die Sollfunktion wird erfüllt, jedoch passiert zusätzlich auch etwas anderes wie mehr Komponenten im System, z.B. zusätzliche Phase, Dampf, Feststoffe, Verunreinigungen, Luft, Wasser, Korrosionsprodukte.
Teilweise	Qualitative Verringerung	Nur einige Teile der Sollfunktion werden erreicht, teilweise oder gänzliches Fehlen eines Stoffes in einem Stoffgemisch.
Umkehrung	logische Umkehrung der Sollfunktion	Bei Vorgängen: - entgegengesetzte chemische Reaktion - entgegengesetzte Fließrichtung
Anders als	andere Betriebszustände	- ungewollte physikalische Vorgänge (Erwärmen statt Abkühlen) - anderer Stoff, anderer Zustand

Tabelle 7-3: Die 7 Leitworte des PAAG-Verfahrens /Bart90/, /Haup94a/

Mit Hilfe der Leitworte werden Gedankenexperimente durchgeführt, um hypothetische Störungen zu identifizieren. Für nicht auszuschließende Störungen mit relevanten Auswirkungen werden wirksame Gegenmaßnahmen erarbeitet. Nachteil des PAAG-Verfahrens ist der hohe Zeitaufwand für die Durchführung einer vollständigen Analyse.

7.4 Modifizierung des PAAG-Verfahrens für die Vorgehensweise

Die Teilanlage wird qualitativ auf mögliche Gefährdungen untersucht. Das heißt, mögliche Abweichungen vom bestimmungsgemäßen Betrieb werden durch qualitative Ausdrücke (z.B. Druck zu hoch/zu niedrig, Temperatur zu hoch/zu niedrig etc.) beschrieben. Im einzelnen sind dies die folgenden Gefährdungen, die als Untermodule (siehe Abschnitt 9.1) angeboten werden:

- Überdruck
- Unterdruck
- zu hohe Temperatur
- zu niedrige Temperatur
- Überfüllung
- zu niedriger Füllstand
- Versagen der Umschließung (z.B. Behälterversagen)
- falsche Zusammensetzung des Aggregateinsatzes
- ungenügende Vermischung
- Hochwasser im Anlagenbereich

Bild 7-2: Untermodule zur sicherheitsgerichteten Auslegung von Teilanlagen

Die im § 3 der Störfallverordnung /Stör00/ geforderte Betrachtung möglicher Gefährdungen infolge des Eingriffs Unbefugter wird nicht vom System erfaßt. Hierfür eine geeignete Lösung im Rahmen SafeCAD's zu entwickeln, ist auch schwer möglich. In diesem Zusammenhang spielt die Umgebung der Anlage, insbesondere die Lage des Unternehmens sowie Nachbaransiedlungen eine wichtige Rolle. Dies alles generell in ein System zu integrieren, ist nicht mit hinreichender Genauigkeit durchführbar. So bleibt hier nur die Einzelfallbetrachtung.

Da SafeCAD gerade in einem möglichst frühen Stadium der Anlagenplanung zum Einsatz kommen soll, in dem möglicherweise noch nicht alle exakten Werte bezüglich des chemischen Gleichgewichts, der Pumpenkennlinien etc. vorliegen, bietet sich der qualitative Ansatz an. Diese Vorgehensweise hat darüber hinaus den Vorteil, daß sie im Gegensatz zum quantitativen Ansatz leichter verständlich ist. Dies soll nicht die Notwendigkeit der numerischen Modellierung von Temperaturverläufen innerhalb des Reaktionsteils der Anlage in Frage stellen, da diese u.a. ein Muß für die Auslegung der Kühl- und Heizkreisläufe sind. Sicherheitstechnisch interessiert jedoch vornehmlich, ob Grenzwerte überschritten werden können oder nicht, /DIN/VDE2180_2/. Ist dies der Fall, dann müssen im folgenden geeignete Maßnahmen zur Vermeidung oder Beherrschung dieser Fehlzustände evaluiert werden. In diesem Zusammenhang spielt dann auch die Zeit bis zur Erreichung der Grenzwerte und die maximal mögliche Abweichung der Parameter (Druck, Temperatur etc.) eine

Rolle. Dies kann durch leichte Überschlagsrechnungen wie in Kapitel 5 gezeigt, unterstützt werden.

Auf Basis mehrerer PAAG Analysen wurde eine sicherheitsgerichtete Fragestruktur entwickelt, die es dem Anwender neben der Identifizierung denkbarer Gefährdungen ermöglicht, geeignete Sicherheitseinrichtungen auszuwählen.

Der Fragekatalog bezieht sich auf Funktionseinheiten. Daher wird die Anlage bis auf diese Ebene zerlegt. Dadurch wird die Anlage für die sicherheitstechnische Betrachtung überschaubarer /Ratg98/. Der Fragekatalog geht dabei heuristisch vor. Es werden mögliche betriebliche Abweichungen und deren Folgen aufgezeigt. Tabelle 7-4 zeigt ein Beispiel.

		Mögliche konstruktive Maßnahmen		
Betriebsabweichungen	**Mögliche Fehlzustände**	**Inhärente/passive Maßnahmen**	**Aktiv**	**Organisatorisch**
Überdruck	Überfüllung mit Flüssigkeit führt zu Überdruck infolge Wärmeausdehnung	• Auslegung des Behälters ermöglicht maximale Druckbelastung. • Befüllung nur mittels offenem Überlaufventil oder Überlaufleitung.	• Notentlastungseinrichtung. • Verriegelung der Zuführungsleitung, um Überfüllung zu vermeiden.	• Anweisungen zur Überwachung des Füllstandes während der Befüllung. • Überprüfung der Füllkapazität des Behälters vor der Befüllung. • Alarm bei hohem Füllstand mit Anweisungen zur Vermeidung von Überfüllung.

Tabelle 7-4: Beispiel der PAAG-basierten Analyse

Auch wenn es nicht möglich ist, a priori alle denkbaren Fehlzustände einer Anlage zu evaluieren, so hilft der auf Erfahrung aufbauende Katalog, die Wiederholung von Fehlern zu vermeiden. Weiterhin ist es Ziel der Anwendung des Fragekataloges, qualitative Aussagen hinsichtlich /Bart88/

- der Spezifizierung der Anlagenteile, bei denen unzulässige Fehlzustände (vgl. Bild 6-5) möglich sind,
- der Ursachen, die zu den Fehlzuständen führen können und
- der Festlegung von Maßnahmen (passiv, aktiv, organisatorisch) zur Vermeidung der Fehlzustände

zu erhalten. Dabei wird vom Anwender die Möglichkeit des Auftretens der Fehlzustände abgeschätzt. Für die als wahrscheinlich betrachteten Fehlzustände kann der Anwender dann aus verschiedenen Sicherheitsmaßnahmen die geeignetsten auswählen. Da die Maßnahmen praxiserprobt sind, können somit aufgrund der Erfahrungen aus der chemischen Industrie Auslegungsfehler von vornherein vermieden werden. Es wird, wie in Kapitel 5.3 beschrieben, unterschieden nach passiven/inhärenten, aktiven und organisatorischen Maßnahmen.

Grundlage für die Abschätzung möglicher Gefährdungen sind Grund- und Verfahrenfließbilder der Anlage und –soweit vorhanden– Datenblätter der technischen Einrichtungen (Pumpen etc.) und die Betriebsdaten der Versorgungssysteme (Druckluft etc.).

Wird für das oben angeführte Beispiel (siehe Tabelle 7-4) als aktive Maßnahme eine „Notentlastungseinrichtung“ ausgewählt, so wird diese im nächsten Schritt weiter spezifiziert. Hier gilt es nun festzulegen, welche Entlastungseinrichtung vor der Gefährdung durch „Überdruck“ schützen soll (z.B. Sicherheitsventil, Berstscheibe). Auf Grundlage der in der Anlage gehandhabten Stoffe und deren Aggregatzustände werden von SafeCAD Vorschläge dazu angeboten. Auch hier bleibt die letztendliche Wahl dem Anwender überlassen.

Zur Unterstützung bei der Auswahl der entsprechenden Sicherheitsmaßnahmen kann sich der Anwender sogenannter Hilfetexte bedienen. Diese sind jeder Betriebsabweichung und den zugehörigen Maßnahmen hinterlegt. Ebenso sind Hinweise auf firmeninterne Regelungen und Richtlinien sowie Gesetzesvorgaben möglich.

8 Verfügbarkeit von Sicherheitssystemen

In diesem Kapitel wird im ersten Abschnitt die zur Untersuchung der Verfügbarkeit von Sicherheitssystemen verwandte Methode, die Fehlerbaumanalyse, näher vorgestellt. Im zweiten Abschnitt wird erläutert, wie SafeCAD den Redundanz- und Diversitätsgrad der betrieblichen und sicherheitstechnischen Einrichtungen festlegt. Im letzten Abschnitt wird beschrieben, wie die Ausgewogenheit hinsichtlich der Verfügbarkeit innerhalb einer Meßkette, bestehend aus Sensor (Anregeebene), Verarbeitungslogik (z.B. Wandler) sowie der Ausführungsebene (z.B. Stellglied) erreicht wird.

8.1 Fehlerbaumanalyse

Mit der Fehlerbaumanalyse können sowohl qualitative als auch quantitative Aussagen über den Zustand eines technischen Systems getroffen werden. Dazu wird ein unerwünschtes Ereignis definiert (z.B. "Überdruck" bei einem Behälter oder Versagen der Kühlung) und nach allen dazu führenden Ursachen gesucht. Die Ursachen können dabei sowohl technischer Natur (z.B. Ausfall einer technischen Komponente) sein als auch menschliches Fehlverhalten (z.B. in Form falscher Handlungen im Anschluß an eine Alarmierung) beinhalten. Diese Verknüpfungen sind deterministisch; zu probabilistischen Aussagen gelangt man, wenn Wahrscheinlichkeiten für die Komponentenausfälle eingesetzt werden. Die logischen Verknüpfungen können vorteilhaft dargestellt werden, indem man Boole'sche („UND"- sowie „ODER"-Gatter) zur Beschreibung der Komponentenzustände und des Systemzustands heranzieht /Barl75/, /Schn99/.

Man benutzt die folgende Definitionen:

$$x_n = \begin{cases} 1 \text{ , wenn die Komponente n ausgefallen ist} \\ \\ 0 \text{ , wenn die Komponente n funktioniert} \end{cases} \qquad (8\text{-}1)$$

für die Komponenten und

$$\Psi(x_1,\ldots,x_N)=\begin{cases}1\text{ , wenn das System ausgefallen ist}\\ \\ 0\text{ , wenn das System funktioniert}\end{cases} \qquad (8\text{-}2)$$

für die Strukturfunktion.

Im allgemeinen ist die Strukturfunktion monoton nicht fallend (isoton). Dies folgt daraus, daß ein System, das ausgefallen ist, im allgemeinen nicht wieder zu funktionieren beginnt, wenn eine weitere Komponente ausfällt. Anders ausgedrückt, ein System, das intakt ist, fällt nicht aus, wenn eine ausgefallene Komponente wieder zu funktionieren beginnt.

Nicht isotone Strukturfunktionen treten auf, wenn die Negation von Primärereignissen in den Fehlerbaum eingeführt wird, so daß er sowohl das Ereignis selbst als auch seine Negation enthält (vgl. /Chu80/, /Pagè86/). Die Negation erfordert die Bildung des komplementären Ereignisses, aus x_n wird $\overline{x}_n = 1 - x_n$.

Die im weiteren behandelten Verfahren gelten für isotone Strukturfunktionen. Sie treffen aber auch für nicht isotone Strukturfunktionen zu, wenn dies nicht ausdrücklich ausgeschlossen wird.

Bevor die Darstellung von Systemen durch Boole‘sche Funktionen erläutert wird, muß noch eine wichtige Eigenschaft Boole‘scher Variabler vorgestellt werden, die Idempotenzeigenschaft:

$$x_n^m = x_n \qquad (\mathrm{m} \neq 0) \qquad (8\text{-}3)$$

Diese Eigenschaft folgt unmittelbar daraus, daß Boole'sche Variablen nur die beiden Werte 0 und 1 annehmen können.

Der Minimalschnitt eines Systems ist die Kombination von Elementen, deren gemeinsamer Ausfall gerade ausreicht, um einen Systemausfall auszulösen. In der Regel existiert für ein technisches System mehr als ein Minimalschnitt, so daß durch die Ermittlung der Minimalschnitte eines Fehlerbaums Aussagen über die Struktur des

durch den Baum abgebildeten Systems getroffen werden können. Es kann festgestellt werden, welche Komponenten am häufigsten in den verschiedenen Minimalschnitten auftreten oder ob es Komponenten gibt, durch deren Versagen allein das unerwünschte Ereignis eintritt.

Dieser barrierefreie Fall, indem das Versagen nur einer Komponente zum unerwünschten Ereignis führt, kann dann z.B. durch Redundanz abgeschwächt werden. Bild 8-1 zeigt die Zusammenhänge schematisch.

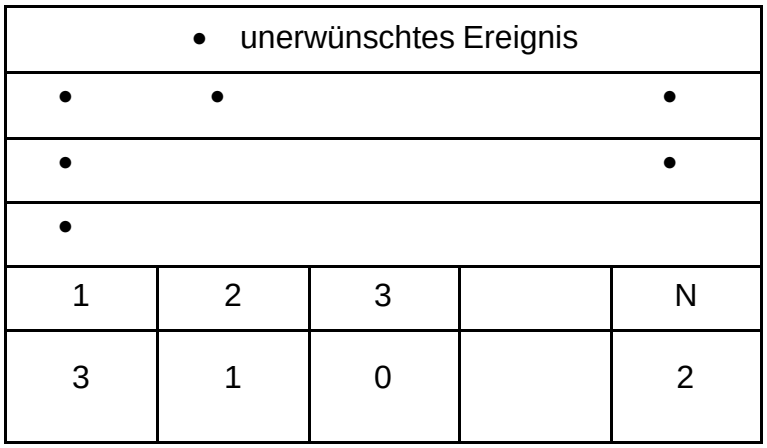


Bild 8-1: Barrieren gegen das Auftreten unerwünschter Ereignisse /Haup88b/

Da aber trotzdem in dem Fall des Minimalschnittes mit nur einer Komponente bei entsprechend hoher Komponentenqualität die Versagenswahrscheinlichkeit geringer sein kann als bei einem Minimalschnitt mit zwei oder mehr Komponenten schlechterer Qualität, ist die quantitative Auswertung des Fehlerbaumes sinnvoll. Denn nur so lassen sich diese Zusammenhänge aufdecken.

8.1.1 Reihenschaltung im Sinne der Zuverlässigkeit

Bild 8.1 zeigt zwei Armaturen, die im Sinne der Zuverlässigkeit in Reihe angeordnet sind (ODER-Gatter; logische Disjunktion). Die Armaturen sind normalerweise geöffnet. Das unerwünschte Ereignis ist in diesem Fall die Unterbrechung des Durchflusses, die dann auftritt, wenn eine der beiden Armaturen V1 oder V2 oder beide Armaturen in geschlossener Stellung versagen.

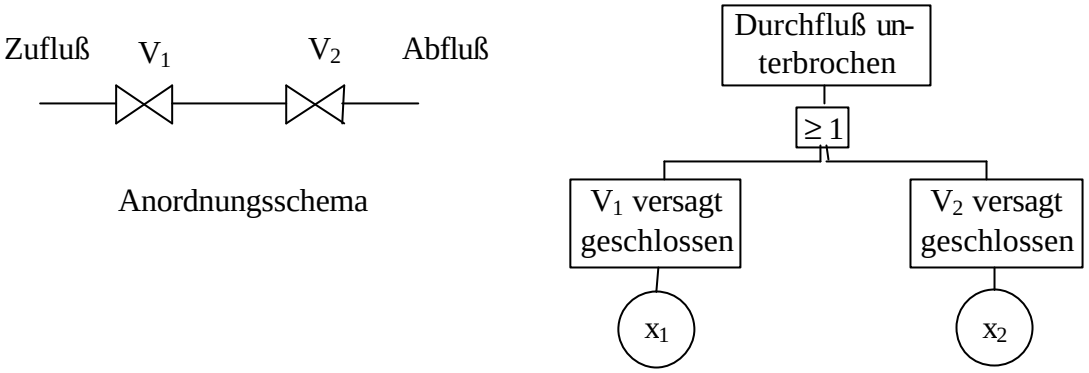


Bild 8-2: Anordnungsschema und Fehlerbaum für eine Reihenschaltung im Sinne der Zuverlässigkeit

In diesem Fall erhält man die folgende Strukturfunktion /Barl75/, /Schn99/:

$$\Psi\left(x_1, x_2\right) = \max\left\{x_1, x_2\right\} = x_1 + x_2 - x_1 \cdot x_2 = \begin{cases} 1 \text{ , wenn } x_1 \text{ oder } x_2 \text{ oder beide=1} \\ \\ 0 \text{ , wenn } x_1 \text{ und } x_2 = 0 \end{cases} \qquad (8\text{-}4)$$

Die Erweiterung der Gl.(8-4) auf N Komponenten ergibt

$$\begin{aligned} &\Psi\left(x_1, \ldots, x_N\right) = \max\left\{x_1, \ldots, x_N\right\} = 1 - \prod_{n=1}^{N}\left(1 - x_n\right) \\ &= \sum_{n=1}^{N} x_n - \sum_{n=1}^{N-1}\sum_{m=n+1}^{N} x_n \cdot x_m + \sum_{n=1}^{N-2}\sum_{m=n+1}^{N-1}\sum_{j=m+1}^{N} x_n \cdot x_m \cdot x_j + \ldots + \left(-1\right)^{N-1} x_1 \cdot \ldots \cdot x_N \end{aligned} \qquad (8\text{-}5)$$

8.1.2 Parallelschaltung im Sinne der Zuverlässigkeit

Man betrachtet das System des Bild 8-3. Das Fluid kann durch jede der beiden Armaturen in ausreichender Menge zum Systemausgang gelangen. Die Armaturen sind normalerweise geöffnet. Folglich tritt das unerwünschte Ereignis "Unterbrechung des Durchflusses" nur dann ein, wenn beide Armaturen in geschlossener Stellung versagen (UND-Gatter; logische Konjunktion).

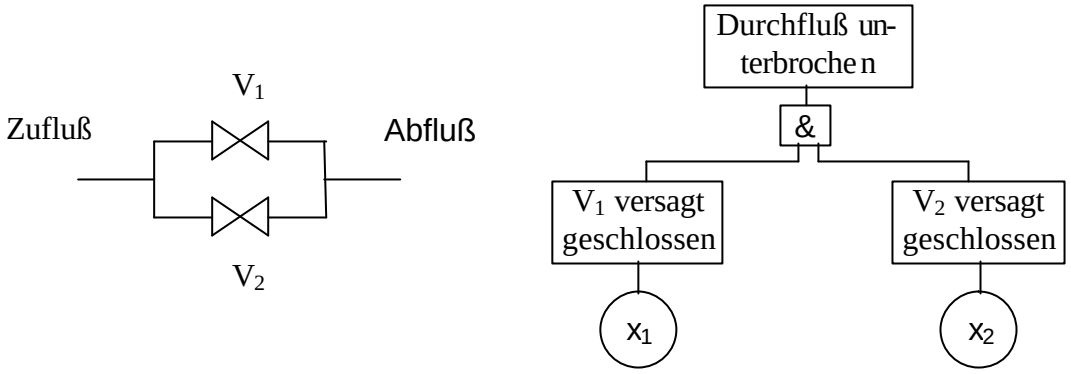


Bild 8-3: Anordnungsschema und Fehlerbaum für eine Parallelschaltung im Sinne der Zuverlässigkeit

Für diesen Fall gilt die folgende Strukturfunktion /Barl75/, /Schn99/

$$\Psi\left(x_1, x_2\right) = \min\left\{x_1, x_2\right\} = x_1 \cdot x_2 = \begin{cases} 1 \text{ , wenn } x_1 \text{ und } x_2 = 1 \\ \\ 0 \text{ , wenn } x_1 \text{ oder } x_2 \text{ oder beide} = 0 \end{cases} \qquad (8\text{-}6)$$

Hat das System N Komponenten, so folgt:

$$\Psi\left(x_1, \ldots, x_N\right) = \min\left\{x_1, \ldots, x_N\right\} = \prod_{n=1}^{N} x_n \qquad (8\text{-}7)$$

Die Methode ist nach DIN 25424 standardisiert. Sie ist eine typische deduktive Methode und liefert bei konsequenter Anwendung alle Ereigniskombinationen, die zum unerwünschten Ereignis führen können. Voraussetzung hierfür ist allerdings ein ausreichender Kenntnisstand seitens des Anwenders. Zum Zeitpunkt der Analyse unbekannte Ereignisse kann die Fehlerbaumanalyse nicht aufdecken.

8.1.3 Bewertungsschaltung des Typs 2 von 3

Bild 8-4 zeigt den Fehlerbaum für das 2 von 3 Auswahlsystem. Dies kann beispielsweise vorliegen, wenn eine Temperatur durch drei Wächter überwacht wird und eine Abschaltung wegen zu hoher Temperatur nur dann erfolgt, wenn mindestens zwei Wächter eine Grenzwertüberschreitung melden.

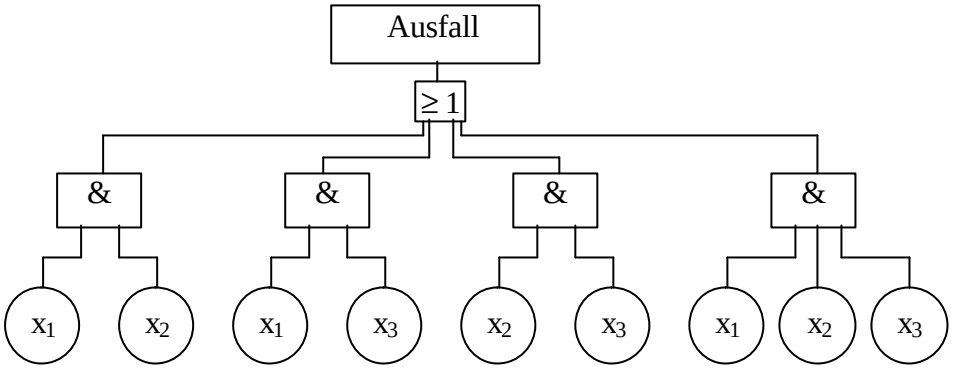


Bild 8-4: Fehlerbaum für ein 2 von 3 Auswahlsystem

Wie man aus dem Bild ablesen kann, tritt ein Systemausfall als Folge des Ausfalls verschiedener Komponentengruppen ein, nämlich K_1 = {1,2}, K_2 = {1,3}, K_3 = {2,3} und K_4 = {1,2,3}, denen die folgenden binären Funktionen zugeordnet sind.

$$k_1 = x_1 \cdot x_2 \;\; ; \;\; k_2 = x_1 \cdot x_3 \;\; ; \;\; k_3 = x_2 \cdot x_3 \;\; ; \;\; k_4 = x_1 \cdot x_2 \cdot x_3 \qquad (8\text{-}8)$$

In den Beziehungen (8-8) treten Produkte binärer Variablen auf, da es sich um Elemente handelt, die im Sinne der Zuverlässigkeit parallel angeordnet sind (vgl. Gl. (8-7)). Jede der Mengen K_1 bis K_4 nennt man Schnittmenge oder Trennung /Gäde77/ (englisch: cut set). Wie man sieht, enthält die Menge K_4 die anderen Mengen. Da ein System mit isotoner Strukturfunktion, das ausgefallen ist, in diesem Zustand verharrt, wenn eine weitere Komponente ausfällt, stellt K_4 keine zusätzliche Ausfallart des Systems dar; K_4 ist überflüssig und wird deshalb eliminiert. Die verbleibenden Mengen heißen Minimalschnitte oder minimale Trennungen. Sie enthalten Komponenten, deren gemeinsamer Ausfall notwendig und hinreichend ist, um einen Systemausfall zu bewirken. Jeder Minimalschnitt stellt eine unterschiedliche Ausfallart des Systems dar. Da die Minimalschnitte miteinander vereinbar sind, erhält man die Strukturfunktion des Systems unter Benutzung der Beziehung für Reihenschaltungen (vgl. Gl.(8-5)).

$$\Psi = 1 - \prod_{i=1}^{3} (1 - k_i) = \sum_{n=1}^{3} k_n - \sum_{n=1}^{2} \sum_{m=2}^{3} k_n \cdot k_m + \sum_{n=1}^{1} \sum_{m=2}^{2} \sum_{j=3}^{3} k_n \cdot k_m \cdot k_j \qquad (8\text{-}9)$$

Vereinfachungen zur Lösung der Gl. (8-9) werden im folgenden Abschnitt anhand eines Beispiels aufgezeigt.

8.1.4 Beispiel „Sicherheitsventil und Druckalarm zum Abschalten der Befüllung eines Behälters“

An einem einfachen Beispiel der Füllstandsüberwachung wird die qualitative Anwendung der Fehlerbaumanalyse demonstriert. Es soll der Fehlerbaum für das unerwünschte Ereignis „Behälter platzt wegen Überfüllung“ entwickelt und die erwartete Eintrittshäufigkeit für ein Zerplatzen des Behälters ermittelt werden (Bild 8-5). Der Behälter wird 26 mal im Jahr befüllt. Den zugehörigen Fehlerbaum zeigt Bild 8-6.

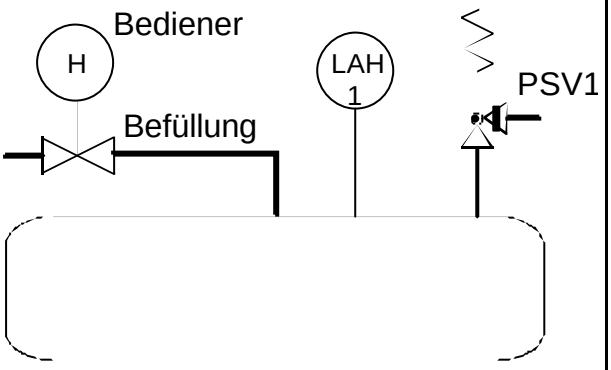


Bild 8-5: Schema des Behälters zur Drucklagerung eines Flüssiggases (mit Sicherheitsventil)

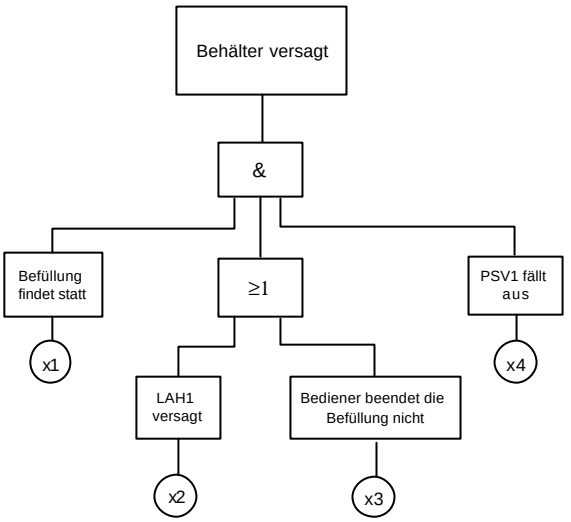


Bild 8-6: Fehlerbaum der Anordnung nach Bild 8-5 für das unerwünschte Ereignis „Behälter versagt“

Die Zuverlässigkeitsdaten* sind:

Primärereignis	Beschreibung		Funktionsprüfungsintervall q
x_1	Befüllung findet statt	Häufigkeit: $26\ a^{-1}$	
x_2	LAH1 versagt	?: $7{,}6\ 10^{-6}\ h^{-1}$	336 h
x_3	Bediener beendet Befüllung nicht	u: $1{,}6\ 10^{-3}$	
x_4	PSV1 fällt aus	?: $17{,}4\ 10^{-6}\ h^{-1}$	8760 h

Tabelle 8-1: Zuverlässigkeitsdaten für die Einrichtungen des Bild 8-5

*Die Funktionswahrscheinlichkeit des Handventils H, das im Falle eines Alarms vom Bediener betätigt wird, um den Zufluß zu unterbrechen, wird mit 1 angenommen.

Die Minimalschnitte des Systems ergeben sich zu:

$$E\left[k_1\right] = E\left[x_1 x_2 x_4\right] = 2,53 \cdot 10^{-3}$$
$$E\left[k_2\right] = E\left[x_1 x_3 x_4\right] = 3,17 \cdot 10^{-3} \qquad (8\text{-}10)$$

Daraus ergibt sich die Strukturfunktion gemäß Formel (8-5) zu:

$$\begin{aligned}\Psi(\vec{x}) &= x_1x_2x_4 + x_1x_3x_4 - x_1x_2x_3x_4 \\ &= x_1\left[x_2x_4 + x_3x_4 - x_2x_3x_4\right]\end{aligned} \qquad (8\text{-}11)$$

Unter der Voraussetzung, daß das System in regelmäßigen Abständen T („periodische Funktionsprüfung“) angefordert wird, kann man die mittlere Nichtverfügbarkeit u für Bereitschaftskomponenten über

$$\bar{u} = \frac{1}{q} \cdot \int_{nq}^{(n+1)\cdot q} \left(1 - e^{-\frac{t-nq}{T}}\right) \cdot dt = 1 + \frac{T}{q} \cdot \left(e^{-\frac{q}{T}} - 1\right) \approx \frac{l \cdot q}{2} \qquad (8\text{-}12)$$

ermitteln. Dabei wurden folgende Annahmen getroffen:

- die Lebensdauern der Komponenten sind exponentialverteilt,
- das Zeitintervall θ zwischen den Prüfungen ist konstant,
- Ausfälle werden nur bei Prüfungen entdeckt,
- die Zeitdauer der Prüfung ist vernachlässigbar gegenüber der mittleren Lebensdauer der Komponenten und kann somit gleich null gesetzt werden und
- die Komponente wird bei jeder Prüfung im Falle des Ausfalls ersetzt oder so instandgesetzt, daß sie danach als „so gut wie neu“ gelten kann.

Aus Gleichung (8-8) folgt für die Nichtverfügbarkeit der einzelnen Komponenten gemäß Tabelle 8-1:

$$\begin{aligned}u_2 &= 0{,}00128 \\ u_3 &= 0{,}0016 \\ u_4 &= 0{,}076212\end{aligned} \qquad (8\text{-}13)$$

Der Erwartungswert einer binären Variablen lautet

$$E\left[x_n\right] = q_n \cdot 1 + p_n \cdot 0 = q_n \qquad (8\text{-}14)$$

In Gl.(8-10) bezeichnet p_n die Funktionswahrscheinlichkeit der Komponente n und $q_n = 1 - p_n$ die zugehörige Ausfallwahrscheinlichkeit.

Die Eigenschaften der Erwartungswerte von Zufallsvariablen bezüglich Summation und Multiplikation sind wie folgt (vgl. z.B. /Gäde77/)

$$E[x_1 + x_2 + \ldots + x_N] = E[x_1] + E[x_2] + \ldots + E\left[x_N\right] \qquad (8\text{-}15)$$

Sind die Zufallsgrößen unabhängig voneinander, so gilt für die Multiplikation

$$E\left[x_1 \cdot x_2 \cdot \ldots \cdot x_N\right] = E[x_1] \cdot E[x_2] \cdot \ldots \cdot E[x_N] \qquad (8\text{-}16)$$

Wendet man die Eigenschaften aus den Gl.(8-10) -(8-12) auf die Gl.(8-7) an, so erhält man die Eintrittshäufigkeit für ein Zerplatzen des Behälters; sofern die q_n Nichtverfügbarkeiten sind:

$$E\left[\Psi\left(x_1, x_2, x_3, x_4\right)\right] = q_1 \cdot q_2 \cdot q_4 + q_1 \cdot q_3 \cdot q_4 - q_1 \cdot q_2 \cdot q_3 \cdot q_4 \qquad (8\text{-}17)$$

Die voranstehend am Beispiel gezeigte Vorgehensweise ist allgemein gültig. Alle Strukturfunktionen können in ihre multilineare Form gebracht werden. Die binären Variablen, die sie enthalten, können dann durch die zugehörigen Wahrscheinlichkeiten „ersetzt“ werden. Dadurch erhält man die entsprechenden Zuverlässigkeitskenngrößen des Systems, das durch die Strukturfunktion beschrieben wird. Es wurde bereits darauf hingewiesen, daß das beschriebene Vorgehen unabhängige Primärereignisse voraussetzt. Die Behandlung von Abhängigkeiten ist nicht Gegenstand der Arbeit. Diesbezüglich wird auf die Literatur, z.B. /Haup94b/, verwiesen.

Betrachtet man Gl.(8-13), so sieht man, daß der dritte Term eine kleine Größe höherer Ordnung darstellt, sofern die Wahrscheinlichkeit $q << 1$, was in der Regel zutrifft. Man kann sie dann vernachlässigen, was zu einer erheblichen Vereinfachung bei der Auswertung der Beziehung (8-5) führt. Es ergibt sich dann nämlich für den allgemeine Fall mit N Minimalschnitten die folgende Abschätzung des Erwartungswertes, die eine obere Schranke darstellt.

$$E\left[\Psi(\vec{x})\right] \approx \sum_{i=1}^{N} E\left[k_i\right] \qquad (8\text{-}18)$$

Durch Einsetzen von Gl. (8-9) in Gl. (8-15) ergibt sich die angenäherte erwartete Häufigkeit des unerwünschten Ereignisse „Behälterzerplatzen“ zu:

$$H = 26a^{-1} \cdot 2{,}19 \cdot 10^{-4} \quad \Rightarrow \quad \underline{H = 5{,}69 \cdot 10^{-3} a^{-1}} \qquad (8\text{-}19)$$

8.2 Überlagertes Redundanzprinzip

Wie in Kapitel 7 beschrieben, wird das Gefahrenpotential der zu untersuchenden Teilanlage mittels DOW's Fire&Explosion Index (F&EI) /Fire94/, /www.cheq/ ermittelt. Dabei wird das Gefahrenpotential einer Chemieanlage in drei Kategorien unterteilt. Diese Kategorien bestimmen dann die Anforderungen an den Redundanzgrad der betrieblichen- und sicherheitstechnischen Ausrüstung („äußere“ sicherheitstechnische Ausgewogenheit). Neben den vorgestellten drei Redundanzgraden, die aufgrund des Gefahrenpotentials der Anlage entsprechend zugeordnet werden (vergleiche Abschnitt 8.3), spielt die Redundanz innerhalb eines Regelkreises bzw. einer Meßkette hinsichtlich Ausgewogenheit ebenso eine wichtige Rolle („innere“ sicherheitstechnische Ausgewogenheit). Die Meßkette besteht dabei im wesentlichen aus den Modulen:

- Wächter,
- Wandler und
- Stellglied.

Bild 8-7 zeigt ein allgemeines Beispiel für eine einfach ausgelegte Meßkette.

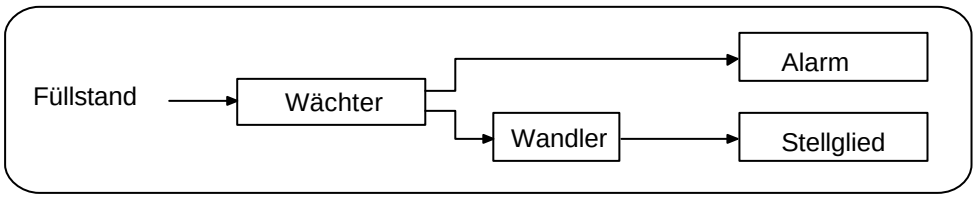


Bild 8-7: Meßkette in Einfachauslegung, schematisch

Die angesprochene Einfachauslegung einer Meßkette bedeutet in diesem Zusammenhang, daß das zuverlässigkeitsmäßig betrachtet stärkste Glied in der Kette Maß-

stab für die anderen Glieder sein sollte. Da der Ausfall eines Gliedes den Ausfall des gesamten Systems bedeutet (unter der Voraussetzung einer Reihenschaltung), sollten die Glieder bezogen auf die Ausfallwahrscheinlichkeit bzw. Nichtverfügbarkeit ausgewogen gestaltet sein. Ist dies nicht der Fall, kann beispielsweise die Redundanz einzelner Glieder das System ausgewogener gestalten. Das folgende Bild zeigt eine Möglichkeit im Vergleich zur Auslegung der Meßkette gemäß Bild 8-7, indem der Füllstandswächter redundant ausgelegt ist.

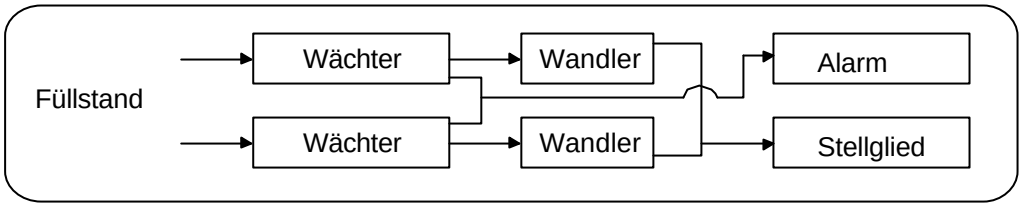


Bild 8-8: Redundanz innerhalb der Meßkette, schematisch

An einem einfachen Beispiel der Füllstandsregelung wird dies im folgenden näher erläutert. Zum einen wird die Füllstandsregelung mittels eines Wächters mit Schwimmkörper und zum anderen mittels eines Wächters mit kapazitivem Sensor betrachtet. In der Literatur findet man Zuverlässigkeitswerte für die Systeme Wächter-Verarbeitungslogik und Stellglied /Haup88a/. Das Stellglied und somit die zugehörige Ausfallrate bleibt in beiden Fällen gleich. Nur die Ausfallrate für die Wächter ist unterschiedlich.

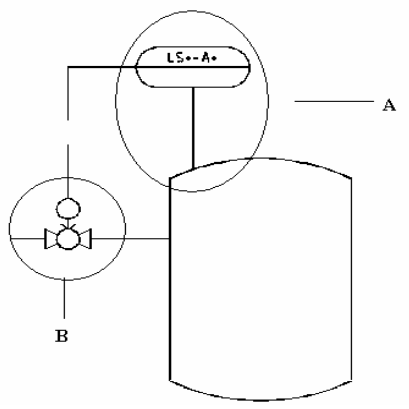


Bild 8-9: Einfach ausgelegte Meßkette

Der Fehlerbaum zu Bild 8-9 ergibt sich wie folgt:

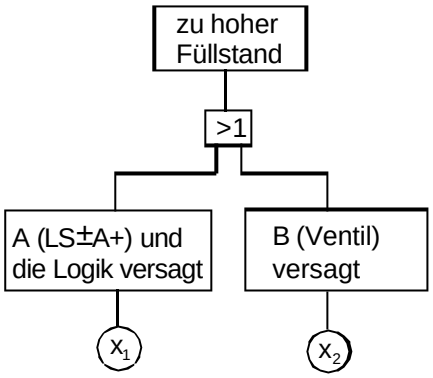


Bild 8-10: Fehlerbaum zu Bild 8-9

Da es sich hier nur um ein Beispiel handelt, wird nicht weiter zwischen der Schaltung (S++) und dem Alarm (A+) unterschieden. Normalerweise müßte der Bedienfehler ebenso wie die Einzelbehandlung von Wandler und Verarbeitungslogik mitbetrachtet werden. Die zugehörigen Ausfallraten sind:

$$\begin{aligned} l_{A_s} &= 14{,}8 \cdot 10^{-6} h^{-1} \text{ => System Wandler-Wächter mit Schwimmkörper} \\ l_{A_k} &= 170 \cdot 10^{-6} h^{-1} \text{ => System Wandler-Wächter mit kapazitivem Sensor} \\ l_{A_k} &= 16{,}8 \cdot 10^{-6} h^{-1} \text{ => Stellglied} \end{aligned} \qquad (8\text{-}20)$$

Wie man an den Zahlenwerten erkennen kann, ist das System Wandler-Schwimmkörper und Stellglied zahlenmäßig ausgewogen, wohingegen der Wert für den kapazitiven Sensor um eine 10er Potenz höher liegt und somit das schwächste Glied ist. Die Nichtverfügbarkeit der Komponenten bei periodischer Funktionsprüfung mit $\Theta = 336\text{h}$ wird gemäß Gl. (8-12) zu

$$u \approx \frac{l \cdot \Theta}{2} \qquad (8\text{-}21)$$

angenähert, da $\lambda \cdot \Theta << 1$.

Aus Gleichung (8-21) folgt für die Komponenten:

$$\begin{aligned} u_{As} &= 2{,}49 \cdot 10^{-3} \text{ => System Wandler-Wächter mit Schwimmkörper} \\ u_{Ak} &= 2{,}86 \cdot 10^{-2} \text{ => System Wandler-Wächter mit kapazitivem Sensor} \\ u_B &= 2{,}82 \cdot 10^{-3} \text{ => Stellglied} \end{aligned} \qquad (8\text{-}22)$$

Bei der Meßkette handelt es sich aus Sicht der Zuverlässigkeit um eine Reihenschaltung, da beide Einrichtungen -Wächter-Logik und Stellglied- funktionieren müssen, damit die Aufgabe erfüllt werden kann. Die Nichtverfügbarkeit der Kette ergibt sich dann zu:

$$u_{System} = u_A + u_B - u_A \cdot u_B \qquad (8\text{-}23)$$

Somit kann die Nichtverfügbarkeit für die Systeme kapazitiver Sensor und Schwimmkörper ermittelt werden:

$$\begin{aligned} u_{SAs} &= 5{,}30 \cdot 10^{-3} \Rightarrow \text{System} \quad \text{Schwimmkörper-Stellglied} \\ u_{SAk} &= 3{,}32 \cdot 10^{-2} \Rightarrow \text{System} \quad \text{kapazitiver} \quad \text{Sensor-Stellglied} \end{aligned} \qquad (8\text{-}24)$$

Eine Lösung zur Angleichung der Nichtverfügbarkeiten des Systems Wächter mit kapazitivem Sensor und Stellglied ist die Wahl eines Sensors gleichen Typs mit einer höheren Zuverlässigkeit, beispielsweise eines anderen Herstellers. Wie bereits erwähnt, ist eine andere Möglichkeit, vor allem wenn die erst genannte sich nicht umsetzen läßt, durch entsprechende Redundanz eine Angleichung der Werte zu erreichen. In diesem Fall kann man einen zweiten Sensor gleichen Typs einbauen, der in 1-von-2-Logik mit dem anderen Sensor verschaltet wird. Bild 8-11 zeigt eine mögliche Anordnung.

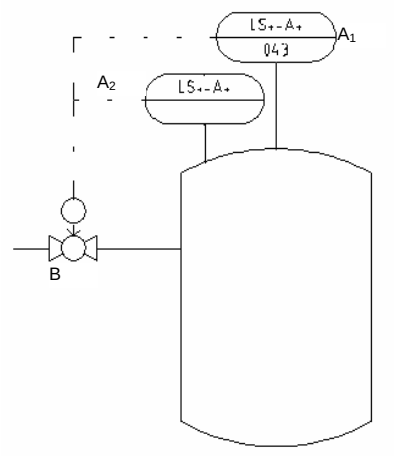


Bild 8-11: Redundante Anregung mit nicht redundanter Ausführung

Der zugehörige Fehlerbaum lautet:

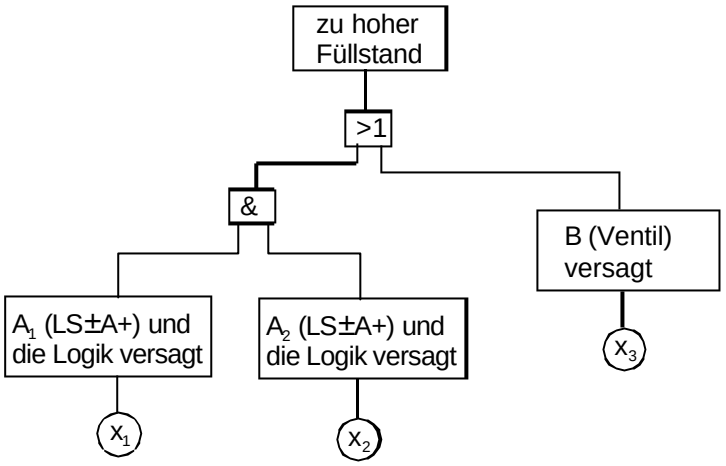


Bild 8-12: Fehlerbaum zu Bild 8-11

Die beiden Wächter stellen eine Parallelschaltung im Sinne der Zuverlässigkeit dar; es müssen beide Sensoren ausfallen, damit das System nicht funktioniert. So ergibt sich die Nichtverfügbarkeit für die Wächter zu:

$$u_{Ak,r} = \left(\frac{l_{Ak} \cdot \Theta}{2} \right)^2 = 0{,}82 \cdot 10^{-3} \qquad (8\text{-}25)$$

Man erkennt hier, daß dieser Wert der redundanten Wächter in einem besseren Verhältnis zu dem des Stellgliedes steht als der Wert eines Wächters allein. Somit wurde ein ausgewogenes Verhältnis innerhalb der Meßkette durch einfache redundante Auslegung des schwächsten Gliedes erreicht. Abschließend kann noch die Nichtverfügbarkeit des Gesamtsystems redundanter Wächter–Verarbeitungslogik und Stellglied ausgerechnet werden:

$$u_{SAk,r} = u_{A_{k,r}} + u_B - u_{A_{k,r}} \cdot u_B = 3{,}64 \cdot 10^{-3} \qquad (8\text{-}26)$$

Auch hier erkennt man, daß dieser Wert nun um eine Größenordnung niedriger liegt als der Wert mit nur einem Wächter. Wegen der Möglichkeit gemeinsam verursachter Ausfälle (GVA) wäre in diesem Fall Diversität angezeigt, das heißt, ein Wächter mit einem anderen pysikalischen Meßprinzip sollte als redundantes Element ausgewählt werden.

Diese Vorgehensweise ist unabhängig von der Wahl der Redundanzgrade der Einzelsysteme, die allein in Abhängigkeit vom Gefahrenpotential festgelegt werden. Die Ausgewogenheit der Meßketten liegt diesen Redundanzgraden zugrunde. Die im

Programm abgelegten Teilsysteme sind hinsichtlich ihrer Zuverlässigkeit ausgewogen gestaltet. Weiterhin ist ein Tool zur Bestimmung der Ausgewogenheit der Meßkette im Programm installiert. Sind dem Nutzer die Ausfallraten der einzelnen Einrichtungen bekannt, können die Systeme auf Ausgewogenheit überprüft werden.

8.3 Differenzierung der Teilsysteme

Betriebliche Einrichtungen (z.B. Füllstandsregelung, Dosierung etc.) und Schutzfunktionen gegen unerwünschte Ereignisse (z.B. Überdruck, Rührerausfall etc.) gleichen sich vielfach und lassen sich hinsichtlich Redundanz und Diversität zur Minderung ihrer Versagenswahrscheinlichkeit unterscheiden. Dabei hängt der Grad der Überlebenswahrscheinlichkeit vom Gefahrenpotential der Anlage ab. Dieser Zusammenhang wurde im Rahmen dieser Arbeit genutzt, um betriebliche und sicherheitstechnische Konfigurationen nach ihren Funktionen und Gefahrenpotential-Kategorien einzustufen.

Tabelle 8-2 zeigt die Zuordnungskriterien der Redundanz- und Diversitätsgrade zu den einzelnen Gefahrenkategorien gemäß Tabelle 7-2. Darauf aufbauend werden die mittels des Expertensystems durch Anwendung der PAAG-basierten Sicherheitsanalyse für notwendig erachteten betrieblichen und sicherheitstechnischen Einrichtungen ausgelegt.

Gefahrenpotential		
Kategorie I =“gering“	Kategorie II =“mittel“	Kategorie III =“hoch“
Mindestens 1 Einrichtung.	Mindestens 2 Einrichtungen.	Dreifach redundante Einrichtungen.
Einzeleingangswert für Alarm.	Mindestens 2 Eingangswerte für den Alarm.	Mindestens 3 Eingangswerte für den Alarm.
1 von 1 Schaltung für den Alarm und die Auslösung der Schutzfunktionen.	1 von 2 (oder mehr als 2) „ODER” Gatter für Alarm und die Auslösung der Schutzfunktionen.	1 von 3 Schaltung für den Alarm und die Auslösung der Schutzfunktionen, wenn Fehlarme nicht berücksichtigt werden müssen, ansonsten Auslösung in 2 von 3.
Einzeleingangswert für die Regelung.	Entweder einzelne oder redundante Eingangswerte für die Regelung; nach Möglichkeit diversitär.	Nach Möglichkeit mehr als ein Eingangswert für die Regelung; nach Möglichkeit diversitär.

Gefahrenpotential		
Kategorie I =“gering“	Kategorie II =“mittel“	Kategorie III =“hoch“
	Alarm, wenn redundante Eingangswerte nicht übereinstimmen.	Alarm, wenn redundante Eingangswerte nicht übereinstimmen.

Tabelle 8-2: Gefahrenpotential-Kategorien und zugeordnete Redundanz- und Diversitätsgrade betrieblicher und sicherheitstechnischer Einrichtungen

Unter der Voraussetzung gleicher Gefährdung wird im folgenden eine mögliche Lösung durch das Expertensystem entsprechend den drei vorgestellten Gefahrenpotential-Kategorien aufgezeigt. Es wurde die Sicherung des Füllstandes betrachtet und als mögliche Gefährdung Überdruck infolge thermischer Ausdehnung im Anschluß an eine Überfüllung des Behälters angenommen. Als Lösung für das Teilsystem ergibt sich in Abhängigkeit des Gefahrenpotentials:

Kategorie	mögliche Gefährdung	Lösung		
		passiv	aktiv	organisatorisch
gering	Überfüllung und anschließende thermische Ausdehnung führt zu Überdruck	ausreichende Dimensionierung	Einfache Verriegelung der Zuführungsleitung über den Füllstand, ein Ventil	Alarm bei zu hohem Füllstand mit Anweisungen zur Füllstandsbegrenzung
mittel		ausreichende Dimensionierung	Verriegelung der Zuführungsleitung über den Füllstand in 1 von 2, wenn möglich, diversitäre Meßwertaufnahme, zwei Ventile	Alarm bei zu hohem Füllstand mit Anweisungen zur Füllstandsbegrenzung
hoch		ausreichende Dimensionierung	Verriegelung der Zuführungsleitung über den Füllstand in 1 von 3, wenn möglich, diversitäre Meßwertaufnahme, zwei Ventile	Alarm bei zu hohem Füllstand mit Anweisungen zur Füllstandsbegrenzung

Bild 8-13: Lösungsbeispiel SafeCAD’s für die drei Gefahrenpotential-Kategorien

Im folgenden werden die Lösungen grafisch dargestellt. Der Übersichtlichkeit halber werden nur die Sicherheitssysteme angezeigt.

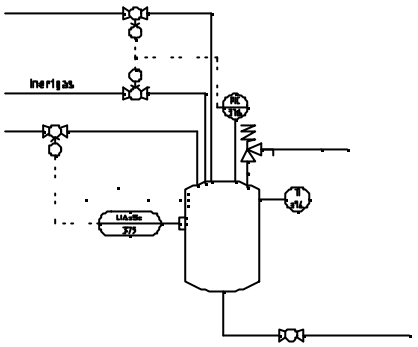
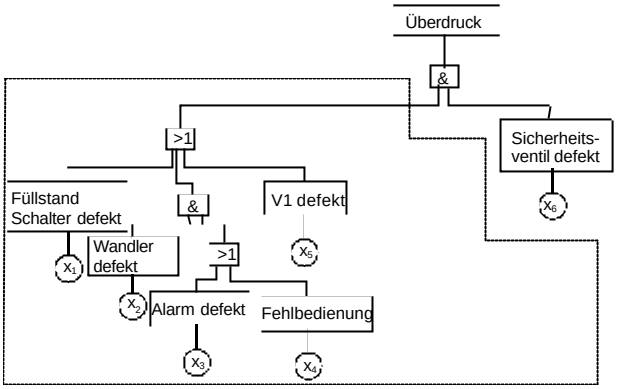
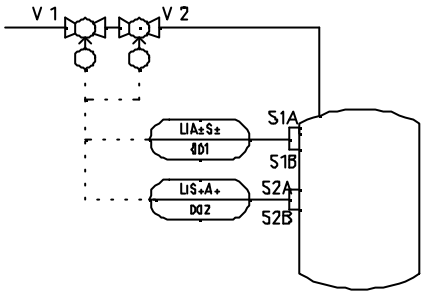
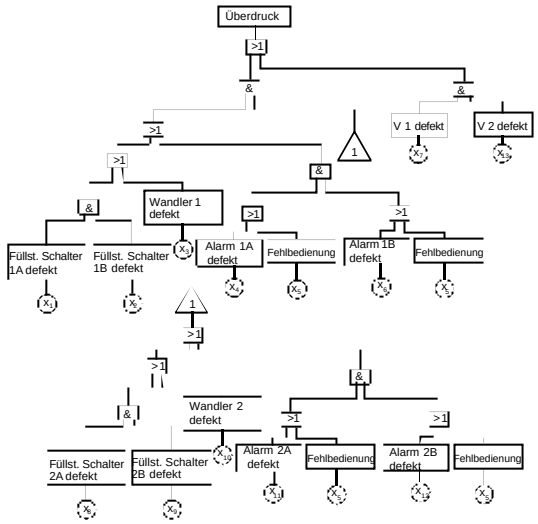
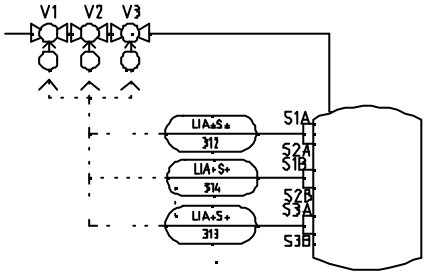
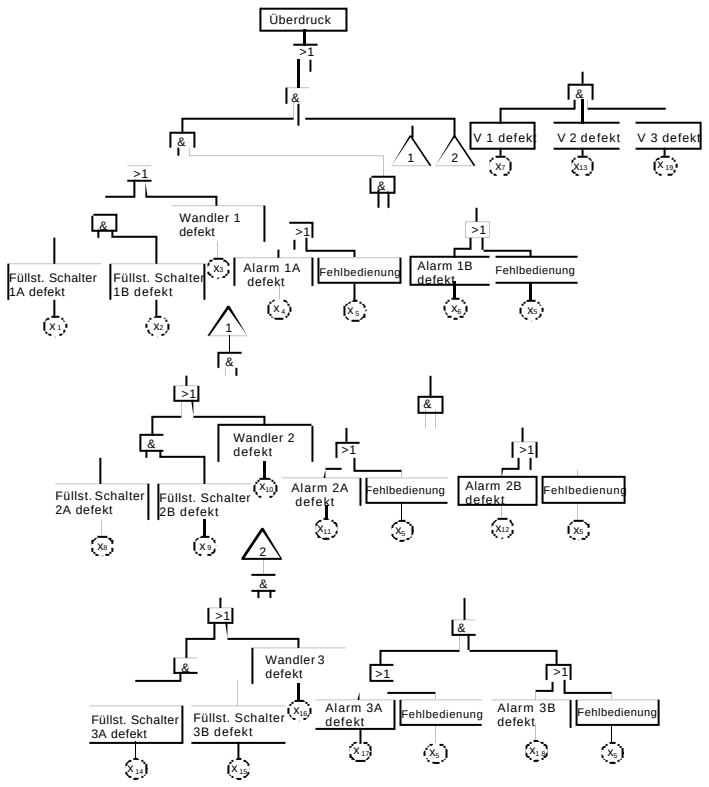
Kategorie	R&I-Fließbild	Fehlerbaum
Leicht		
Mittel		
Hoch		

Bild 8-14: Beispiel für eine Füllstandsüberwachung mit Schaltfunktion

Der Nachweis der Angemessenheit der unterschiedlich redundanten Ausführung wird mittels der Fehlerbaummethode (siehe Abschnitt 8.1) vorgenommen. Deren grundsätzliche Anwendbarkeit auf Chemieanlagen wurde bereits in /Haup87/, /Haup85b/, /Haup80/, /Heal78/, /Risk82/ und /Haup95/ nachgewiesen. Auch wenn bemängelt wurde, daß kein ausreichendes Datenmaterial vorliegt /Haup95/ und /Sche87/, kann man, bei Verwendung derselben Datenbasis, die Fehlerbaumanalyse zum Nachweis der Tauglichkeit dieses Systems und zur Auswahl der geeigneten Konfigurationen anwenden. Darüber hinaus bietet die neuere Literatur mittlerweile sehr wohl Angaben zu Ausfallraten technischer Komponenten (siehe z.B. /Ored97/, /Haup88a/, /Guid89/) an.

Obwohl es keine formalen Ziele bezüglich der tolerierbaren Häufigkeit von Unfällen bzw. Systemversagen im deutschen Recht gibt, können die Ergebnisse helfen zu entscheiden, ob die Konfigurationen entsprechend den drei Gruppen (siehe Tabelle 7-2) angemessen ausgeführt sind oder nicht. Hierbei sollte nicht vergessen werden, daß mit der DIN EN 61508 /IEC 61508/ und der DIN IEC 61511 /IEC 61511/ bereits zwei internationale Richtlinien existieren, die Anforderungen an die Qualität von Sicherheitsausrüstungen hinsichtlich ihrer Nichtverfügbarkeit stellen. Tabelle 8-3 zeigt die SIL[7]-Klassen der DIN IEC 61511 /IEC 61511/ im Vergleich mit den Anforderungsklassen der DIN V 19250 /DIN V 19250/ bzw. den Anforderungsklassen gemäß VDI/VDE 2180 /DIN/VDE2180_2/.

[7] Safety Integrity Level

IEC 61511	DIN V 19250	VDI/VDE 2180	
SIL / Ausfallwahrscheinlichkeit bei Anforderung	**Anforderungsklasse**	**Risikobereich**	
–	1	I	
1 / > 10^{-2} bis < 10^{-1}	2		
	3		
2 / > 10^{-3} bis < 10^{-2}	4		
3 / > 10^{-4} bis < 10^{-3}	5	II	
	6		
4 / > 10^{-5} bis < 10^{-4}	7	–	nicht allein durch PLT-Schutzeinrichtung abdeckbar
	8		

Tabelle 8-3: Anforderungsklassen nach IEC 61511 im Vergleich

„*Die numerische Festlegung des Sicherheitsintegritätslevels ermöglicht einen objektiven Vergleich alternativer Entwürfe und Lösungen. Es wird jedoch beim gegenwärtigen Stand des Wissens anerkannt, daß viele Ursachen für systematische Ausfälle nur qualitativ abgeschätzt werden können*“ /IEC 61511/.

Die Zuordnung der Wahrscheinlichkeitsbänder zu den einzelnen Sicherheitsintegritätsleveln kann somit nicht restriktiv erfolgen und wird von SafeCAD mindestens eingehalten, wie Tabelle 8-5 entnommen werden kann.

Die entsprechenden Fehlerbäume in Bild 8-14 mit der mathematischen Auswertung für die Systeme zeigen die Unterschiede hinsichtlich ihrer erwarteten Ausfallhäufigkeit.

Zur simulativen Ermittlung der Minimalschnitte der Bäume wurde das Programm FEMO verwand. Ihre zuverlässigkeitsmäßige Bewertung wurde unter Verwendung des Programms EVAL vorgenommen. Die Grundlagen sind teilweise in /Haup79/ dargestellt. Die zur Berechnung benutzten Zuverlässigkeitsdaten zeigt Tabelle 8-4. Für die Kategorie „Leicht“ wird der Einfluß des Sicherheitsventils auf die Gesamtverfügbarkeit nicht berücksichtigt, da das Ventil nicht das auslösende Ereignis „Überfül-

lung“ verhindern kann sondern nur die möglichen Konsequenzen im Falle einer Überfüllung und anschließender thermischer Ausdehnung zu begrenzen vermag.

Die Nichtverfügbarkeiten der verschiedenen Kategorien zeigt Tabelle 8-5.

In Bild 8-14 sind aus Gründen der Übersichtlichkeit nur die Minimalschnitte der Kategorie „Leicht“ aufgeführt. Sie stehen für „V1 versagt“, (1), „Füllstandsschalter versagt“, (2), „Wächter und Alarm versagen“, (3) und „Wächter versagt und Bedienfehler“, (4). Diese Minimalschnitte stellen die Grundlage für die Überprüfung auf innere Ausgewogenheit dar (vergleiche Kapitel 8.2). Den Unterschied auf Basis der Analyseergebnisse der Konfiguration gemäß Bild 8-7 zeigt Bild 8-8. Durch einen zusätzlichen Wächter konnte hier das System in Bezug auf die Nichtverfügbarkeit ausgewogen gestaltet werden. Durch die Modifikation konnte die Nichtverfügbarkeit um den Faktor 3 gesenkt werden. Die modifizierte Konfiguration ist die Grundlage für die Auslegung der 1-von-2 und 1-von-3 Systeme der anderen beiden Kategorien. Für ein 2-von-3 System unter der Voraussetzung, daß Fehlalarme berücksichtigt werden müssen, ergibt sich eine Nichtverfügbarkeit von $7{,}4 \cdot 10^{-6}$ und für eine Konfiguration mit zwei Ventilen von $2{,}5 \cdot 10^{-5}$.

Da die Sicherheitseinrichtungen Bereitschaftssysteme sind und somit ihre Funktion nicht regelmäßig während des Betriebs überprüft wird, wird davon ausgegangen, daß das Prüfintervall zwei Jahre beträgt. Eine Befüllung findet alle zwei Wochen statt. Sie ist für einige Komponenten als Funtionsprüfungsintervall gleichzusetzen.

Es darf nicht vergessen werden, daß die ermittelten Werte sich ändern, wenn der Behälter nicht 26 mal im Jahr befüllt wird. Gleiches gilt, wenn die Zeiten zwischen den Funktionsprüfungen der Sicherheitseinrichtungen verändert werden.

Die zugehörigen Zuverlässigkeitskenngrößen sind:

Komponente	Median der Ausfallrate λ_{50} in h^{-1}	Unsicherheitsfaktor K_{95}	Zeit zwischen den Anforderungen durch Betrieb, bzw. zwischen den Funktionsprüfungen der Bereitschaftskomponenten in h
Füllst. Schalter	$48{,}0 \cdot 10^{-6}$	1,5	336 / 17520
Wandler	$2{,}7 \cdot 10^{-6}$	3,3	
Ventil	$17{,}8 \cdot 10^{-6}$	3,3	
Alarm	$7{,}7 \cdot 10^{-6}$	3,0	
1-von-3 Logik	$0{,}9 \cdot 10^{-6}$	3,0	
Fehlbedienung (keine Reaktion auf den Alarm oder falsche Maßnahmen)	$1 \cdot 10^{-4}$	10	–

Tabelle 8-4: Zuverlässigkeitsdaten für das Beispiel der Kategorie "gering" aus Bild 8-14

Da für die Beispiele die gleiche Ausrüstung und die gleichen Voraussetzungen gelten, sind die Zuverlässigkeitskenngrößen für die anderen Beispiele aus Bild 8-14 analog.

		Minimalschnitte	Nichtverfügbarkeit	
Leicht	Ausführungsebene	(1): x_5	$3{,}8 \cdot 10^{-3}$	$4{,}0 \cdot 10^{-3}$
	Aktivierungsebene	(2): x_1	$8{,}3 \cdot 10^{-3}$	$8{,}3 \cdot 10^{-2}$
		(3): $x_2 x_3$	$9{,}5 \cdot 10^{-7}$	
		(4): $x_2 x_4$	$1{,}6 \cdot 10^{-7}$	
	Nichtverfügbarkeit des Teilsystems		**$1{,}21 \cdot 10^{-2}$**	
	Ausgewogenheit durch innere Redundanz			
Leicht	Ausführungsebene		$3{,}9 \cdot 10^{-3}$	
	Aktivierungsebene		$6{,}9 \cdot 10^{-5}$	
	Nichtverfügbarkeit des Teilsystems		**$4{,}0 \cdot 10^{-3}$**	
Mittel	Ausführungsebene		$1{,}5 \cdot 10^{-5}$	
	Aktivierungsebene		$1{,}8 \cdot 10^{-8}$	
	Nichtverfügbarkeit des Teilsystems		**$1{,}5 \cdot 10^{-5}$**	
Hoch	Ausführungsebene		$5{,}9 \cdot 10^{-8}$	
	Aktivierungsebene		$< 10^{-9}$	
	Nichtverfügbarkeit des Teilsystems		**$5{,}9 \cdot 10^{-8}$**	

Tabelle 8-5: Ergebnisse der Beispiele aus Bild 8-14

Auch wenn –wie bereits erwähnt– nach deutschem Recht derzeit keine quantitativen Anforderungen an die Zuverlässigkeit von Sicherheitsausrüstungen bestehen, hilft das System dem Anlagenplaner zu entscheiden, ob der Umfang der Ausrüstung dem Gefahrenpotential angemessen ist oder nicht. Darüber hinaus sorgt die innere Optimierung durch das System (Kapitel 8.2) für einen Sicherheitsgewinn bei sehr geringem Aufwand.

Die Nichtverfügbarkeit im Falle der Kategorie „hoch“ erscheint mit $5{,}9 \cdot 10^{-8}$ sehr gering. Dies liegt daran, daß gemeinsam verursachte Ausfälle nicht betrachtet wurden. Diese für Chemieanlagen zu berücksichtigen, ist aufgrund mangelnder empirischer Kenngrößen schwierig und könnte allenfalls generisch erfolgen, wie z.B. in /Haup85a/ aufgezeigt.

Es bietet sich hier die Anwendung der in England üblichen pragmatischen Vorgehensweise an /Prob89/, indem alle Wahrscheinlichkeiten für Teilsysteme, die $< 10^{-5}$ sind, auf diesen Wert als Grenzwert herauf gesetzt werden. Im Rahmen dieser Arbeit werden gemeinsame verursachte Ausfälle nicht berücksichtigt.

Entscheidend bei der Auswahl geeigneter Teilsysteme ist neben der Evaluierung des Gefahrenpotentials und möglicher betrieblicher Abweichungen die Festlegung der Prozeßsicherungsgrößen. Sie dient der Erkennung des nichtbestimmungsgemäßen Betriebs einer Anlage. Im vorgenannten Beispiel ist dies der Füllstand. Der Druck als Prozeßsicherungsgröße fällt aus, da er einen zu hohen Füllstand nicht vermeiden kann.

9 Das Programm SafeCAD

SafeCAD ermöglicht dem Anwender auf Grundlage der Literatur und des Wissens eines (oder mehrerer) Experten eine Lösung für ein Problem zu finden. Dabei ist neben der Wissensdarstellung die vom Expertensystem benutzte Problemlösungsstrategie von Bedeutung. *Puppe* /Pupp91/ unterscheidet drei Haupttypen:

- Diagnostik: Die Lösung wird aus einer Menge vorgegebener Alternativen ausgewählt.
- Konstruktion: Die Lösung wird aus kleinen Bausteinen zusammengesetzt.
- Simulation: Aus dem Ausgangszustand werden Folgezustände hergeleitet.

Bild 9-1: Problemlösungstypen

SafeCAD basiert zum einen auf dem diagnostischen und zum anderen auf dem konstruktiven Problemlösungsansatz. Die Ermittlung möglicher Gefährdungen mittels des modifizierten PAAG-Verfahrens bedient sich der diagnostischen Variante, indem die Lösung aus einer vorgegebenen Menge ausgewählt wird. Die Umsetzung in eine CAD-Zeichnung folgt dem konstruktiven Ansatz, indem die Konfigurierung der Teilsysteme unter Berücksichtigung besonderer Anforderungen (Festlegung des Redundanzgrades und Auswahl geeigneter Sicherheitsmaßnahmen im Rahmen des Analyseteils des Programms) durchgeführt wird.

9.1 Darstellung des Wissens

Die sicherheitstechnische Auslegung von Anlagen und Aggregaten der chemischen Industrie ist eine vielschichtige Aufgabe. Neben der Bestimmung des Gefahrenpotentials muß die betriebliche Grundinstrumentierung zur Erfüllung der betrieblichen Erfordernisse festgelegt werden, um darauf aufbauend in Abhängigkeit vom Gefährdungsgrad die sicherheitstechnischen Einrichtungen festlegen zu können. Somit ist die Wahl eines geeigneten Repräsentationsformalismus ausschlaggebend für die Lösung der gestellten Aufgabe mittels eines Expertensystems. In diesem Zusammenhang ist der Aufbau der Wissensbasis (siehe Abschnitt 3.2) von Bedeutung. Ein klarer und strukturierter Aufbau ermöglicht dabei eine gute Nachvollziehbarkeit. Ein weiteres Qualitätsmerkmal von Expertensystemen ist die Wartbarkeit der Wissensbasis. Aus diesen Gründen wurde die Wissensbasis modular aufgebaut. Es können Module und Untermodule in der Wissensbasis erzeugt werden, wobei jedem Unter-

modul weitere Untermodule hinzugefügt werden können, so daß die Strukturtiefe nicht auf zwei Ebenen beschränkt ist. Somit kann das Wissen strukturiert gespeichert und überarbeitete Module gegen alte ausgetauscht sowie problemlos neue Module integriert werden. Als Module sind die Ermittlung von DOW's Fire & Explosion Index sowie derzeit die Teilsysteme Behälter, Reaktor und Absorptionskolonne implementiert. In den Untermodulen werden unter anderem denkbare Gefährdungen abgebildet. Für die Teilsysteme werden die in Bild 7-2 aufgeführten Gefährdungsarten als Untermodul angeboten.

Beim Einsatz des Programms werden die Gefährdungen vom Anwender auf ihre Eintrittsmöglichkeit hin untersucht. Dazu kann er sich an im Programm formulierten Eintrittsszenarien orientieren. Daran anschließend werden entsprechende Gegenmaßnahmen zur Vermeidung oder Beherrschung der als wahrscheinlich erachteten Gefährdungen angeboten.

Verschiedene Repräsentationsmöglichkeiten werden in /Beie00/ vorgestellt. Safe-CAD verwendet „if-then“-Regeln zur Darstellung, wodurch ein Regelinterpreter zur Wissensverarbeitung erforderlich wird. Eine klare Trennung zwischen Wissensbasis und Wissensverarbeitung sorgt darüber hinaus für eine gute Wartbarkeit. Die gewählte Wissensdarstellung durch Boole'sche-Regeln unterstützt diese Trennung /Pupp91/.

Für die Implementierung des Systems wurde ein semantisches Netz als Mittel der Wissensrepräsentation gewählt. Eine besondere Form des Netzes ist der Baum, der die einzelnen Knoten in einer Hierarchie anordnet. Vorteile der Baumstruktur sind leichte Programmier- und Wartbarkeit. Voraussetzung für die Anwendung der Baumstruktur ist die hierarchische Ordnung des Wissens. Durch die Gliederung in Module und Untermodule wurde dem Rechnung getragen.

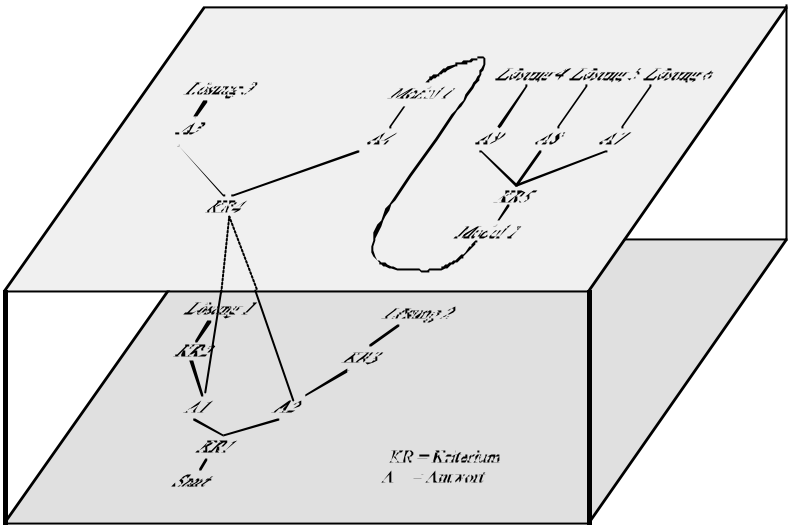


Bild 9-2: Regelstruktur

Bild 9-2 zeigt einen Ausschnitt aus der Regelstruktur des Programms. Die Wurzel (Root) repräsentiert den Ausgangspunkt, die einzelnen Zweige die Zwischenlösungen (Antworten) und die Blätter die Problemlösungen. Eine Charakteristik der Baumstruktur ist, wie allgemein in hierarchischen Systemen, eine Vereinfachung der Verwaltung und Navigation. Die Rekursion innerhalb der Fragenmenge eines Baumes ist restriktiv, so daß jede Lösung über einen eigenen Weg läuft. Bei beispielsweise drei aufeinander folgenden Parametern mit jeweils zehn Lösungen ergibt sich somit bei der Baumstruktur eine maximal mögliche Anzahl von Knoten beziehungsweise Lösungen in Höhe von $10^3 = 1000$. Jede Kombination von Eingangsgrößen führt zu einer eigenen Lösung und damit zu einer enormen Lösungsmenge. Der Vorteil ist eine einfache Verwaltung und Lösungssuche. Der Nachteil ist eine Unzahl redundanter Regeln („Regelspaghetti" /Pupp91/).

Im Gegensatz dazu ermöglicht SafeCAD auch Querverbindungen, das heißt durch Kombination verschiedener Antworten ergeben sich neue Kriterien. Die Modularisierung in Verbindung mit Mehrfachverwendung vermeidet bei entsprechender Programmierung einen übermäßigen Redundanzgrad in der Lösungsmenge. Dabei ist ein Sprung von verschiedenen Stellen innerhalb des Baumes in denselben Unterbaum, also Untermodul, möglich. Das heißt, die Baumstruktur wird dahingehend verletzt, daß horizontale Verzweigungen zulässig sind. Ein Ebenenwechsel durch Sprung zu einem Modul als Folge auf eine Antwort ist in Bild 9-2 dargestellt. Für die Wissensrepräsentation wurde ein Format gewählt, das die Regeln als semantisches

Netz darstellt, sich an der Baumstruktur orientiert, ohne den Restriktionen des Baumes zu unterliegen. Grafisch wird der Unterschied in Bild 9-3 und Bild 9-4 deutlich:

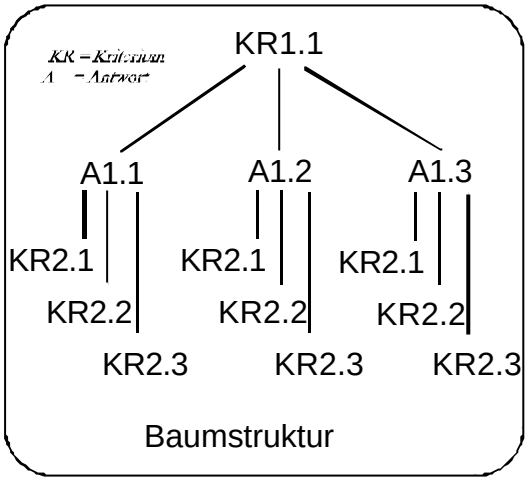


Bild 9-3: Baumstruktur

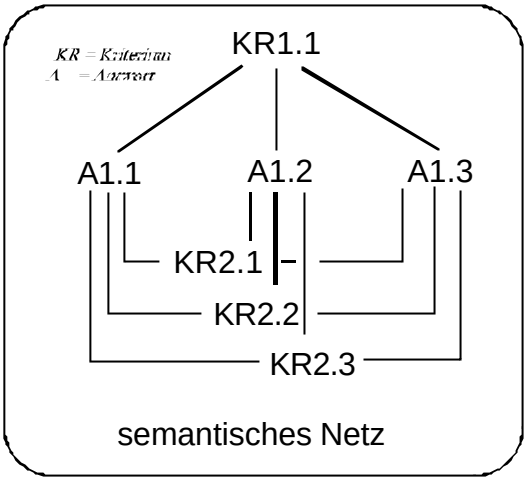


Bild 9-4: Semantisches Netz

In der Baumstruktur kann zu einem Knotenpunkt nur von einem Punkt aus navigiert werden. Im semantischen Netz hingegen kann ein Knotenpunkt von mehreren Punkten aus erreicht werden. Dies erleichtert die Anwendung bei der Wissensfüllung, verlangt aber dafür eine strukturierte Abarbeitung der einzelnen Wissensgebiete, um die Übersichtlichkeit für die Wartung und Pflege des Systems nicht zu verkomplizieren. Die Vorgehensweise ist deterministisch, die Zweige sind nicht mit Wahrscheinlichkeiten belegt, das heißt eine Antwort beziehungsweise eine Gruppe von Antworten hat immer dieselbe Frage als Folge.

Zur Implementierung der beiden Module Editor und Analyzer wurde Microsoft Visual C++ 6.0 verwendet. Dabei kommt die Klassenbibliothek „WAPIO"[8] zum Einsatz. Vorteil der Anwendung von MS Visual C++ ist die Schaffung einer benutzerfreundlichen Oberfläche des Analyzers, die die Akzeptanz des Systems beim Anwender erhöht.

Bei der Wissensakquisition bzw. den daraus resultierenden Regeln wurde darauf geachtet, diese möglichst allgemeingültig zu halten und nicht bestimmte Sonderfälle abzudecken. Das in SafeCAD implementierte, modifizierte PAAG-Verfahren bezieht sich auf Apparatetypen, nicht auf bestimmte Prozesse. Somit ist SafeCAD auf alle Anlagentypen anwendbar, die die in SafeCAD behandelten Apparatetypen aufwei-

[8] Win32APIObjects

sen. Sonderfälle können dann nach entsprechender Erweiterung der Wissensbasis bearbeitet werden.

9.2 Aufbau von SafeCAD

Das Programm besteht aus einem Editor und dem Analyzer. Im Editor kann der Experte eine beliebige Anzahl an Modulen und Untermodulen anlegen. Innerhalb der Module und Untermodule formuliert der Experte sein Wissen in Form von geschlossenen Fragen mit dazugehörigen Antworten. Des weiteren soll es einem Experten möglich sein, ohne Programmierkenntnisse sein Wissen zu formulieren und in der Wissensbasis zu verwalten. Dabei sind folgende Aufgaben zu erfüllen:

1. Konsultation des Experten
   Der Experte kann die Wissensbasis selbständig verwalten. Dazu gehört:

   - Formulierung der Regeln ohne Kenntnis einer Programmiersprache.
   - Eingabe der Regeln entsprechend dem üblichen Arbeitsablauf zur Lösung des Problems.
   - Übersichtliche Darstellung der Wissensbasis.
   - Testmöglichkeit des Expertensystems während der Konsultationsphase.

2. Befragung des Anwenders zur Konfiguration der Anlage.
   Die Befragung sollte für den Benutzer möglichst transparent erfolgen, damit dieser sich auf die fachliche Bearbeitung des Problems konzentrieren kann. Das bedeutet für das Programm unter anderem:

   - Einfache Benutzerführung und Navigation in der Liste der Fragen.
   - Wenn möglich, Formulierung der Fragen als Entscheidungsfragen („Multiple Choice“).
   - Auf Wunsch Erläuterung und Hilfe zu Fragen und Antworten in Form eines Hypertextsystem, welches auf Maus-Klick Hilfetexte zur Verfügung stellt.
   - Problemorientierte Abfolge der Fragen.
   - In Abhängigkeit von den gewählten Lösungen Unterdrückung irrelevanter Fragen.

3. Finden einer Lösung für das ermittelte Problem

   Der Lösungsweg als auch die einzelnen Zwischenlösungen sollten für den Anwender transparent sein. Jedes Problem sollte eine eindeutige Lösung besitzen.

4. Präsentation der Lösung und Dokumentation des Lösungsweges

   Die Lösung besteht aus einer Auslegungsalternative der gewählten Teilanlage im dwg-Format unter Berücksichtigung der während der Sitzung evaluierten Gefährdungen in Form von Sicherheits- und Instrumentierungsvorschlägen. Diese wird darüber hinaus als HTML-Dokument ausgegeben (siehe Bild 9-8).

9.2.1 Editor des Programms

Der Experte kann einzelne Fragen erstellen. Eine der Fragen wird als Startpunkt (Root) festgelegt. Jeder Frage wurden folgende Komponenten zugeordnet:

- Fragetext: dient der Formulierung der Frage.
- Textfeld für Gesetze: dient dem Verweis oder der Angabe von Gesetzen, die die Frage betreffen.
- Mehrere Antworten: als Vorgabe zur Lösung einer Frage.
- Hilfetext: dient der Erläuterung der Antworten. Zusätzliche Informationen, Firmeninterna etc. können hier ebenso hinterlegt werden.
- Ein „Sprungziel“: legt die Folgefrage fest, falls diese nicht durch die Antworten spezifiziert wird.
- Beliebige Aktionen: dies sind hauptsächlich Wertzuweisungen an Variable. Zur Formulierung der Aktionen (Regeln) wurde eine Scriptsprache entwickelt, die eine Untermenge der Sprache Java beziehungsweise JavaScript enthält. Der Regelinterpreter wertet diese Regeln aus, um die nächste Teillösung zu finden. Java wurde als Sprache gewählt, da deren Syntax einfach und weit verbreitet ist. Folgende Aktionen sind derzeit implementiert:
  - Änderung des Sprungziels unter Verwendung komplexer Ausdrücke.
  - Wertzuweisung an Antworten und Variable unter Verwendung komplexer Ausdrücke.

- Ergebnisausgabe in das Ausgabemedium (als Ausgabemedium sind derzeit ASCII-, XML- und HTML- Formate möglich) unter Verwendung von:
  - Parametern,
  - Variablenreferenzen und
  - komplexen Ausdrücken.
- Nachricht an den Anwender.

Es gib auch die Möglichkeit, die Textfelder für die Hilfe und Gesetze auszulassen. Bild 9-5 zeigt einen Ausschnitt der Bearbeitungsoberfläche des Editors.

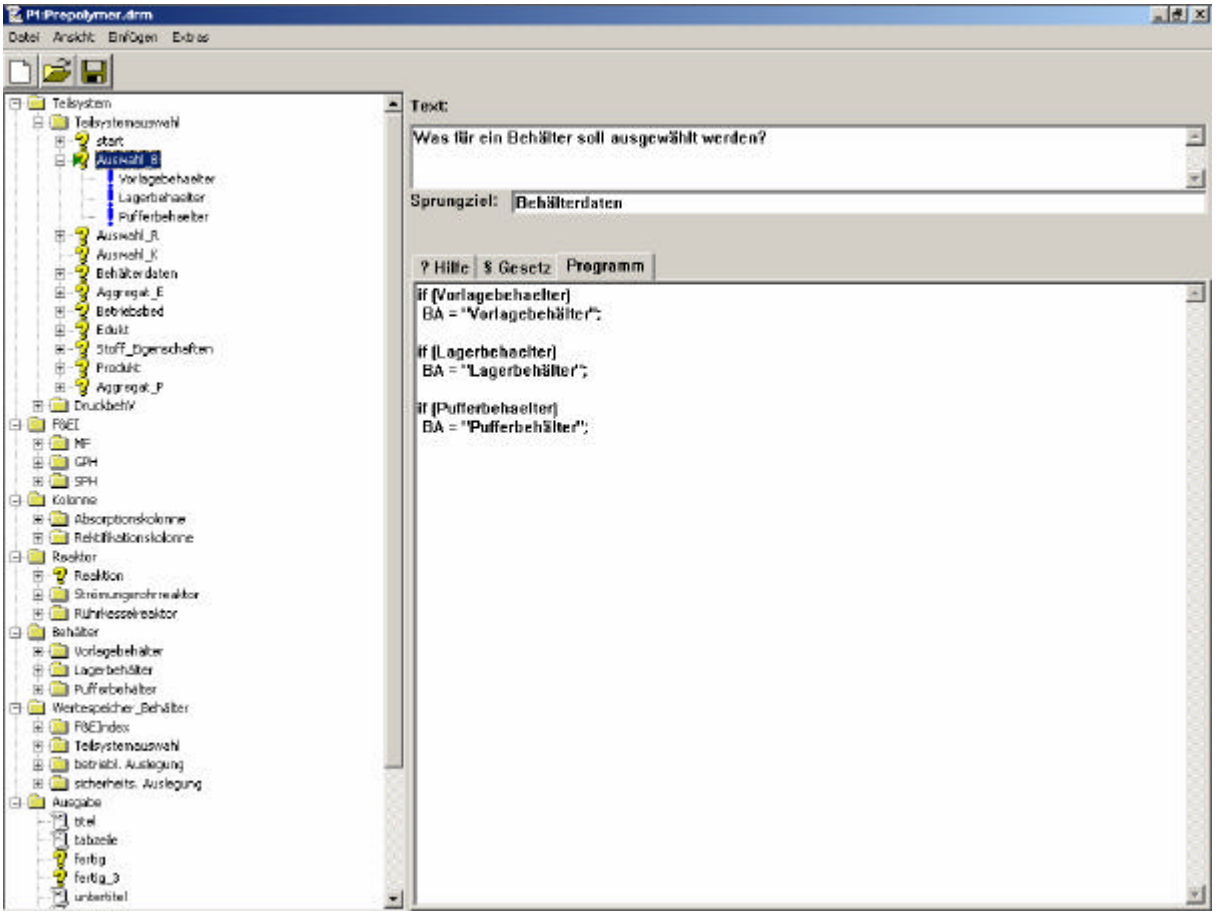


Bild 9-5: Editor des Programms

Im günstigen Fall führt jede Antwort zu einer neuen Zwischenlösung. Darüber hinaus können beispielsweise verschiedene Antworten zu derselben Frage führen oder die Reihenfolge der Fragen auf der Grundlage weiter zurückliegender Antworten ermittelt werden. Jede Antwort kann als Datenspeicher dienen. Das heißt, es können entweder Werte eingegeben oder durch Programmierung zugewiesen werden. Diese Wer-

te können später bei der Programmnutzung abgefragt oder in der Auswertung ausgegeben werden. Folgende Datentypen sind vorgesehen:

- Ja/Nein: wird als Checkbox dargestellt und kann die Werte „true" oder „false" enthalten: Einsatz z.B., um die Möglichkeit der Entstehung einer Gefährdung festzulegen. Diese wird dann mit den gewählten Maßnahmen in der Auswertungsdatei angezeigt.
- Zeichen: beliebige Eingabe. Einsatz z.B. zur Festlegung der Maßnahmen bzw. deren Ausgabe in der Auswertungsdatei.
- Zahl: Gleitkommazahlen mit dem Format entsprechend der Einstellung in der Systemsteuerung des Computers. Einsatz z.B. um den F&EI zu ermitteln.
- Ganzzahl: nur Ziffern und die Zeichen + und -. Einsatz z.B. um den F&EI zu ermitteln.

Bild 9-6 zeigt den entsprechenden Ausschnitt aus dem Editor.

Bild 9-6: Auswahl des Datentypes

Insgesamt lassen sich die Vorteile des Editors wie folgt beschreiben:

- Darstellung als semantisches Netz.
- Deklarative Beschreibung der Fragen und Antworten.
- Einfache Anweisungen zur Regelformulierung.
- Möglichkeit der prozeduralen Steuerung der Navigation.
- Erstellung beliebig vieler Submodule (Hierarchie).
- Anschauliche Oberfläche zur Erleichterung der Bearbeitung.

9.2.2 Analyzer des Programms

Die Benutzerschnittstelle wird durch den Analyzer präsentiert. Dem Anwender werden die Fragen der Wissensbasis anschaulich über die im folgenden Bild gezeigte Oberfläche angeboten. In Abhängigkeit des vom Nutzer ausgewählten Teilsystems werden ihm Fragen zur Auslegung gestellt. Dabei bestimmen die Antworten die Folge der Fragen und damit auch die schrittweise Navigation im Lösungsraum hin zur Gesamtlösung.

Dem Anwender stehen hierbei die problembezogenen Hilfetexte zur Verfügung, die über die Hilfetextfelder des Editors in das Programm vom Experten eingegeben wurden. Zusätzlich wird ihm der Fortschritt der Problemlösung angezeigt. Der Anwender kann an jedem Punkt der Problemdarlegung seine Antworten revidieren, indem er im Netz der Fragen rückwärts navigiert. Die Antworten können an jedem Punkt der Problemlösung abgespeichert und später weiterbearbeitet werden. Somit ist auch eine einfache Generierung mehrerer Varianten möglich. Ein Beispiel einer Frage zeigt das folgende Bild.

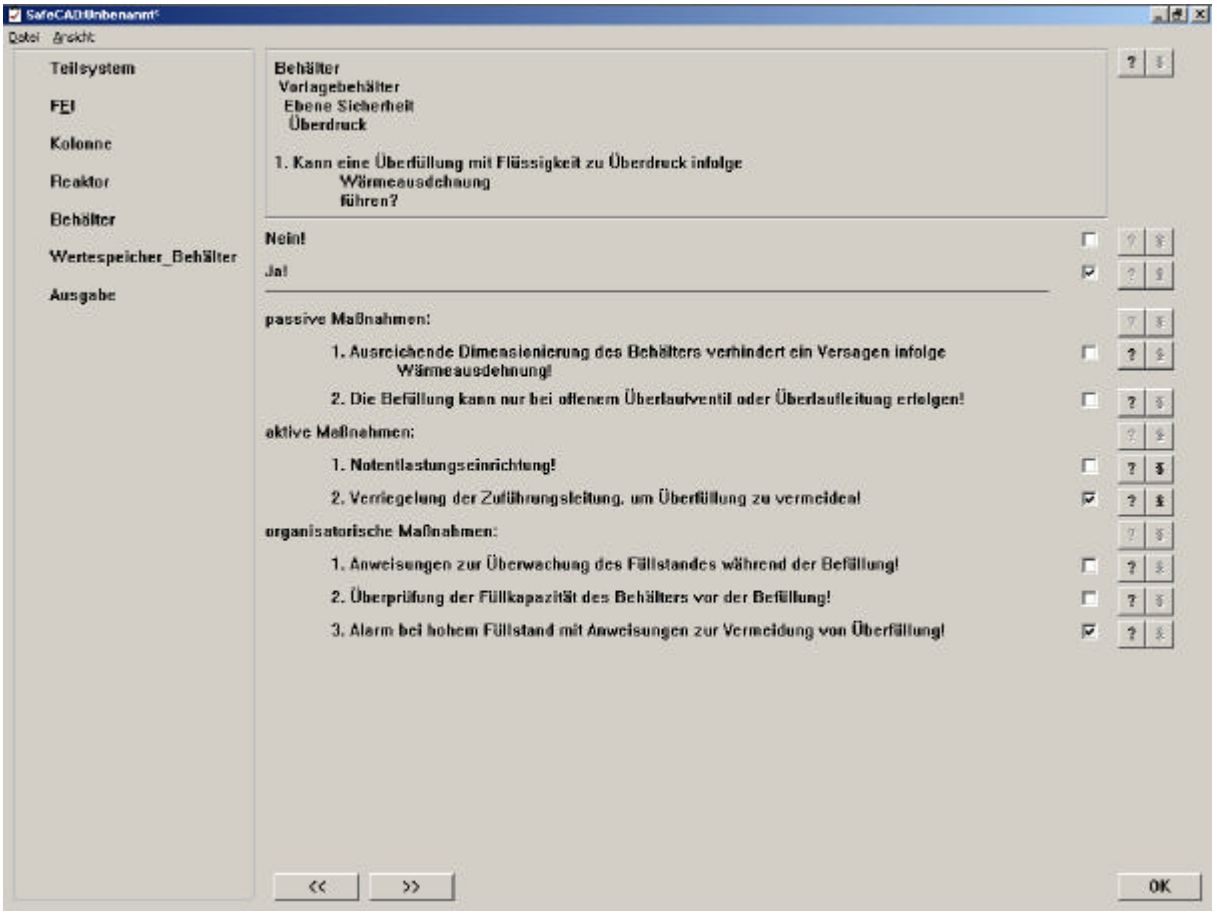


Bild 9-7: Analyzer des Programms

Die Hilfetexte zu der Frage und den Antworten wird durch Mausklick auf das ? – Symbol (siehe Bild 9-7) sichtbar. Ebenso können einschlägige Gesetze angezeigt werden. Dazu muß entsprechend das § – Symbol angeklickt werden. Ist keine Hilfe bzw. kein Gesetz hinterlegt, erscheinen die Symbole als Wasserzeichen.

9.2.3 Lösung SafeCAD

SafeCAD sucht im Dialog mit dem Benutzer die dem Gefahrenpotential der gewählten Teilanlage geeignete Konfigurierung der Einrichtungen der betrieblichen sowie überwachungsseitigen Ebene und Schutzebene. Dazu sind Angaben

- zur Teilanlage (Vorlagebehälter, semi-batch Reaktor, Absorptionskolonne),
- zu Masse, Toxizität, Reaktivität der Edukte, Zwischenprodukte und Produkte und
- zum F&EI

nötig. Im weiteren Verlauf werden über den Dialog die betriebliche Ebene der Teilanlage festgelegt. Im einzelnen sind dies die Punkte (am Beispiel des Vorlagebehälters):

- Rührerregime
- Regelung der Kühlung / Heizung
- Regelung des Drucks
- Regelung der Zu- und Abführung
- Regelung der Inertisierung

Darauf aufbauend werden über die PAAG-basierte Vorgehensweise (siehe Tabelle 7-4) die denkbaren Gefährdungen ermittelt. Aus einer Liste kann sich der Anwender die geeignetsten Gegenmaßnahmen für die als möglich erachteten Gefährdungen auswählen. Dabei wird er durch Hilfetexte unterstützt.

Das Ergebnis von SafeCAD wird zum einen in einer HTML-Datei mit Angabe der Gründe für die gewählten Entscheidungen ausgegeben (Erklärungskomponente), zum anderen werden die Entscheidungen bezüglich der Auslegung der betrieblichen

und überwachungsseitigen Ebene sowie Schutzebene unter Berücksichtigung der Redundanz- und Diversitätsanforderungen in eine CAD Zeichnung umgesetzt.

Einen Ausschnitt der Lösung des Systems als HTML-Datei zeigt Bild 9-8. Die HTML-Datei bietet den Vorteil einer individuellen Formatierung, wie zum Beispiel:

- Gestaltung von Tabellen.
- Formatierung von Überschriften.
- Einfügen von Bildern.
- Einfügen von Literaturstellen und Hyperlinks etc.

Auswertung der Teilanlage: Vorlagebehälter

Allg. Apparateangaben

TOP

allg. Angaben	Betriebsparameter		Lösung
Vol. des Behälters [im m3]			4,00

Gefahrenpotential

TOP

S1	S2	S3	Lösung
Material Factor			4

betriebl. Auslegung

TOP

S1	S2	S3	Lösung
Die Füllstandsregelung erfolgt über die			Zuleitung

überwachungsseitige Auslegung

TOP

S1	S2	S3	Lösung
Alarm erfolgt bei			zu hohem und zu tiefem Füllstand

sicherheitst. Auslegung

TOP

S1	S2	S3	Lösung
Mögliches Gefährdungsscenario	Überdruck durch	Überfüllung mit Flüssigkeit führt zu Überdruck infolge Wärmeausdehnung!	
	passive Maßnahme(n)		
			Ausreichende Dimensionierung des Behälters verhindert ein Versagen infolge Wärmeausdehnung!
	aktive Maßnahme(n)		
			Notentlastungseinrichtung!
			Verriegelung der Zuführungsleitung, um Überfüllung zu vermeiden!
	organisatorische Maßnahme(n)		
			Anweisungen zur Überwachung des Füllstandes während der Befüllung!

Bild 9-8: Ausschnitt der Lösung im HTML-Format

Im CAD-Format besteht die Möglichkeit, zwischen zwei Anzeigemodi zu wählen. Zum einen kann die Lösung als vollständiges R&I angezeigt werden. Dies setzt jedoch voraus, daß dem System eine Zeichnung vorgegeben wurde, die dann im Verlauf des Dialogs mit dem Anwender auf Grundlage der getroffenen Entscheidungen bearbeitet wird. Hierzu muß der Bearbeitungsalgorithmus gemäß Abschnitt 9.3 vollständig im Programm implementiert sein. Diese Vorgehensweise bietet sich für weitgehend standardisierte Verfahren an, da die Fließbilder dieser Verfahren sehr ähnlich sind und so dem Programm nur einmal vorgegeben werden müssen.

Darüber hinaus besteht die programmtechnisch weniger aufwendige Möglichkeit, nur die Teilsysteme (wie Reaktorkühlung, Druckentlastung etc.) im CAD-Format abzubilden. Diese müssen dann vom Bearbeiter in das Fließbild integriert werden. Dieser Möglichkeit bietet den Vorteil, daß die Adressierung der Teilsysteme innerhalb des Fließbildes vom Anwender frei gewählt werden kann. Der Aufwand der Implementierung ist aufgrund der Anwenderfreundlichkeit des Programms sehr gering. Ein Beispiel für die Komponenten einer Prepolymeranlage der Gefahrenpotentialkategorie „gering“ zeigt das folgende Bild. Ausführlich wird die Industrieanlage und die Lösungen SafeCAD’s für die drei Gefahrenpotentialkategorien in Abschnitt 10.2 beschrieben.

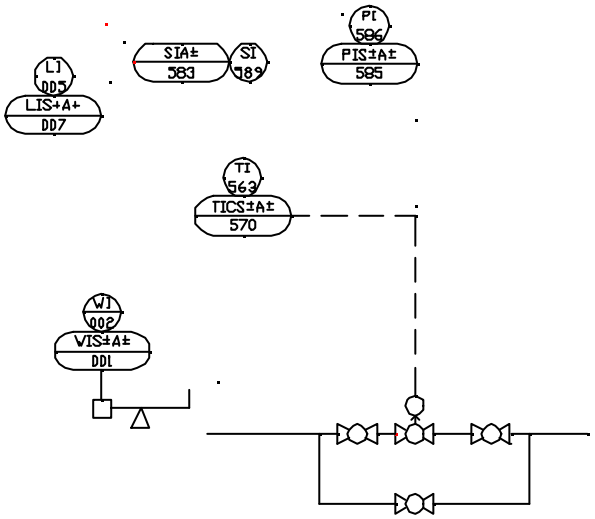


Bild 9-9: Ausgabe der Lösung als Teilsystem im CAD-Format

Einen Vorteil bietet diese Vorgehensweise bei der Behandlung von Mehrstoffanlagen. So können Teilsysteme für die Auslegung der verschiedenen Reaktionen einfach miteinander kombiniert werden; für alle Reaktionen geltende Komponenten

werden bei den anderen Programmdurchläufen gelöscht und nur die neu hinzukommenden müssen in die Zeichnung integriert werden. Die HTML-Dokumentation weist jeder Komponente eindeutig ihren Aufgabenbereich zu.

Übersichtlich zeigt das folgende Bild noch einmal die Gesamtstruktur des Systems:

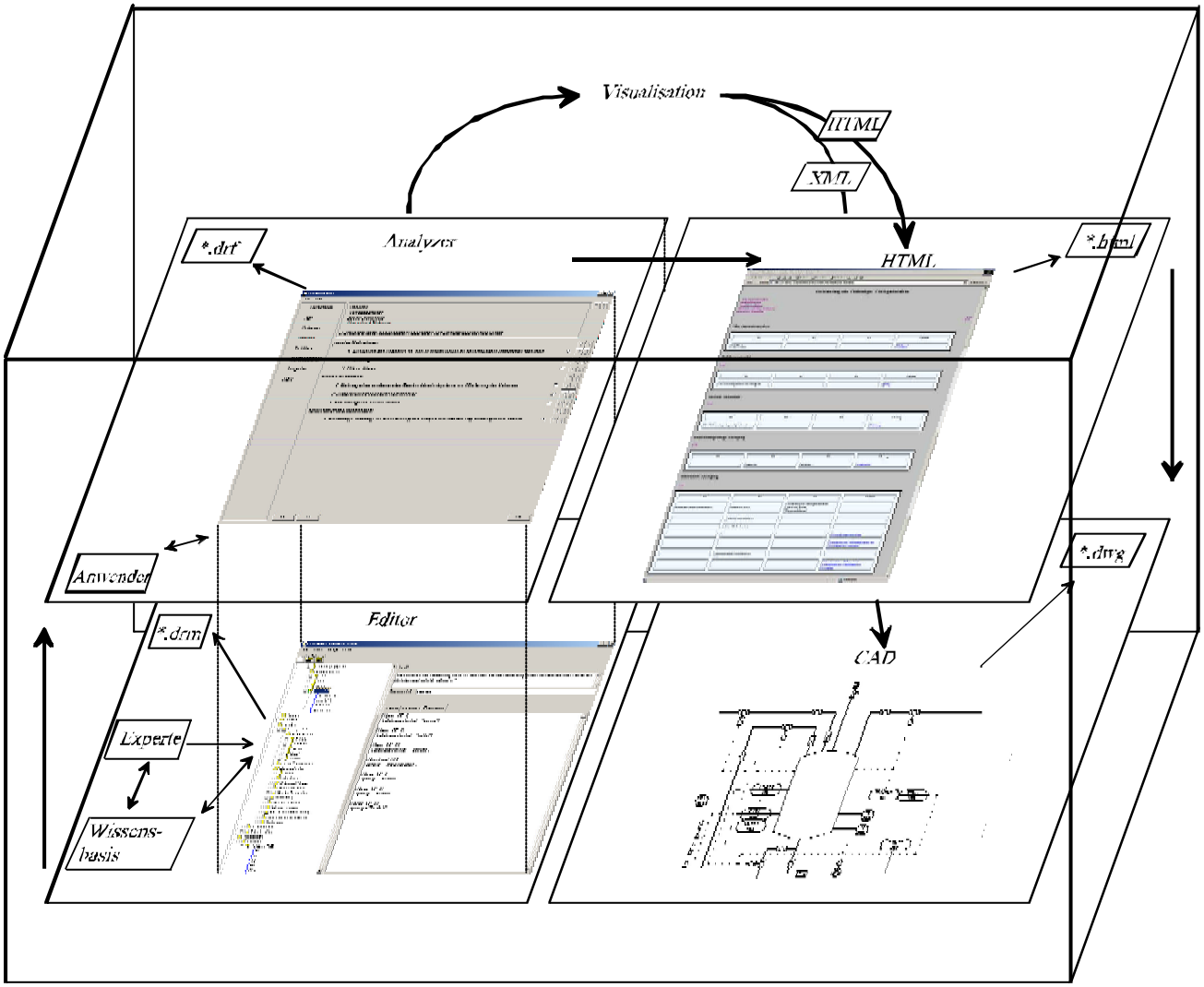


Bild 9-10: Aufbau des Expertensystems

Wendet man nun die gemäß Bild 3-1 wünschenswerten Eigenschaften eines idealtypisch guten Expertensystems auf SafeCAD an, so ergibt sich:

	Forderungen	**Lösung des Systems**
1	*Anwendung des Wissens eines oder mehrerer Experten zur Lösung von Problemen in einem bestimmten Anwendungsbereich.*	Durch Gliederung in Teilsysteme wird der Anwendungsbereich klar abgegrenzt.
2	*Explizite, möglichst deklarative Darstellung des Expertenwissens.*	Siehe ersten Abschnitt nach der Tabelle.
3	*Unterstützung des Wissenstransfers vom Experten zum System*.	Leichte Programmierbarkeit über wenige und einfache Befehle im Editor ermöglichen es dem Experten, ohne die Schnittstelle eines Wissens-Ingenieurs, die Wissensbasis zu erweitern und zu pflegen.
4	*Leichte Wartbarkeit und Erweiterbarkeit des im System enthaltenen Wissens.*	Durch Aufteilung in Editor und Analyzer ist dies gegeben.
5	*Darstellung des Wissens in einer leicht lesbaren Form*.	Unterstützung durch Hilfetexte, die in einfachen Textfeldern angeboten werden.
6	*Verwendung unsicheren Wissens (Sowohl Expertenwissen als auch Wissen über einen gegebenen Fall ist oft mit Unsicherheiten verbunden).*	Eine Lösung hierfür ist nicht vorgesehen.
7	*Möglichst natürliche und anschauliche Benutzerschnittstelle.*	Durch benutzerfreundliche Gestaltung des Analyzers wurde dieser Punkt umgesetzt.
8	*Begründung und Erklärung der Ergebnisse.*	Durch Formulierung der Fragen und Antworten sowie Unterstützung durch Hilfetexte. In der Ausgabe werden die Lösungswege ausgegeben.
9	*Klare Trennung von Faktenwissen und Problemlösungsheuristiken.*	Erfolgt, indem die Regelauswertung durch den Interpreter vorgenommen wird.
10	*Wiederverwendbarkeit von einmal erworbenem Wissen in verwandten Problembereichen.*	Durch Zuordnung von verschiedenen Lösungen zu Einzelproblemen bereits programmintern gelöst.

Bild 9-11: Zur Qualitätsbeurteilung von SafeCAD

Im Editor erfolgt die Beschreibung der Fragen und Antworten deklarativ, das heißt, die Darstellung der Fragen und Antworten erfolgt im Analyzer über das Programm. Dabei spielt der zugeordnete Typ (siehe Bild 9-6) keine Rolle. Die Wahl eines semantischen Netzes unterstützt die deklarative Darstellung der Wissensbasis. Safe-

CAD ermöglicht darüber hinaus durch einfache Anweisungen zur Regelformulierung eine prozedurale Steuerung der Navigation. Somit erfüllt das Programm die Forderungen von *Friedrichs et. al* /Frie90/ in diesem Punkt, geht aber durch die Möglichkeit der eigenständigen Regelformulierung noch darüber hinaus. Dadurch, daß der Experte im semantischen Netz Sprungziele vorgeben kann, wird die Problemlösungsheuristik transparent. Somit wird hier dem Punkt 2 in Bild 9-11 teilweise widersprochen, der Grundgedanke bleibt jedoch erhalten. Wenige Anweisungen konzentrieren sich nun auf die Darstellung des Wissens. Die Regeln führen von einer Teillösung zur nächsten. Somit muß nicht ein Algorithmus formuliert werden, der direkt zur Gesamtlösung führt. Dadurch wird die Abarbeitung von komplexen, anspruchsvollen technischen Problemen möglich.

Das vorliegende System kann nicht als Ersatz für Expertenleistungen angesehen werden. Es kann einen Experten keinesfalls ersetzen. Dieses Kriterium erfüllt bisher auch noch kein Expertensystem /Wach95/. Vielmehr soll es den Anwender bei der sicherheitstechnischen Auslegung einer Teilanlage unterstützen, denn die Kontrolle durch den Menschen ist essentiell. Eine unkritische Übernahme von Lösungen ist aufgrund der genannten Schwachstellen eines Expertensystems gefährlich. So schreibt *Puppe* /Pupp91/, daß ein Expertensystem unter anderem in solchen Gebieten eingesetzt werden sollte, wo *das Expertensystem keine endgültige Entscheidung trifft, sondern in einen redundanten Entscheidungsprozeß eingebettet ist*.

Weiterhin schreibt *Puppe* /Pupp91/, mittelfristiges Ziel sei es, Expertensysteme zu entwickeln, die es dem Experten ermöglichen, ohne die Schnittstelle „Wissensingenieur" ihr Wissen eigenständig formalisiert in das System einzubringen und auszutesten. Durch die Aufteilung des Systems SafeCAD in einen Editor und einen Analyzer ist dies gelungen. Lediglich wenige, leicht erlernbare Befehle befähigen den Experten dazu, sein Wissen in die vorgegebene Struktur einzubinden. Über den Aufruf des Analyzers können die Neuerungen jederzeit problemlos überprüft werden. Da der Editor eigene Dateien erzeugt, kann dies unabhängig von bestehenden Strukturen vorgenommen werden, indem einfach eine neue Datei gleichen Inhalts angelegt wird.

Somit ergeben sich durch den begleitenden Einsatz von SafeCAD während der Entwicklung von Anlagen folgende Vorteile /Göri93/:

- Verkürzung der sicherheitstechnischen Durchsprache in der Anlagenplanung.
- Zeitersparnis durch die automatische Übernahme von Fließbildinformationen.
- Fließbildübergreifende Vorgehensweise zur Vermeidung leicht übersehbarer Fehler.
- Gleichbleibende Qualität und Nachvollziehbarkeit der durchgeführten Betrachtungen aufgrund der standardisierten Vorgehensweise.
- Durchführung von Routineüberprüfungen und damit Entlastung von Fachexperten.
- Verwendung als Schulungssystem.
- Sicherung vorhandenen Wissens bei Ausscheiden oder Abwesenheit von Fachleuten.

Im Anschluß an diese Vorgehensweise kann unter Umständen die Durchführung einer probabilistischen Analyse der Gesamtanlage sinnvoll sein. Somit kann überprüft werden, ob die optimierten Teilanlagen die optimale Auslegung der Gesamtanlage ausreichend gut annähern.

9.3 SafeCAD und CAD

Grundlage für die Darstellung der Lösung als CAD-Zeichnung ist die Erzeugung der Lösungsmenge im Phyton-Format /www.pyth/. Durch den Editor werden die Phyton-Befehle automatisch erzeugt. Dazu wurden verschiedene Phyton-Tools programmintern hinterlegt. Diese werden parallel in Abhängigkeit von der Lösung des Expertensystems über den Analyzer in eine Datei geschrieben. Das CAD-System greift über das Aufsatzprogramm ACFlow 2D /www.acpl/ auf diese Datei zu und erstellt daraus auf der Grundlage bestehender Zeichnungen der entsprechenden Teilsysteme die Lösung als CAD-Zeichnung. Dies hat den Vorteil, daß firmeninterne Regelungen und gesetzliche Vorgaben direkt in den Vorlagezeichnungen umgesetzt werden können. Die Erstellung eines R&I-Fließbildes aus dem „Nichts“ ist programmtechnisch wegen der Schwierigkeit der Zuordnung der Adressen innerhalb des CAD-Systems nur mit einem enormen Aufwand zu betreiben. Dieser ist für den gedachten Anwendungsfall aber nicht erforderlich, da vorhandenes Wissen strukturiert angeboten werden soll und dazu bietet sich die Bearbeitung von Zeichnungsvorlagen wesentlich besser an. Derzeit besteht die Möglichkeit, über die Phyton-Tools Ausrüstungen zu löschen und

die PLT-Symbole zu bearbeiten. Es können zusätzliche Funktionen eingefügt werden oder ein Zuviel an Meß- und Regelfunktionen eliminiert werden.

AutoCAD weist jedem Zeichnungselement zur eindeutigen Identifizierung automatisch sogenannte „Handles“ zu. SafeCAD nutzt diese Handles in der Lösungsgenerierung zur korrekten Zuweisung der Phytonalgorithmen „Löschen“ und „Ändern“. Dabei möglicherweise auftretende „Lücken“ beispielsweise innerhalb der Rohrleitung nach Löschen eines Ventils werden vom Aufsatzprogramm ACFlow 2D automatisch geschlossen.

Mit ACFlow 2D können Schemazeichnungen gemäß DIN 28004 schnell und sehr einfach erstellt werden. Durch die offene Struktur des Programms ergeben sich vielfältige Anwendungsgebiete:

- Rohrleitungsplanung
- Chemie- und Industrieanlagenbau
- Nahrungsmittel- und Getränkeindustrie
- Energie- und Wasserwirtschaft
- Umwelt-/Wassertechnik
- Meß- / Regeltechnik
- Erstellung von Dokumentationen

Standardmäßig werden über 300 Symbole gemäß DIN 19227, Teil II über die Programmbibliothek angeboten. Bild 8-10 zeigt einen Ausschnitt aus der Symbole-Box, über die die ausgewählten Symbole in die Zeichnung eingefügt werden.

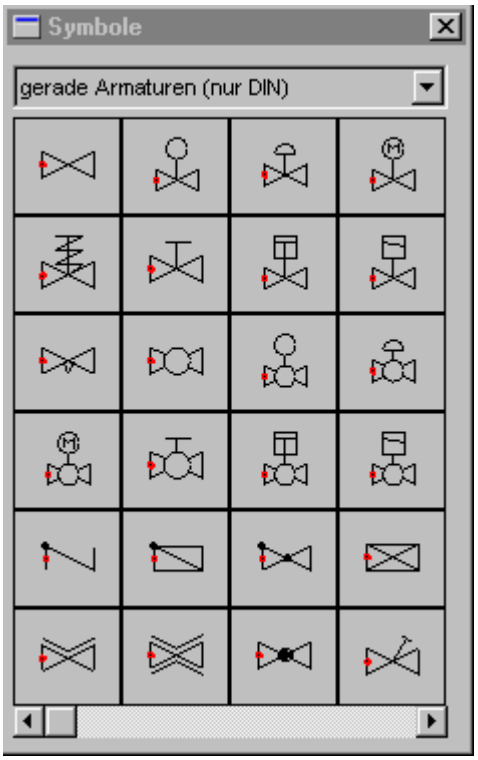


Bild 9-12: Symbol-Verzeichnis

Bild 9-13: Elementinspektor

Ein Assistent hilft bei der Erstellung eigener Symbole, die sofort automatisch in die bestehende Bibliothek eingebunden werden. Ein eigens für firmenspezifische Erweiterungen reservierter Bereich steht zur Verfügung und ermöglicht eine übersichtliche Verwaltung.

Ein Schema kann ohne Kenntnisse des darunterliegenden CAD-Systems (derzeit AutoCAD ®) einfach und intuitiv erstellt werden. Dabei wird der Anwender durch die Möglichkeiten des dahinterstehenden Objektmodells unterstützt. Zusammenhängende Teile werden als solche erkannt und entsprechend behandelt.

MSR-Symbole werden ebenso über das Symbol-Verzeichnis in die Zeichnung eingefügt. Die Kennzeichnung erfolgt über den so genannten Elementinspektor (Bild 9-13). Neben der Kennzeichnung und Numerierung können die Grenzwerte der Meßgrößen eingefügt werden.

SafeCAD wurde unabhängig von anderen Anwendungen konstruiert. So kann es in bestehende CAD-Systeme installiert werden, ohne daß es zu Komplikationen kommt. Das CAD Aufsatzprogramm ACFlow 2D ist nicht erforderlich. Die Lösungen im CAD-Format *.dwg sind in einer programminternen Datenbank abgelegt und so von jedem

dwg-tauglichen Programm darstellbar. Da für deren Entwicklung AutoCAD 14.01 verwendet wurde, empfiehlt sich allerdings für die Anwendung von SafeCAD die vorherige Installation von AutoCAD 14.01. Einzig für Erweiterungen oder Änderungen muß auch ACFlow 2D installiert werden.

Als Grundlage für SafeCAD wurde auf Standardsoftware zurückgegriffen, um die Vorteile dieser Programme in ihren Aufgabenbereichen unabhängig von SafeCAD weiter nutzen zu können. Darüber hinaus ist SafeCAD weitgehend unabhängig von der Hardware, so daß sich der Einsatzbereich des Systems verbreitert.

Die Anlagentopologie spielt bei SafeCAD derzeit keine Rolle, da Instrumentierungsvorschläge die Lösung des Systems sind. Denkbar ist jedoch, nach Einarbeitung der Vorschläge in das R&I, dieses in einem weiteren Entwicklungsschritt auszulesen. Unter der Voraussetzung, daß für die Fließbildgenerierung ACFlow 2D verwendet wird, ist dies auch möglich, da das Programm das Fließbild in einem Baum strukturiert ablegt. So kann z.B. die Anlage auf Konsistenz hinsichtlich Fließrichtung und möglicher offener Anschlüsse überprüft werden. Dies ist insbesondere hinsichtlich der Verknüpfung mehrerer Teilanlagen sinnvoll. Hierzu bedarf es jedoch, wie bereits erwähnt, einer Ergänzung von SafeCAD, die im Rahmen zukünftiger Weiterentwicklungen angestrebt werden sollte.

10 Anwendung auf industrielle Teilanlagen

In Anlehnung an Abschnitt 8.3 wird hier die Vorgehensweise auf zwei bestehende Anlagen angewendet. Es wird zum einen das Teilsystem „Vorlagebehälter“ behandelt, so daß die Ergebnisse des Abschnitts 8.3 transparenter werden. Zum anderen wird eine Anlage zur Herstellung von Prepolymer untersucht.

Der Ablauf des Programms wird in diesem Kapitel zusammengefasst dargestellt; der gesamte Dialog mit dem Anwender kann dem Anhang entnommen werden.

10.1 Vorlagebehälter

10.1.1 Anlagenbeschreibung

Der folgende Ausschnitt aus einem R&I-Fließbild zeigt das Beispiel eines Behälters, der als Vorlagebehälter für einen anschließenden Batch-Prozeß dient.

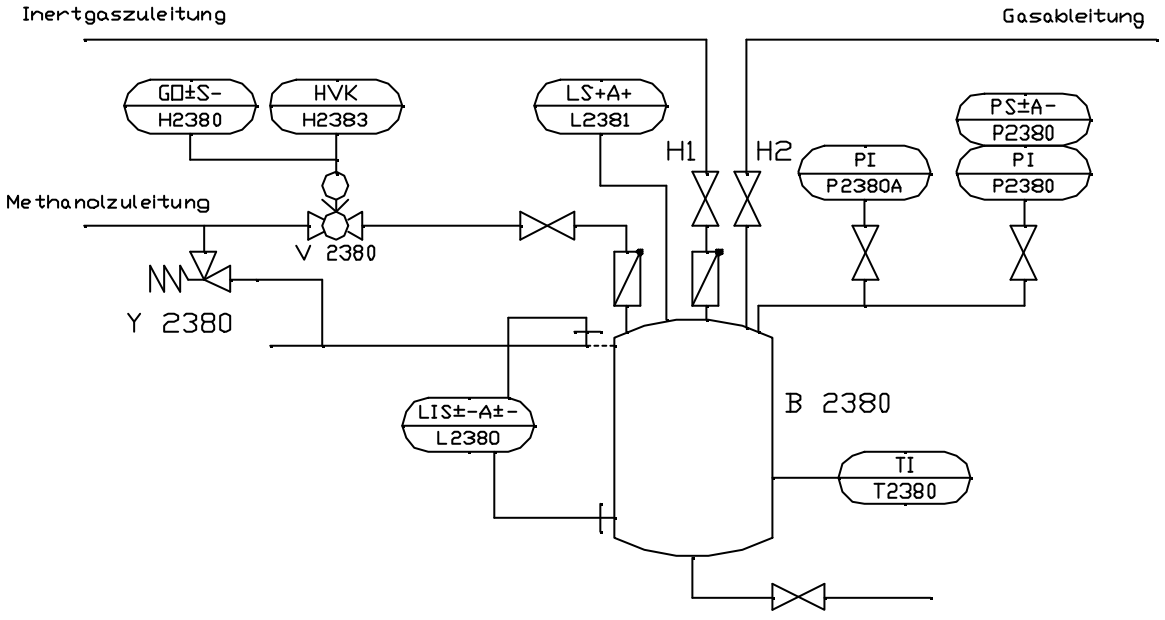


Bild 10-1: Methanol-Vorlagebehälter, Industrie-Beispiel

Die Befüllung des Behälters erfolgt über einen etwa 1 m^3 großen Methanol-Pendelbehälter, der in einem abgeschlossenen Raum an die Zuführungsleitung angeschlossen wird. Der Behälter wird immer erst bei Bedarf mit Methanol beschickt, d.h. wenn der Batch-Prozeß gefahren wird, so daß der Behälter nach der VbF (der Behälter wurde noch nach den Grundsätzen der VbF ausgelegt; diese wurde von der

Betriebssicherheitsverordnung /Betr02/ ersetzt) nicht als Lagerbehälter zählt, da Methanol nicht über einen Zeitraum von mehr als 24 Stunden ortsfest gelagert wird. Die Regeln der VbF wurden dennoch bei der Auslegung beachtet.

Zu Beginn der Befüllung wird vom Anlagenfahrer sichergestellt, daß die benötigte Menge Methanol auch im Behälter vorliegt. Dieser darf nicht vollständig leerlaufen (Brüdensperre). Ferner darf der maximale Befüllungsgrad von 80% nicht überschritten werden. Das abgasseitige Handventil wird geöffnet, so daß während des Befüllvorganges kein Druckaufbau stattfinden kann. Nach erfolgter Befüllung wird das Ventil wieder geschlossen und das Inertgas-Handventil geöffnet. Dadurch wird ein Arbeitsdruck von drei bar eingestellt. Das Ventil wird bei Erreichen des Arbeitsdruckes per Hand geschlossen. Der Zulauf in den tiefer liegenden Batch-Reaktor erfolgt zum einen schwerkraftbedingt aufgrund des Höhenunterschieds und zum anderen infolge des Druckes im Behälter, der allerdings mit sinkendem Füllstand abnimmt.

Da Methanol brennbar ist und ein explosives Gemisch mit Sauerstoff bilden kann, ist die Anlage entsprechend der Verordnung zum Explosionsschutz (§5 der Betriebssicherheitsverordnung) /Betr02/ nach Zone 1 im inneren und Zone 2 im Außenbereich des Behälters ausgelegt. Dazu wurden entsprechende Dichtungen gemäß Werksnorm des Industrieunternehmens ausgewählt. Der Behälter ist weder isoliert noch wird er gekühlt oder geheizt.

Eine Temperaturanzeige befindet sich vor Ort, eine weitere Überwachung und eventuelle Maßnahme gegen Temperaturanstieg ist nicht vorhanden.

Weiterhin wird der Druck sowohl vor Ort als auch in der Warte über einen Fühler mit entsprechender Messwertverarbeitung angezeigt. Alarm wird bei zu niedrigem Druck gegeben, da dann die Gefahr besteht, daß vom angeschlossenen Batch-Prozeß Gase/Dämpfe in den Behälter zurückströmen (eine Rückschlagklappe ist nicht vorgesehen) bzw. der Behälter durch Leerlaufen einem zu hohen Unterdruck ausgesetzt werden kann. In diesem Falle wird das Ventil in der Abführungsleitung automatisch geschlossen. Bevor der Batch-Prozeß gestartet werden kann, wird kontrolliert, ob der Druck im Behälter groß genug ist; erst dann erfolgt die Freigabe zur Öffnung der Abführungsleitung.

Außerdem kann der Batch-Prozeß erst gestartet werden, wenn ein Mindestfüllstand vorhanden ist. Wird der Mindestfüllstand unterschritten, so wird die Abführungsleitung automatisch geschlossen.

Ein zu hoher Druck im Behälter kann nur entstehen, wenn die Standregelung versagt und der Behälter bis zum Rand mit kaltem Methanol gefüllt wird. Eine kritische Druckerhöhung infolge des Überfüllens und Druckanstieges durch die Pumpe ist nicht möglich, da der Staudruck der Pumpe unter dem Auslegungsdruck des Behälters liegt. Unzulässiger Überdruck durch die Inertisierung ist betriebsbedingt ebenso nicht möglich, da auch der Druck in der Inertgasleitung unterhalb des Auslegungsdrucks des Behälters liegt. Mögliche Ausfälle in der Reduzierstation der Inertgasleitung sind äußerst selten und werden daher nicht berücksichtigt.

Da die Zuführungsleitung nach der Befüllung geschlossen wird, kann durch thermische Ausdehnung des Methanols in der Leitung der dadurch entstehende Überdruck deren zulässigen Überdruck übersteigen. Ein Sicherheitsventil in der Zuführungsleitung mit Ableitung in den Behälter verhindert dies.

Die bei der Auslegung der Anlage evaluierten Gefährdungen und die getroffenen Gegenmaßnahmen sind im einzelnen:

		Maßnahmen		
Gefährdung	**Fehlzustand**	**passiv**	**aktiv**	**organisatorisch**
Überdruck	Überfüllung mit Inertgas führt zu Überdruck.	Auslegungsbedingt nicht möglich!		
	Überfüllung mit Flüssigkeit führt zu Überdruck infolge Wärmeausdehnung im Behälter.		Verriegelung der Zuführungsleitung bei maximalem Füllstand.	Alarm bei zu hohem Füllstand mit Anweisungen.
	Überfüllung mit Flüssigkeit führt zu Überdruck im Behälter.	Auslegungsbedingt nicht möglich!		
	Entzündung der Dampfphase im Behälter.	Spülen des Behälters mit Inertgas.		

		Maßnahmen		
Gefährdung	**Fehlzustand**	**passiv**	**aktiv**	**organisatorisch**
Unterdruck	Durch Leerlaufen des Behälters entsteht ein unzulässiger Unterdruck.			Alarm bei zu geringem Füllstand mit Anweisungen.

Tabelle 10-1: Bei der Auslegung des Vorlagebehälters betrachtete Gefährdungen und die gewählten Gegenmaßnahmen

Die Funktionen der PLT-Symbole im Überblick sind:

	Funktion	Schaltung
$\frac{\text{LIS}\pm-\text{A}\pm-}{\text{L2380}}$	Steuert die Eduktzuführung. Anzeige des aktuellen Füllstands in der Leitwarte.	Schaltet ab einem bestimmten oberen Grenzwert die Eduktzuleitung ab. Bei einem festgelegten unterem Grenzwert wird die Abführungsleitung geschlossen. In beiden Fällen ertönt ein Alarm.
$\frac{\text{PS}\pm\text{A}-}{\text{P2380}}$	Überwachung des Behälterdrucks.	Schaltet ab einem bestimmten unteren Grenzwert die Abführungsleitung zu. Dies wird dann durch einen Alarm signalisiert.
$\frac{\text{LS}+\text{A}+}{\text{L2381}}$	Redundanz zur Sicherung gegen Überfüllung zu $\frac{\text{LIS}\pm-\text{A}\pm-}{\text{L2380}}$.	Schaltet ab einem bestimmten oberen Grenzwert die Eduktzuleitung ab. Zusätzlich erfolgt eine Alarmierung.

Tabelle 10-2: Funktionsbeschreibung der PLT-Symbole

Die Anwendung SafeCAD's auf das Industriebeispiel wird im folgenden Abschnitt beschrieben.

10.1.2 Abbildung des Vorlagebehälters durch das Expertensystem

Die Auswertung durch SafeCAD weist dem Gefahrenpotential der Anlage die Kategorie „gering" zu. Als Ergebnis des Dialogs mit dem Expertensystem ergibt sich für das Beispiel auf der betrieblichen Seite:

- Keine Temperaturregelung.
- Kein Rührerregime.
- Niveauregelung erfolgt über den Zulauf innerhalb einer Obergrenze zum Abschalten und einer Untergrenze zum Einschalten des Zulaufs.
- Druckregelung über Inertgas.
- Ablauf bestimmt durch nachfolgenden Prozeß.

Anschließend erfolgt die sicherheitstechnische Betrachtung des Vorlagebehälters. Insgesamt ergibt die Befragung zur Beispielanlage:

- Zu hohe Temperatur des Methanols sehr unwahrscheinlich.
- Hoher Druck durch Wämeausdehnung denkbar.
- Hoher Druck durch Pumpe auslegungsbedingt nicht möglich.
- Hoher Druck infolge Inertgasüberspeisung betriebsbedingt unwahrscheinlich.
- Eintritt/Zulauf eines anderen Mediums nur durch Abführungsleitung möglich.
- Als Prozeßsicherungsgröße kommt nur der Füllstand in Frage.

Die Zuordnung der entsprechenden Maßnahmen zu den betrachteten Gefährdungen zeigt folgende Tabelle:

		Maßnahmen		
Gefährdung	**Fehlzustand**	**passiv**	**aktiv**	**organisatorisch**
Überdruck	Überfüllung mit Inertgas führt zu Überdruck.	Auslegungsbedingt nicht möglich!		
	Überfüllung mit Flüssigkeit führt zu Überdruck infolge Wärmeausdehnung im Behälter		Verriegelung der Zuführungsleitung bei maximalem Füllstand.	Alarm bei zu hohem Füllstand mit Anweisungen.
	Überfüllung mit Flüssigkeit führt zu Überdruck.	Auslegungsbedingt nicht möglich!		
Unterdruck	Durch Leerlaufen des Behälters entsteht ein unzulässiger Unterdruck.		Verriegelung der Abführungsleitung bei minimalem Füllstand.	Alarm bei zu geringem Füllstand mit Anweisungen.

Tabelle 10-3: Ergebnis der Anwendung SafeCAD's auf einen Vorlagebehälter

Umgesetzt in das R&I-Format ergibt sich daraus die Auslegung entsprechend Bild 10-2.

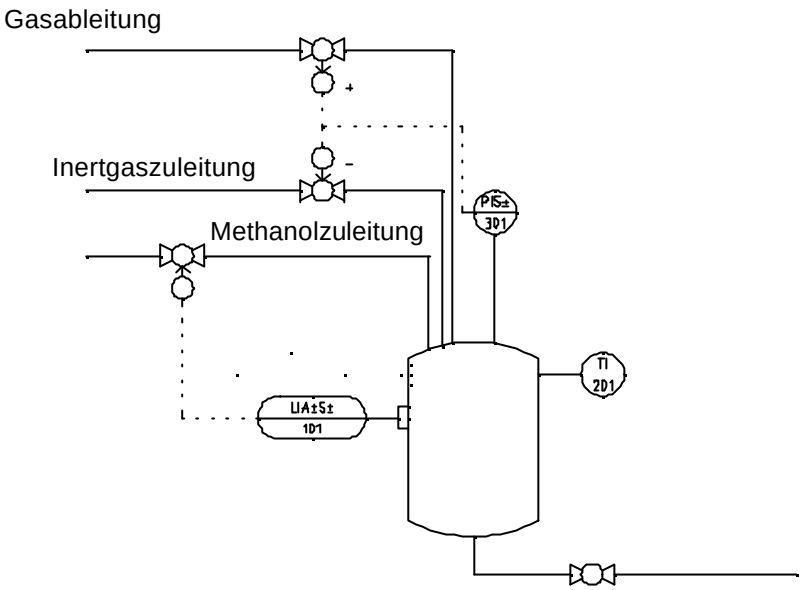


Bild 10-2: Ergebnis des Expertensystems für das Gefahrenpotential „gering“

Der Unterschied zur Industrieausführung besteht darin, daß der Zulauf und die Inertgasbespeisung automatisch eingeschaltet werden. Aufgrund der Einstufung als „gering“ durch den F&EI sind Redundanzen meß- und regelungstechnischer Art (bis auf den Druck) nicht vorgesehen. Dies entspricht ebenso der realen Anlage aus der Industrie. Die Einstellung des Drucks wird einfach ausgelegt, da Überdruck infolge Inertgasüberspeisung betriebsbedingt nicht möglich ist.

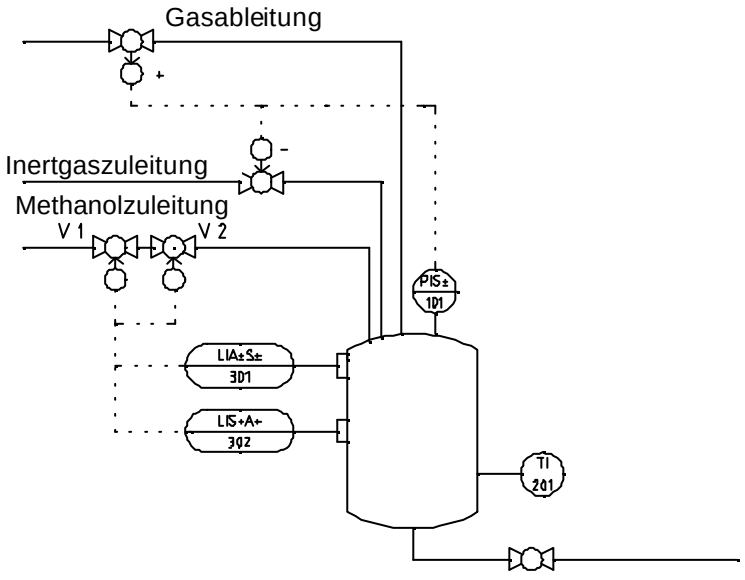


Bild 10-3: Auslegungsalternative für mittleres Gefahrenpotential

Sollte der Behälter unter sonst gleichen Bedingungen für eine größere Menge Methanol, z.B. 5000 l, oder eine gefährlichere Flüssigkeit ausgelegt werden, so würde

der F&EI von „gering“ auf „mittel“ ansteigen und die Auslegung mit Hilfe des Expertensystems würde Bild 10-3 entsprechen.

In diesem Fall wird der Füllstand redundant überwacht. Beide Absperrventile werden von beiden Sensoren angesprochen, V2 spricht bei geringfügig höherem Füllstand an als V1. Betrieblich wird jedoch nur Ventil V1 angesteuert, so daß sich unterschiedliche Funktionsprüfungszeiten für beide Ventile ergeben (vergleiche Abschnitt 8.3). Diese Vorgehensweise hat vor allem betriebliche Gründe, da durch das vermehrte Ansprechen des betrieblich genutzten Ventils nicht immer dessen einwandfreie Dichtigkeit garantiert werden kann. Neben Abnutzungserscheinungen des Ventilkegels besteht auch immer die Möglichkeit, daß es infolge von kleinen Schmutzpartikeln nicht vollständig geschlossen werden kann. Hierbei treten in der Regel nur noch minimale Flüssigkeitsmengen aus, aber gerade bei hochtoxischen oder hochreaktiven Medien können diese mitunter schon ausreichen, um die Sicherheit der Anlage zu gefährden.

Für den Fall der Kategorie mit dem größten Gefahrenpotential bietet das Expertensystem, ebenfalls unter sonst gleichen Bedingungen, als Lösung an:

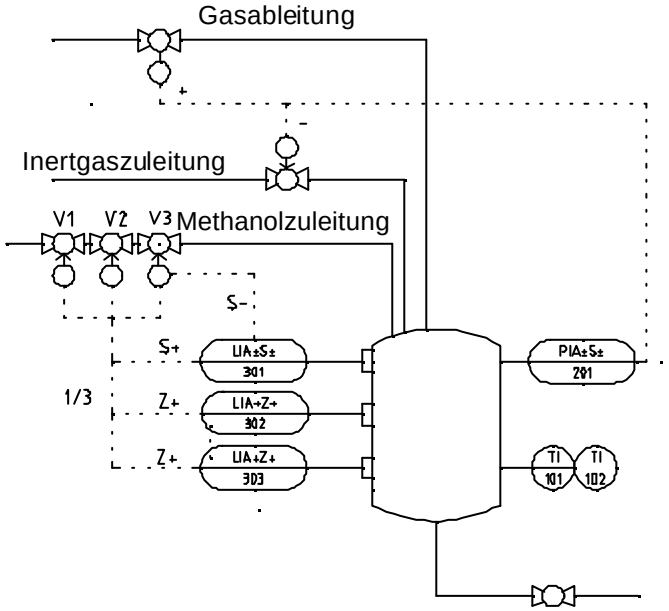


Bild 10-4: Auslegungsalternative für die Gefahrenpotential-Kategorie "hoch"

In diesem Fall wird der Füllstand in 1-von-3 Logik dreifach überwacht, da Fehlalarme nicht berücksichtigt werden müssen. Andernfalls würde eine 2-von-3 Logik angebo-

ten, um die Verfügbarkeit der Anlage zu erhöhen. Ebenso sorgen drei Ventile für eine sichere Verriegelung der Zuführungsleitung für den Fall des Ansprechens eines Sensors. Die Regelung des Druckes ändert sich nicht, da hier, wie bei den Lösungen zu den anderen beiden Kategorien, die Gefahr von Überdruck durch Überspeisung ausgeschlossen werden kann.

Im Gegensatz zu den anderen beiden Kategorien werden hier zwei Überwachungen als Z-Schaltung ausgelegt, um dem hohen Gefahrenpotential gerecht zu werden. Die Entscheidung, ob eine Z- oder S-Schaltung vorzusehen ist, wird –wie in Kapitel 2 bereits erwähnt– allerdings nicht von SafeCAD übernommen. Der Anwender kann hier weiterhin frei wählen. Die Zuordnung der Z-Schaltung zu den Schutzeinrichtungen der dritten Kategorie erfolgte nur exemplarisch; Gespräche mit der Industrie bestätigten jedoch die Zuordnung der Z-Schaltung zu den Sicherheitsschaltungen der dritten Kategorie.

10.2 Rührkesselreaktor (semi-batch)

10.2.1 Anlagenbeschreibung

Bei der betrachteten Industrie-Anlage handelt es sich um einen Rührkesselreaktor zur Herstellung von Prepolymer. Dazu wird in den Behälter Polyol vorgelegt und im Anschluß daran Isocyanat hinzudosiert (semi-batch). Das R&I-Fließbild der Anlage zeigt das folgende Bild.

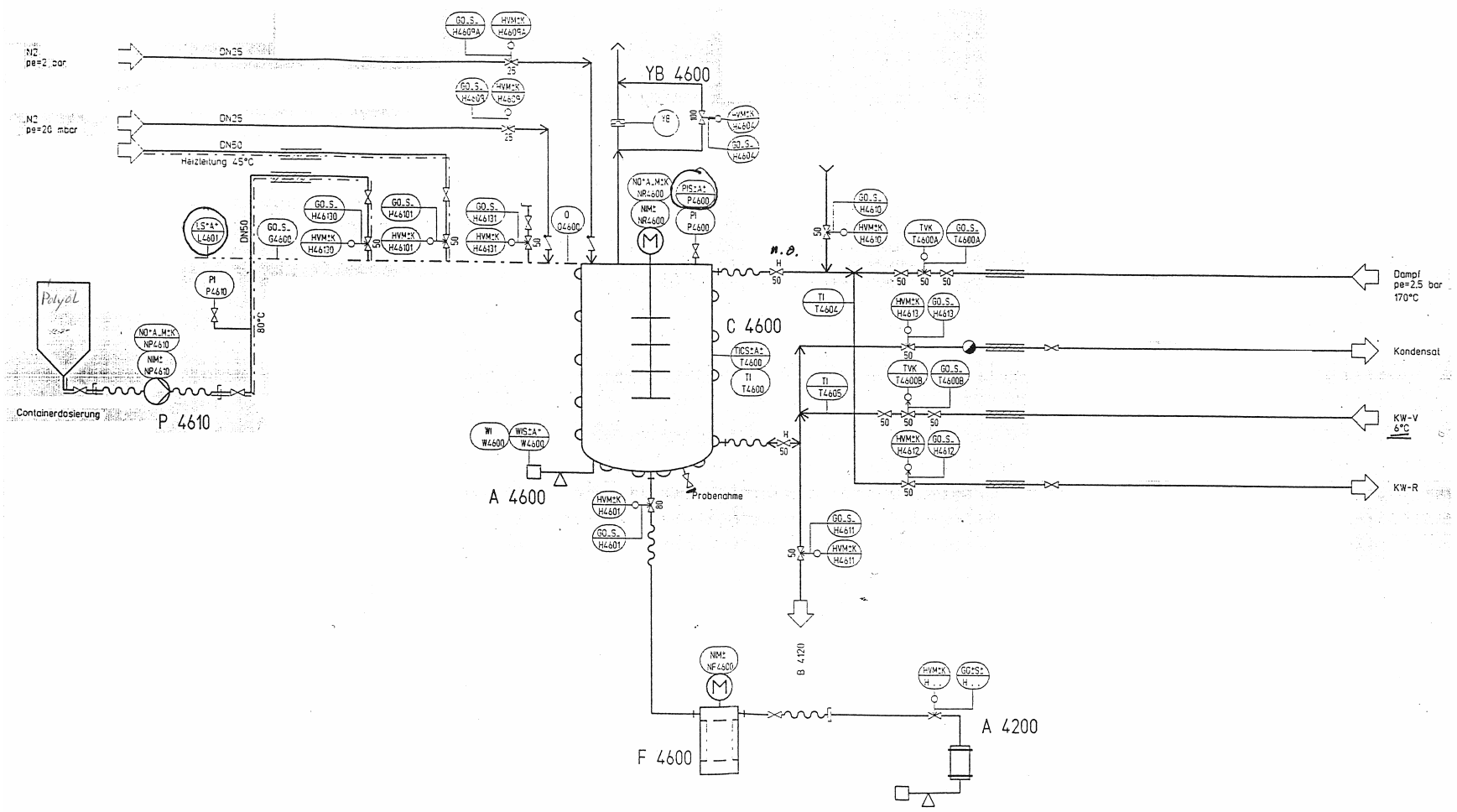


Bild 10-5: Industrielle Prepolymeranlage

Die Rezeptursteuerung erfolgt über ein Prozeßleitsystem, das über die Wägeeinrichtung $\frac{WIS \pm A +}{W4600}$ die nötigen Informationen bekommt. Zusätzlich wird über die S-Schaltung der Füllstand überwacht. Im Falle des Ansprechens werden beide Edukt-leitungen über die Ventile $\frac{HVM \pm K}{H46130}$ und $\frac{HVM \pm K}{H46101}$ geschlossen. Im Polyolcontainer befindet sich gerade so viel Polyol, wie für die Charge benötigt wird. Vor der Befüllung wird der Behälter mit Stickstoff (20 mbar) gespült, da Feuchtigkeit im Behälter zu einer Reaktion von Isocyanat zu Harnstoff und CO_2 führen kann. Das entstehende CO_2 würde eine Druckerhöhung im Behälter bewirken. In diesem Fall öffnet $\frac{PIS \pm A \pm}{P4600}$ mittels S+ die Abblaseleitung über $\frac{HVM \pm K}{H4604}$. Sinkt der Druck im Behälter, öffnet $\frac{PIS \pm A \pm}{P4600}$ (S-) die 20 mbar Stickstoffleitung. In beiden Fällen werden automatisch die Eduktleitungen –ebenfalls über die Ventile $\frac{HVM \pm K}{H46130}$ und $\frac{HVM \pm K}{H46101}$ – geschlossen.

$\frac{TICS \pm A \pm}{T4600}$ regelt die Kühlung des Behälters. Die Dampfzuführung $\frac{TVK}{T4600\,A}$ wird für diesen Prozeß nicht genutzt. Sie wird daher nicht weiter betrachtet. Die Stickstoff Leitung (2 bar) dient nur dem Austreiben des Behälterinhalts, sollte es im Filter F 4600 zu einem Rückstau kommen. Der Filter ist ebenfalls nicht Gegenstand der Betrachtung im Rahmen der Arbeit.

Der Motor des Rührers wird über $\frac{N0 + A - M \pm K}{NR4600}$ auf Stromabnahme überwacht. Eine Schaltung oder Verriegelung in Zusammenhang mit dem Motor ist nicht vorgesehen. Bei Ausfall des Rührers besteht die Möglichkeit der lokalen Isocyanateakkumulation, so daß es im Falle des Wiederanfahrens des Rührers zu einem Durchgehen der Reaktion mit Druckanstieg kommen kann. Eine Berstsicherung soll hier die Auswirkungen begrenzen.

Die Ventile sind fail-safe ausgelegt und gehen im Falle eines Ausfalls der Antriebsenergie in den sicheren Zustand (Eduktventile $\frac{HVM \pm K}{H46130}$ und $\frac{HVM \pm K}{H46101}$ werden ge-

schlossen, Ventile $\frac{\text{TVK}}{\text{T46008}}$ und $\frac{\text{HVM} \pm \text{K}}{\text{H4612}}$ für die Regelung des Kühlwasservor- und rücklaufs werden geöffnet etc.) über.

$\frac{\text{LS} + \text{A} +}{\text{L4601}}$ überwacht als redundante Einrichtung bezüglich des Überfüllens zu $\frac{\text{WIS} \pm \text{A} +}{\text{W4600}}$ den Füllstand im Behälter. Bei Überschreiten eines Grenzwertes werden automatisch die Eduktleitungen geschlossen und ein Alarm benachrichtigt das Personal.

Die Reaktion läuft bei leichtem Überdruck (20 mbar) und maximal 120°C ab. Das Risiko der Anlage als Maß für das Gefahrenpotential wurde von der Betreiberfirma in Anlehnung an /DIN V 19250/ der Anforderungsklasse 4 zugeordnet.

Die bei der Auslegung der Anlage evaluierten Gefährdungen und die getroffenen Gegenmaßnahmen sind im einzelnen:

		Maßnahmen		
Gefährdung	**Fehlzustand**	**passiv**	**aktiv**	**organisatorisch**
Überdruck	Überfüllung mit Inertgas führt zu Überdruck.	Auslegungsbedingt nicht möglich!		
	Überfüllung mit Flüssigkeit führt zu Überdruck infolge Wärmeausdehnung	Auslegungsbedingt nicht möglich!	Verriegelung der Zuführungsleitung bei maximalem Füllstand.	Alarm bei zu hohem Füllstand mit Anweisungen.
	Überfüllung mit Flüssigkeit führt zu Überdruck.	Auslegungsbedingt nicht möglich!		
	Reaktion mit falschen Inhaltsstoffen.	Spülen des Behälters mit Inertgas.	• Öffnen der Abblaseleitung. • Berstsicherung.	Alarm bei zu hohem Druck mit Anweisungen.
Unterdruck	Durch Leerlaufen des Reaktors entsteht ein unzulässiger Unterdruck.		Öffnen der Inertgasleitung.	Alarm bei zu geringem Füllstand mit Anweisungen.

Tabelle 10-4: Bei der Auslegung der Prepolymeranlage betrachtete Gefährdungen und die gewählten Gegenmaßnahmen

Die Funktionen der PLT-Symbole im Überblick sind:

Symbol	Funktion	Schaltung
$\frac{WIS \pm A +}{W4600}$	Steuert die Eduktzuführung über ein PLS. Anzeige des Ist-Wertes in der Warte. Alarm bei oberen Grenzwert.	Schaltet ab einem bestimmten oberen und unteren Grenzwert die Eduktzuleitungen ab.
$\frac{PIS \pm A \pm}{P4600}$	Überwachung des Behälterdrucks. Anzeige des Ist-Wertes in der Warte. Alarm bei unterem und oberen Grenzwert.	Schaltet ab einem bestimmten unteren Grenzwert die Inertgasleitung auf und ab einem oberen Grenzwert die Abblaseleitung über $\frac{HVM \pm K}{H4604}$ auf. Dabei werden automatisch die Edukt-leitungen geschlossen.
$\frac{TICS \pm A \pm}{T4600}$	Regelt die Temperatur im Reaktor über den Kühlwasservor- und -rücklauf. Anzeige des Ist-Wertes in der Warte. Alarm bei unterem und oberen Grenzwert.	Schaltet ab einem bestimmten oberen und unteren Grenzwert die Eduktzuleitungen ab.
$\frac{LS + A +}{L4601}$		Schaltet ab einem bestimmten oberen Grenzwert die Eduktzuleitungen ab. In Bezug auf die Füllstandsüberwachung ist es eine Redundanz zu $\frac{WIS \pm A +}{W4600}$.
$\frac{N0 + A - M \pm K}{NR4600}$	Überwachung der Stromaufnahme des Rührermotors. Alarm bei zu geringer Stromaufnahme.	

Tabelle 10-5: Funktionsbeschreibung der PLT-Symbole

Die Lösung SafeCAD's wird im folgenden Abschnitt gezeigt.

10.2.2 Abbildung der Prepolymeranlage durch das Expertensystem

Die Auswertung durch SafeCAD weist dem Gefahrenpotential der Prepolymeranlage die Kategorie „moderat" zu. Als Ergebnis des Dialogs mit dem Expertensystem ergibt sich für die Anlage auf der betrieblichen Seite:

- Temperaturregelung in „once through", Halbrohraußenschlangen.
- Rührerregime mit Elektromotor.
- Wägeeinrichtung steuert Eduktzuführung innerhalb fester Grenzen.
- Inertisierung des Gasraums.
- Ablauf bestimmt durch Prozeß stromabwärts.

Anschließend erfolgt die sicherheitstechnische Betrachtung des Vorlagebehälters. Insgesamt ergibt die Befragung zur Beispielanlage:

- Zu hoher Druck durch Überfüllung mit Flüssigkeit und anschließender thermischer Ausdehnung denkbar.
- Zu hoher Druck durch Reaktion mit falschen Inhaltsstoffen denkbar.
- Zu hoher Druck durch Akkumulationsabbau denkbar.
- Zu hoher Druck durch Pumpe auslegungsbedingt nicht möglich.
- Zu hoher Druck infolge Inertgasüberspeisung auslegungsbedingt nicht möglich.
- Als Prozeßsicherungsgröße kommen der Füllstand und der Druck in Frage.

Die bei der Anwendung von SafeCAD auf die Anlage evaluierten Gefährdungen und die gewählten Gegenmaßnahmen sind im einzelnen:

		Maßnahmen		
Gefährdung	**Fehlzustand**	**passiv**	**aktiv**	**organisatorisch**
Überdruck	Überfüllung mit Inertgas führt zu Überdruck.	Auslegungs-bedingt nicht möglich!		
	Überfüllung mit Flüssigkeit führt zu Überdruck infolge Wärme-ausdehnung im Behälter.		• Verriegelung der Zuführungsleitung bei maximalem Füllstand. • Berstsicherung	Alarm bei zu hohem Füllstand mit Anweisun-gen.
	Überfüllung mit Flüssigkeit führt zu Überdruck.	Auslegungs-bedingt nicht möglich!		
	Hoher Druck durch Reaktion mit falschen In-haltsstoffen.		• Öffnen der Abbla-seleitung und Schließen der Eduktleitungen bei hohem Druck. • Berstsicherung	Alarm bei zu hohem Druck mit Anweisungen.
	Hoher Druck durch lokalen Akkumulations-abbau.		• Abschalten der Eduktzuleitungen bei zu hoher Drehzahl (Wel-lenbruch) oder zu niedriger Dreh-zahl (Viskositäts-änderung) des Rührermotors • Berstsicherung	Alarm bei zu hoher Drehzahl (Wellenbruch) oder zu niedriger Drehzahl (Visko-sitätsänderung) des Rührermo-tors (asynchron) mit Anweisun-gen.
Unterdruck	Durch Leerlaufen des Behälters entsteht ein un-zulässiger Unter-druck.		Verriegelung der Abführungsleitung bei minimalem Füll-stand und Öffnen der Inertgasleitung.	Alarm bei zu geringem Füll-stand mit Anwei-sungen.

Tabelle 10-6: Ergebnis der Anwendung SafeCAD's auf eine Prepolymeranlage

Daraus ergibt sich die Lösung im R&I-Format unter der Voraussetzung der Ausgewogenheit innerhalb der Meßkette (vgl. Abschnitt 8.2) wie folgt:

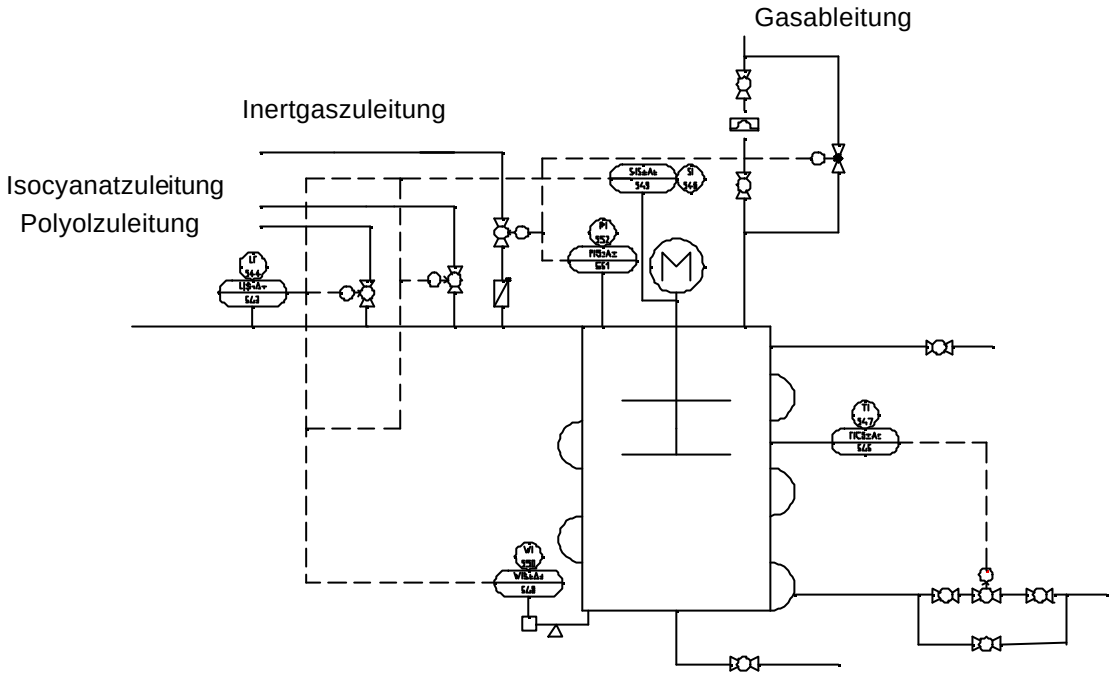


Bild 10-6: Lösung SafeCAD's für die Gefahrenpotential-Kategorie „moderat"

Die Aufgaben der PLT-Einrichtungen sind:

Symbol	Funktion	Schaltung
$\frac{\text{WIS} \pm \text{A} \pm}{495}$	Steuert die Eduktzuführung. Alarm ertönt in beiden Fällen bei Überschreiten eines etwas höheren bzw. niedrigeren Grenzwertes als der zur Steuerung genutzte.	Schaltet ab einem bestimmten oberen und unteren Grenzwert die Eduktzuleitungen ab.
$\frac{\text{PIS} \pm \text{A} \pm}{499}$	Steuerung des Behälterdrucks. Anzeige des Ist-Wertes in der Warte. Alarm ertönt in beiden Fällen.	Schaltet ab einem bestimmten unteren Grenzwert die Inertgasleitung auf und ab einem oberen Grenzwert die Abblaseleitung auf. Dabei werden automatisch die Eduktleitungen geschlossen.
$\frac{\text{TICS} \pm \text{A} \pm}{493}$	Regelt die Temperatur im Reaktor über den Kühlwasservorlauf. Anzeige des Ist-Wertes in der Warte. Alarm ertönt in beiden Fällen.	Schaltet ab einem bestimmten oberen und unteren Grenzwert die Eduktzuleitungen ab.
$\frac{\text{LIS} + \text{A} +}{491}$	Überwachung des Füllstands im Behälter. Anzeiges des Füllstandes in der Leitwarte. Alarm bei zu hohem Füllstand.	Schaltet ab einem bestimmten oberen Grenzwert die Eduktzuleitungen ab. In Bezug auf die Füllstandsüberwachung ist es eine Redundanz zu $\frac{\text{WIS} \pm \text{A} \pm}{495}$.

Symbol	Funktion	Schaltung
$\frac{\text{SIS} \pm \text{A} \pm}{496}$	Überwachung der Drehzahl der Rührerwelle. Anzeige der aktuellen Drehzahl in der Warte. Alarm ertönt in beiden Fällen.	Schaltet ab einem bestimmten oberen Grenzwert die Eduktzuleitungen ab.

Tabelle 10-7: Funktionsbeschreibung der PLT-Symbole der Prepolymeranlage

Im Gegensatz zur bestehenden Anlage würde die Drehzahl des Rührers überwacht und zusätzlich zur Berstsicherung als auswirkungsbegrenzende Maßnahme wird die Eduktzuführung bei zu hoher und zu niedriger Drehzahl abgeschaltet. Bei zu hoher Drehzahl kann ein Wellenbruch der Grund sein. In diesem Fall würde die Vermischung der Edukte nicht gewährleistet und eine lokale Eduktakkumulation ist möglich. Ist die Drehzahl zu gering, kann dies zum einen an fehlender Motorleistung liegen und zum anderen an einer Viskositätserhöhung des Behälterinhalts. In beiden Fällen kann eine ausreichende Durchmischung nicht gewährleistet werden. Um einer möglichen weiteren Akkumulation vorzubeugen, wird die Eduktzuleitung unterbunden. Da weder bei zu geringer noch zu hoher Drehzahl eine Akkumulation sicher ausgeschlossen werden kann, dient die Berstsicherung einer Vorsorge gegen eine Überlastung des Behälters infolge eines Druckaufbaus aufgrund spontanen Abreagierens des akkumulierten Eduktanteils. Ein Sicherheitsventil kommt nicht in Betracht, da dessen einwandfreie Wirkung durch die für Polymerisationsreaktionen typische Gefahr des Verklebens des Ventils nicht gegeben ist. Somit ist anders als bei einer Auslegung mit Sicherheitsventil im Ansprechfall die Anlage in jedem Fall herunterzufahren.

Darüber hinaus schaltet $\frac{\text{WIS} \pm \text{A} \pm}{495}$ im Gegensatz zur Industrieanlage auch bei niedrigem Füllstand die Eduktzuleitungen ab, um ein Leerlaufen und somit möglichen Unterdruck im Behälter zu vermeiden.

Im Falle der Gefahrenpotential-Kategorie I ergibt sich die Lösung SafeCAD's zu:

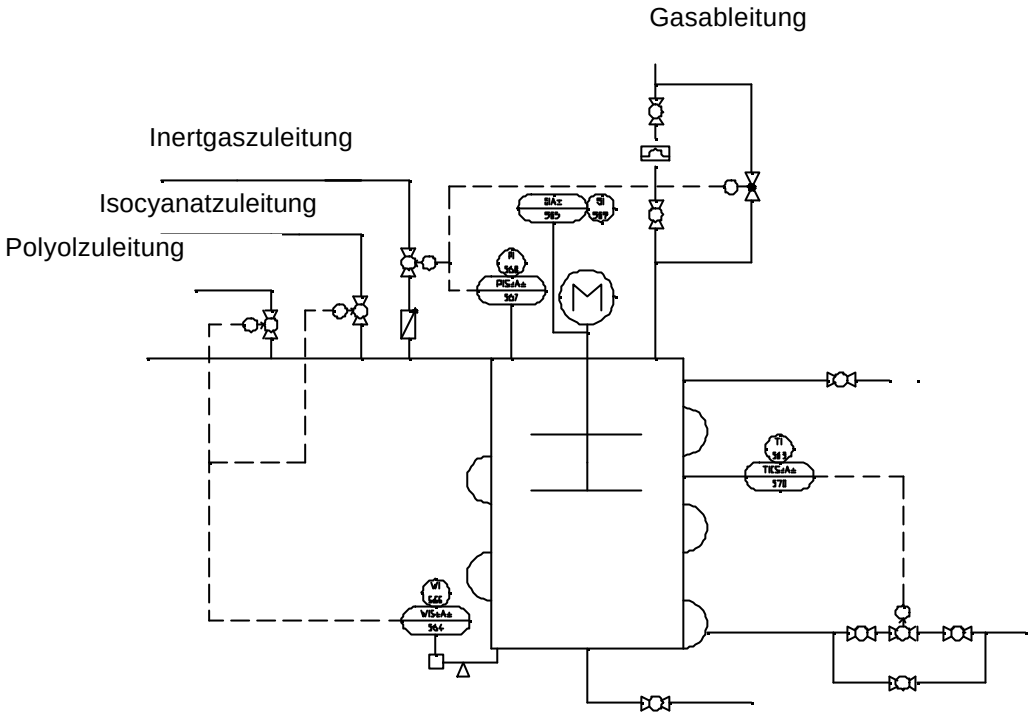


Bild 10-7: Lösung SafeCAD's für die Gefahrenpotential-Kategorie „gering"

Die betriebliche Auslegung bleibt unverändert. Im Gegensatz zur Lösung durch SafeCAD für die Kategorie „moderat" wird hier die Drehzahl der Rührerwelle nur überwacht, es erfolgt keine Sicherheitsschaltung. Ein Alarm informiert das Anlagenpersonal im Falle einer Abweichung. Entsprechende Gegenmaßnahmen müssen dann vom Personal auf Grundlage des Betriebshandbuchs vorgenommen werden.

Der Füllstand wird nicht mehr redundant überwacht, sondern ausschließlich über die Wägeeinrichtung.

Im Falle der höchsten Gefahrenpotentialkategorie liefert SafeCAD bei sonst gleichen Gefährdungen die Lösung entsprechend Bild 10-8.

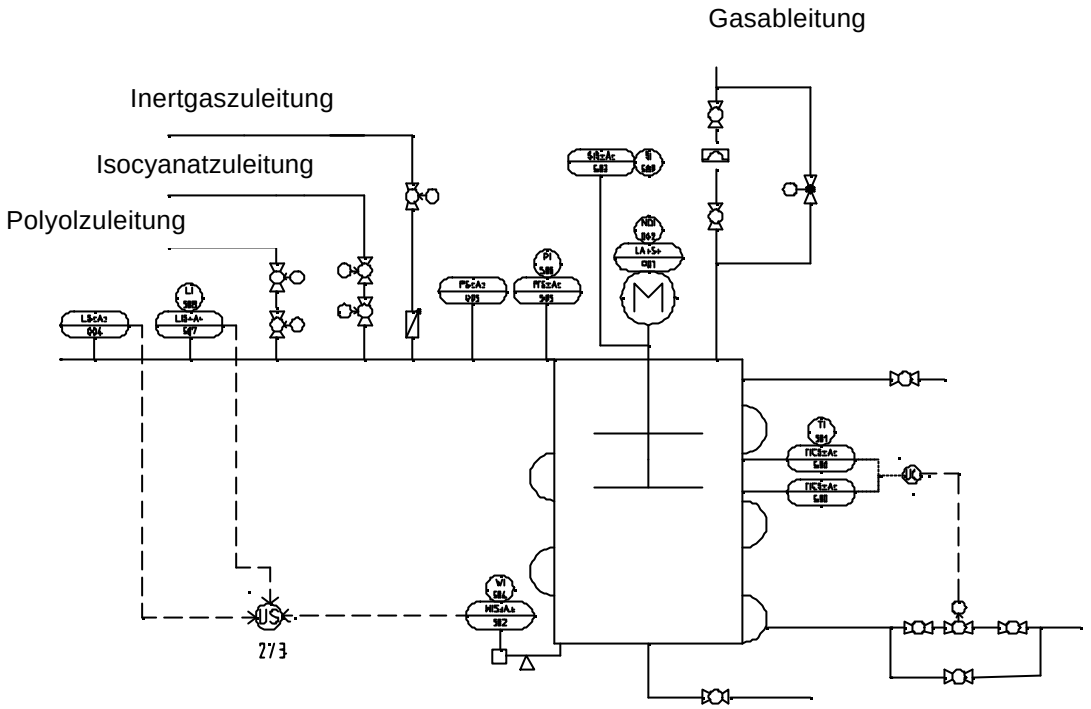


Bild 10-8: Lösung SafeCAD's für die Gefahrenpotential-Kategorie „hoch"

Der Füllstand wird in 2-von-3 Logik durch die Wägeeinrichtung und zwei Füllstandssensoren überwacht. Somit werden die Anforderungen gemäß Tabelle 8-2 erfüllt. Der Druck wird redundant überwacht und schaltet in 1-von-2 Logik die Inertgasleitung beziehungsweise die Abführungsleitung auf und die Eduktzuleitungen zu.

Neben der Rührerdrehzahl wird die Leistungsaufnahme des Motors überwacht. Sowohl bei einem oberen als auch einem unteren Grenzwert werden die Eduktleitungen in 1-von-2 Logik geschlossen. Die Temperatur wird über zwei Sensoren geregelt. Ebenso wird bei zu hoher oder zu niedriger Temperatur im Behälter die Eduktzufuhr unterbrochen.

Aus Gründen der Übersichtlichkeit sind in diesem R&I Fließbild nur einige Wirklinien eingezeichnet. Über die Dokumentation, die ebenfalls von SafeCAD geliefert wird, sind alle Verbindungen eindeutig zuzuordnen.

11 Zusammenfassung und Ausblick

Neben der Auswahl geeigneter Betriebs- und Sicherheitssysteme spielt deren Zuverlässigkeit für den sicheren Betrieb einer Chemieanlage eine entscheidende Rolle. Diese muß dem Gefahrenpotential der Anlage angemessen sein. Da sich das Gefahrenpotential einer Anlage in erster Linie nach den in ihr befindlichen Stoffen und den Verfahrenparametern wie Druck und Temperatur richtet, wurde zur Evaluierung des Gefahrenpotentials eine Rastermethode ausgewählt. SafeCAD verwendet hierfür DOW's Fire & Explosion Index. Darüber hinaus müssen die Möglichkeiten von Gefährdungen aufgrund des Gefahrenpotentials und deren Folgen bestimmt werden. Das PAAG-Verfahren hat sich in der chemischen Industrie als zuverlässig und umfangreich für diese Aufgabe erwiesen. So greift SafeCAD auf Lösungen bereits durchgeführter Analysen zurück und bietet sie in Form möglicher betrieblicher Abweichungen mit den dazugehörigen Gegenmaßnahmen an. Der Anwender muß nun entscheiden, ob die Abweichungen wahrscheinlich sind oder nicht. Für die als wahrscheinlich erachteten Abweichungen können dann geeignete Gegenmaßnahmen ausgewählt werden. Dabei richtet sich der Redundanz- und Diversitätsgrad der gewählten Maßnahmen nach dem Gefahrenpotential der Anlage. Die Lösung des Systems wird abschließend im R&I-Format sowie als HTML-Datei ausgegeben.

Die Sicherheit einer Chemieanlage ist Gegenstand des Auslegungsprozesses. Derzeit erfolgt ihre Bewertung meist retrospektiv. SafeCAD ermöglicht die Berücksichtigung von Sicherheitskonzepten bereits im Entstehungsprozeß einer Anlage. Evaluierten Gefährdungen werden mittels probabilistischer Untersuchungen quantitativ ausgeglichen gestaltete und dem Gefahrenpotential der Anlage angemessene Gegenmaßnahmen angeboten. Neue Regelungen wie z.B. /IEC 61508/ und /IEC 61511/ unterstützen diese Vorgehensweise.

Die modellierten Beispiele zeigen, daß eine Verbindung von Sicherheitsüberlegungen und CAD möglich ist. So wird eine sichere Auslegung angeboten, die kostspielige Nachrüstungsaktionen zu vermeiden hilft. Die modulare Struktur des Verfahrens ermöglicht es, betriebliche Auslegungsvorschriften und Änderungen in der geltenden Gesetzgebung leicht zu integrieren.

Der schwierigste Teil der Beherrschung des Gefahrenpotentials ist die Beherrschung der physikalisch-chemischen Reaktionseigenschaften durch die Anlagentechnik, einschließlich der Auswahl der Maßnahmen zum Halten des Prozesses im bestimmungsgemäßen Betriebsbereich. Da eine Formalisierung für alle Reaktions- und Reaktortypen allein aufgrund der Vielzahl an Möglichkeiten schwierig ist, hilft das entwickelte System bei der Auswahl geeigneter Maßnahmen. Anspruch auf Vollständigkeit kann aus den genannten Gründen nicht erhoben werden. Aufgrund der modularen Programmierung kann aber jeder Experte die Wissensbasis des Programms an seine Vorstellungen anpassen und erweitern. Somit ist es gelungen, ein dynamisches System zu entwickeln, daß neuen Erkenntnissen schnell und unkompliziert angepaßt werden kann. Das Expertensystem kann helfen, Mißverständnisse an den Grenzen der verschiedenen Fachbereiche zu lösen, so daß daraus denkbare Fehler bei konsequenter Anwendung des Systems verhindert werden können. Hierzu ist die Beherrschung nur weniger und einfacher Programmierbefehle erforderlich, die verständlich über die Hilfefunktion des Programms autodidaktisch erlernt werden können.

SafeCAD ermöglicht die Auslegung einzelner Teilanlagen. Da Anlagen in der Regel aus mehreren Teilanlagen bestehen, können diese der Reihe nach bearbeitet und anschließend im CAD-System zusammengefügt werden. Eine Schnittstelle zur Verbindung der Teilanlagen ist derzeit nicht implementiert. Entscheidend ist hierbei die Wahl des Gefahrenpotentials. Aus sicherheitstechnischer Sicht sollte hier konservativ dasjenige der Teilanlage mit dem höchsten Potential für alle Teilanlagen ausgewählt werden. Die Entscheidung bleibt aber dem Anwender überlassen.

Insgesamt lassen sich die Vorteile von SafeCAD wie folgt zusammenfassen:

- Ermittlung des Gefahrenpotentials,
- Festlegung des Redundanz- und Diversitätsgrades auf Grundlage des Gefahrenpotentials,
- Ermittlung möglicher Gefährdungen, mittels einer modifizierten PAAG-Vorgehensweise die zum Wirksamwerden des Gefahrenpotentials führen können,
- Festlegung geeigneter Gegenmaßnahmen für die als wahrscheinlich erachteten Gefährdungen,

- Gestaltung der sich aus den gewählten Gegenmaßnahmen ergebenden Teilsysteme entsprechend dem Redundanz- und Diversitätsgrad,
- Ausgabe der Teilsysteme im CAD - Format, dadurch ist eine leichte Einbindung in CAD-Zeichnungen möglich,
- Zeiteinsparung durch Automatisierung von Standardaufgaben bei der Anlagenauslegung,
- Dokumentation der gewählten Entscheidungen,
- Ausgabe als vollständiges R&I - Fließbild für einfache, sich wiederholende Teilanlagen ist möglich und
- einfache Archivierung der Ergebnisse.

Als Erweiterung für das System bietet sich die Anbindung einer Stoffdatenbank an, so daß die Eigenschaften der in der Anlage gehandhabten Stoffe automatisch eingelesen werden können.

Eine zusätzliche Erweiterung des Expertensystems hinsichtlich der Auslegung der Prozeßleittechnik ist ebenso denkbar und aufgrund der modularen Struktur des Systems auch ohne große Komplikationen umsetzbar.

Darüber hinaus wären weitere Aggregate wie z.B. Destillationskolonnen oder Lagereinrichtungen einzubeziehen.

12 Literatur

/AD-Merkblatt A1/ AD-Merkblatt A1: Sicherheitseinrichtungen gegen Drucküberschreitungen – Berstsicherungen, Beuth Verlag, Berlin, 1995.

/AD-Merkblatt A2/ AD-Merkblatt A2: Sicherheitseinrichtungen gegen Drucküberschreitungen – Sicherheitsventile, Beuth Verlag, Berlin, 1995.

/AD-Merkblatt A6/ AD-Merkblatt A6: Sicherheitseinrichtungen gegen Drucküberschreitung – MSR-Sicherheitseinrichtungen, Beuth Verlag, Berlin, 1986.

/Badh84/ Badhwar, I., Trehan, M.: Bhopal: city of death. India Today, Dec. 31, 4, 1984.

/Barl75/ Barlow, R.E., F. Proschan: Statistical Theory of Reliability and Life Testing – Probability Models, New York, 1975.

/Bart88/ Bartholl, H. et al.: Anlagensicherung mit Mitteln der MSR-Technik, Praxis Sicherheitstechnik, Vol. 1, 1988.

/Bart90/ Bartels, K.; Hoffmann, H.; Rossinelli, L.: Risikobegrenzung in der Chemie: PAAG-Verfahren (HAZOP). Internationale Sektion der IVSS für die Verhütung von Arbeitsunfällen und Berufskrankheiten in der chemischen Industrie, Heidelberg, 1990.

/Beie00/ Beierle, C., Kern-Isberner, G.: Methoden wissensbasierter Systeme, Vieweg Verlag, Braunschweig/Wiesbaden, 2000.

/Betr02/ BetrSichV: Verordnung zur Rechtsvereinfachung im Bereich der Sicherheit und des Gesundheitsschutzes bei der Bereitstellung von Arbeitsmitteln und deren Benutzung bei der Arbeit, der Sicherheit beim Betrieb überwachungsbedürftiger Anlagen und über der Organisation des betrieblichen Arbeitsschutzes, 2002.

/Biro97/ Birolini, A.: Zuverlässigkeit von Geräten und Systemen, Springer-Verlag, Berlin, 1997.

/Boll96/ Bollinger, R. E. et al: Inherently Safer Chemical Processes – A Life Cycle Approach, , A CCPS Concept Book, American Institute of Chemical Engineers, New York, 1996.

/Brus88/ Brusa, P.: Anlagensicherung mit Mitteln der MSR-Technik, Schweizer Ingenieur und Architekt Nr. 29, S. 556-562, Zürich, 1988.

/Buch84/ Buchanan, B.G., Shortliffe, E.H.: Rule-based expert systems. The MYCIN experiments of the Stanford Heuristic Programming Project. Addison-Wsley, Reading, MA, 1984.

/Cast97/ Castillo, E., Gutierrez, J.G., Hadi, A.S.: Expert systems and

probabilistic network models. Springer Verlag, 1997.

/Chem94/ Chemical Exposure Index Guide, The Dow Chemical Company, Midland, Michigan, May 1994.

/Cher99/ Cheremisinoff, N. P.: Handbook of industrial toxicology and hazardous materials, Marcel Dekker, Inc., New York, 1999.

/Chu80/ Chu, T.L., G. Apostolakis: Methods for Probabilistic Analysis of Noncoherent Fault Trees, IEEE Transaction on Reliability. Vol. R-29, No. 5, 354-360, 1980.

/DeHa86/ De Haas, K., Magin, R., Storck, H.: Sicherung chemischer Produktionsanlagen mit Mitteln der Elektro-/ Meß-, Steuerungs- und Regelungstechnik, Chem.-Ing.-Tech. 58 (1986) Nr. 3, S. 177-182.

/Der 80/ Der Störfall im chemischen Betrieb – Verhütung durch Prognose, Auffinden der Ursachen, Abschätzen der Auswirkungen, Gegenmaßnahmrn (PAAG-Verfahren), Berufsgenossenschaft der chemischen Industrie, Heidelberg, 1980.

/DIN 25419/ DIN 25419 Ereignisablaufanalyse, Beuth Verlag, Berlin, 1985.

/DIN 25424/ DIN 25424 Fehlerbaumanalyse, Teil 1 und 2, Beuth Verlag, Berlin, 1981, 1990.

/DIN 25448/ DIN 25448: Ausfalleffetanalyse, Beuth Verlag, Berlin, 1990.

/DIN EN 61512-1/ DIN EN 61512-1: Chargenorientierte Fahrweise, Teil 1: Modelle und Terminologie, Beuth Verlag, Berlin, 1998.

/DIN V 19250/ DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, 1994.

/DIN/VDE2180_1/ DIN/VDE 2180, Blatt 1: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln Prozeßleittechnik (PLT) –Einführung, Begriffe, Erklärungen, Beuth Verlag, Berlin, 1998.

/DIN/VDE2180_2/ DIN/VDE 2180, Blatt 2: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln Prozeßleittechnik (PLT) – Klassifizierung von PLT-Einrichtungen – Ausführung, Betrieb und Prüfung von PLT-Schutzeinrichtungen, Beuth Verlag, Berlin, 1998.

/DIN/VDE2180_3/ DIN/VDE 2180, Blatt 3: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln Prozeßleittechnik (PLT) – Bauliche und installationstechnische Maßnahmen zur Funktionssicherung von PLT-Einrichtungen in Ausnahmezuständen, Beuth Verlag, Berlin, 1998.

/DIN/VDE2180_4/ DIN/VDE 2180, Blatt 4: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln Prozeßleittechnik (PLT) – Berechnungsmethoden für Zuverlässigkeitskenngrößen von PLT-

Schutzeinrichtungen, Beuth Verlag, Berlin, 1998.

/DIN28004_1/ DIN 28004, Teil 1: Fließbilder verfahrenstechnischer Anlagen, Begriffe, Fließbildarten, Informationsinhalt, 1988.

/Engl92/ Englund, S. M., Grinwis, D. J.: Provide the Right Redundancy for Control Systems, Chemical Enginnering Progress, pp. 36-44, October 1992.

/Erma80/ Erman, L.D. et al.: The HEARSAY II Speech Understanding System: Integrating Knowledge to Resolve Uncertainty, Computing Surveys, Vol. 12, No. 2, p. 213-253, 1980.

/Eute95/ Euteneuer, U. et al.: Prozeßleittechnik in Anlagen der chemischen Industrie: Anlagenschutz und sicherheitsrelevante Komponenten, Landesumweltamt NRW, Essen, 1995.

/Fire94/ Fire & Explosion Index Hazard Classification Guide, The Dow Chemical Company, Midland, Michigan, May 1994.

/Frie90/ Friedrich, G., Stumtner, M.: Einführung. In Gottlob, G., Frühwirth, Th., Horn, W., editors, Expertensysteme, Springers Angewandte Informatik, S. 1-9. Springer-Verlag, 1990.

/Gäde77/ Gäde, K.-W.: Zuverlässigkeit - Mathematische Modelle, München, Wien 1977.

/Gefahr99/ Gefahrstoffe 1999, Universum Verlagsanstalt, Wiesbaden, 1998.

/Geik90-96/ Geike, R.: Analyse der Sicherheit für Chemieanlagen, Kz. 8253 im Handbuch Abwehr betrieblicher Störfälle, Erich Schmidt Verlag Berlin, 1990-96.

/Geik96/ Geike, R.: Sicherheit von Chemieanlagen, Sicherheit in der Rohrleitungstechnik, Vulkan-Verlag Essen, 1996.

/Gese/ Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz - BImSchG).

/Gibs87/ Gibson, N., Rogers, R.L. and Wright, T.K.: Chemical reaction hazards: an integrated approach. Hazards from pressure (Rugby: Instn Chem. Engrs) 1987.

/Göri93/ Göring, M.; Schecker, H.-G.: Sicherheitsbetrachtung verfahrenstechnischer Anlagen, Technische Überwachung, TÜ Bd. 34 (1993) Nr.4 – April.

/Graf00/ Graf, H.: Ein modellbasierter Ansatz zur rechnergestützten Sicherheitsbetrachtung von Chemieanlagen während der Planungsphase, Fortschr.-Ber. VDI Reihe 3 Nr. 642. Düsseldorf: VDI Verlag 2000.

/Grei87/ Greiner, B., Weidlich, S., Wilhelm, H.: Konzeption von MSR-Einrichtungen zur Anlagensicherung in der Chemischen Industrie, aus: Sicherheitskonzepte in verfahrenstechnischen Anlagen und Kraftwerken, Forst, H.-J. [Hrsg.], S. 11-37, vde-verlag, Berlin, 1987.

/Grei91/ Greiner, B., Weidlich, S.: Anlagensicherung mit Mitteln der MSR-Technik, atp 33 (1991) 1, S. 5-12.

/Grei91/ Greiner, B., Weidlich, S.: Anlagensicherung mit Mitteln der MSR-Technik, atp 33 (1991) 1, S. 5-12.

/Guid89/ Guidelines for Process Equipment Reliability Data, American Institute of Chemical Engineers, New York, 1989.

/Guid92/ Guidelines for Hazard Evaluation Procedures, American Institute of Chemical Engineers, New York, 1992.

/Guid93a/ Guidelines for Engineering Design for Process Safety, American Institute of Chemical Engineers, New York, 1993.

/Guid93b/ Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, New York, 1993.

/Guid95/ Guidelines for Chemical Reactivity Evaluation and Application to Process Design, American Institute of Chemical Engineers, New York, 1995.

/Guid98/ Guidelines for Design Solutions for Process Equipment Failures, American Institute of Chemical Engineers, New York, 1998.

/Guid99/ Guidlines for Process Safety in Batch Reaction Systems, American Institute of Chemical Engineers, New York, 1999.

/Gyga88/ Gygax, R.: Thermische Prozeß-Sicherheit, Expertenkommission für Sicherheit in der chemischen Industrie der Schweiz (ESCIS), Ciba-Geigy AG, Basel, 1988.

/Haup79/ Hauptmanns, U: Métodos para la evaluación de árboles de fallos. Energía Nuclear España, 23 (1979), 122, 393-402.

/Haup80/ Hauptmanns, U.: Fault Tree of a Proposed Ethylene Vaporization Unit, I&EC Fundamentals, Vol. 19, S. 300, August 1980.

/Haup85a/ Hauptmanns, U. et al.: Ermittlung der Kriterien für die Anwendung systematischer Methoden zur Durchführung von Sicherheitsanalysen für Chemieanlagen, Gesellschaft für Reaktorsicherheit (GRS) mbH, GRS-59, Dezember 1985.

/Haup85b/ Hauptmanns, U. et al.: Ermittlung der Kriterien für die Anwendung systematischer Methoden zur Durchführung von Sicherheitsanalysen für Chemieanlagen, Gesellschaft für Reaktorsi-

cherheit (GRS) mbH, GRS-59, Dezember 1985.

/Haup87/ Hauptmanns, U et al.: Technische Risiken – Ermittlung und Bewertung, Springer-Verlag, Berlin, 1987.

/Haup88a/ Hauptmanns, U., et al: Ermittlung von Zuverlässigkeitskenngrößen für Chemieanlagen, GRS-A-1500, Köln, Oktober 1988.

/Haup88b/ Hauptmanns, U.: Fault Tree Analysis for Process Plants in Kandel, A. and E. Avni (Eds.): Engineering Risk and Hazard Assessment, Vol. I, Boca Raton, Florida 1988.

/Haup94a/ Hauptmanns, U.: PAAG-Verfahren und seine Anwendung auf eine Anlage zur Herstellung von Nitroglykol. Ruhr-Univesität Bochum und Verein Deutscher Ingenieure VDI Bochumer Bezirksverein, 1994.

/Haup94b/ Hauptmanns, U., Kreuser, A. und J. Peschke: Vorgehensweise bei der Behandlung von GVA, GRS-A-2160, Köln, Juli 1994.

/Haup95/ Hauptmanns, U.: Untersuchungen zum Arbeitsschutz bei An- und Abfahrvorgängen einer Nitroglykol-Anlage, Chem.-Ing.-Tech. 67 Nr. 2, S. 179-183, 1995.

/Heal78/ Health and Safety Executive: Canvey: An Investigation of Potential Hazards from Operations in the Canvey Island,Thurrock Area. London 1978.

/Hend00/ Hendershot, D.C.: Process Minimization: Making Plants safer, Chemical Engineering Progress, January, 2000.

/Heng81/ stenberg, J., Sturm, B., Winkler, O.: Messen, Steuern und Regeln in der Chemischen Technik, Springer-Verlag, Berlin, 1981.

/Hugo80/ Hugo, P.: Anfahr- und Betriebsverhalten von exothermen Batch-Prozessen, Chem.-Ing.-Tech. 52 (1980) Nr. 9, S. 712-723.

/Hugo94/ Hugo, P., Seidel.Morgenstern, A. & Steinbach, J.: Grundzüge der Technischen Chemie I (Reaktionskinetik), Technische Universität Berlin, 1994.

/IEC 61508/ IEC 61508: Functional safety of electrical/electronic/programmable electronic safety related systems, Teile 1 bis7.

/IEC 61511/ IEC 61511: Functional safety: Safety instrumented systems for the process industry, Teile 1 bis 3.

/Impe85/ Imperial Chemical Industries (Hrsg.): The Mond Index 2nd Edition, 1985.

/Inte93/ International Atomic Energy Agency (IAEA): Manual for the classification and prioritization of risk due to major accidents in proc-

ess and related industries, Wien, 1993.

/Joch00/ Jochum, C.: Gefahrenanalyse zur Bewertung des Gefahrenpotentials von prozessbezogenen Anlagen, Forschungsbericht Fb 895, Dortmund/Berlin, 2000.

/Kess89/ Kessler, R.: Prozeßorientierte Strukturierung von verfahrenstechnischen Anlagen, atp 31 (1989) 10, S. 461-467.

/Kier83/ Kier, B.; Müller, G.: Erweiterung der Störfalldatenbank und Erstellung des Handbuchs –Störfälle–, Forschungsbericht 10409303, Rheinisch-Westfälischer Überwachungs-Verein, Essen, 1983.

/Klet78/ Kletz, T.A.: What you don't have can't leak, Chemistry and Industry, S. 287-92, May, 1978.

/Klet98/ Kletz, T.: Process Plants: A Handbook for Inherently Safer Design, Taylor & Francis, Philadelphia, 1998.

/Köni87/ König, J.: Sicherheitstechnische Aspekte der Prozeßleittechnik, Chem.-Ing.-Tech. 59 (1987) Nr. 3, S. 196-204.

/Krem78/ Kremer, G.: Die Sicherheit verfahrenstechnischer Anlagen, Schriftenreihe Chemie und Fortschritt, Heft 1/1978.

/Kühn97/ Kühnreich et al: Ermittlung und Bewertung des Gefahrenpotentials für Beschäftigte in Anlagen und Lagereinrichtungen, Forschungsbericht Fb 794, BauA, Dortmund, 1997.

/Laub89/ Lauber, R.: Prozeßautomatisierung, Band 1, Springer Verlag, Berlin, 1989.

/Lawl70/ Lawley, H.G. (1974). Operability Studies and Hazard Analysis. *CEP* 70:4**,** 45-60.

/Lees96_1/ Lees, F. P.: Loss Prevention in the process Industries, Vol. I, Reed Educational and Professional Publishing Ltd, 1996.

/Lees96_2/ Lees, F. P.: Loss Prevention in the process Industries, Vol. II, Reed Educational and Professional Publishing Ltd, 1996.

/Lees96_3/ Lees, F. P.: Loss Prevention in the process Industries, Vol. III, Reed Educational and Professional Publishing Ltd, 1996.

/Mäde90/ Mäder, S.: Sicherheitstechnische Maßnahmen für Lagerbehälter mit gefährlichen Stoffen, S. 396-402, in: Thier, B. (Hrsg.): Handbuch „Apparate“. Technik, Bau, Anwendung. 1. Ausgabe, Vulkan-Verlag, Essen, 1990.

/Marx01/ Marx, M. and U. Hauptmanns: Development of a Methodology for Integrating Process Safety in CAD in: Pasman, H. J., Fredholm, O. and A. Jacobsson (eds.) Loss Prevention and Safety Promo-

tion in the Process Industries. Proceedings of the 10th International Symposium, 19-21 June 2001, Stockholm/Sweden, Vol.2, pp. 507 - 517.

/Marx02/ Marx, M. and U. Hauptmanns: Integration of Process Safety in CAD in Bonano, E. J., Camp, A. L., Majors, M. J. and R. A. Thompson (eds.) Proceedings of the 6th International Conference on Probabilistic Safety Assessment & Management - PSAM 6, San Juan/Puerto Rico/USA, 23–28 June 2002.

/Merk00/ Merkblatt zur Sicherung von verfahrenstechnischen Anlagen mit Mitteln der Prozessleittechnik (PLT) –Prozessleitwarten, Mess-, Steuer- und Regelanlagen, VdS 2556 : 2000-10 (01).

/Merk95/ Merkblatt R001: Exothermische chemische Reaktionen – Grundlagen, BG Chemie, Heidelberg, Nov. 1995.

/Merk96/ Merkblatt R002: Exothermische chemische Reaktionen – Maßnahmen zur Beherrschung, BG Chemie, Heidelberg, Dez. 1996.

/Mert93/ Mertens, P. et al.: Betriebliche Expertensystem-Anwendungen. Springer-Verlag, Berlin-Heidelberg-New York, 1993.

/Mori95/ Moritz, H.-U.: Reaktionskalorimetrie und sicherheitstechnische Aspekte von Polyreaktionen, in: Sichere Handhabung chemischer Reaktionen, Praxis Sicherheitstechnik, Vol. 3, 1995.

/Müll90/ Müller, R.: Anlagensicherung mit Mitteln der Prozeßleittechnik, 4160, in: Abwehr betrieblicher Störfälle: Brandschutz, Umweltschutz, Werkschutz, Lehmke, E., Polthier, K. (Hrsg.), Schmidt-Verlag, Berlin, 1990.

/NAMU93/ NAMUR-Empfehlung 31: Anlagensicherung mit Mitteln der Prozeßleittechnik, 1993.

/Nett93/ Netter, P.: Anlagensicherung mit Mitteln der Prozeßleittechnik, NAMUR Statusbericht ´93, S. 121-127, Oldenbourg Verlag, München, 1993.

/Niss97/ Nissen, V.: Einführung in Evoltionäre Algorithmen, Vieweg Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1997.

/Onke96/ Onken, U., Behr, A.: Chemische Prozeßkunde, Lehrbuch der Technischen Chemie, Band 3, Georg Thieme Verlag Stuttgart, 1996.

/Ored97/ Oreda: Offshore Reliability Data, OREDA Participants, SINTEF Industrial Management, Trondheim, 1997.

/Orsi77/ Orsini, B. (chrmn): Parliamentary Commission of Inquiry on the Escape of Toxic Substances on 10 July 1976 at the ICMESA Establishment and the Consequent Potential Dangers to Health and the Environment due to Industrial Activity. Final Report (Rome),

1977.

/Pagè86/ Pagès, A., M. Gondran: System Reliability – Evaluation & Prediction in Engineering, New York, Berlin, Heidelberg, Tokyo, 1986.

/Park75/ Parker, R.J. (chrmn): The Flixborough Disaster. Report of the Court of Inquiry (London: HM Stationery Office), 1975.

/Pers/ Persönliche Mitteilungen der BASF Schwarzheide.

/Pilz87/ Pilz, V.: Sicherheitsanalysen zur systematischen Überprüfung von Verfahren und Anlagen – Methoden, Nutzen und Grenzen, Chem.-Ing.-Tech. 57 Nr. 4, S. 289-307, 1985.

/Pohl00/ Pohlheim, H.: Evolutionäre Algorithmen, Springer Verlag, Berlin, 2000.

/Polk94/ Polke, M.: Process Control Engineering, VCH Verlagsgesellschaft mbH, Weinheim, 1994.

/Prob89/ Probabilistic safety criteria at the safety function/system level. IAEA-TEDOC-523, Vienna, 1989.

/Pupp91/ Puppe, F.: Einführung in Expertensysteme, Springer-Verlag, Berlin, 1991.

/Ratg98/ Ratgeber Anlagensicherheit, Band 1, Universum Verlagsgesellschaft, Wiesbaden, 1998.

/Risk82/ Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area - A Pilot Study. A Report to the Rijnmond Public Authority, Dordrecht, Holland/Boston, USA/London, England 1982.

/Rodg95/ Rodgers, R., Petry, S.: Expert Systems in Process Safety, A CCPS Concept Book, American Institute of Chemical Engineers, New York, 1995.

/Rodg95/ Rodgers, B. R., Petry, F. S.: Expert Systems in Process Safety, Center For Chemical Process Safety (CCPS), American Institut of Chemical Engineers, New York, 1995.

/Roth90/ Roth, L.; Weller, U.: Gefährliche chemische Reaktionen, ecomed Verlagsgesellschaft, Landsberg/Lech, 1990.

/SanD89/ SAnDOC – A Safety Analysis Team Work And Documentation Tool, Technical Research Centre of Finland, Tampere, 1989.

/Satt00_1/ Sattler, K., Kasper, W.: Verfahrenstechnische Anlagen, Planung, Bau und Betrieb, Band 1, Wiley-VCH Verlag, Weinheim, 2000.

/Sche87/ Schecker, G.: Bewertung sicherheitsanalytischer Methoden für chemische und verfahrenstechnische Anlagen, Teil 2, Chem.-

Ing.-Tech. 59 Nr.12, 1987.

/Schn99/ Schneeweiss, W.: Die Fehlerbaummethode, LiLoLe-Verlag, Hagen, 1999.

/Schr02/ Schritte zur Ermittlung des Standes der Sicherheitstechnik, Leitfaden der Störfallkommission, SFK-GS-33, 2002.

/Schu95/ Schuler, H.: Prozeßführung, R. Oldenbourg Verlag, München, 1999.

/Seve96/ Seveso II Richtlinie: Richtlinie 96/82/EG des Rates vom 09. Dezember 1996.

/Sonn95/ Sonnenschein, R.: Ein wissensbasiertes System zur Instrumentierung von Chemieanlagen, VDI-Verlag, Düsseldorf, 1995.

/Stei98/ Steinbach, J. et. al.: Methoden zur Bewertung des Gefahrenpotentials von verfahrenstechnischen Anlagen und Verfahren, Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Fb 820, Berlin, 1998.

/Stoc79/ Stockburger, D., Kühner, H.: Sicherheitsüberlegungen bei der Planung von Chemieanlagen, Chem.-Ing.-Tech. 51 (1979) Nr.2, S.84-91.

/Stoe93/ Stoessel, F.: What is your thermal risk? Chemical Engineering Progress (1993) 10, 68-75.

/Stoe95/ Stoessel, F.: Design Thermally Safe Semibatch Reactors, Chemical Engineering Progress (1995) 9, 46-53.

/Stör00/ Verordnung zur Umsetzung EG-rechtlicher Vorschriften betreffend die Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen, April 2000.

/Stro78/ Strohrmann, G.: Anlagensicherung heute – die Problematik erzwingt neue Lösungskonzepte, Chem.-Ing.-Tech. 5 (1978) Nr. 6, S. 435-439.

/TAA 94/ TAA Leitfaden: Rückhaltung von gefährlichen Stoffen aus Druckentlastungseinrichtungen, 1994.

/TAA-GS-05/ TAA-GS-05: Leitfaden Erkennen und Beherrschen exothermer chemischer Reaktionen, Technischer Ausschuß für Anlagensicherheit, April 1994.

/Tech00/ Technische Regeln zur Druckbehälterverordnung, Taschenbuch-Ausgabe, HVBG, Januar 2000.

/TRbF30/ TRbF 30: „Füllstellen, Entleerstellen, Flugfeldbetankungsstellen“, 2002.

/TRbF600/ TRbF. Technische Regeln für brennbare Flüssigkeiten, Reihe

600.

/Ullr96/ Ullrich, H.: Wirtschaftliche Planung und Abwicklung verfahrenstechnischer Anlagen, Vulkan-Verlag, Essen, 1996.

/VDI/VDE 3542/ VDI/VDE 3542: Sicherheitstechnische Begriffe für Automatisierungssysteme, Beuth Verlag, Berlin, 1988.

/Vero00/ Verordnung zur Umsetzung EG-rechtlicher Vorschriften betreffend die Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen, 2000.

/Wach95/ Wachsmuth, I. in: Einführung in die künstliche Intelligenz, Görz, G. (Hrsg.), Addison-Wesley (Deutschland), 1995.

/Weid96/ Weidlich, S.: Aktualisierung der VDI/VDE 2180 „Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozeßleittechnik, S. 55-64, 3. Fachtagung Anlagen-, Arbeits- und Umweltsicherheit, GVC VDI, Düsseldorf, 1996.

/www.acpl/ http://www.acplant.com/

/www.cheq/ http://www.cheque.uq.edu.au/ugrad/theses/1998/authors/DaveA/dow.html

/www.pyth/ http://www.python.org

/www.uni-/ http://www.uni-magdeburg.de/iaut/as/index.de.html

/Zach81/ Zachmann, H.G.: Mathematik für Chemiker, Verlag Chemie, Weinheim, Deerfield Beach, Forida, Basel, 1981.

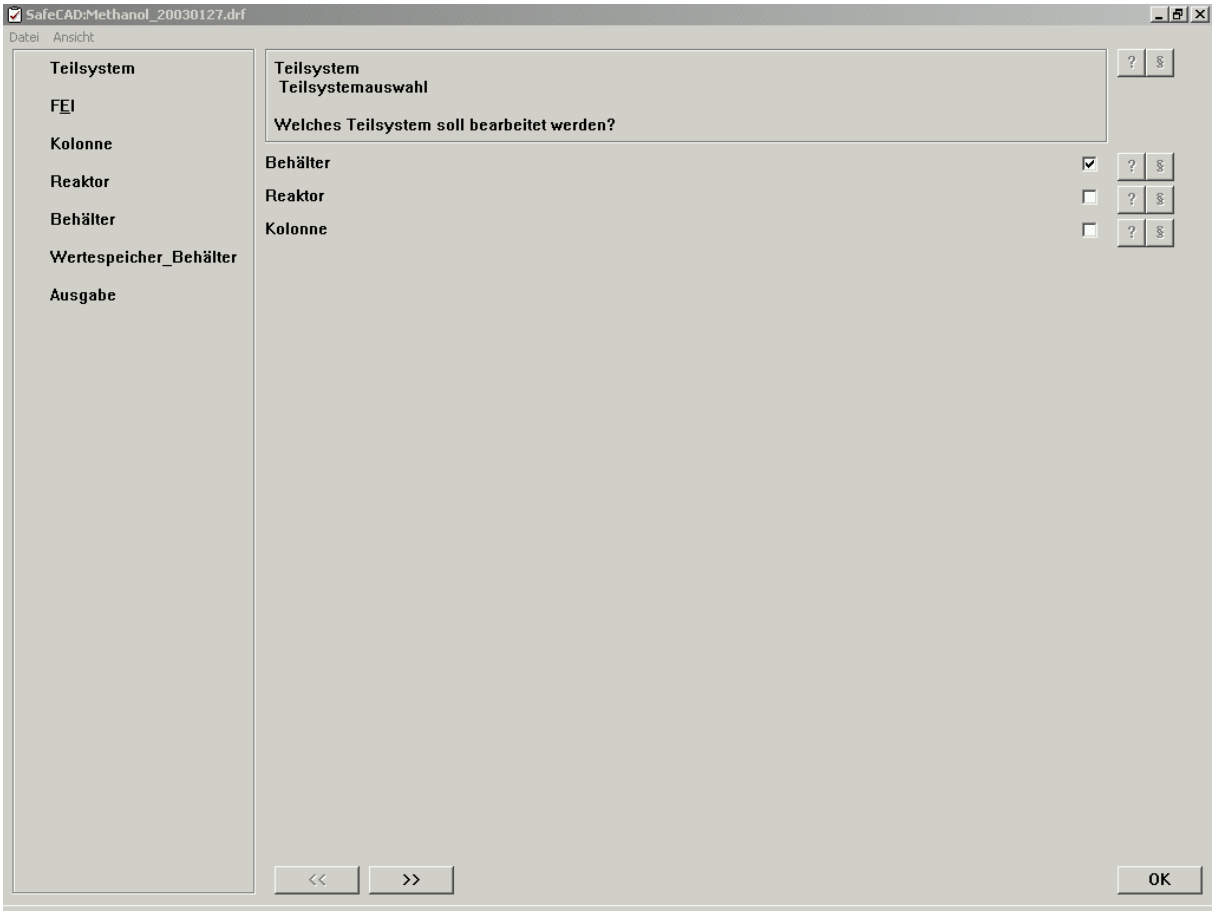
/Zogg87/ Zogg, H.A.: Zürich-Gefahrenanalyse. Zürich-Versicherungsgruppe, 1987.

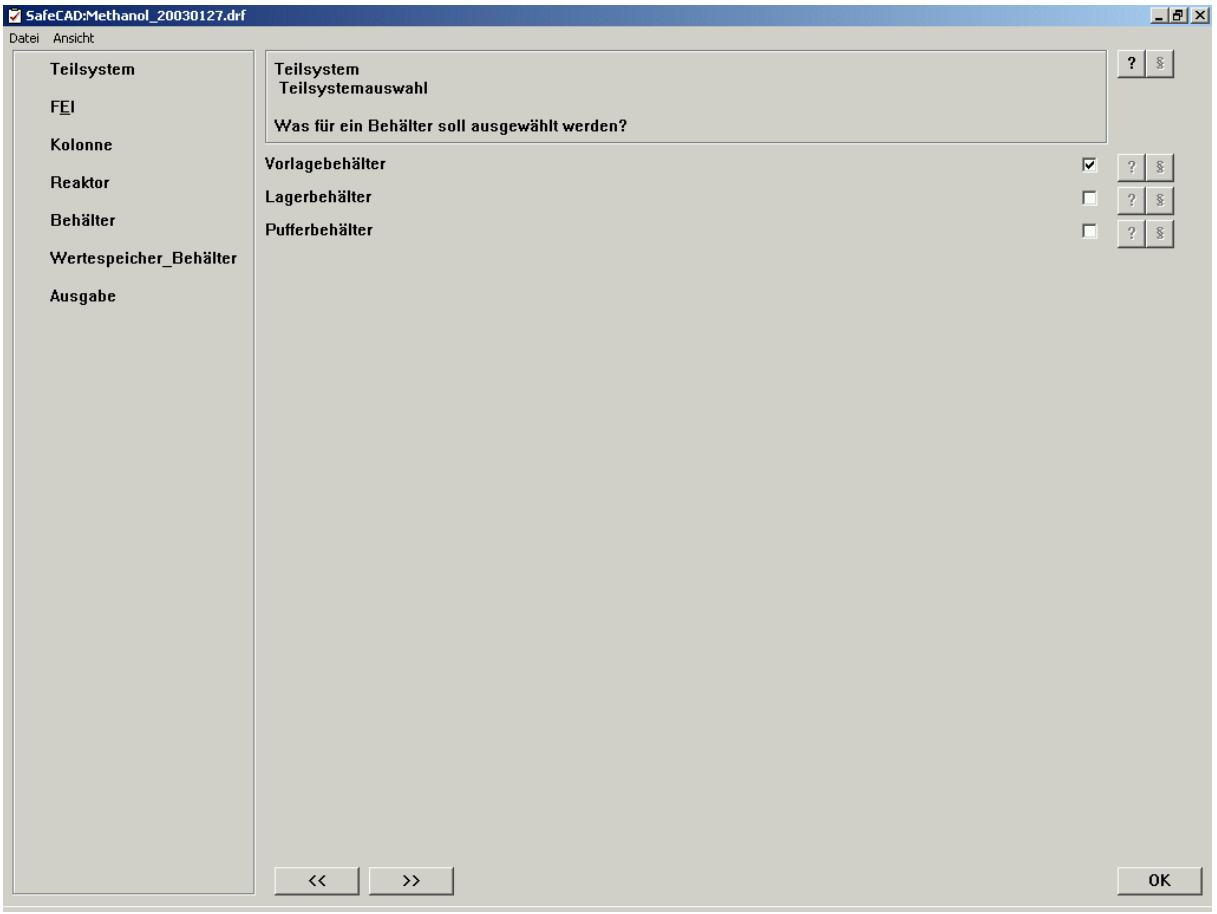
Anhang

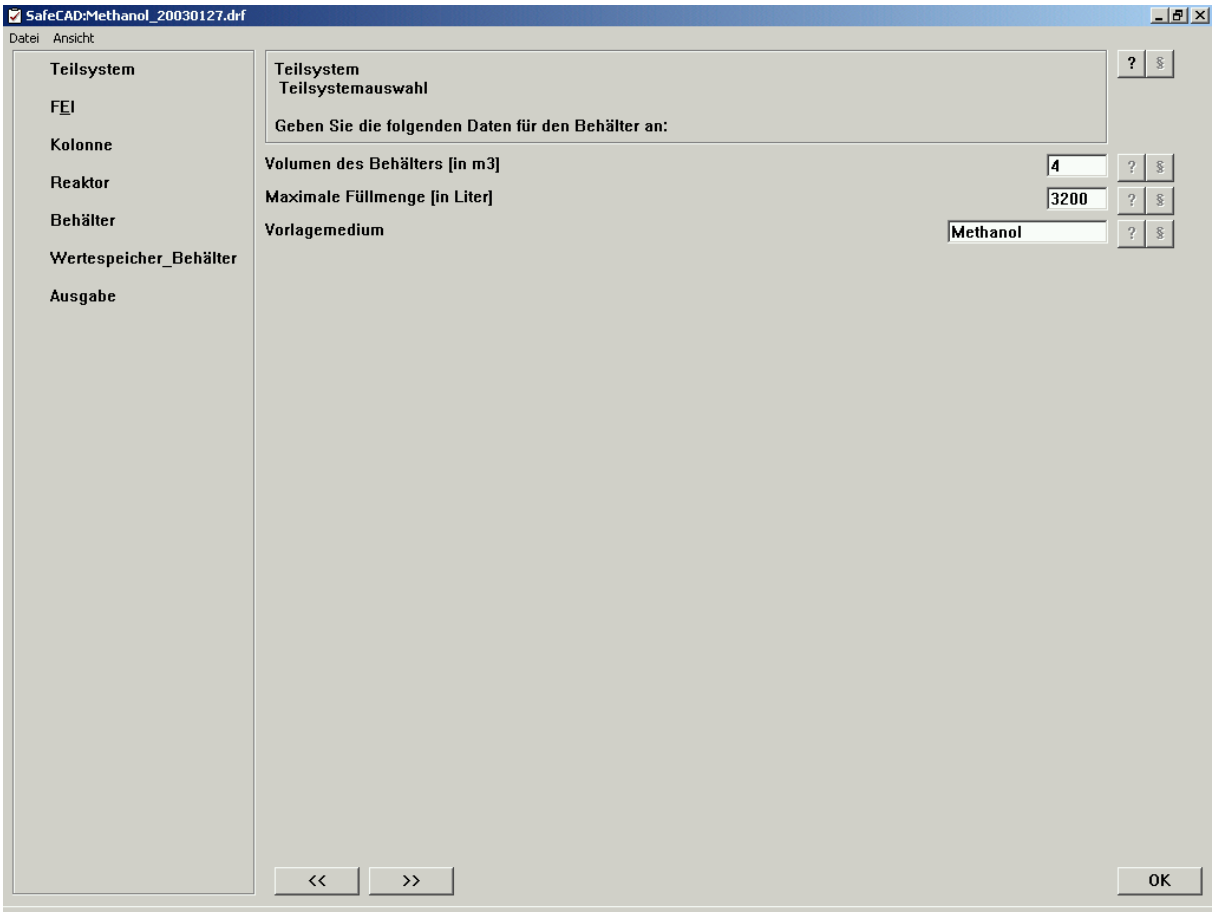
Im folgenden werden auszugesweise Screenshots SafeCAD's abgebildet, um die Ergebnisse des Kapitels 10 transparenter zu machen. Es werden nicht alle Schritte abgebildet, da einige kein Mehr an Information liefern. Im einzelnen sind dies:

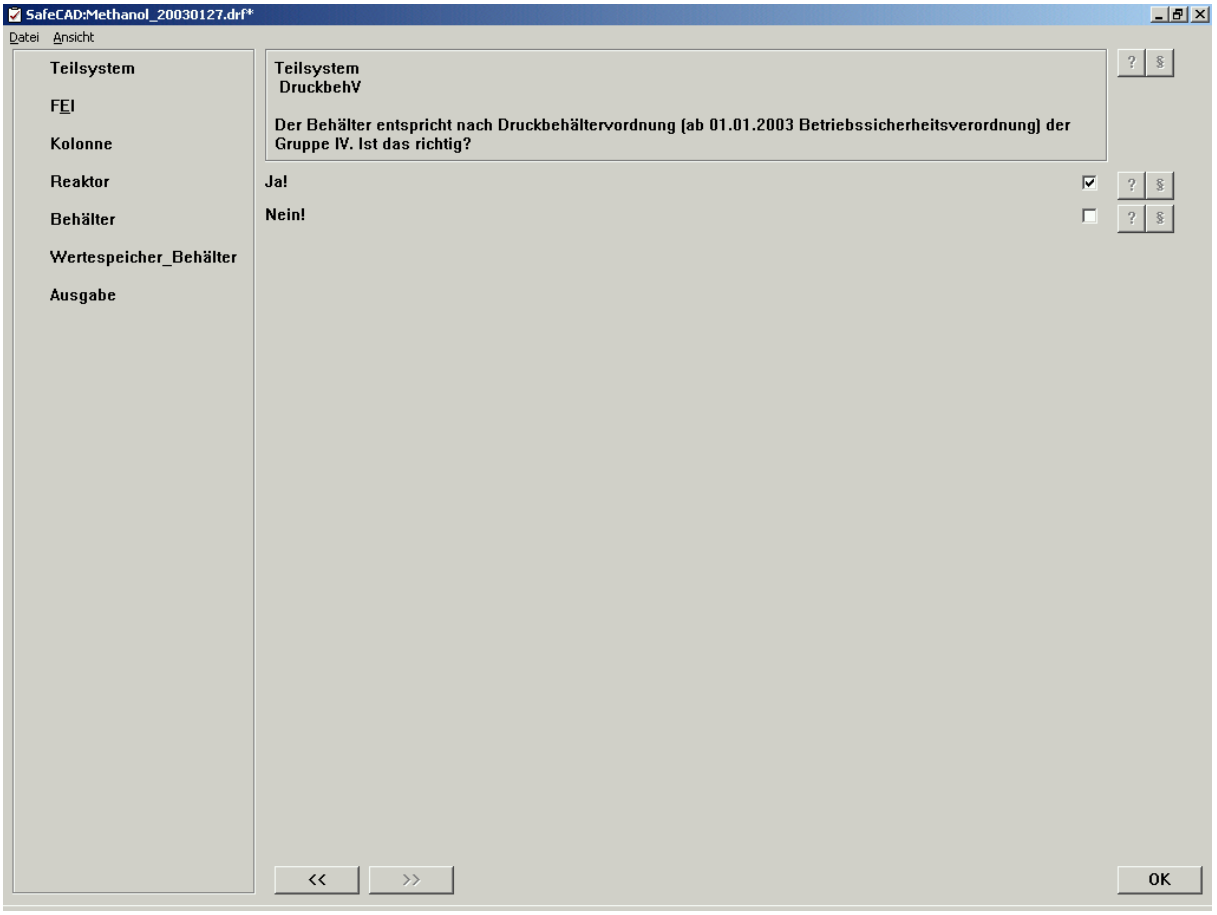
- Die Ermittlung des Gefahrenpotentials der Teilanlagen wird nur durch die erste und letzte Seite gezeigt und
- Bei der Gefährdungsermittlung werden nur die als wahrscheinlich erachteten Gefährdungen angezeigt.
- Bei einigen Punkten gibt es in der Praxis mehr Auswahlpunkte als die derzeit im Programm hinterlegten und im folgenden gezeigten Auswahlmöglichkeiten, z.B. bei der Wahl des Heiz-/Kühlsystems. Bei der Weiterentwicklung des Programms wird diese entsprechend berücksichtigt und ergänzt.

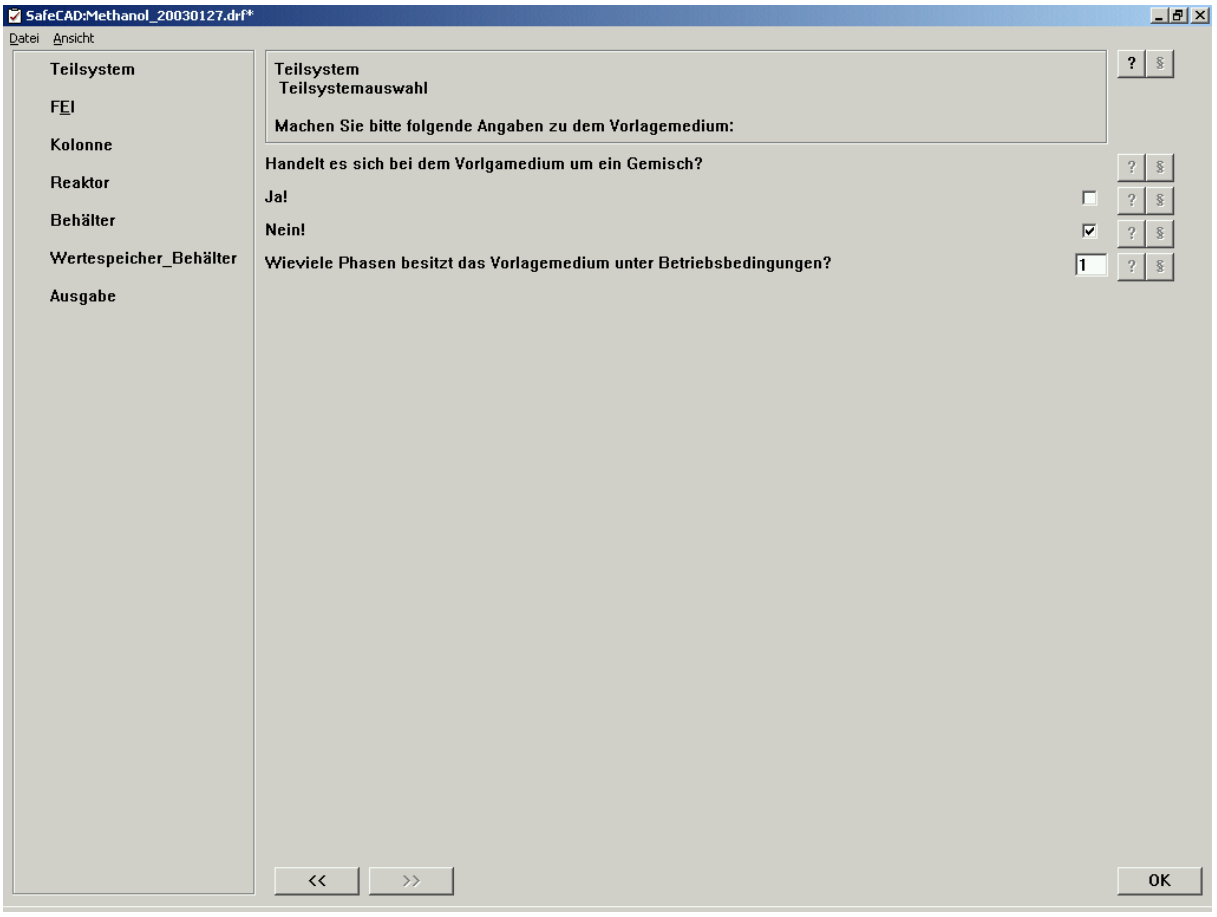
A.1 Methanolvorlagebehälter

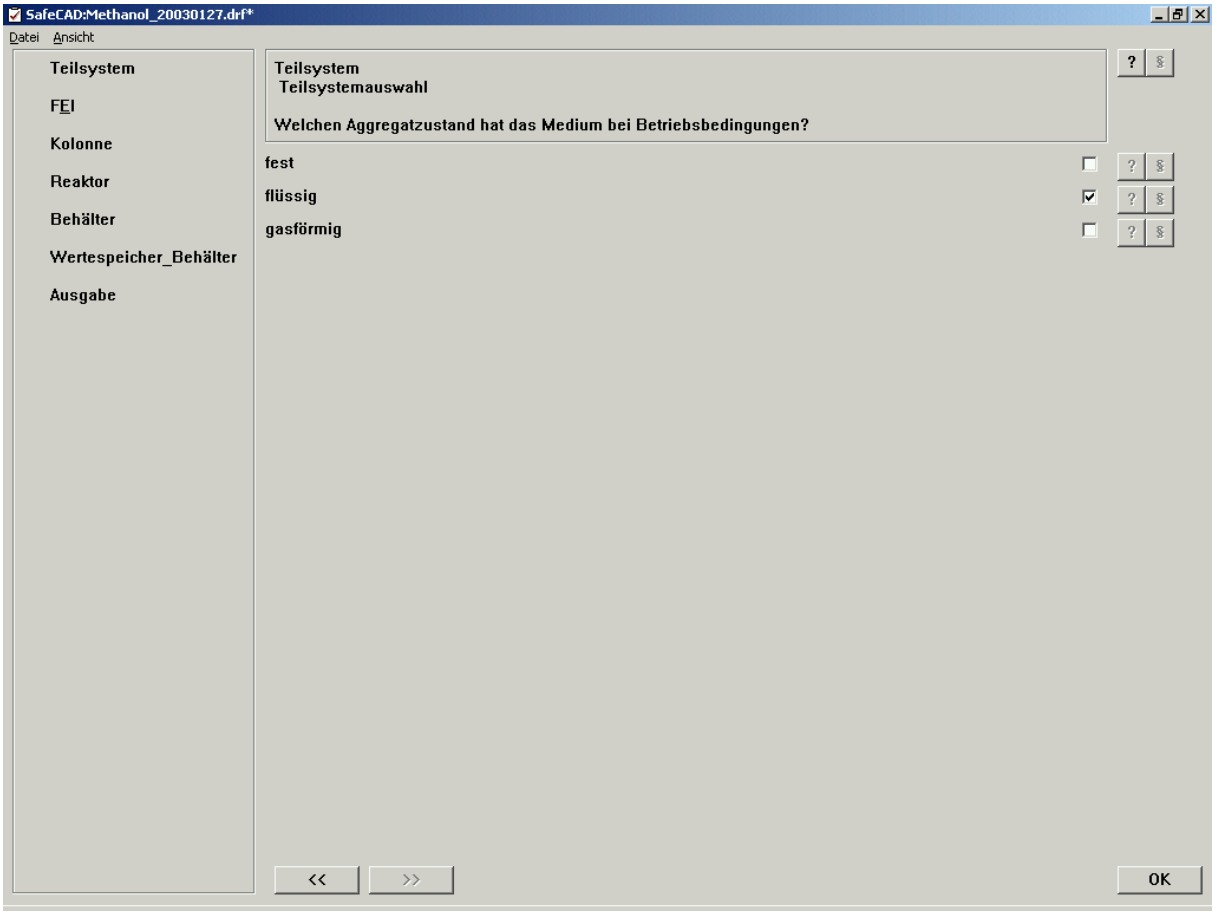


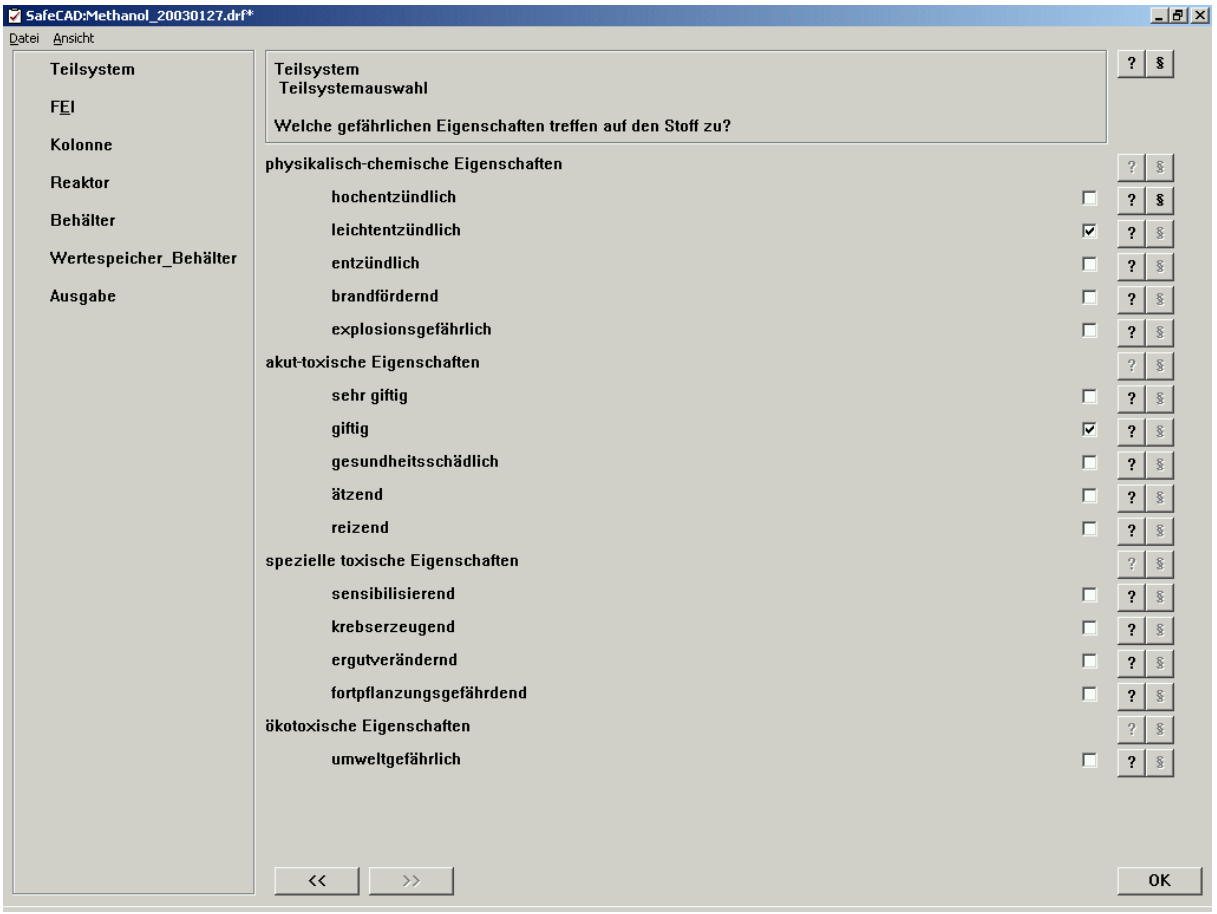

SafeCAD:Methanol_20030127.drf
Datei
Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Was für ein Behälter soll ausgewählt werden?
Vorlagebehälter
Lagerbehälter
Pufferbehälter
<<
>>
OK

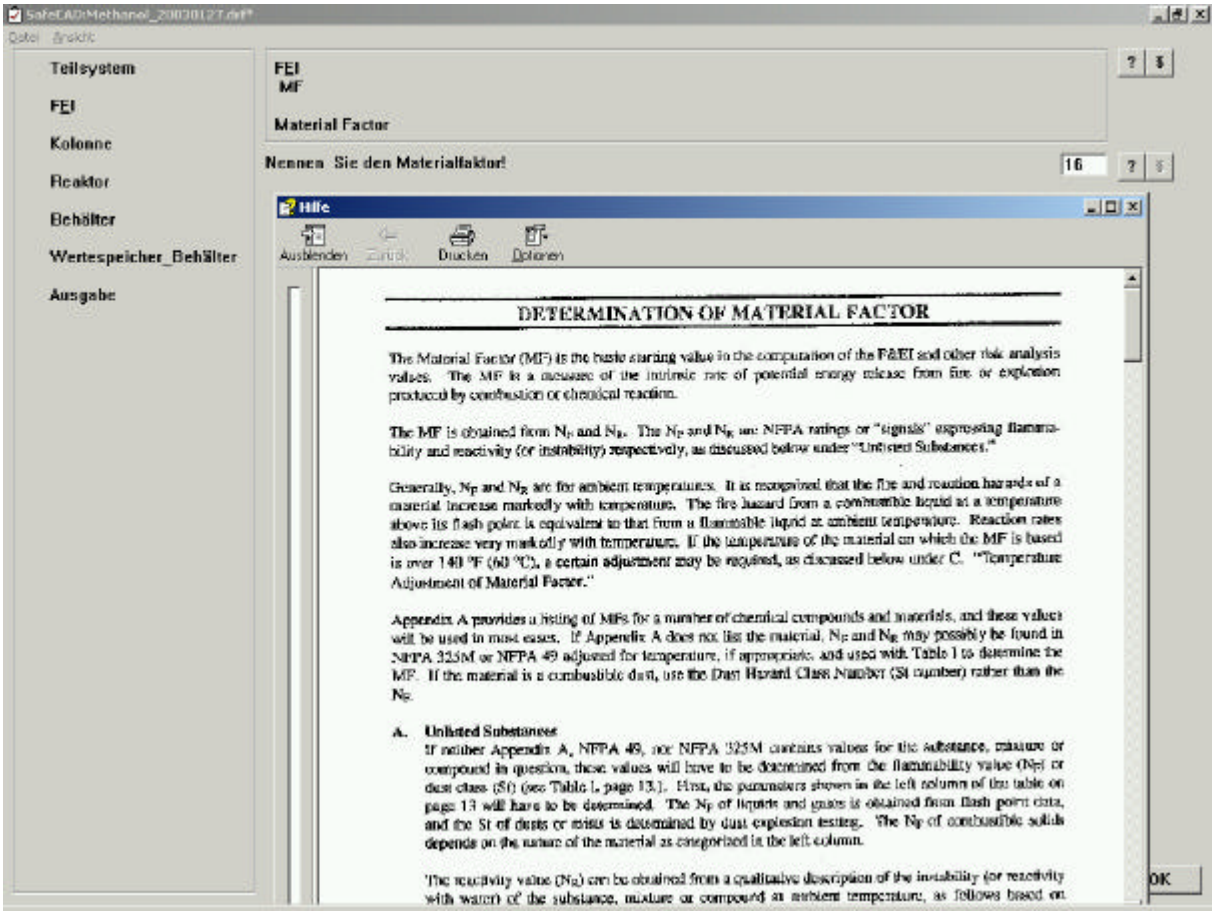

SafeCAD:Methanol_20030127.drf
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Geben Sie die folgenden Daten für den Behälter an:
Volumen des Behälters [in m3]
4
Maximale Füllmenge [in Liter]
3200
Vorlagemedium
Methanol
<<
>>
OK

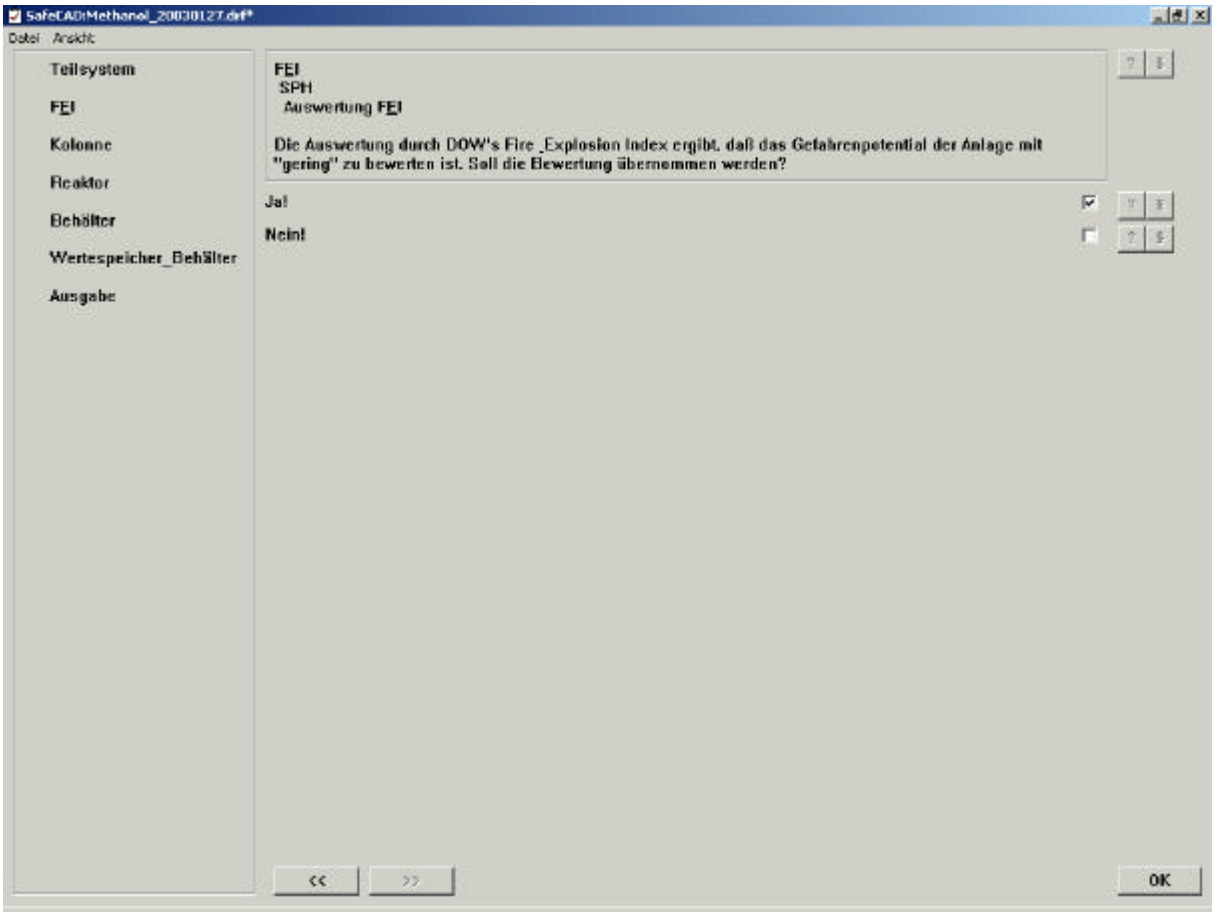

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
DruckbehV
Der Behälter entspricht nach Druckbehältervordnung (ab 01.01.2003 Betriebssicherheitsverordnung) der Gruppe IV. Ist das richtig?
Ja!
Nein!
<<
>>
OK

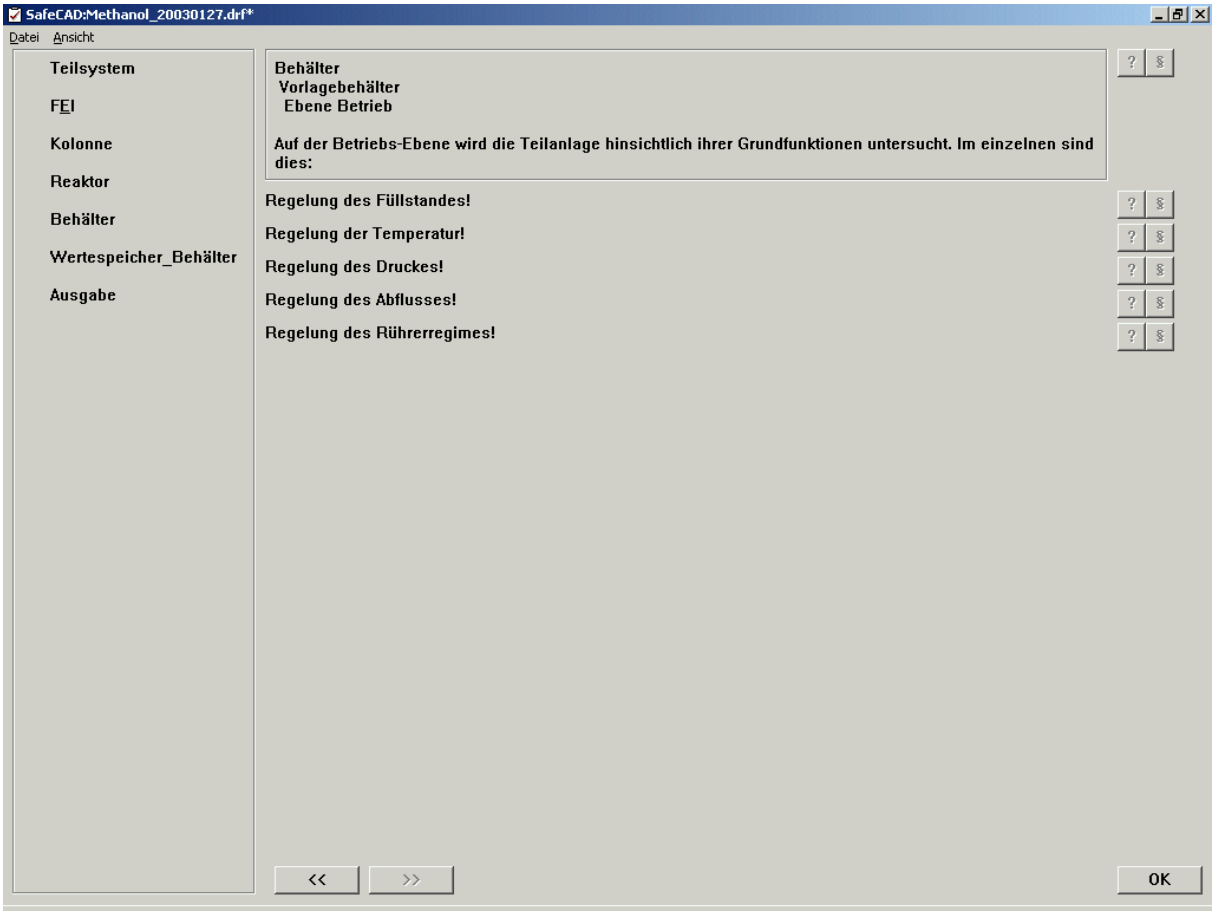

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Machen Sie bitte folgende Angaben zu dem Vorlagemedium:
Handelt es sich bei dem Vorlgamedium um ein Gemisch?
Ja!
Nein!
Wieviele Phasen besitzt das Vorlagemedium unter Betriebsbedingungen?
1
<<
>>
OK

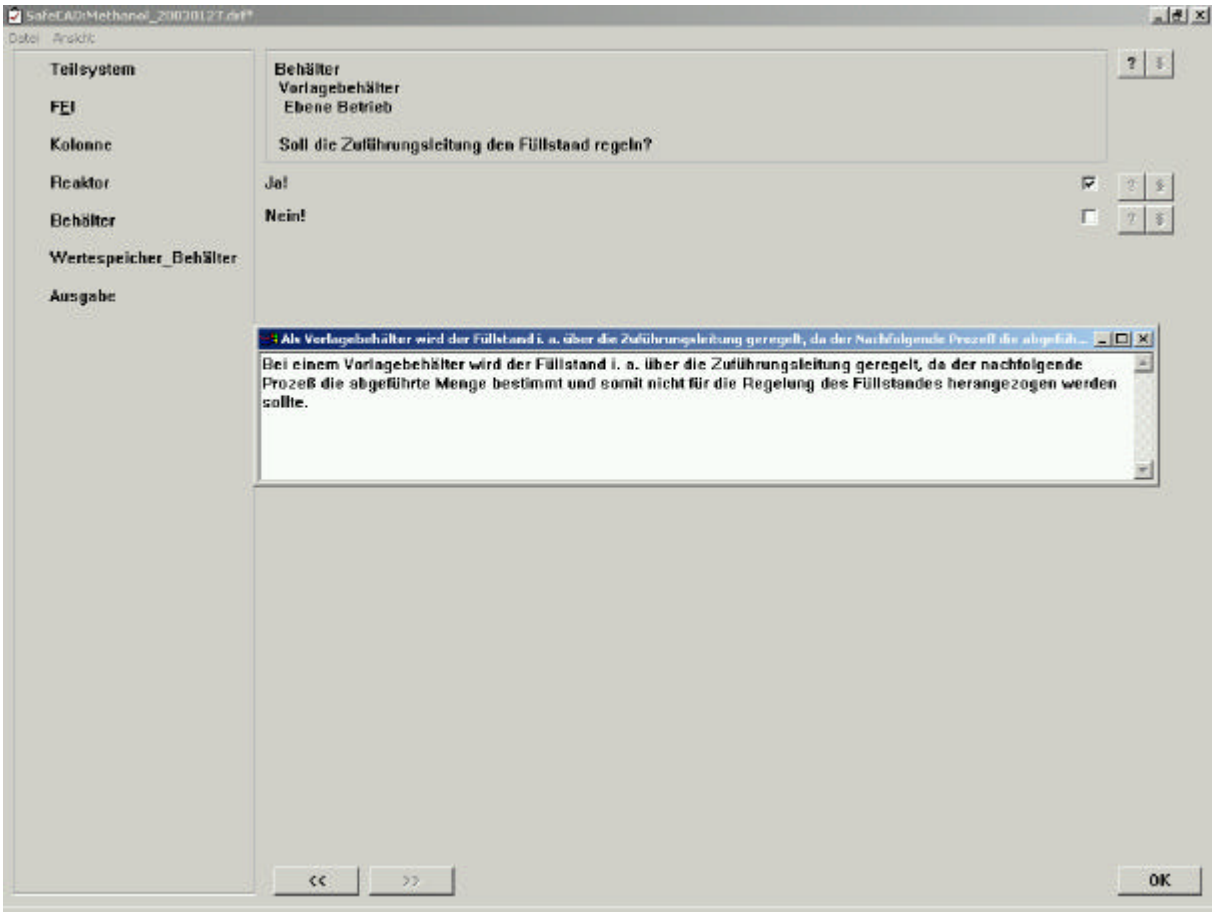

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Welchen Aggregatzustand hat das Medium bei Betriebsbedingungen?
fest
flüssig
gasförmig
<<
>>
OK

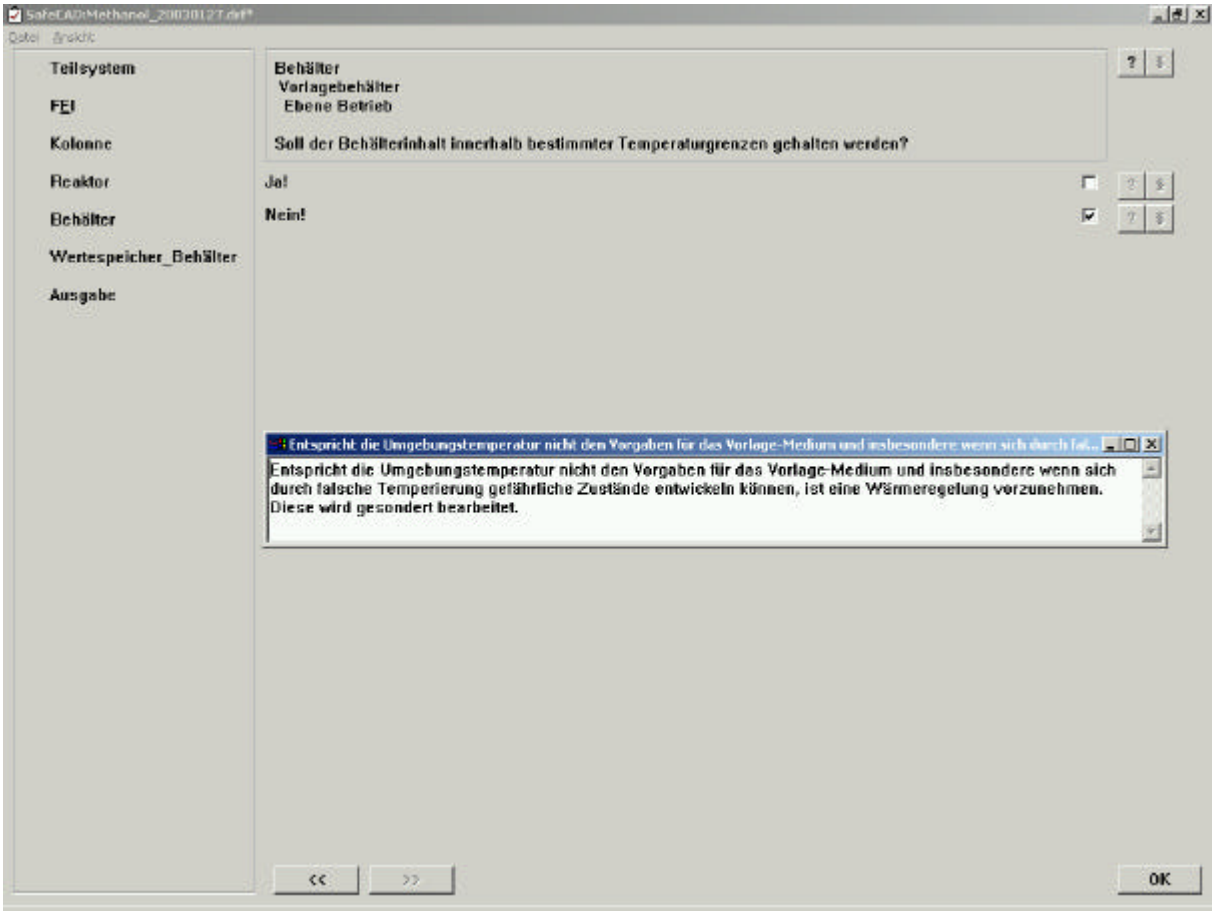

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Welche gefährlichen Eigenschaften treffen auf den Stoff zu?
physikalisch-chemische Eigenschaften
hochentzündlich
leichtentzündlich
entzündlich
brandfördernd
explosionsgefährlich
akut-toxische Eigenschaften
sehr giftig
giftig
gesundheitsschädlich
ätzend
reizend
spezielle toxische Eigenschaften
sensibilisierend
krebserzeugend
ergutverändernd
fortpflanzungsgefährdend
ökotoxische Eigenschaften
umweltgefährlich
<<
>>
OK

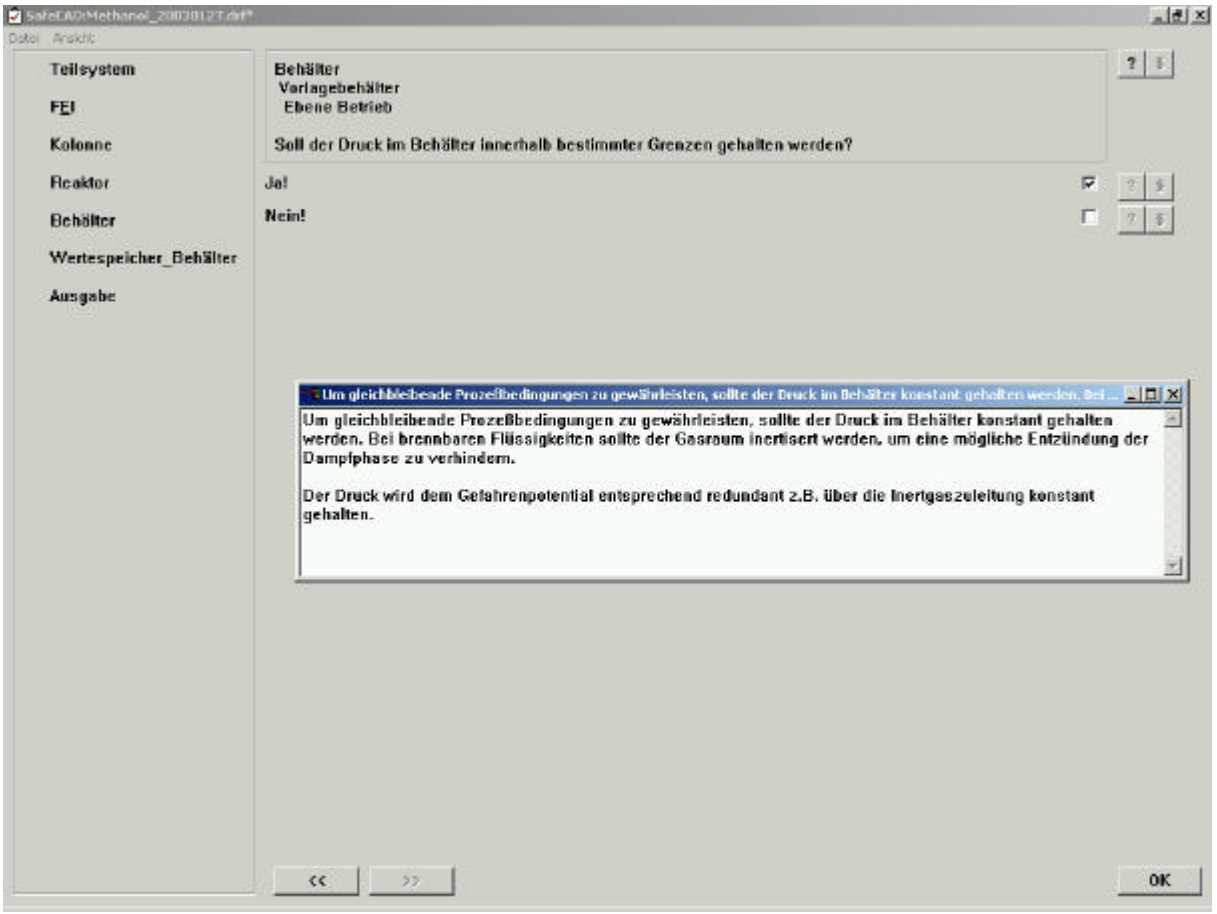

Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
FEI
MF
Material Factor
Nennen Sie den Materialfaktor!
16
Hilfe
Ausblenden
Zurück
Drucken
Optionen
DETERMINATION OF MATERIAL FACTOR
OK

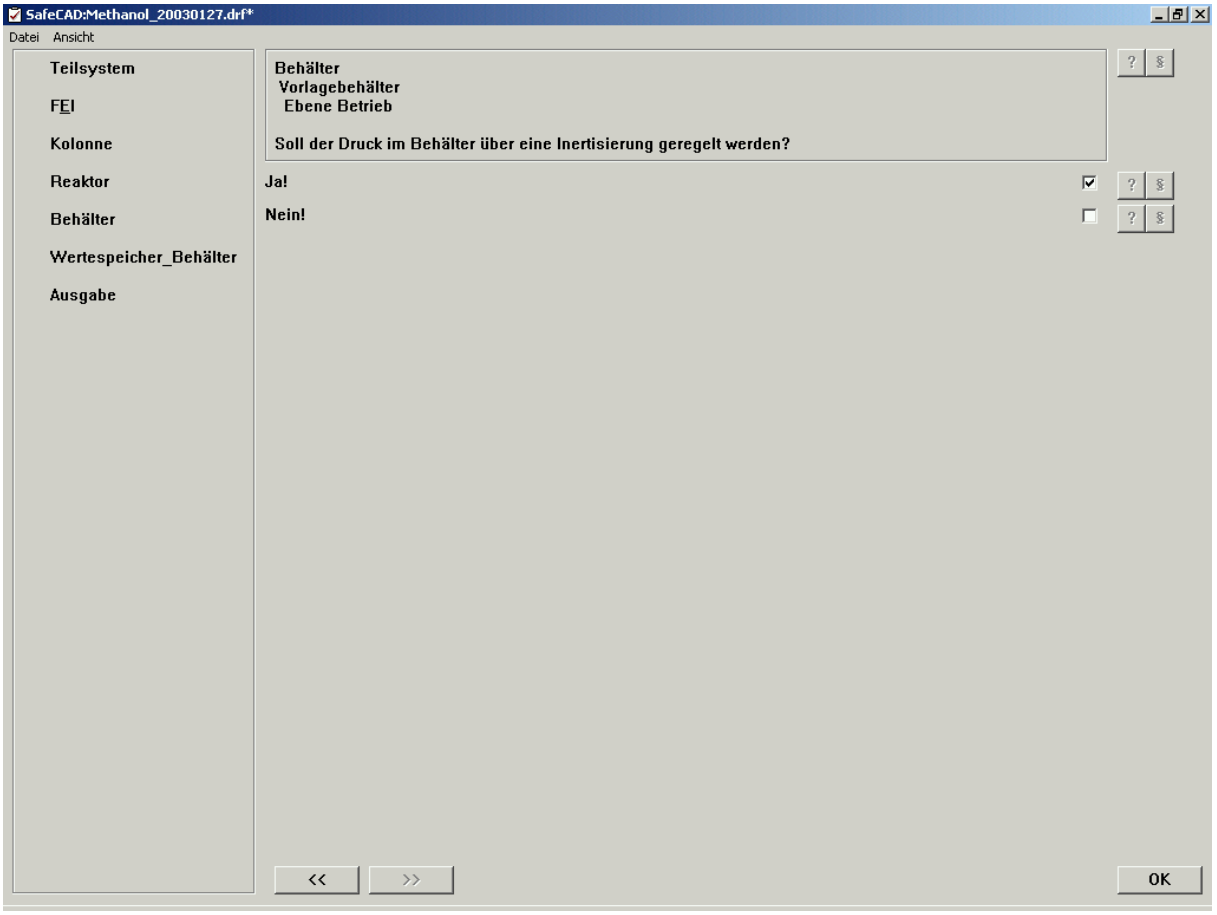

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
FEI
SPH
Auswertung FEI
Die Auswertung durch DOW's Fire _Explosion Index ergibt, daß das Gefahrenpotential der Anlage mit "gering" zu bewerten ist. Soll die Bewertung übernommen werden?
Ja!
Nein!
<<
>>
OK

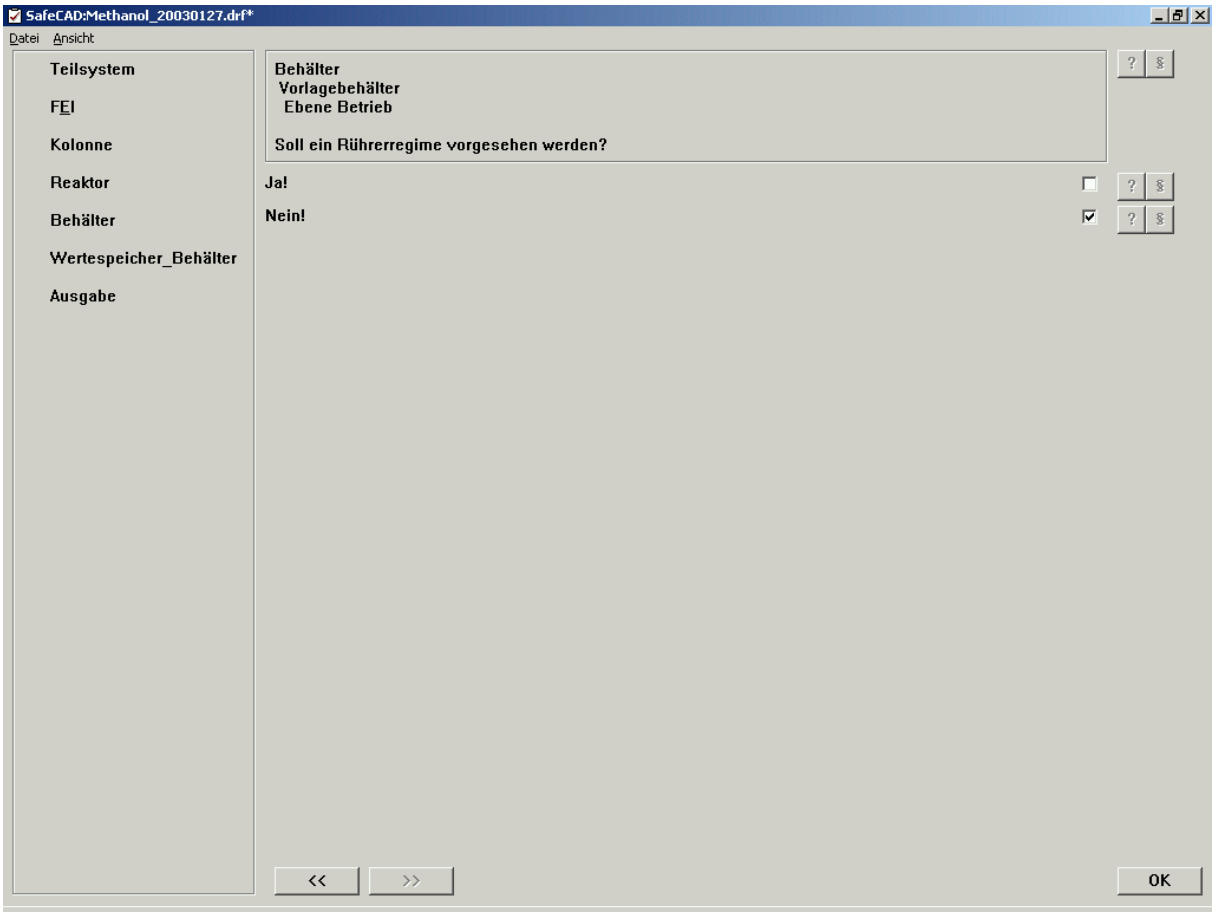

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Betrieb
Auf der Betriebs-Ebene wird die Teilanlage hinsichtlich ihrer Grundfunktionen untersucht. Im einzelnen sind dies:
Regelung des Füllstandes!
Regelung der Temperatur!
Regelung des Druckes!
Regelung des Abflusses!
Regelung des Rührerregimes!
<<
>>
OK

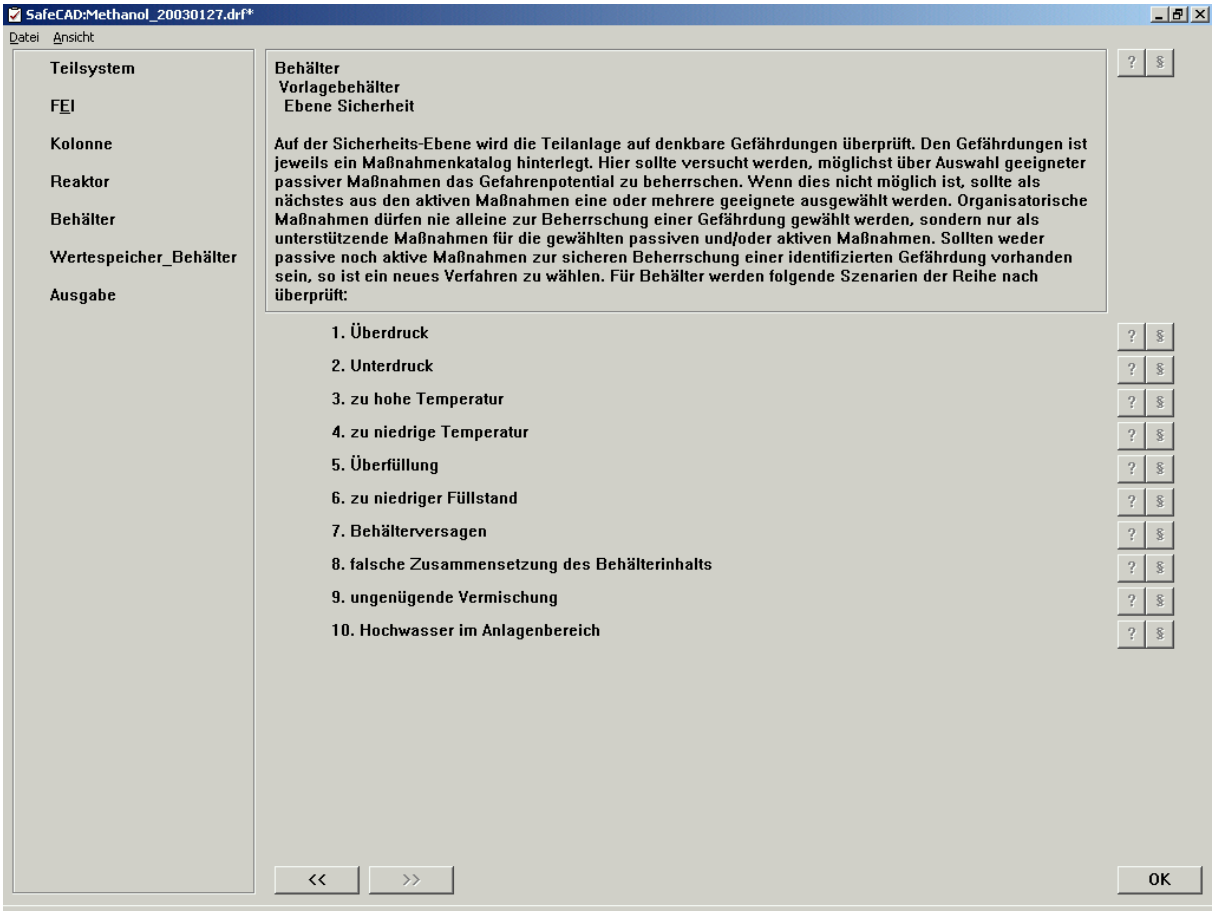

Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Betrieb
Soll die Zuführungsleitung den Füllstand regeln?
Ja!
Nein!
Bei einem Vorlagebehälter wird der Füllstand i. a. über die Zuführungsleitung geregelt, da der nachfolgende Prozeß die abgeführte Menge bestimmt und somit nicht für die Regelung des Füllstandes herangezogen werden sollte.
<<
>>
OK

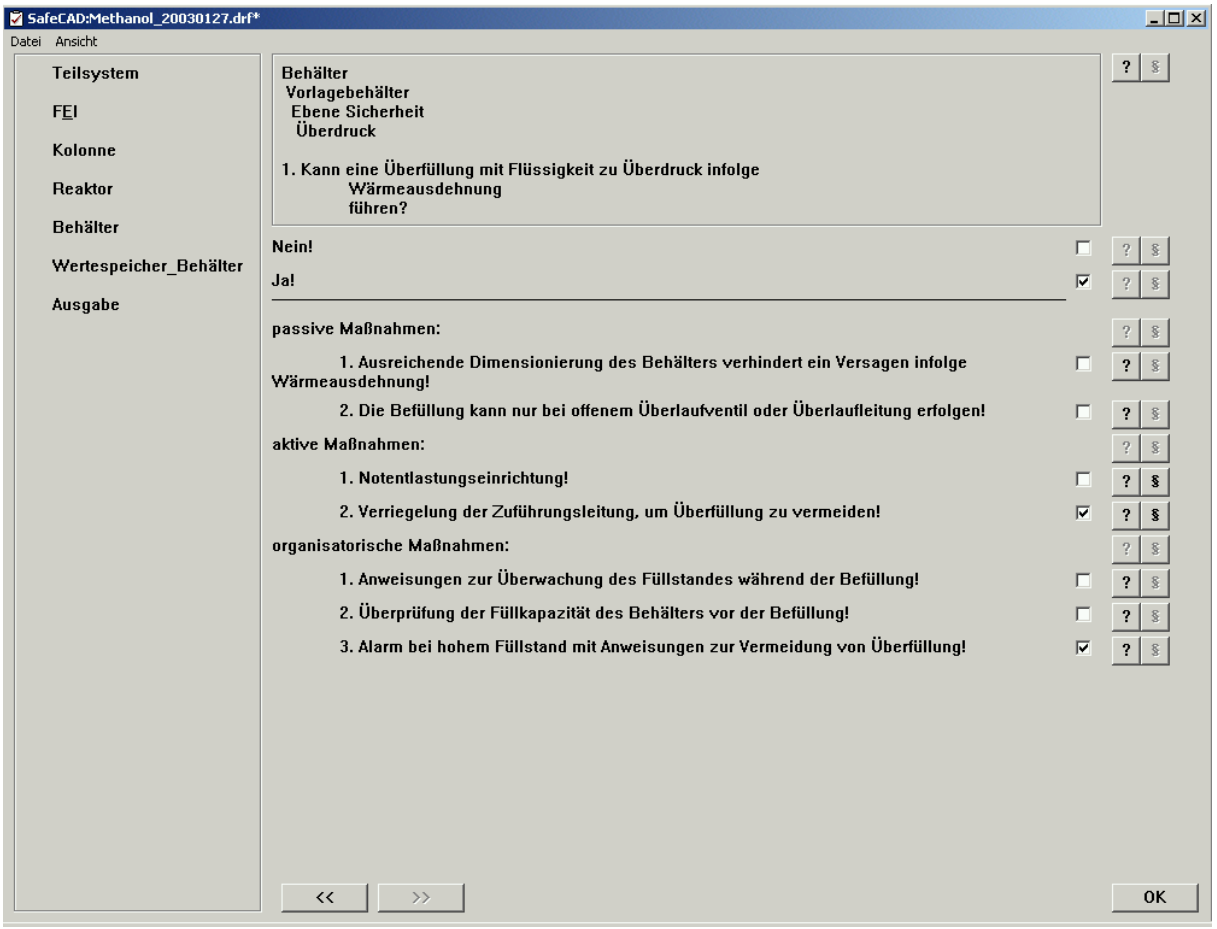

Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Betrieb
Soll der Behälterinhalt innerhalb bestimmter Temperaturgrenzen gehalten werden?
Ja!
Nein!
Entspricht die Umgebungstemperatur nicht den Vorgaben für das Vorlage-Medium und insbesondere wenn sich durch falsche Temperierung gefährliche Zustände entwickeln können, ist eine Wärmeregelung vorzunehmen. Diese wird gesondert bearbeitet.
<<
>>
OK

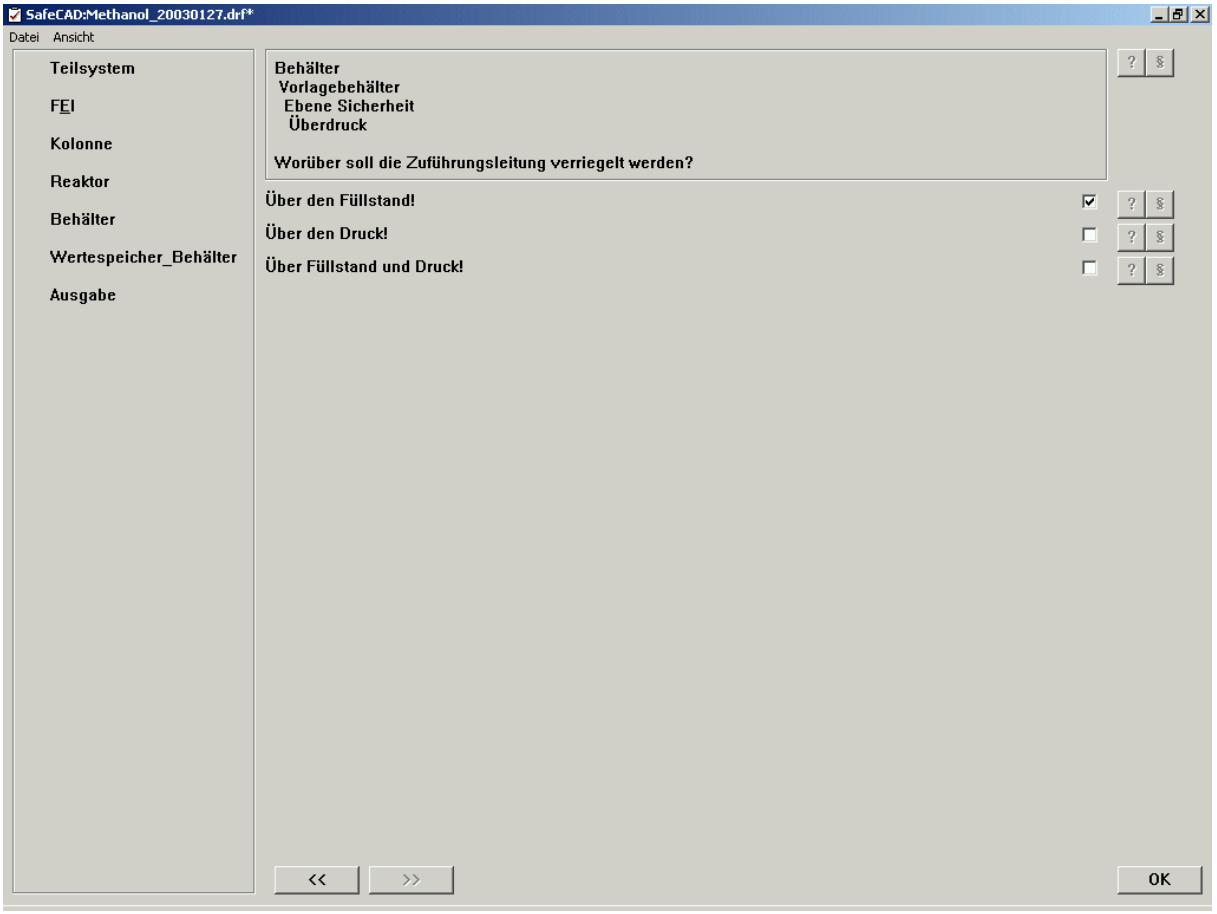

Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Betrieb
Soll der Druck im Behälter innerhalb bestimmter Grenzen gehalten werden?
Ja!
Nein!
Um gleichbleibende Prozeßbedingungen zu gewährleisten, sollte der Druck im Behälter konstant gehalten werden. Bei brennbaren Flüssigkeiten sollte der Gasraum inertisert werden, um eine mögliche Entzündung der Dampfphase zu verhindern.
Der Druck wird dem Gefahrenpotential entsprechend redundant z.B. über die Inertgaszuleitung konstant gehalten.
<<
>>
OK

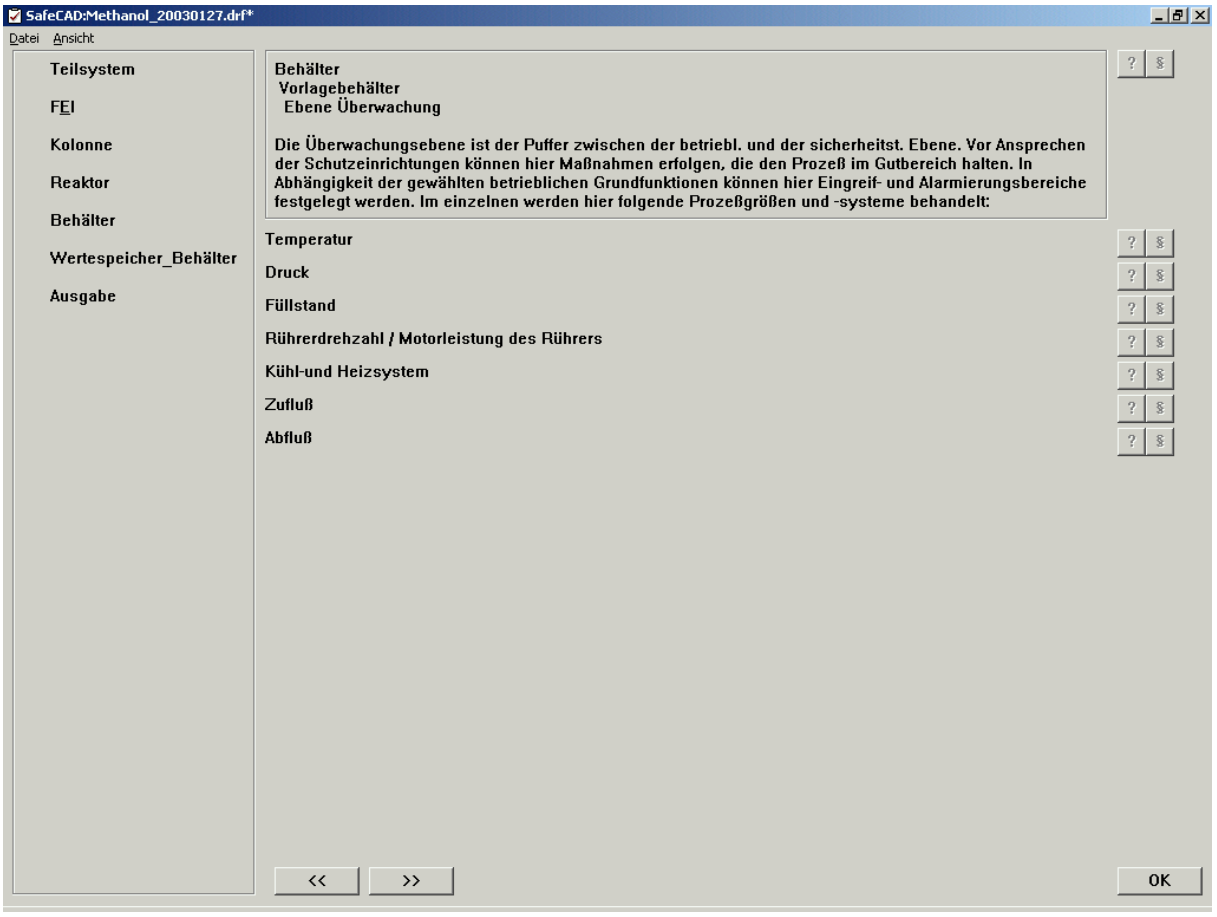

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Betrieb
Soll der Druck im Behälter über eine Inertisierung geregelt werden?
Ja!
Nein!
<<
>>
OK

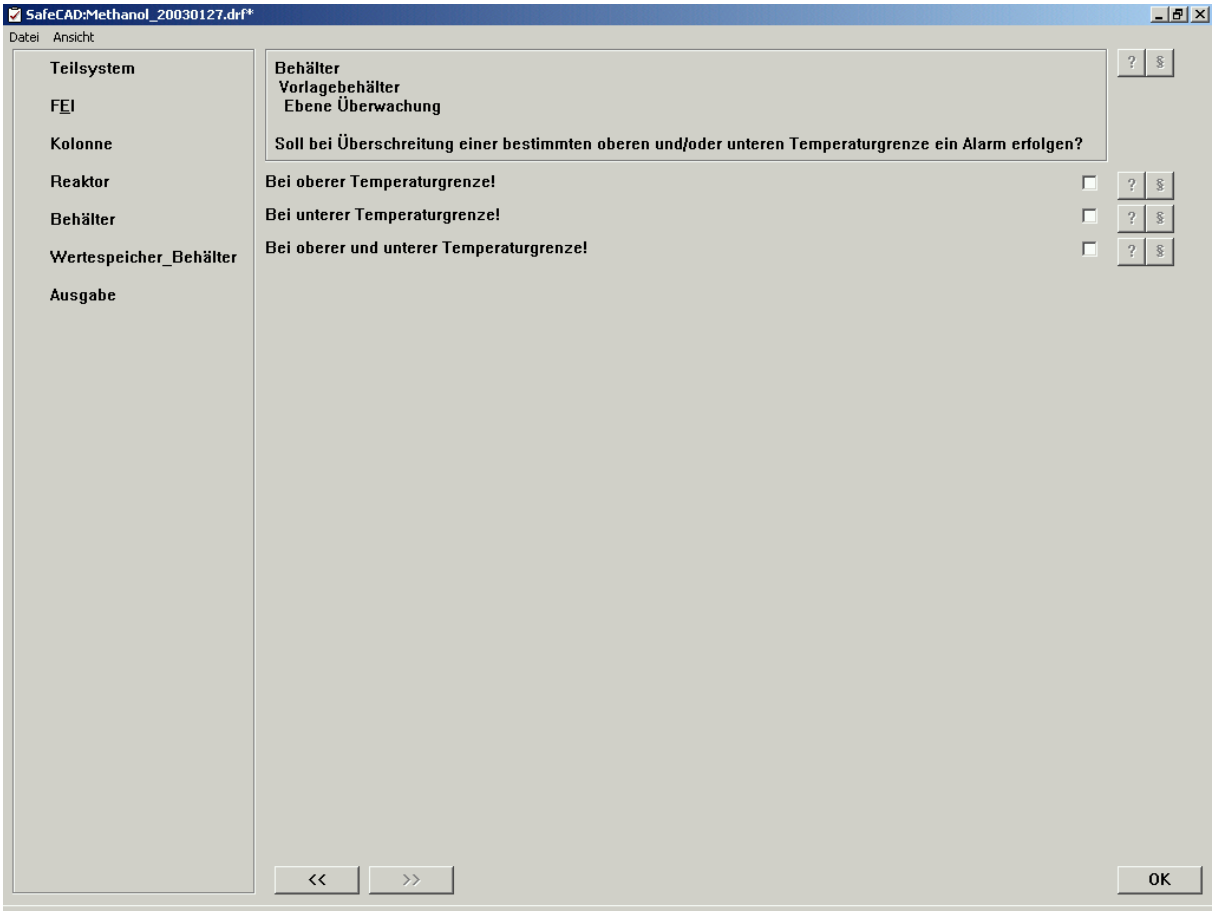

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Betrieb
Soll ein Rührerregime vorgesehen werden?
Ja!
Nein!
<<
>>
OK

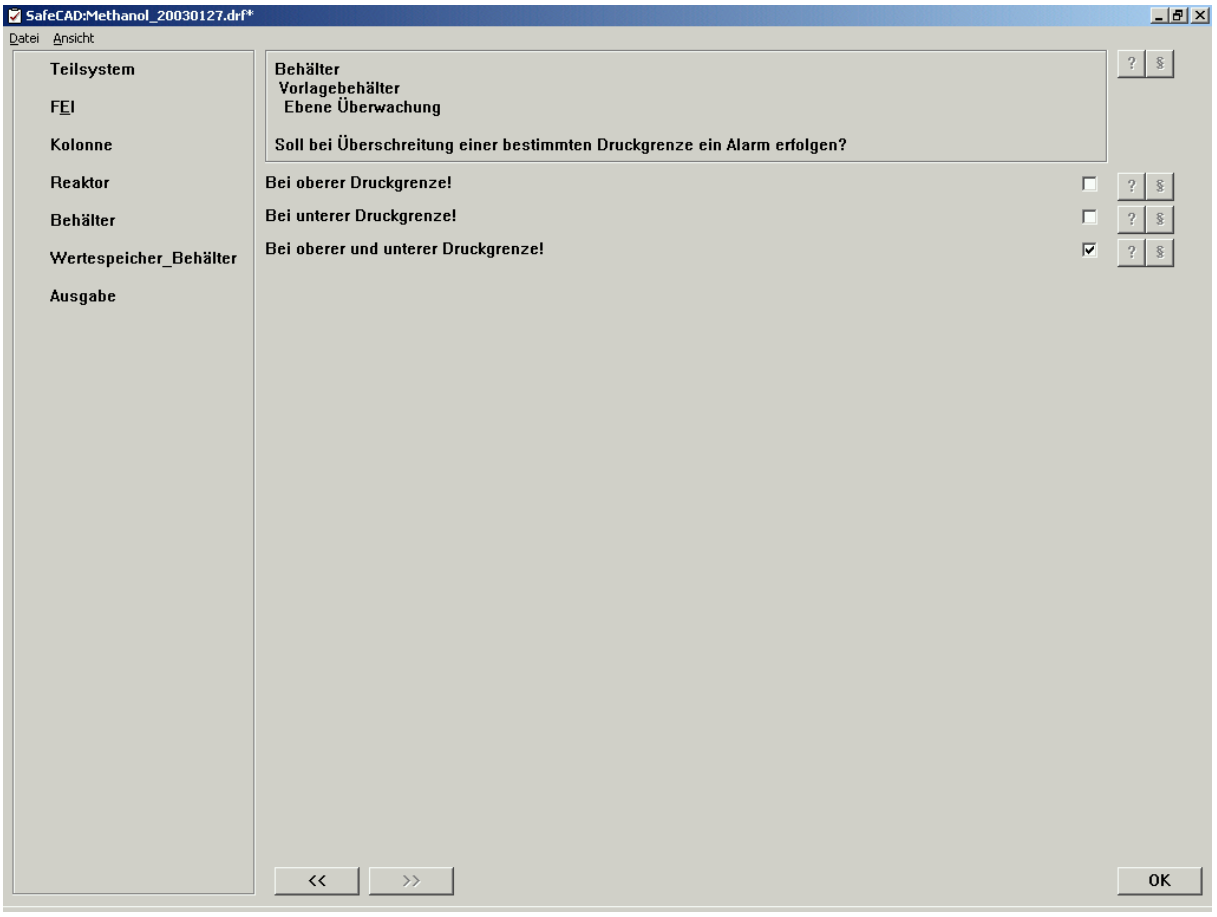

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Sicherheit
Auf der Sicherheits-Ebene wird die Teilanlage auf denkbare Gefährdungen überprüft. Den Gefährdungen ist jeweils ein Maßnahmenkatalog hinterlegt. Hier sollte versucht werden, möglichst über Auswahl geeigneter passiver Maßnahmen das Gefahrenpotential zu beherrschen. Wenn dies nicht möglich ist, sollte als nächstes aus den aktiven Maßnahmen eine oder mehrere geeignete ausgewählt werden. Organisatorische Maßnahmen dürfen nie alleine zur Beherrschung einer Gefährdung gewählt werden, sondern nur als unterstützende Maßnahmen für die gewählten passiven und/oder aktiven Maßnahmen. Sollten weder passive noch aktive Maßnahmen zur sicheren Beherrschung einer identifizierten Gefährdung vorhanden sein, so ist ein neues Verfahren zu wählen. Für Behälter werden folgende Szenarien der Reihe nach überprüft:
1. Überdruck
2. Unterdruck
3. zu hohe Temperatur
4. zu niedrige Temperatur
5. Überfüllung
6. zu niedriger Füllstand
7. Behälterversagen
8. falsche Zusammensetzung des Behälterinhalts
9. ungenügende Vermischung
10. Hochwasser im Anlagenbereich
<<
>>
OK

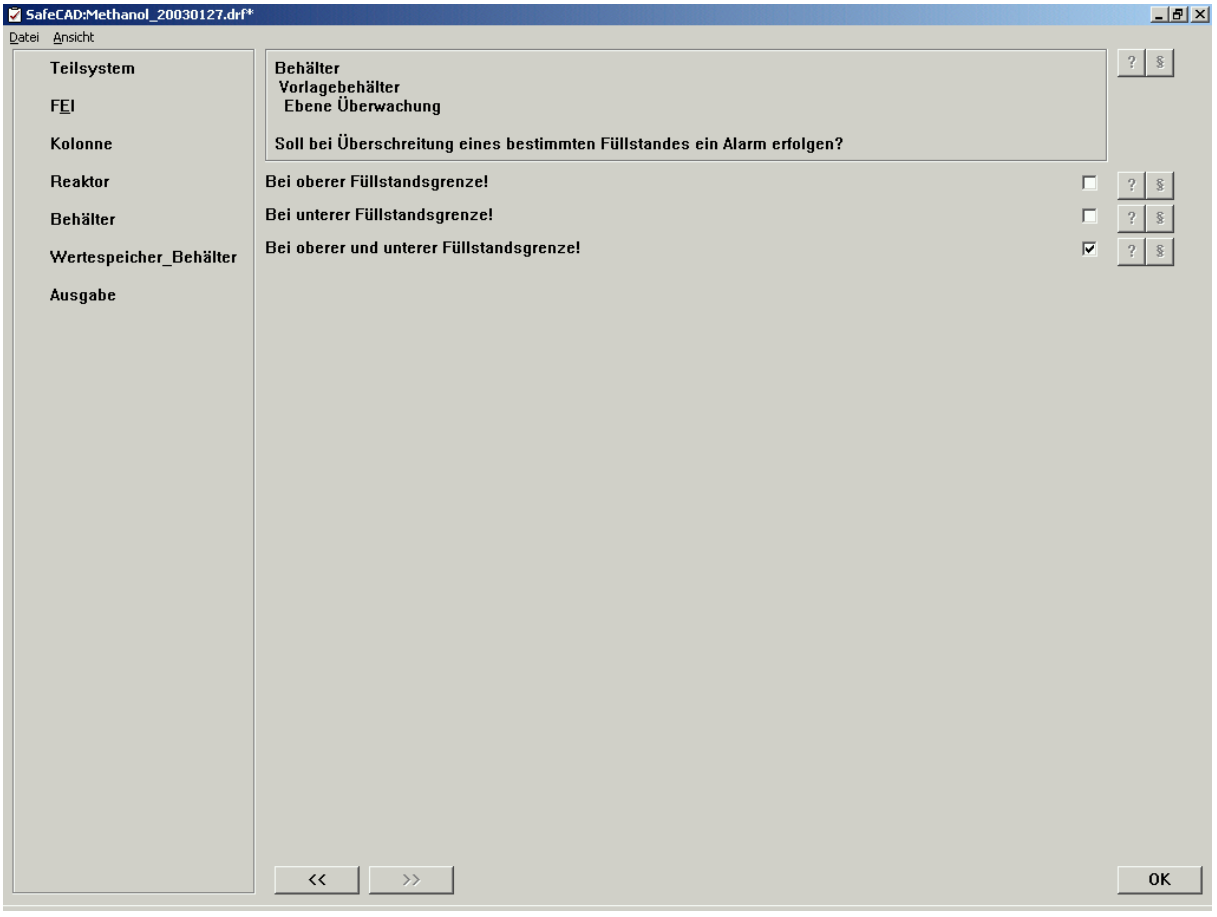

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Sicherheit
Überdruck
1. Kann eine Überfüllung mit Flüssigkeit zu Überdruck infolge Wärmeausdehnung führen?
Nein!
Ja!
passive Maßnahmen:
1. Ausreichende Dimensionierung des Behälters verhindert ein Versagen infolge Wärmeausdehnung!
2. Die Befüllung kann nur bei offenem Überlaufventil oder Überlaufleitung erfolgen!
aktive Maßnahmen:
1. Notentlastungseinrichtung!
2. Verriegelung der Zuführungsleitung, um Überfüllung zu vermeiden!
organisatorische Maßnahmen:
1. Anweisungen zur Überwachung des Füllstandes während der Befüllung!
2. Überprüfung der Füllkapazität des Behälters vor der Befüllung!
3. Alarm bei hohem Füllstand mit Anweisungen zur Vermeidung von Überfüllung!
<<
>>
OK

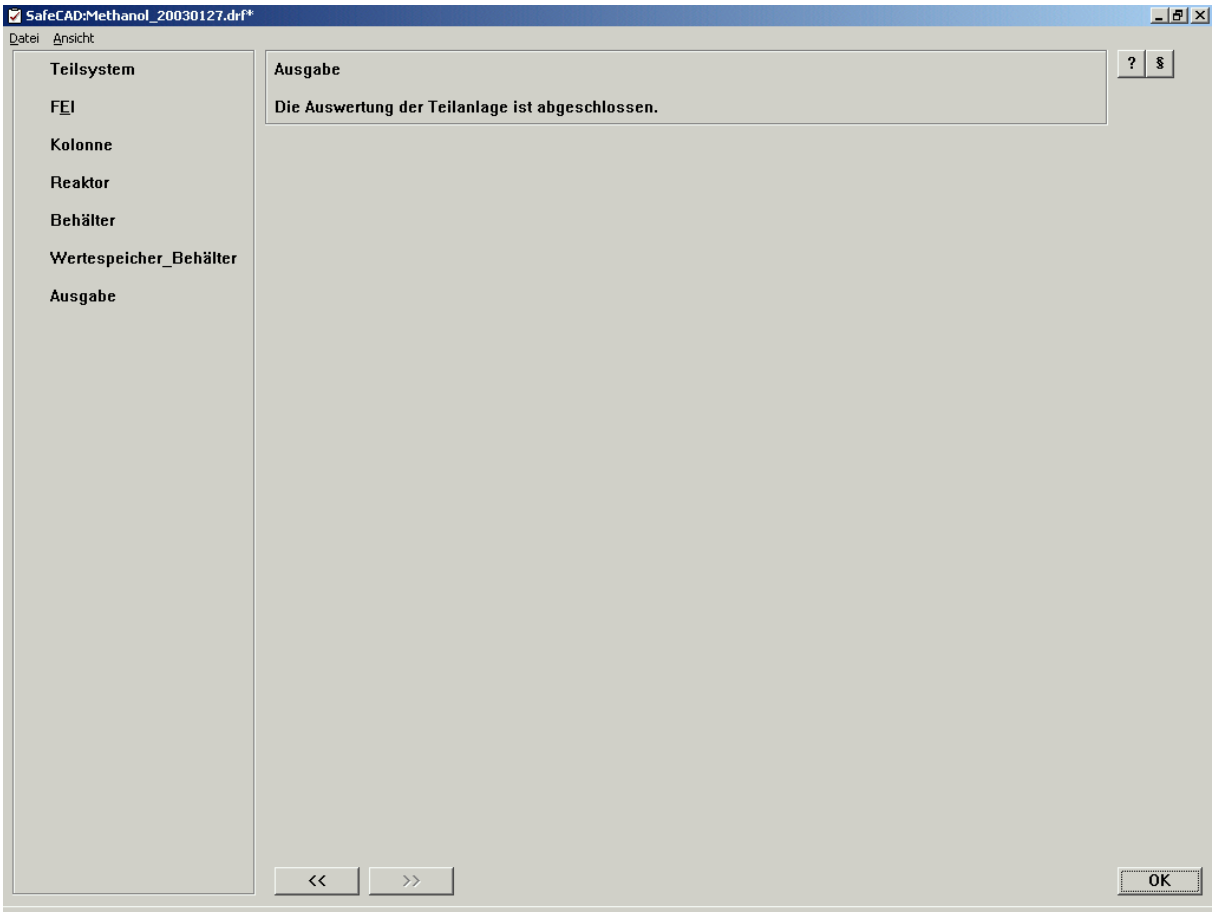

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Sicherheit
Überdruck
Worüber soll die Zuführungsleitung verriegelt werden?
Über den Füllstand!
Über den Druck!
Über Füllstand und Druck!
<<
>>
OK

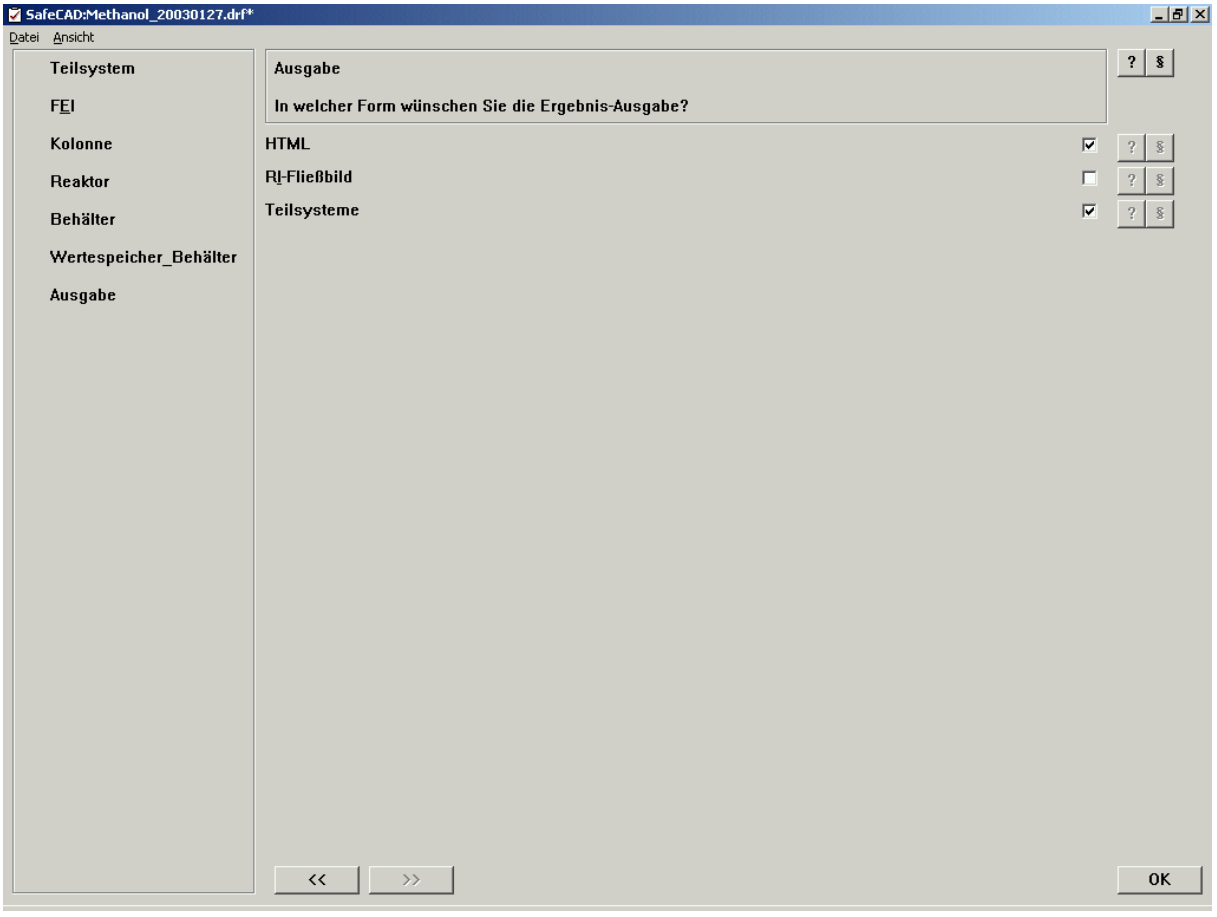

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Überwachung
Die Überwachungsebene ist der Puffer zwischen der betriebl. und der sicherheitst. Ebene. Vor Ansprechen der Schutzeinrichtungen können hier Maßnahmen erfolgen, die den Prozeß im Gutbereich halten. In Abhängigkeit der gewählten betrieblichen Grundfunktionen können hier Eingreif- und Alarmierungsbereiche festgelegt werden. Im einzelnen werden hier folgende Prozeßgrößen und -systeme behandelt:
Temperatur
Druck
Füllstand
Rührerdrehzahl / Motorleistung des Rührers
Kühl-und Heizsystem
Zufluß
Abfluß
<<
>>
OK


SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Überwachung
Soll bei Überschreitung einer bestimmten oberen und/oder unteren Temperaturgrenze ein Alarm erfolgen?
Bei oberer Temperaturgrenze!
Bei unterer Temperaturgrenze!
Bei oberer und unterer Temperaturgrenze!
<<
>>
OK

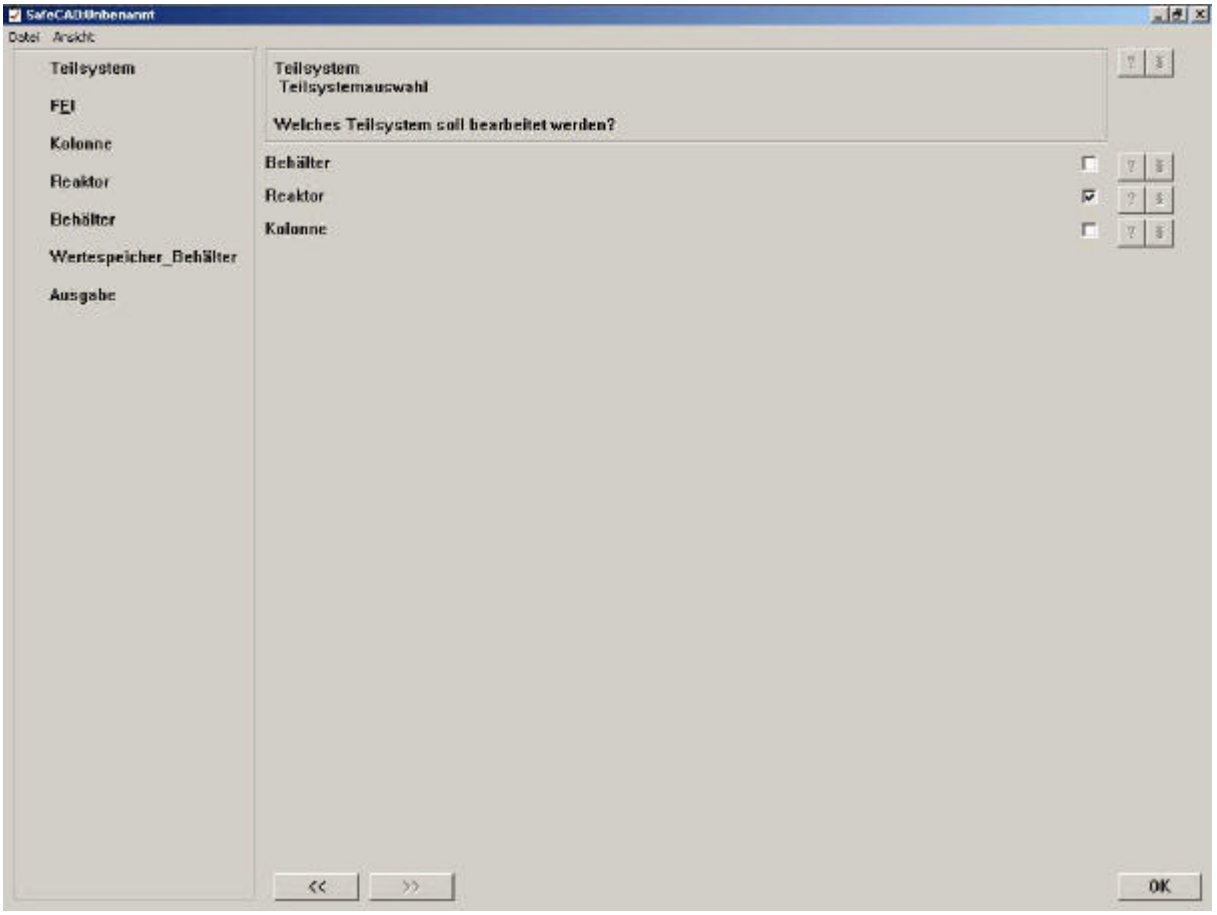

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Überwachung
Soll bei Überschreitung einer bestimmten Druckgrenze ein Alarm erfolgen?
Bei oberer Druckgrenze!
Bei unterer Druckgrenze!
Bei oberer und unterer Druckgrenze!
<<
>>
OK

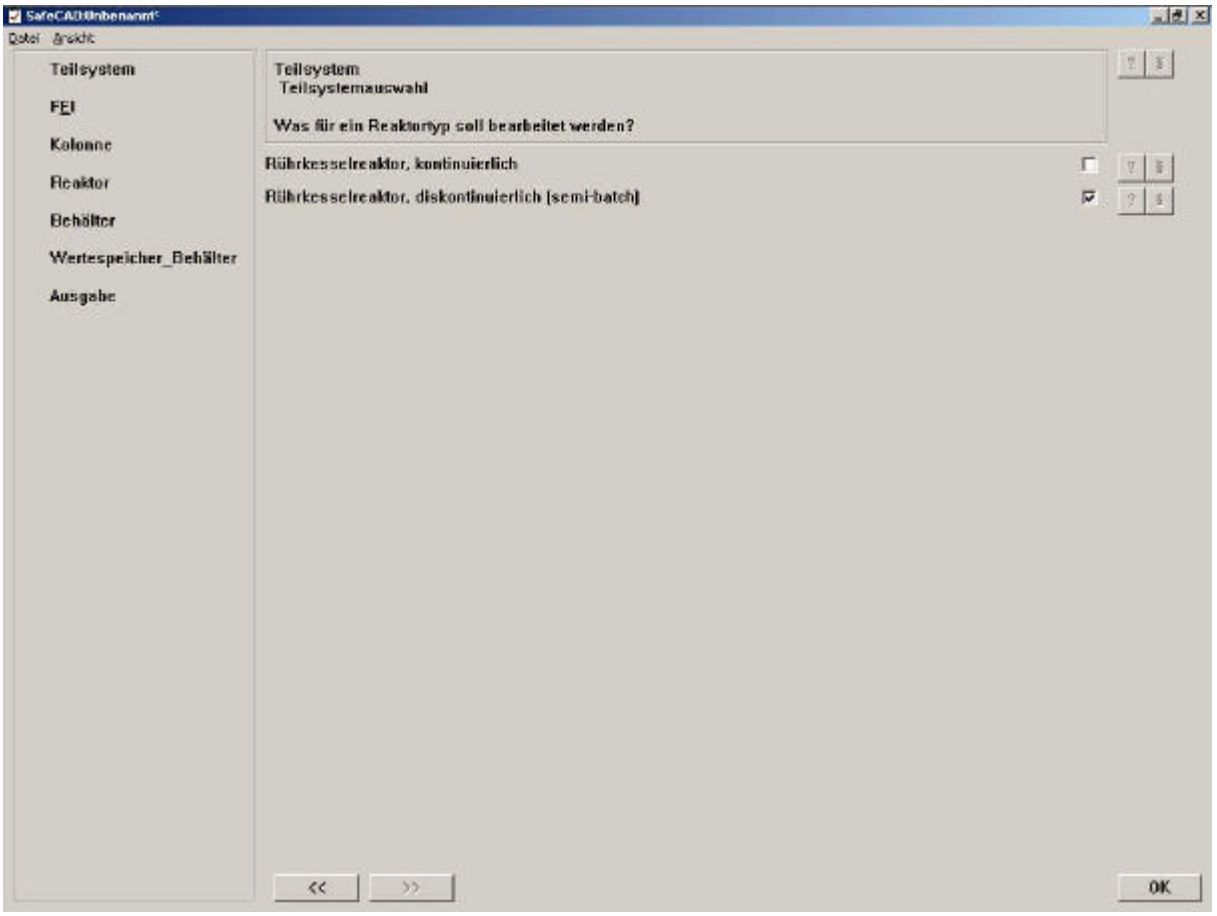

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Behälter
Vorlagebehälter
Ebene Überwachung
Soll bei Überschreitung eines bestimmten Füllstandes ein Alarm erfolgen?
Bei oberer Füllstandsgrenze!
Bei unterer Füllstandsgrenze!
Bei oberer und unterer Füllstandsgrenze!
<<
>>
OK

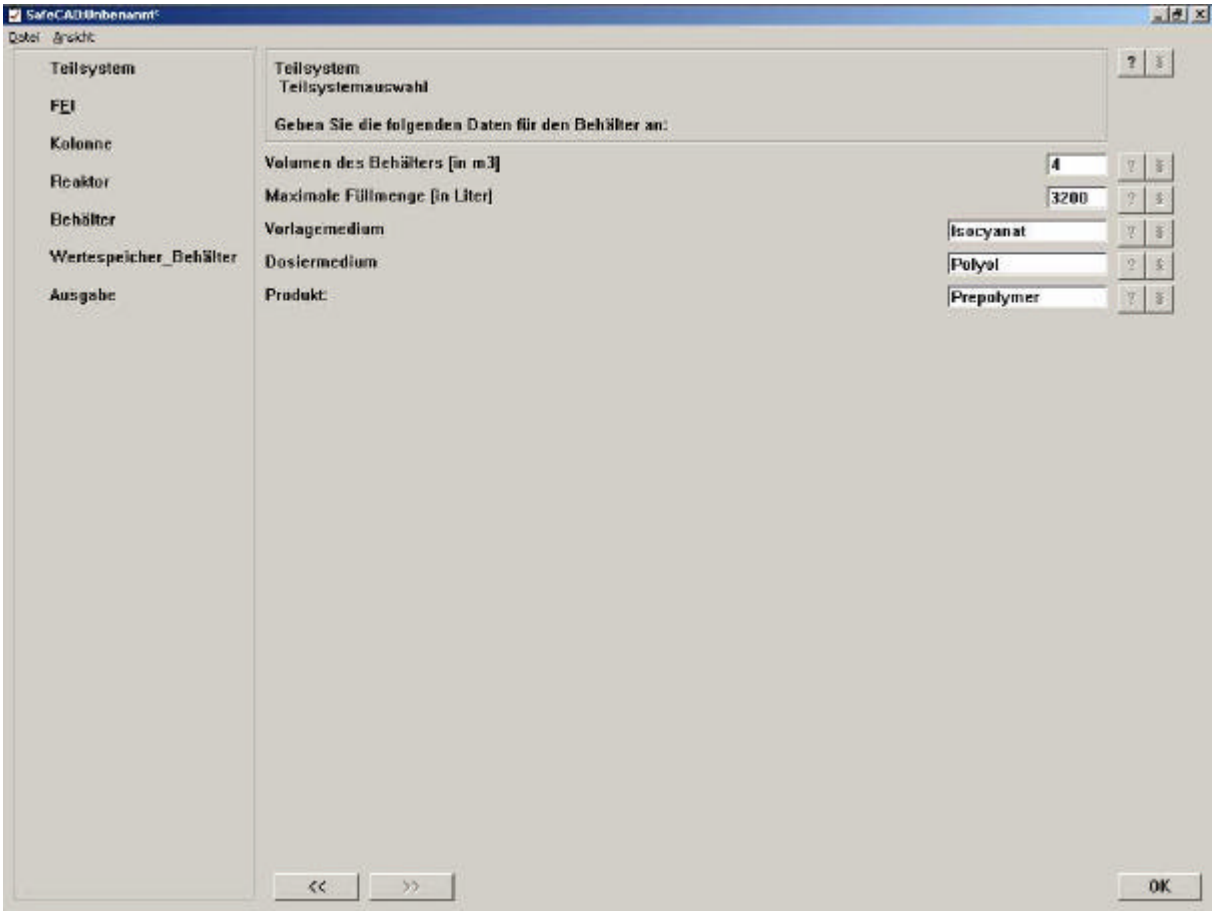

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Ausgabe
Die Auswertung der Teilanlage ist abgeschlossen.
?
§
<<
>>
OK

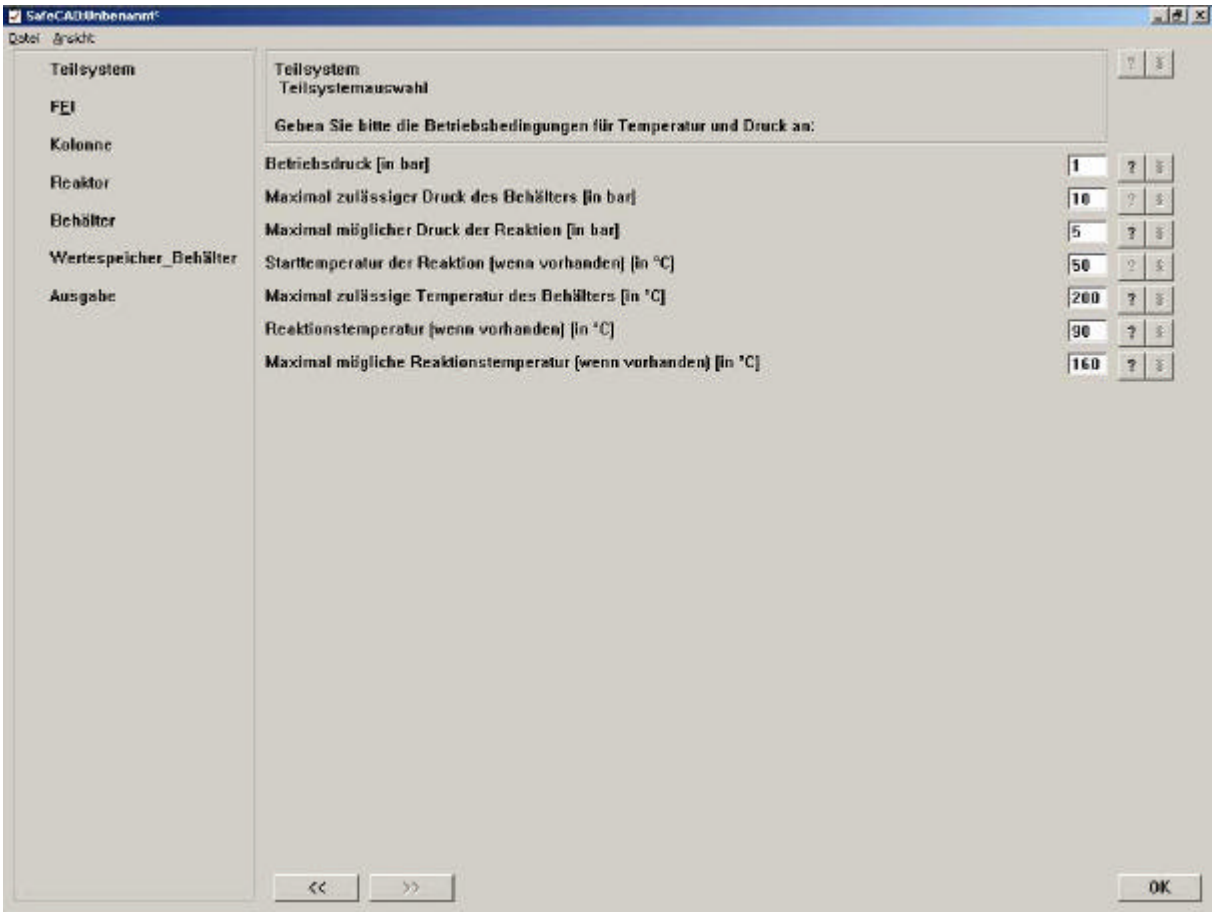

SafeCAD:Methanol_20030127.drf*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Ausgabe
In welcher Form wünschen Sie die Ergebnis-Ausgabe?
HTML
RI-Fließbild
Teilsysteme
?
§
<<
>>
OK

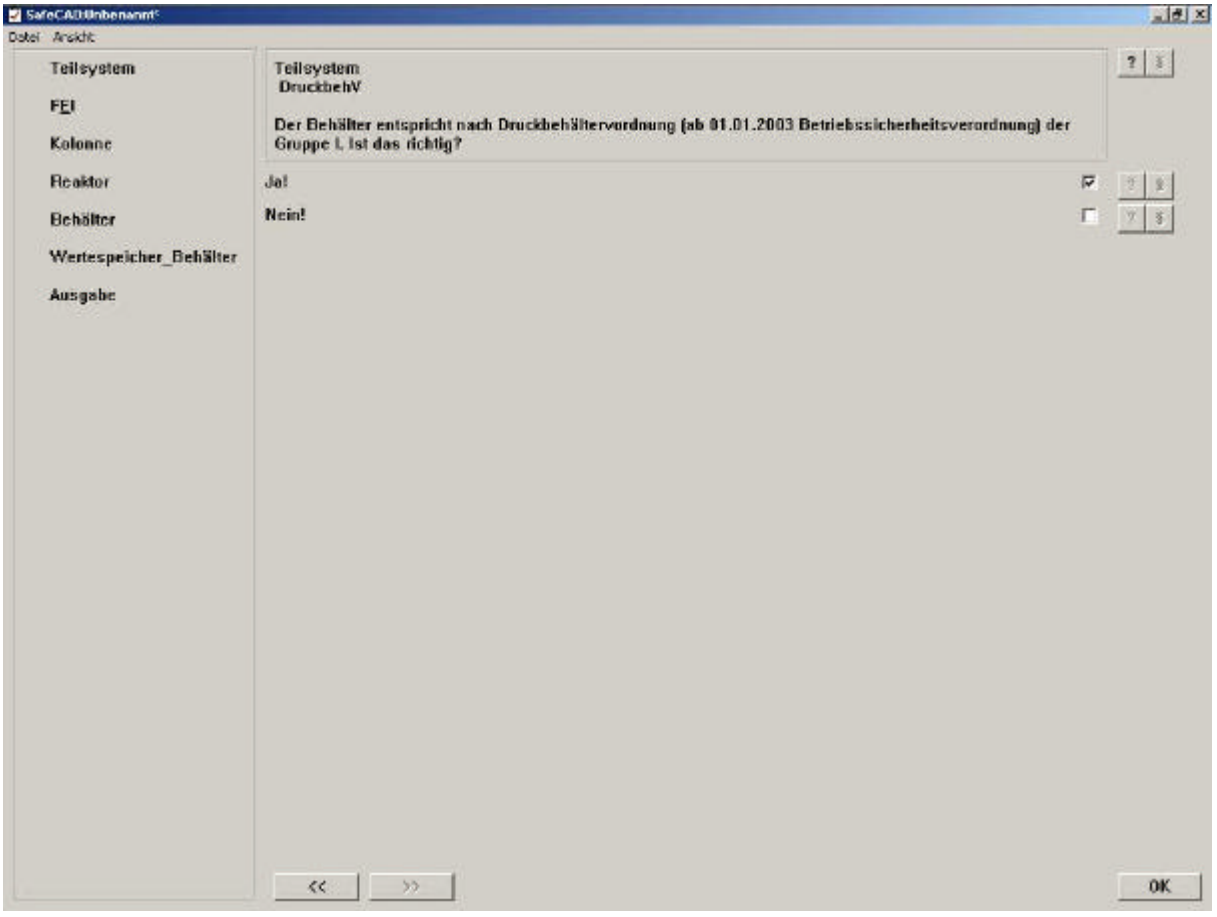
A.2 Prepolymeranlage

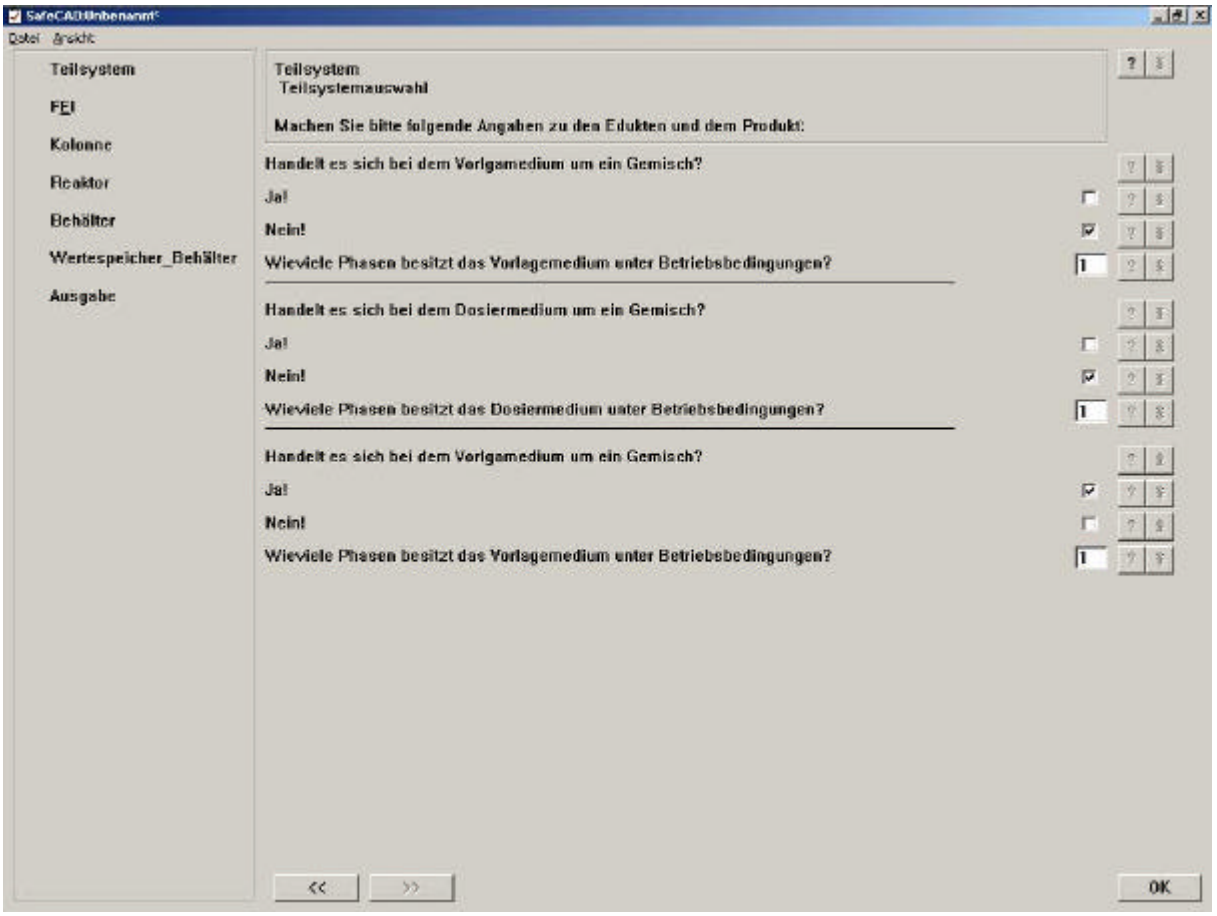


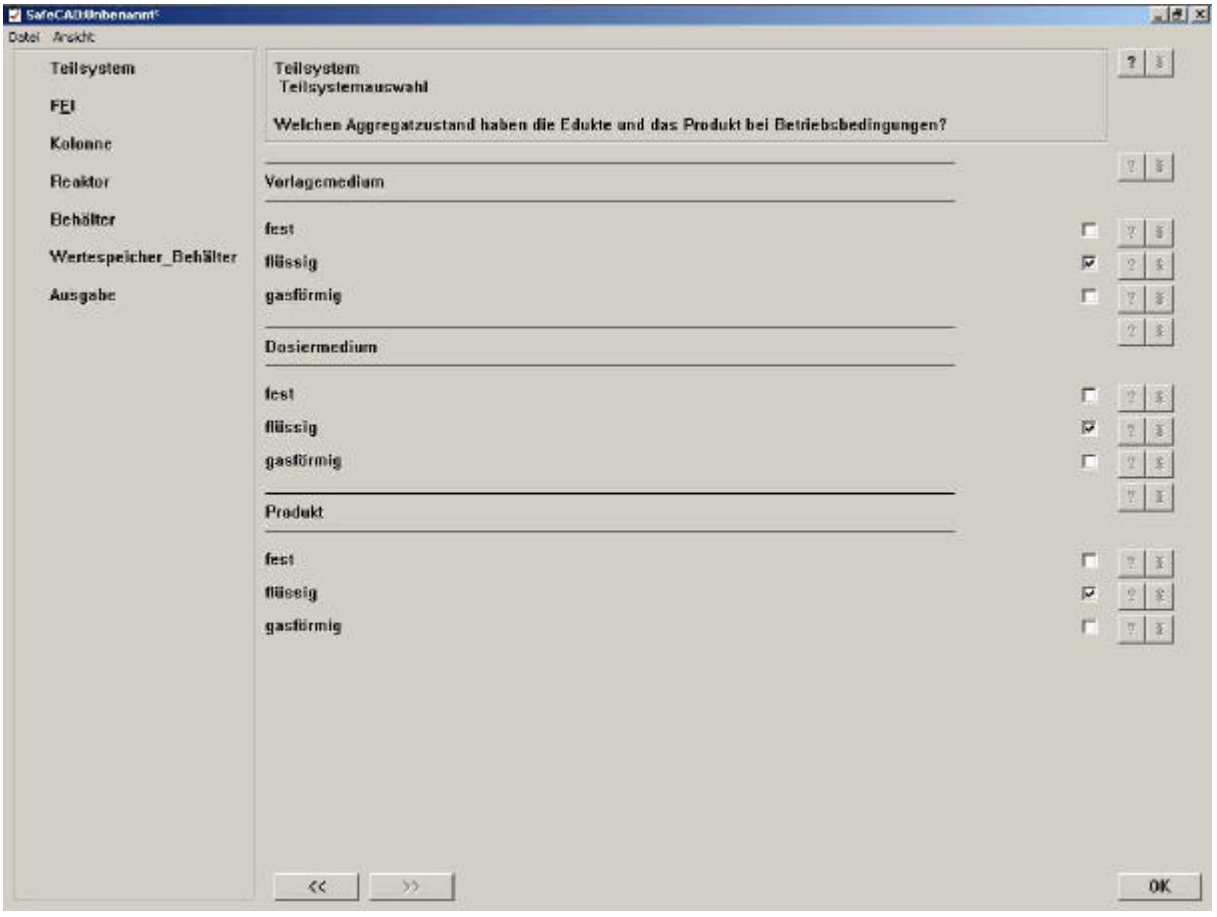

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Was für ein Reaktortyp soll bearbeitet werden?
Rührkesselreaktor, kontinuierlich
Rührkesselreaktor, diskontinuierlich (semi-batch)
<<
>>
OK

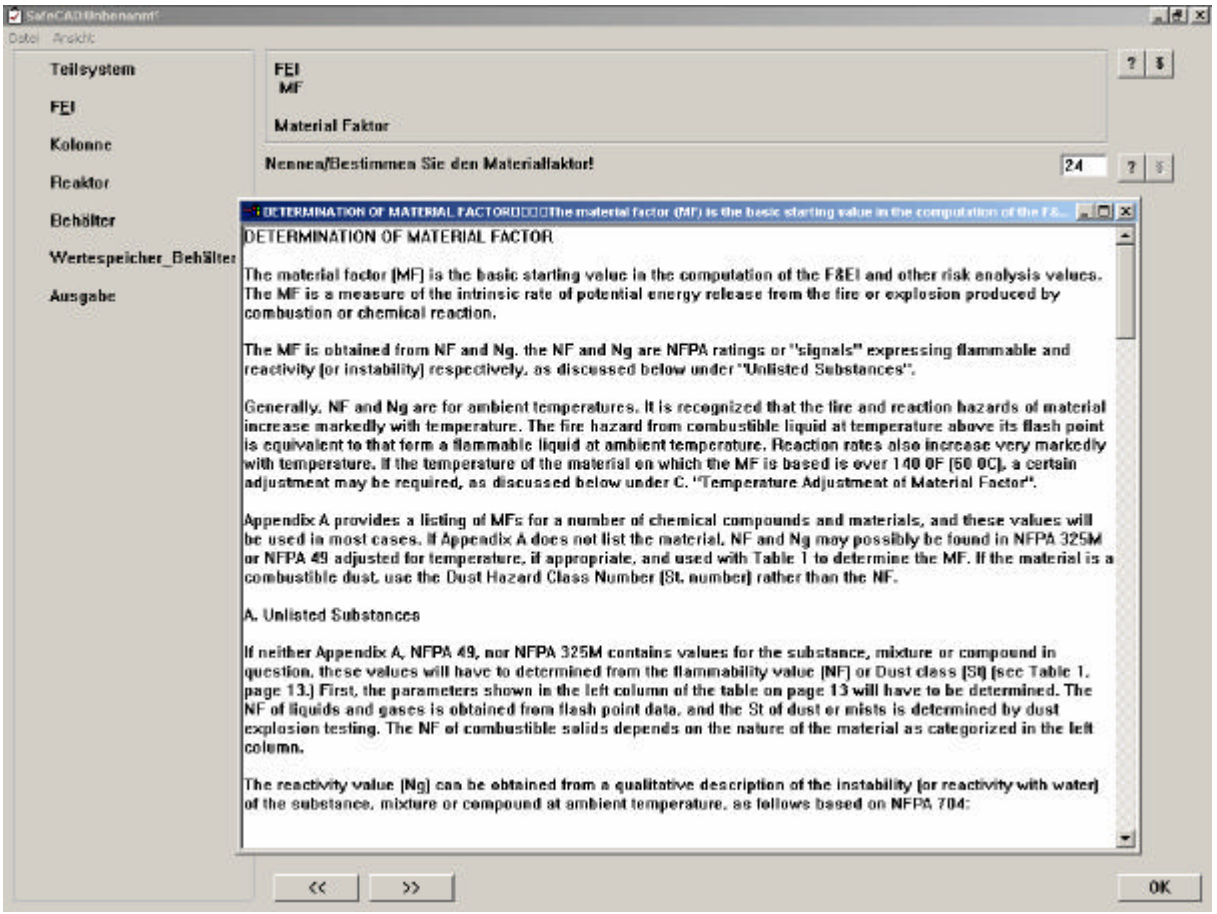

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Geben Sie die folgenden Daten für den Behälter an:
Volumen des Behälters [in m3]
4
Maximale Füllmenge [in Liter]
3200
Vorlagemedium
Isocyanat
Dosiermedium
Polyol
Produkt:
Prepolymer
<<
>>
OK

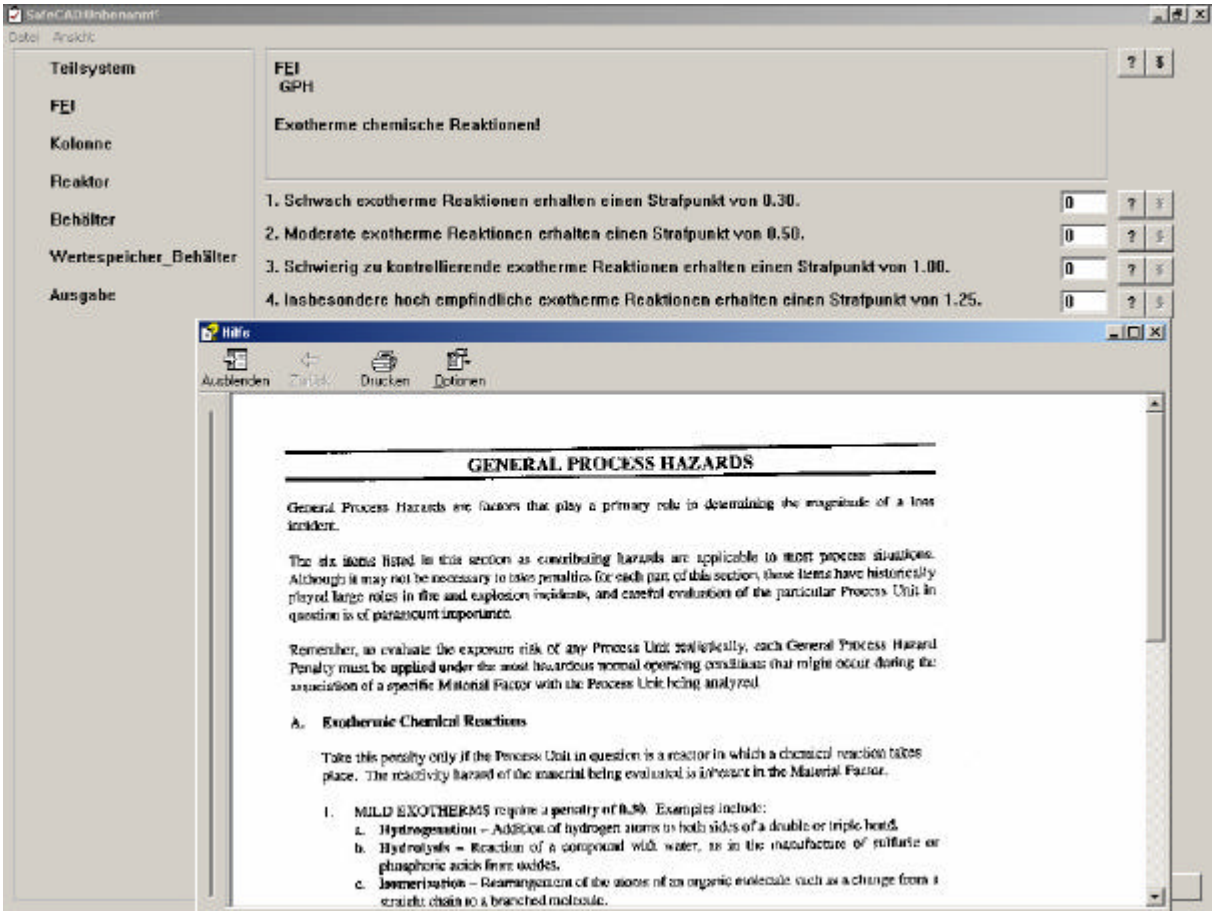

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Geben Sie bitte die Betriebsbedingungen für Temperatur und Druck an:
Betriebsdruck [in bar] 1
Maximal zulässiger Druck des Behälters [in bar] 10
Maximal möglicher Druck der Reaktion [in bar] 5
Starttemperatur der Reaktion (wenn vorhanden) [in °C] 50
Maximal zulässige Temperatur des Behälters [in °C] 200
Reaktionstemperatur (wenn vorhanden) [in °C] 90
Maximal mögliche Reaktionstemperatur (wenn vorhanden) [in °C] 160
<<
>>
OK

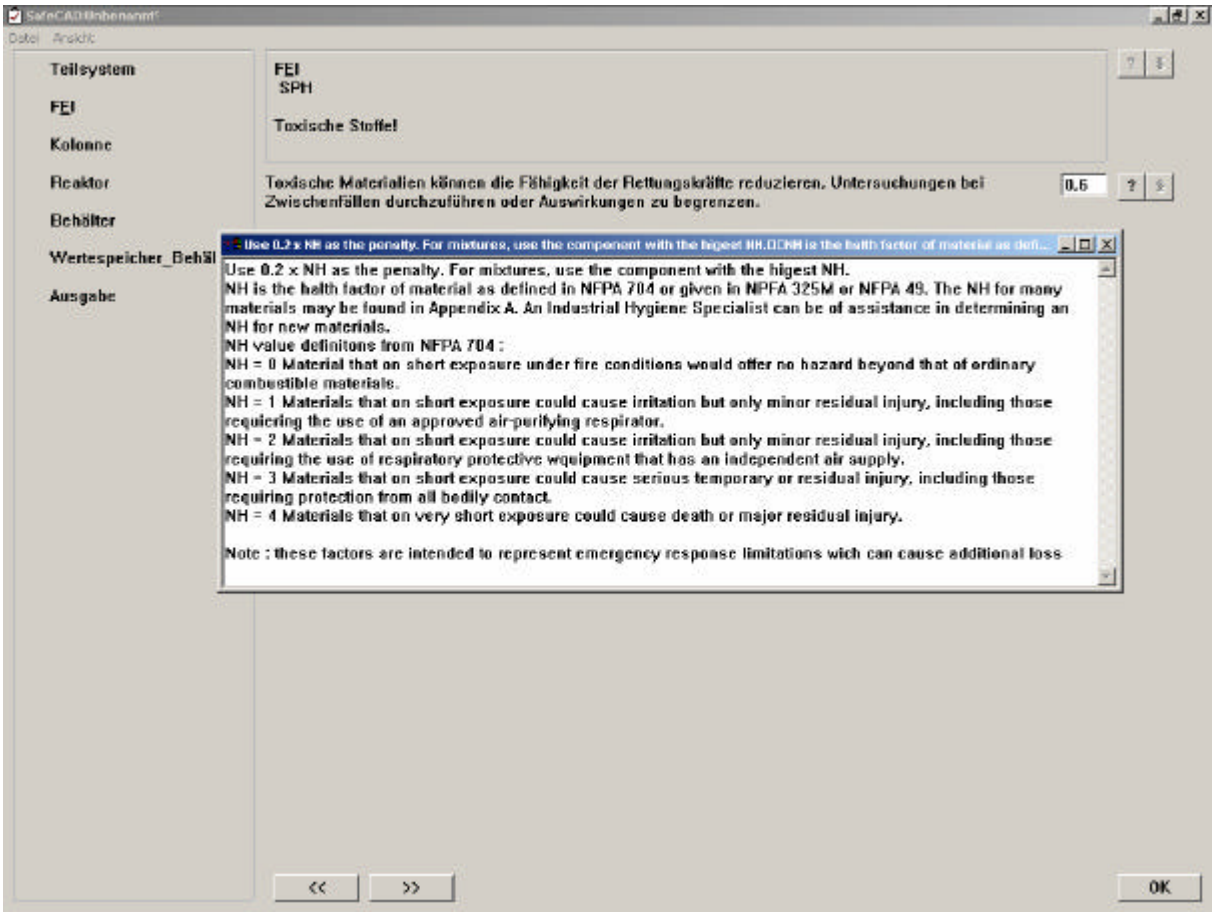

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
DruckbehV
Der Behälter entspricht nach Druckbehältervordnung (ab 01.01.2003 Betriebssicherheitsverordnung) der Gruppe I. Ist das richtig?
Ja!
Nein!
<<
>>
OK

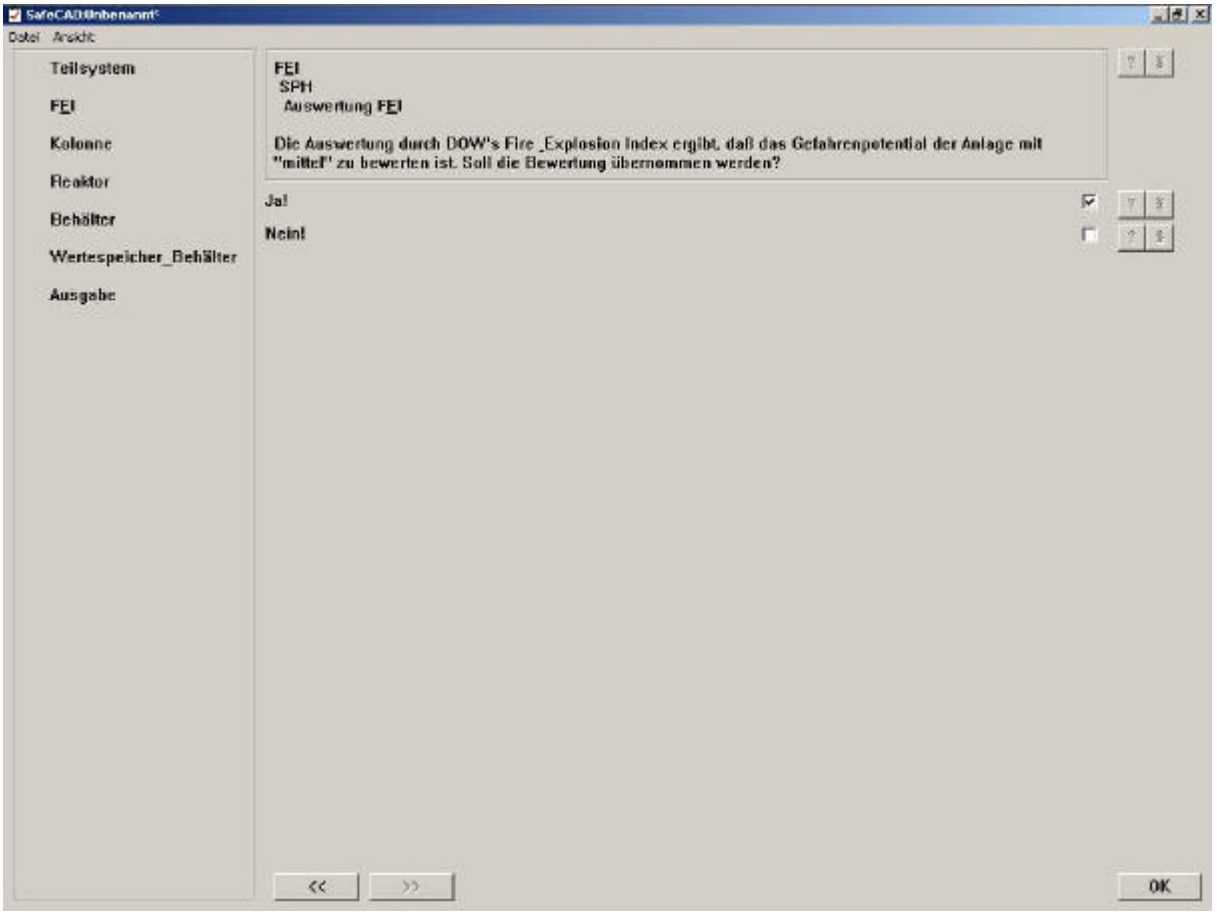

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Machen Sie bitte folgende Angaben zu den Edukten und dem Produkt:
Handelt es sich bei dem Vorlagemedium um ein Gemisch?
Ja!
Nein!
Wieviele Phasen besitzt das Vorlagemedium unter Betriebsbedingungen?
1
Handelt es sich bei dem Dosiermedium um ein Gemisch?
Ja!
Nein!
Wieviele Phasen besitzt das Dosiermedium unter Betriebsbedingungen?
1
Handelt es sich bei dem Vorlagemedium um ein Gemisch?
Ja!
Nein!
Wieviele Phasen besitzt das Vorlagemedium unter Betriebsbedingungen?
1
<<
>>
OK

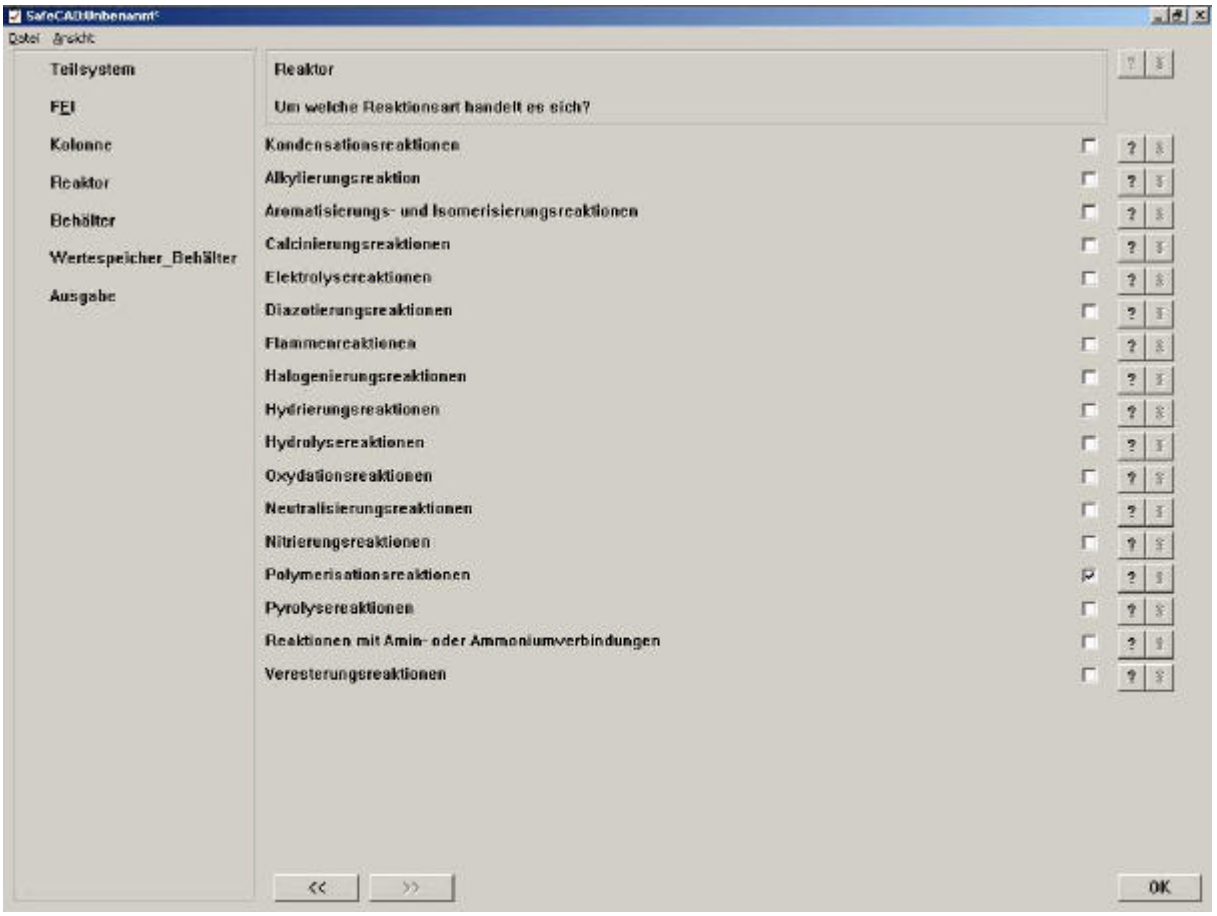

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Teilsystem
Teilsystemauswahl
Welchen Aggregatzustand haben die Edukte und das Produkt bei Betriebsbedingungen?
Vorlagemedium
fest
flüssig
gasförmig
Dosiermedium
fest
flüssig
gasförmig
Produkt
fest
flüssig
gasförmig
<<
>>
OK

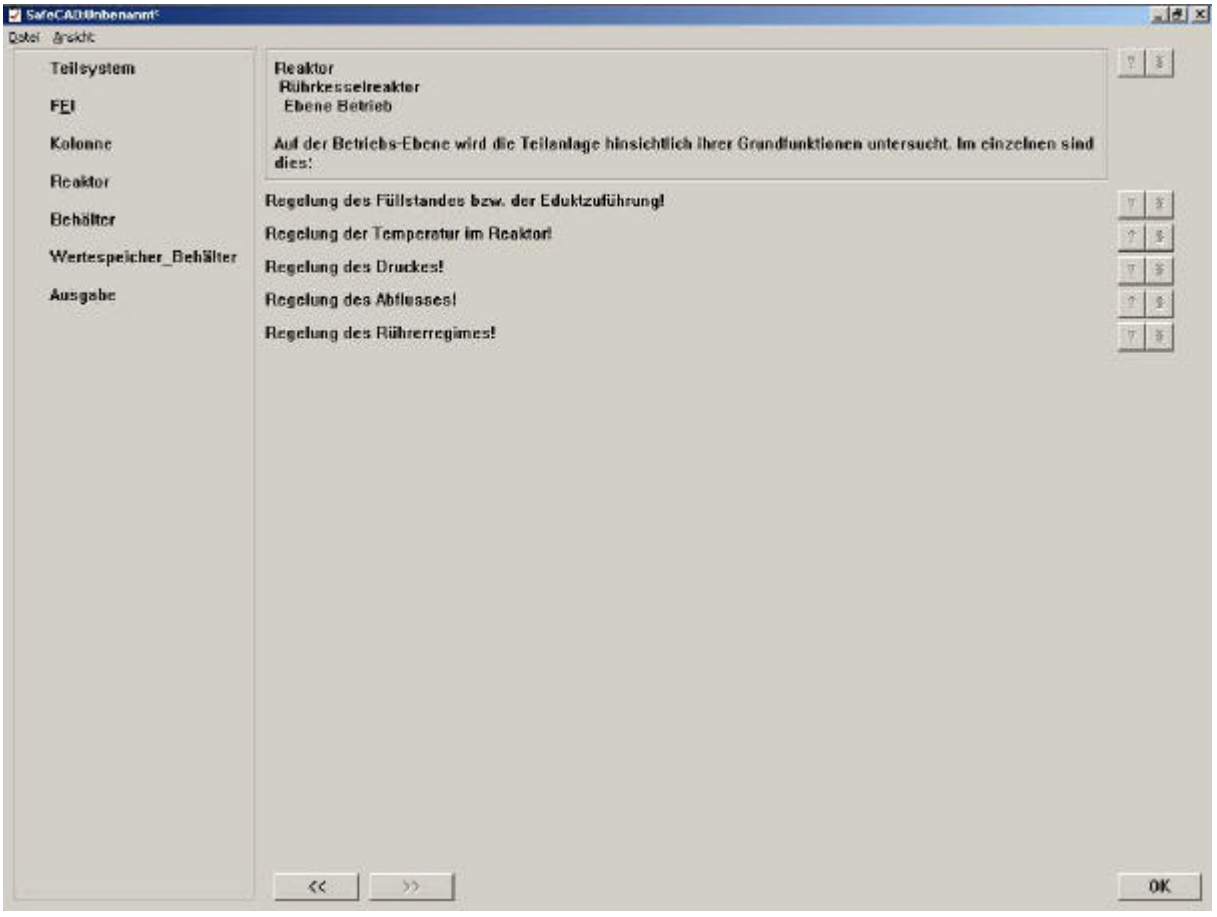

SafeCAD\Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
FEI
MF
Material Faktor
Nennen/Bestimmen Sie den Materialfaktor!
24
DETERMINATION OF MATERIAL FACTOR
The material factor (MF) is the basic starting value in the computation of the F&EI and other risk analysis values. The MF is a measure of the intrinsic rate of potential energy release from the fire or explosion produced by combustion or chemical reaction.
The MF is obtained from NF and Ng, the NF and Ng are NFPA ratings or "signals" expressing flammable and reactivity (or instability) respectively, as discussed below under "Unlisted Substances".
Generally, NF and Ng are for ambient temperatures. It is recognized that the fire and reaction hazards of material increase markedly with temperature. The fire hazard from combustible liquid at temperature above its flash point is equivalent to that form a flammable liquid at ambient temperature. Reaction rates also increase very markedly with temperature. If the temperature of the material on which the MF is based is over 140 0F (60 0C), a certain adjustment may be required, as discussed below under C. "Temperature Adjustment of Material Factor".
Appendix A provides a listing of MFs for a number of chemical compounds and materials, and these values will be used in most cases. If Appendix A does not list the material, NF and Ng may possibly be found in NFPA 325M or NFPA 49 adjusted for temperature, if appropriate, and used with Table 1 to determine the MF. If the material is a combustible dust, use the Dust Hazard Class Number (St. number) rather than the NF.
A. Unlisted Substances
If neither Appendix A, NFPA 49, nor NFPA 325M contains values for the substance, mixture or compound in question, these values will have to determined from the flammability value (NF) or Dust class (St) (see Table 1, page 13.) First, the parameters shown in the left column of the table on page 13 will have to be determined. The NF of liquids and gases is obtained from flash point data, and the St of dust or mists is determined by dust explosion testing. The NF of combustible solids depends on the nature of the material as categorized in the left column.
The reactivity value (Ng) can be obtained from a qualitative description of the instability (or reactivity with water) of the substance, mixture or compound at ambient temperature, as follows based on NFPA 704:
<<
>>
OK

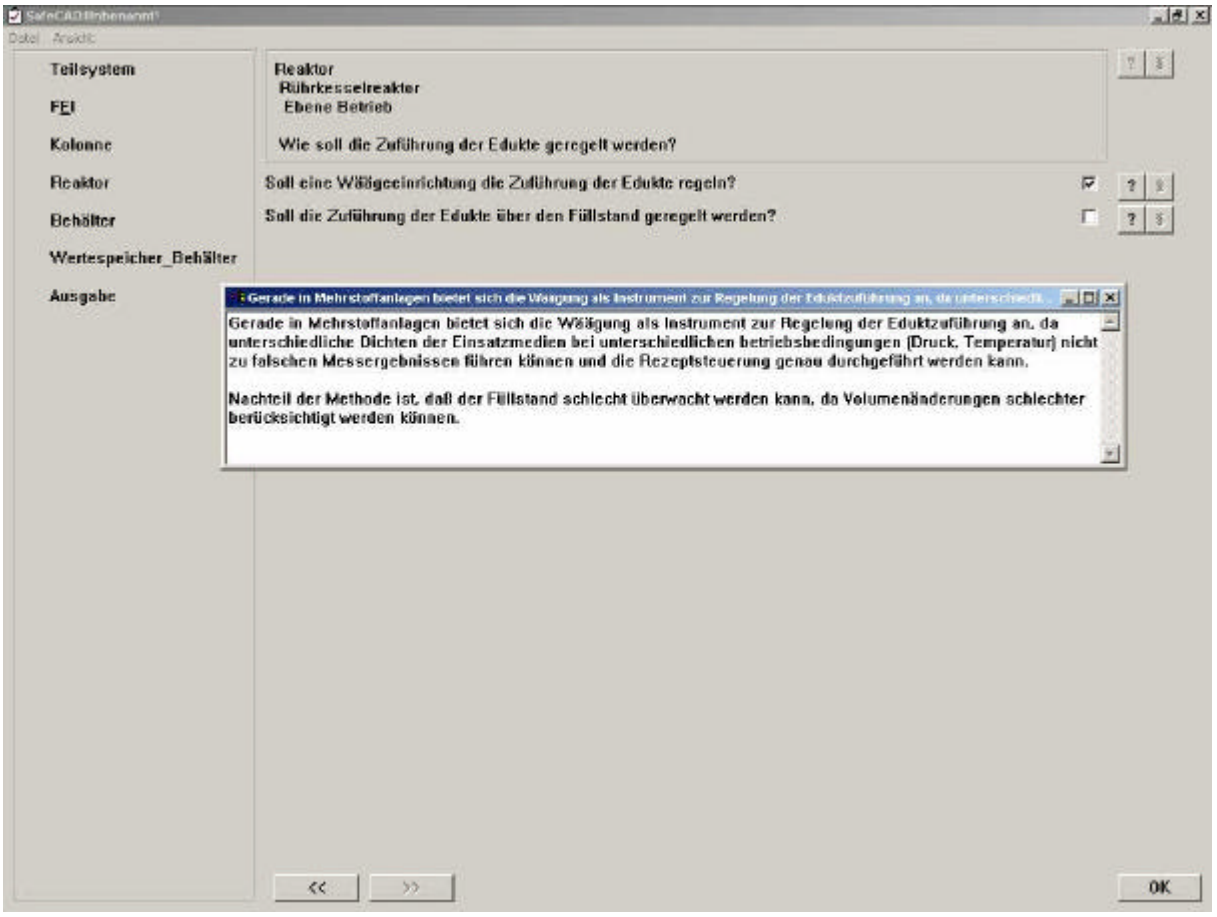

SafeCAD\Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
FEI
GPH
Exotherme chemische Reaktionen!
1. Schwach exotherme Reaktionen erhalten einen Strafpunkt von 0.30.
2. Moderate exotherme Reaktionen erhalten einen Strafpunkt von 0.50.
3. Schwierig zu kontrollierende exotherme Reaktionen erhalten einen Strafpunkt von 1.00.
4. Insbesondere hoch empfindliche exotherme Reaktionen erhalten einen Strafpunkt von 1.25.
Hilfe
Ausblenden
Zurück
Drucken
Optionen
GENERAL PROCESS HAZARDS
General Process Hazards are factors that play a primary role in determining the magnitude of a loss incident.
The six items listed in this section as contributing hazards are applicable to most process situations. Although it may not be necessary to take penalties for each part of this section, these items have historically played large roles in fire and explosion incidents, and careful evaluation of the particular Process Unit in question is of paramount importance.
Remember, to evaluate the exposure risk of any Process Unit realistically, each General Process Hazard Penalty must be applied under the most hazardous normal operating conditions that might occur during the association of a specific Material Factor with the Process Unit being analyzed.
A. Exothermic Chemical Reactions
Take this penalty only if the Process Unit in question is a reactor in which a chemical reaction takes place. The reactivity hazard of the material being evaluated is inherent in the Material Factor.
1. MILD EXOTHERMS require a penalty of 0.30. Examples include:
a. Hydrogenation – Addition of hydrogen atoms to both sides of a double or triple bond.
b. Hydrolysis – Reaction of a compound with water, as in the manufacture of sulfuric or phosphoric acids from oxides.
c. Isomerization – Rearrangement of the atoms of an organic molecule such as a change from a straight chain to a branched molecule.

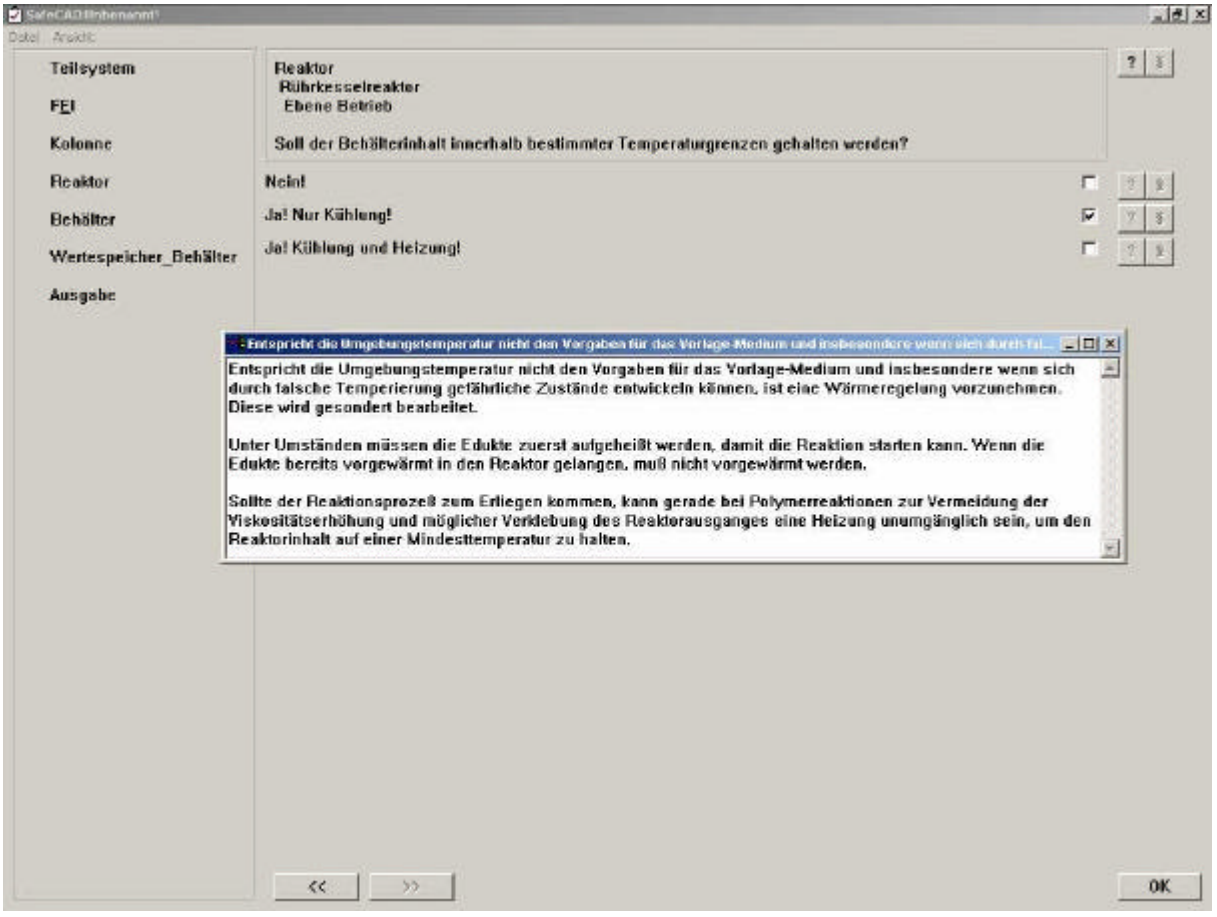

Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behäl
Ausgabe
FEI
SPH
Toxische Stoffe!
Toxische Materialien können die Fähigkeit der Rettungskräfte reduzieren. Untersuchungen bei Zwischenfällen durchzuführen oder Auswirkungen zu begrenzen.
0.6
Use 0.2 x NH as the penalty. For mixtures, use the component with the higest NH.
NH is the halth factor of material as defined in NFPA 704 or given in NFPA 325M or NFPA 49. The NH for many materials may be found in Appendix A. An Industrial Hygiene Specialist can be of assistance in determining an NH for new materials.
NH value definitons from NFPA 704 :
NH = 0 Material that on short exposure under fire conditions would offer no hazard beyond that of ordinary combustible materials.
NH = 1 Materials that on short exposure could cause irritation but only minor residual injury, including those requiring the use of an approved air-purifying respirator.
NH = 2 Materials that on short exposure could cause irritation but only minor residual injury, including those requiring the use of respiratory protective wqeipment that has an independent air supply.
NH = 3 Materials that on short exposure could cause serious temporary or residual injury, including those requiring protection from all bedily contact.
NH = 4 Materials that on very short exposure could cause death or major residual injury.
Note : these factors are intended to represent emergency response limitations wich can cause additional loss
<<
>>
OK

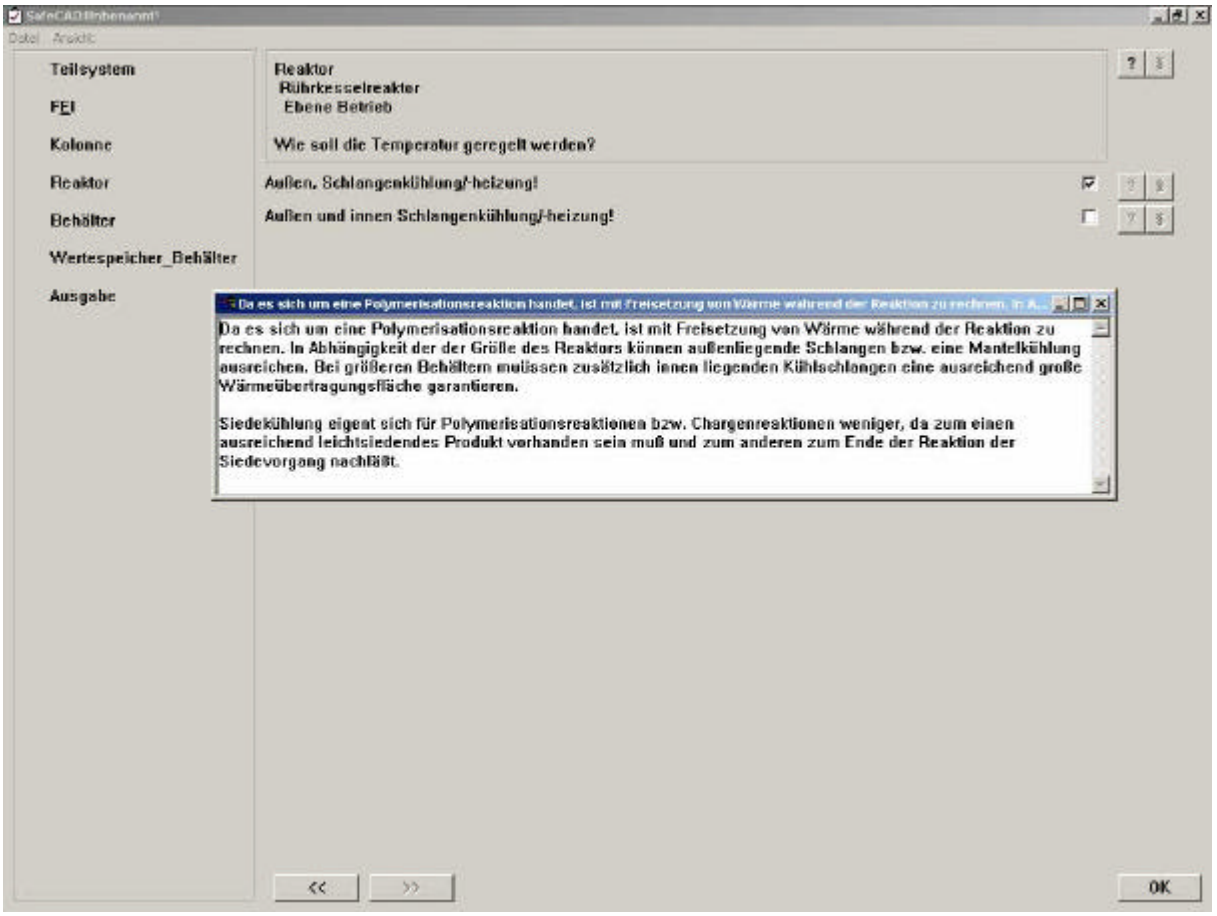

Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
FEI
SPH
Auswertung FEI
Die Auswertung durch DOW's Fire _Explosion Index ergibt, daß das Gefahrenpotential der Anlage mit "mittel" zu bewerten ist. Soll die Bewertung übernommen werden?
Ja!
Nein!
<<
>>
OK

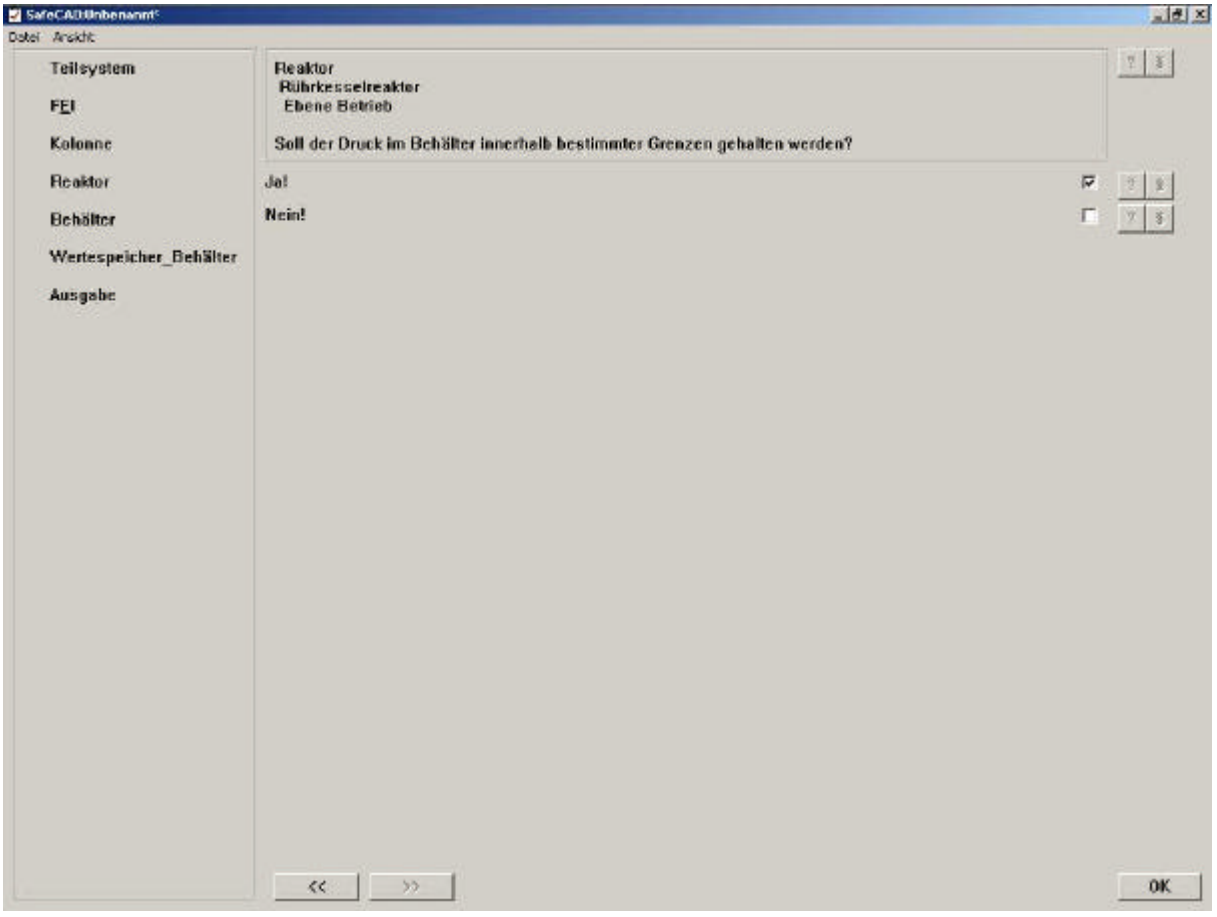

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Um welche Reaktionsart handelt es sich?
Kondensationsreaktionen
Alkylierungsreaktion
Aromatisierungs- und Isomerisierungsreaktionen
Calcinierungsreaktionen
Elektrolysereaktionen
Diazotierungsreaktionen
Flammenreaktionen
Halogenierungsreaktionen
Hydrierungsreaktionen
Hydrolysereaktionen
Oxydationsreaktionen
Neutralisierungsreaktionen
Nitrierungsreaktionen
Polymerisationsreaktionen
Pyrolysereaktionen
Reaktionen mit Amin- oder Ammoniumverbindungen
Veresterungsreaktionen
<<
>>
OK

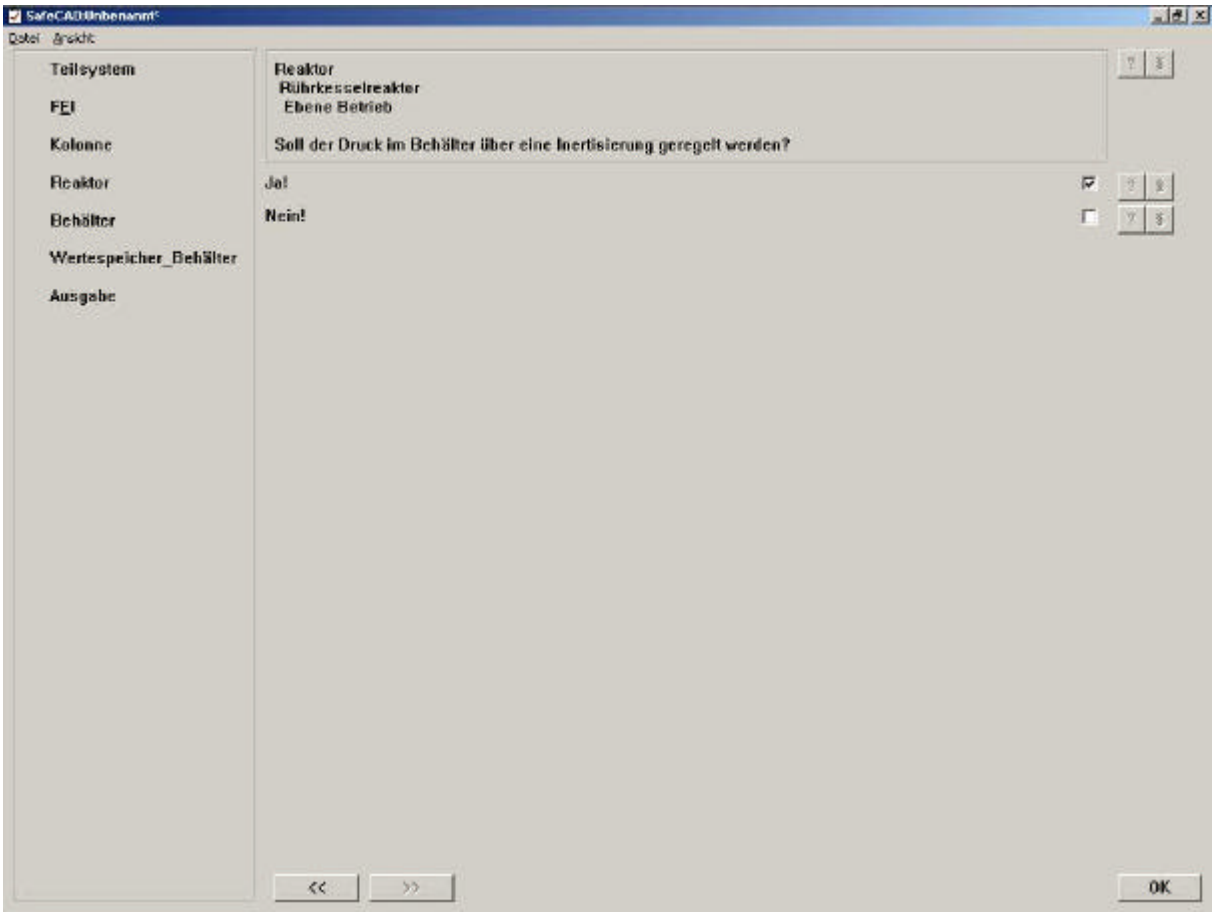

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Auf der Betriebs-Ebene wird die Teilanlage hinsichtlich ihrer Grundfunktionen untersucht. Im einzelnen sind dies:
Regelung des Füllstandes bzw. der Eduktzuführung!
Regelung der Temperatur im Reaktor!
Regelung des Druckes!
Regelung des Abflusses!
Regelung des Rührerregimes!
<<
>>
OK

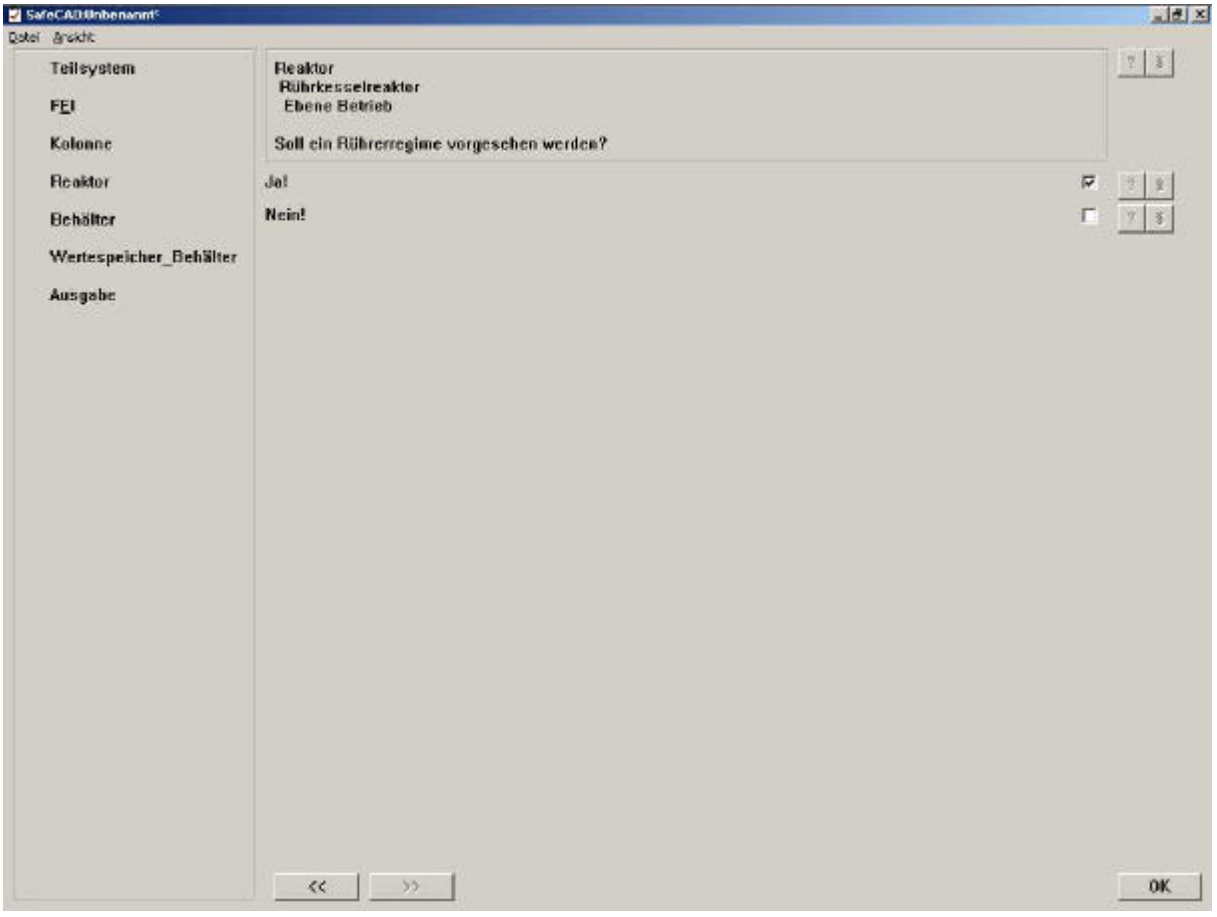

Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Wie soll die Zuführung der Edukte geregelt werden?
Soll eine Wägeeinrichtung die Zuführung der Edukte regeln?
Soll die Zuführung der Edukte über den Füllstand geregelt werden?
Gerade in Mehrstoffanlagen bietet sich die Wägung als Instrument zur Regelung der Eduktzuführung an, da unterschiedliche Dichten der Einsatzmedien bei unterschiedlichen betriebsbedingungen (Druck, Temperatur) nicht zu falschen Messergebnissen führen können und die Rezeptsteuerung genau durchgefährt werden kann.
Nachteil der Methode ist, daß der Füllstand schlecht überwocht werden kann, da Volumenänderungen schlechter berücksichtigt werden können.
<<
>>
OK

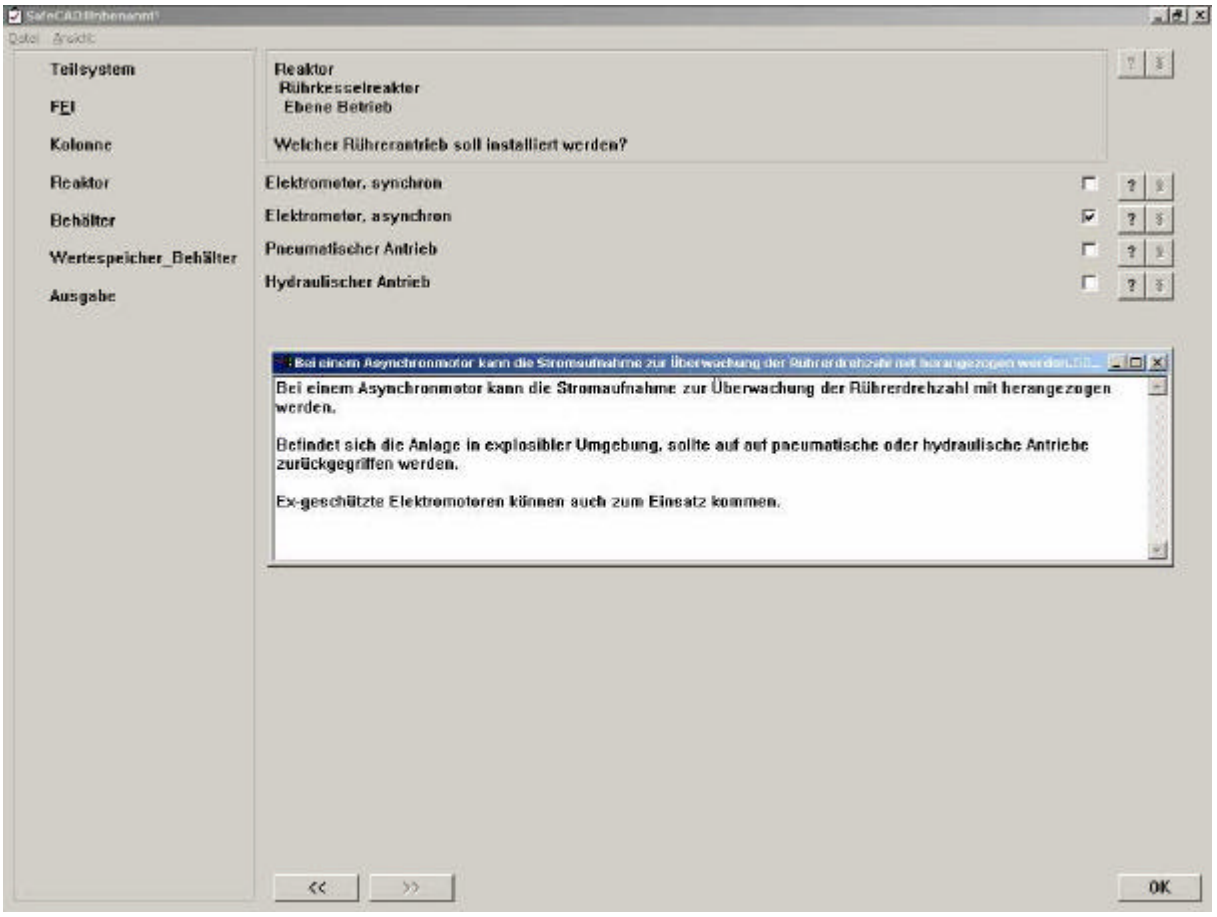

Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Soll der Behälterinhalt innerhalb bestimmter Temperaturgrenzen gehalten werden?
Nein!
Ja! Nur Kühlung!
Ja! Kühlung und Heizung!
Entspricht die Umgebungstemperatur nicht den Vorgaben für das Vorlage-Medium und insbesondere wenn sich durch falsche Temperierung gefährliche Zustände entwickeln können, ist eine Wärmeregelung vorzunehmen. Diese wird gesondert bearbeitet.
Unter Umständen müssen die Edukte zuerst aufgeheißt werden, damit die Reaktion starten kann. Wenn die Edukte bereits vorgewärmt in den Reaktor gelangen, muß nicht vorgewärmt werden.
Sollte der Reaktionsprozeß zum Erliegen kommen, kann gerade bei Polymerreaktionen zur Vermeidung der Viskositätserhöhung und möglicher Verklebung des Reaktorausganges eine Heizung unumgänglich sein, um den Reaktorinhalt auf einer Mindesttemperatur zu halten.
<<
>>
OK

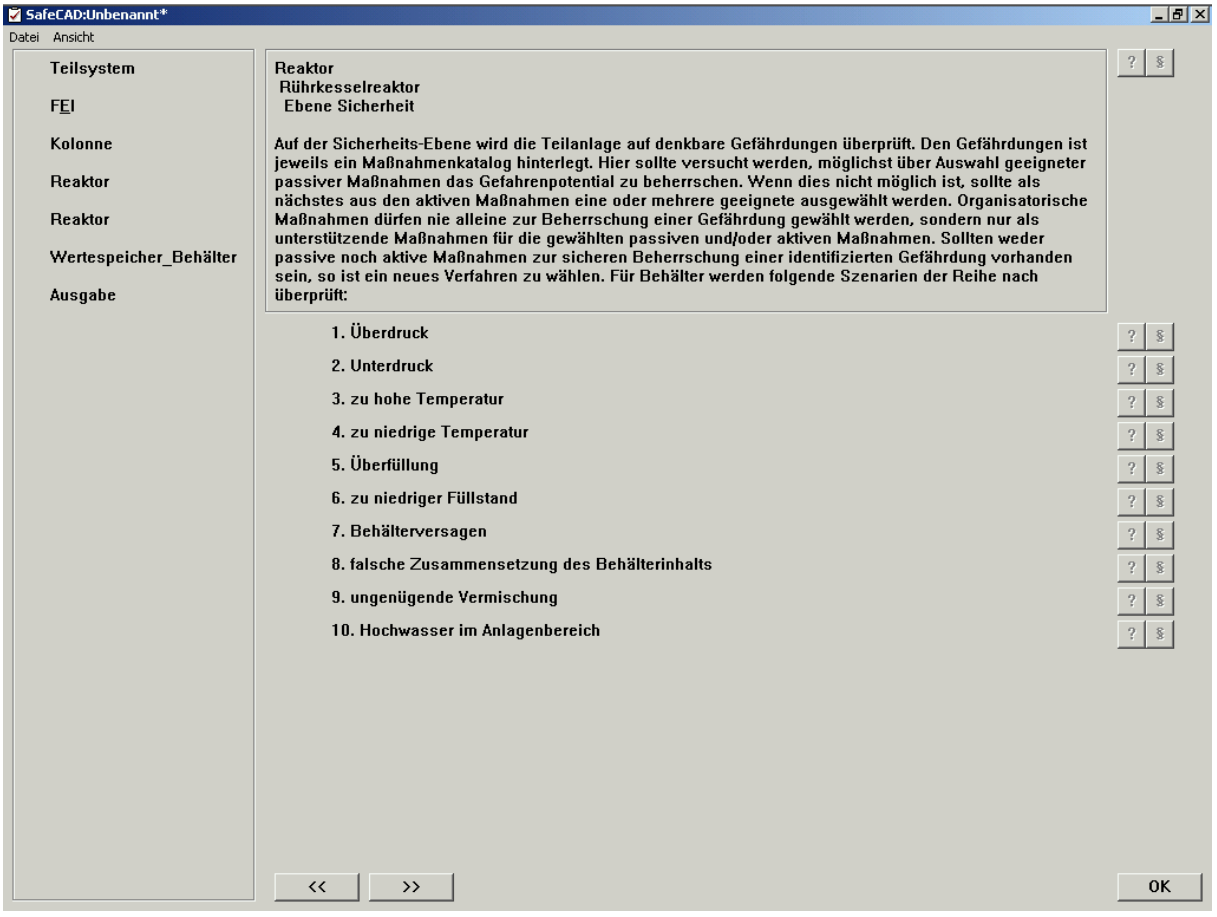

Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Wie soll die Temperatur geregelt werden?
Außen, Schlangenkühlung/-heizung!
Außen und innen Schlangenkühlung/-heizung!
Da es sich um eine Polymerisationsreaktion handelt, ist mit Freisetzung von Wärme während der Reaktion zu rechnen. In Abhängigkeit der der Größe des Reaktors können außenliegende Schlangen bzw. eine Mantelkühlung ausreichen. Bei größeren Behältern müssen zusätzlich innen liegenden Kühlschlangen eine ausreichend große Wärmeübertragungsfläche garantieren.
Siedekühlung eigent sich für Polymerisationsreaktionen bzw. Chargenreaktionen weniger, da zum einen ausreichend leichtsiedendes Produkt vorhanden sein muß und zum anderen zum Ende der Reaktion der Siedevorgang nachläßt.
<<
>>
OK

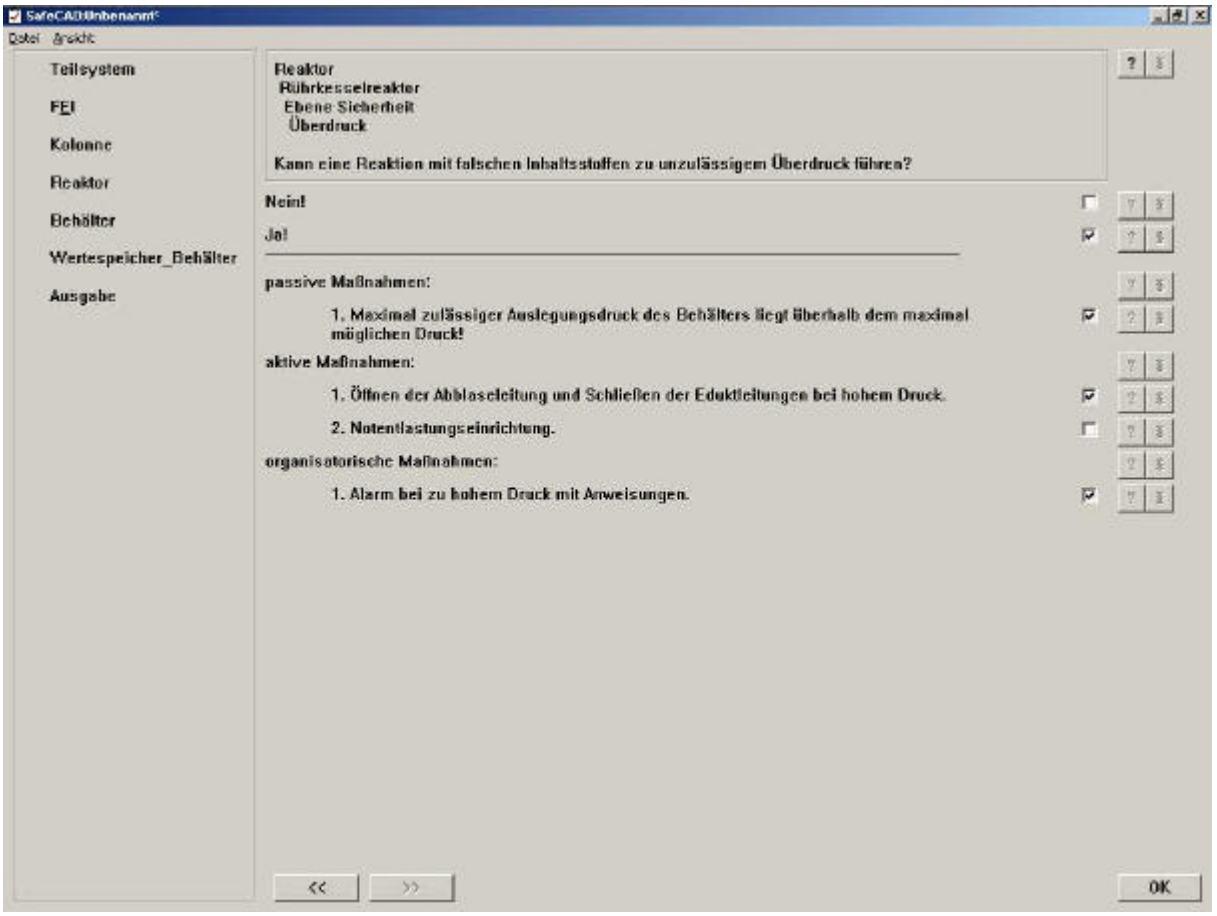

Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Soll der Druck im Behälter innerhalb bestimmter Grenzen gehalten werden?
Ja!
Nein!
<<
>>
OK

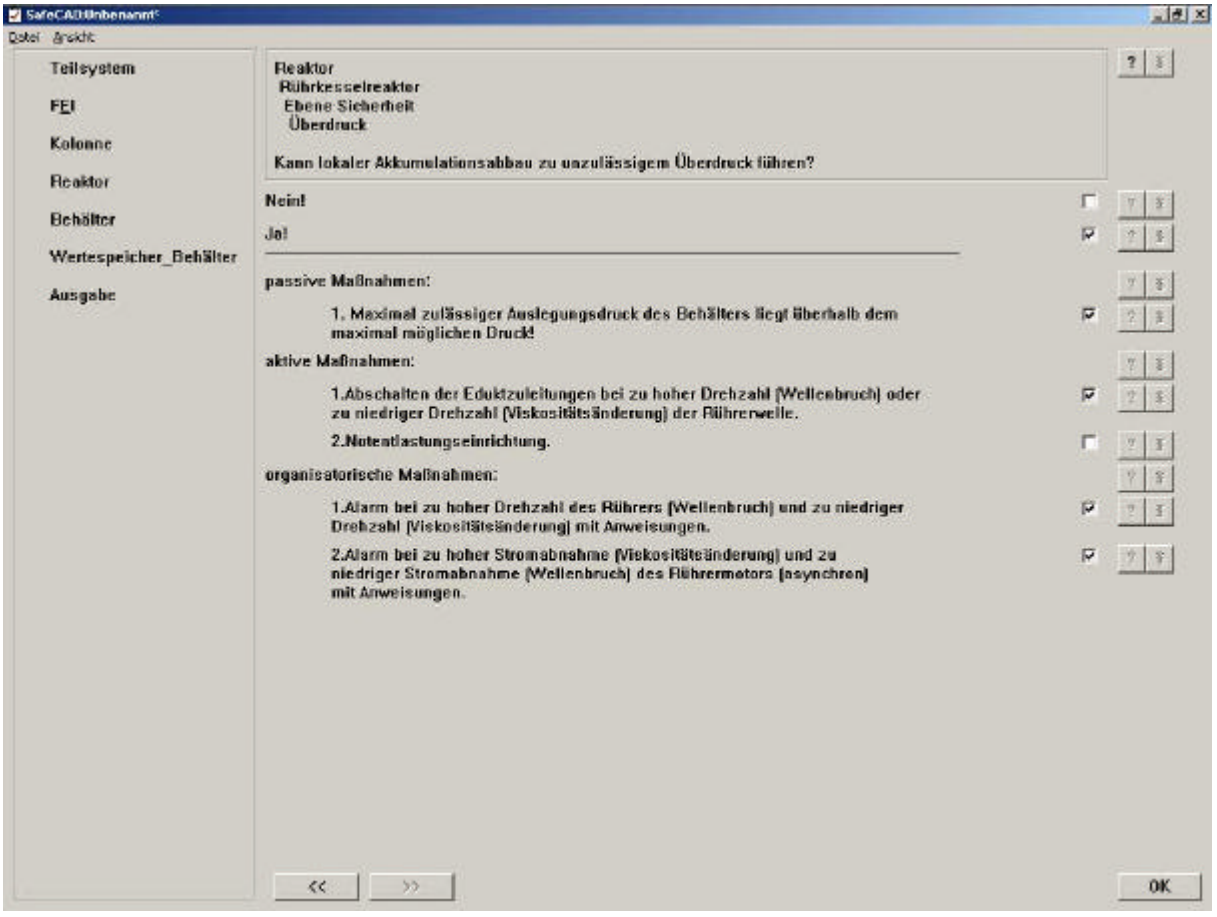

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Soll der Druck im Behälter über eine Inertisierung geregelt werden?
Ja!
Nein!
<<
>>
OK

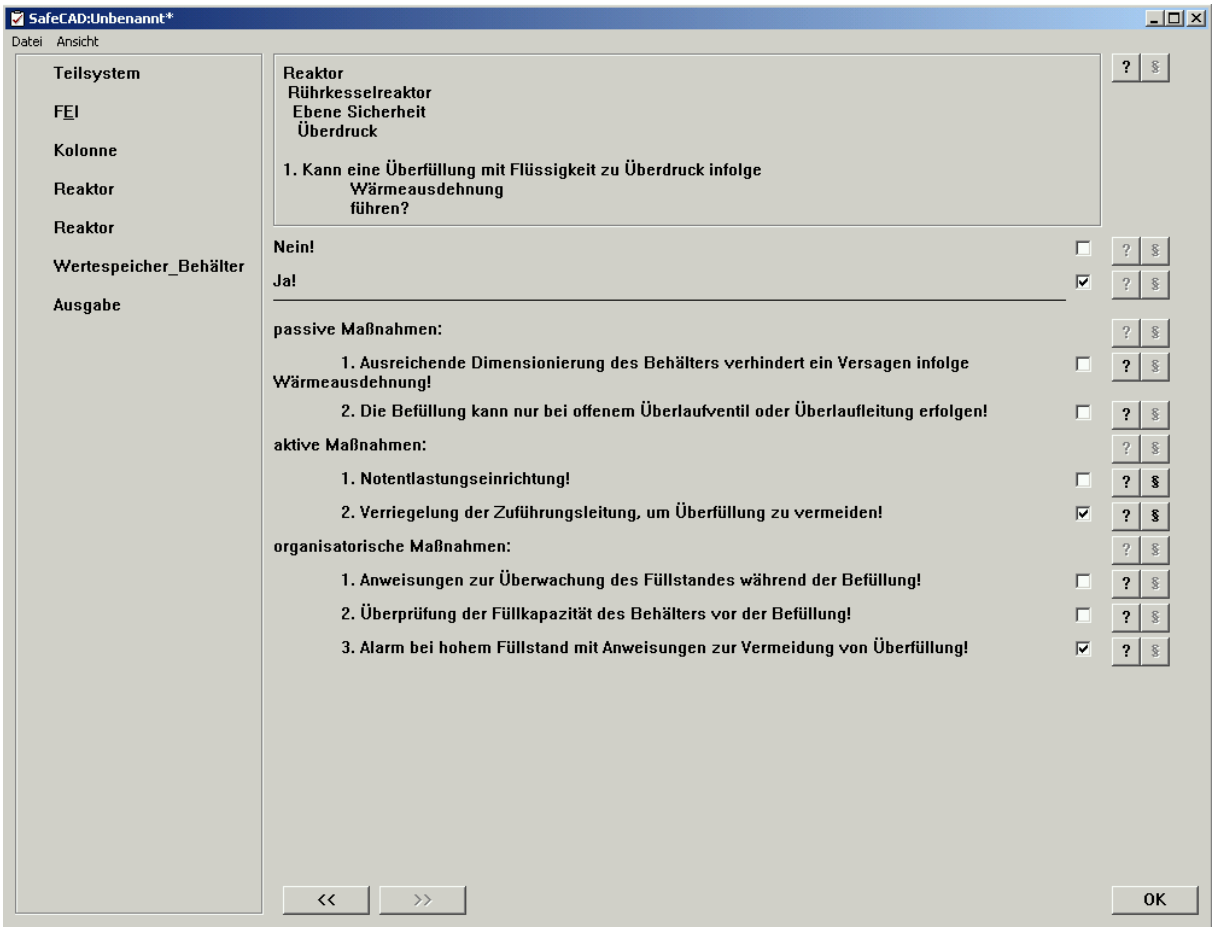

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Soll ein Rührerregime vorgesehen werden?
Ja!
Nein!
<<
>>
OK

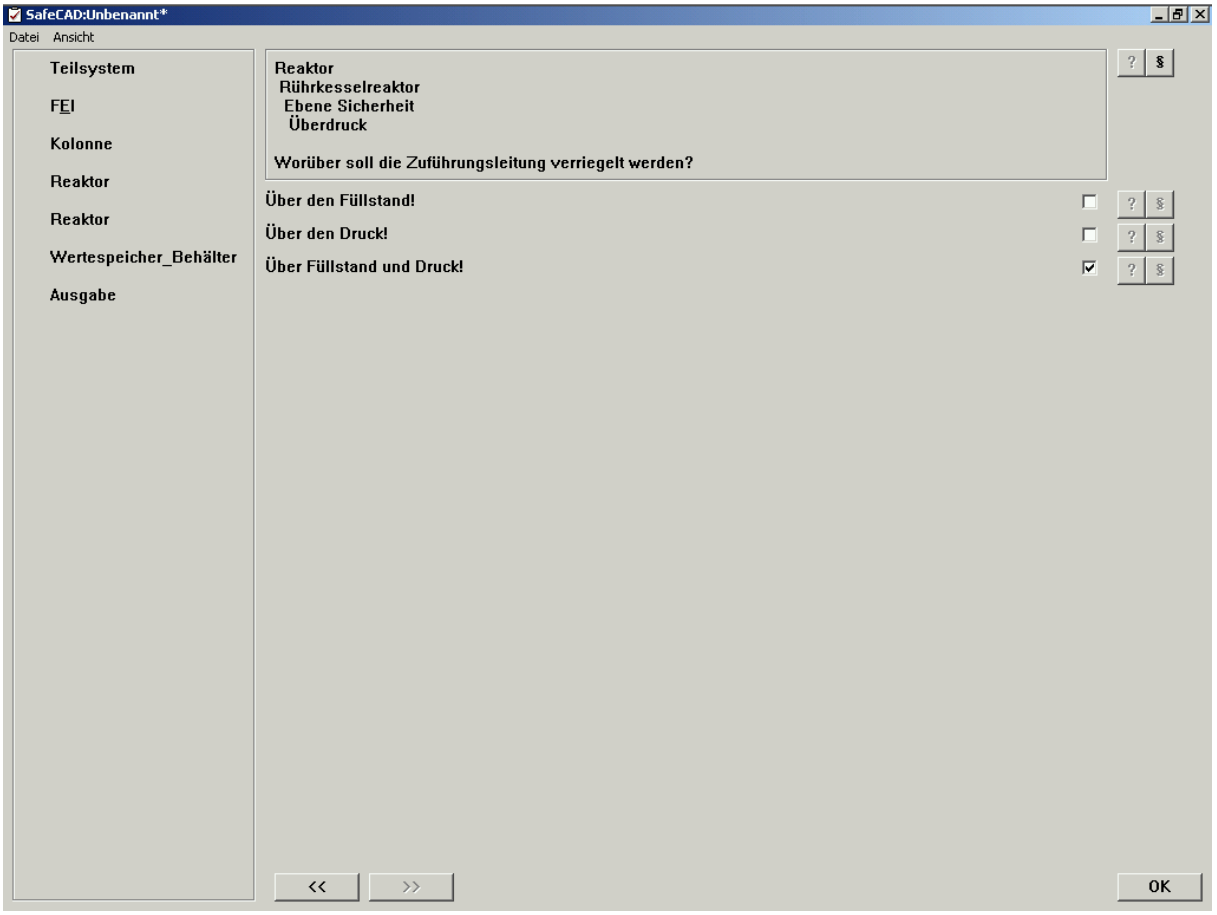

Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Betrieb
Welcher Rührerantrieb soll installiert werden?
Elektrometer, synchron
Elektrometer, asynchron
Pneumatischer Antrieb
Hydraulischer Antrieb
Bei einem Asynchronmotor kann die Stromaufnahme zur Überwachung der Rührerdrehzahl mit herangezogen werden.
Befindet sich die Anlage in explosibler Umgebung, sollte auf auf pneumatische oder hydraulische Antriebe zurückgegriffen werden.
Ex-geschützte Elektromotoren können auch zum Einsatz kommen.
<<
>>
OK

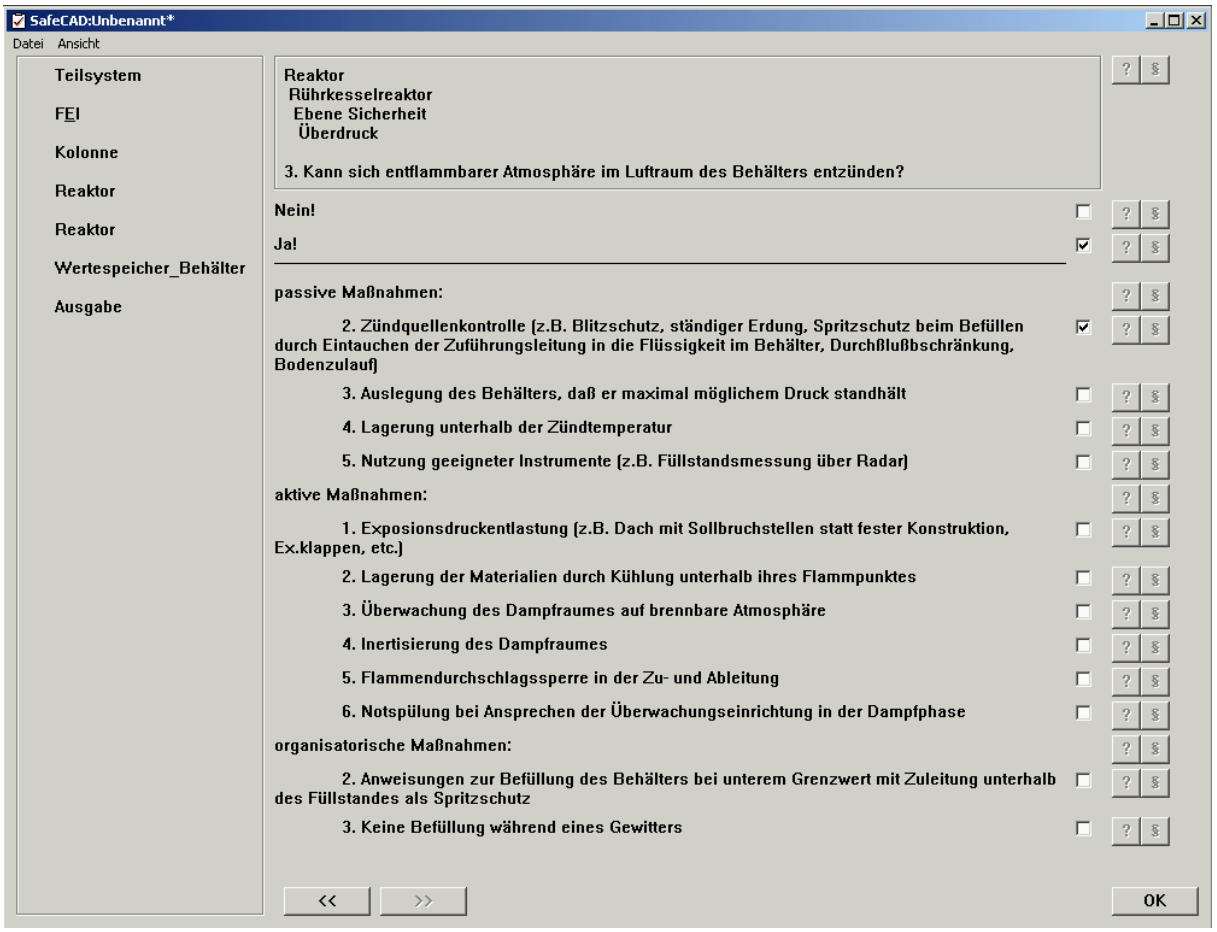

SafeCAD:Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Reaktor
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Sicherheit
Auf der Sicherheits-Ebene wird die Teilanlage auf denkbare Gefährdungen überprüft. Den Gefährdungen ist jeweils ein Maßnahmenkatalog hinterlegt. Hier sollte versucht werden, möglichst über Auswahl geeigneter passiver Maßnahmen das Gefahrenpotential zu beherrschen. Wenn dies nicht möglich ist, sollte als nächstes aus den aktiven Maßnahmen eine oder mehrere geeignete ausgewählt werden. Organisatorische Maßnahmen dürfen nie alleine zur Beherrschung einer Gefährdung gewählt werden, sondern nur als unterstützende Maßnahmen für die gewählten passiven und/oder aktiven Maßnahmen. Sollten weder passive noch aktive Maßnahmen zur sicheren Beherrschung einer identifizierten Gefährdung vorhanden sein, so ist ein neues Verfahren zu wählen. Für Behälter werden folgende Szenarien der Reihe nach überprüft:
1. Überdruck
2. Unterdruck
3. zu hohe Temperatur
4. zu niedrige Temperatur
5. Überfüllung
6. zu niedriger Füllstand
7. Behälterversagen
8. falsche Zusammensetzung des Behälterinhalts
9. ungenügende Vermischung
10. Hochwasser im Anlagenbereich
<<
>>
OK

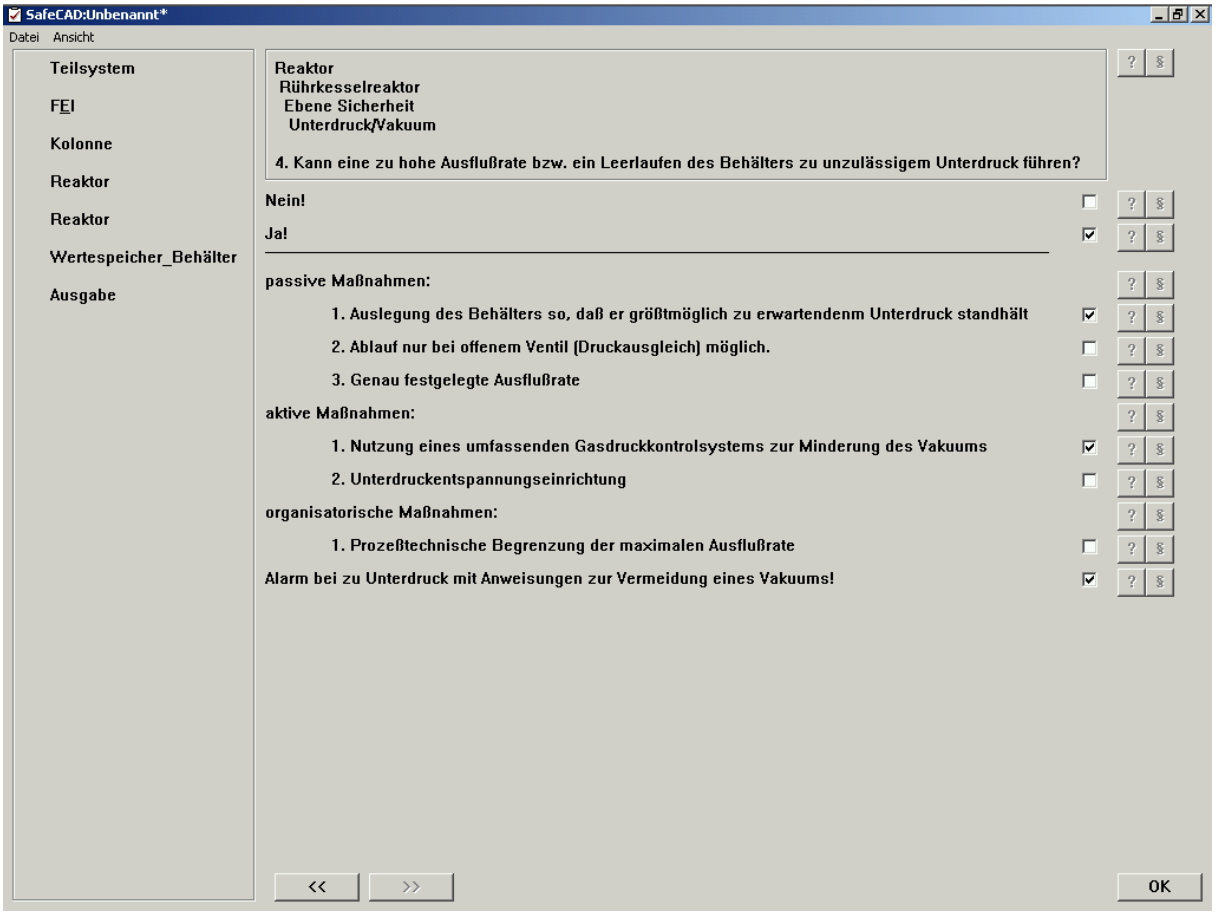

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Sicherheit
Überdruck
Kann eine Reaktion mit falschen Inhaltsstoffen zu unzulässigem Überdruck führen?
Nein!
Ja!
passive Maßnahmen:
1. Maximal zulässiger Auslegungsdruck des Behälters liegt überhalb dem maximal möglichen Druck!
aktive Maßnahmen:
1. Öffnen der Ablaseleitung und Schließen der Eduktleitungen bei hohem Druck.
2. Notentlastungseinrichtung.
organisatorische Maßnahmen:
1. Alarm bei zu hohem Druck mit Anweisungen.
<<
>>
OK

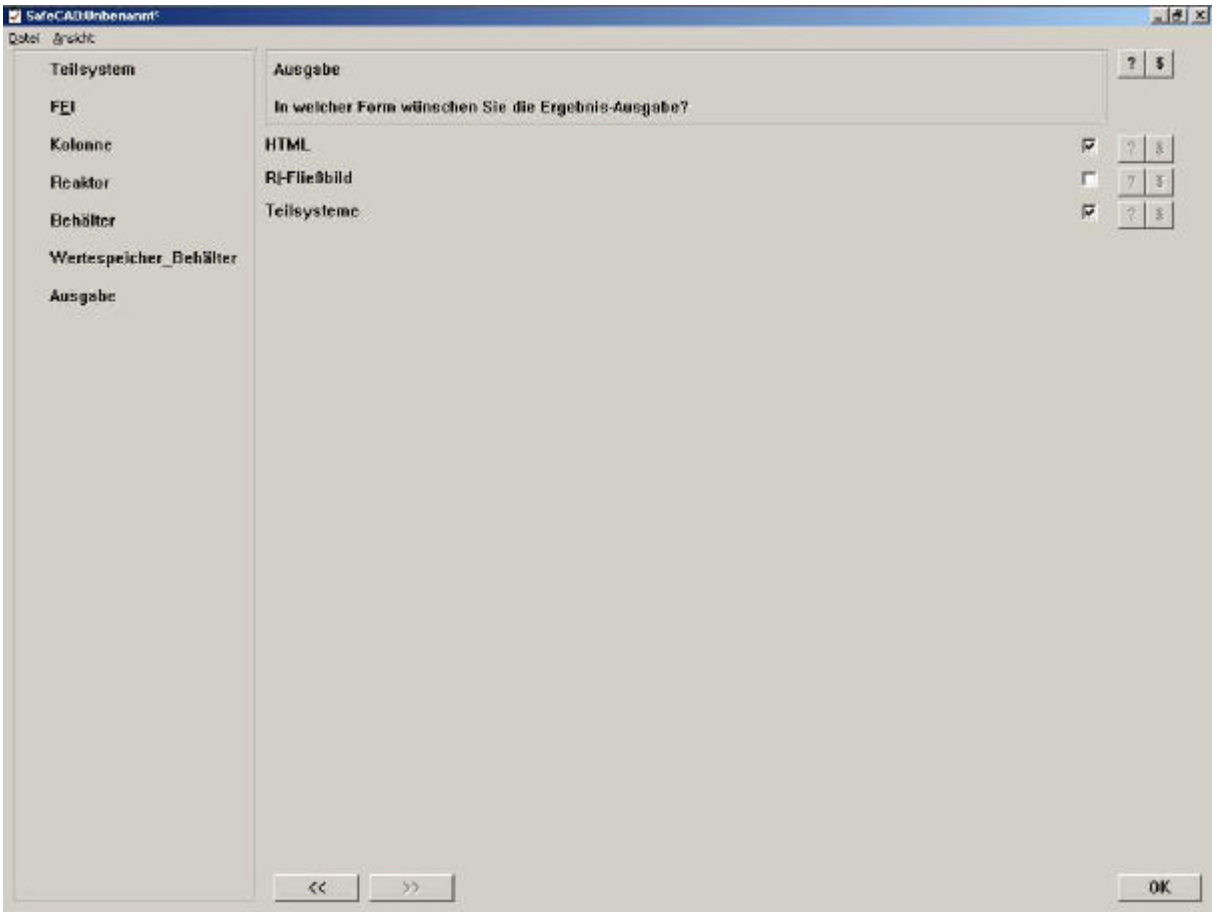

SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Sicherheit
Überdruck
Kann lokaler Akkumulationsabbau zu unzulässigem Überdruck führen?
Nein!
Ja!
passive Maßnahmen:
1. Maximal zulässiger Auslegungsdruck des Behälters liegt überhalb dem maximal möglichen Druck!
aktive Maßnahmen:
1.Abschalten der Eduktzuleitungen bei zu hoher Drehzahl (Wellenbruch) oder zu niedriger Drehzahl (Viskositätsänderung) der Rührerwelle.
2.Notentlastungseinrichtung.
organisatorische Maßnahmen:
1.Alarm bei zu hoher Drehzahl des Rührers (Wellenbruch) und zu niedriger Drehzahl (Viskositätsänderung) mit Anweisungen.
2.Alarm bei zu hoher Stromabnahme (Viskositätsänderung) und zu niedriger Stromabnahme (Wellenbruch) des Rührermotors (asynchron) mit Anweisungen.
<<
>>
OK


SafeCAD:Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Reaktor
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Sicherheit
Überdruck
1. Kann eine Überfüllung mit Flüssigkeit zu Überdruck infolge Wärmeausdehnung führen?
Nein!
Ja!
passive Maßnahmen:
1. Ausreichende Dimensionierung des Behälters verhindert ein Versagen infolge Wärmeausdehnung!
2. Die Befüllung kann nur bei offenem Überlaufventil oder Überlaufleitung erfolgen!
aktive Maßnahmen:
1. Notentlastungseinrichtung!
2. Verriegelung der Zuführungsleitung, um Überfüllung zu vermeiden!
organisatorische Maßnahmen:
1. Anweisungen zur Überwachung des Füllstandes während der Befüllung!
2. Überprüfung der Füllkapazität des Behälters vor der Befüllung!
3. Alarm bei hohem Füllstand mit Anweisungen zur Vermeidung von Überfüllung!
<< >>
OK


SafeCAD:Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Reaktor
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Sicherheit
Überdruck
Worüber soll die Zuführungsleitung verriegelt werden?
Über den Füllstand!
Über den Druck!
Über Füllstand und Druck!
<< >>
OK


SafeCAD:Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Reaktor
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Sicherheit
Überdruck
3. Kann sich entflammbarer Atmosphäre im Luftraum des Behälters entzünden?
Nein!
Ja!
passive Maßnahmen:
2. Zündquellenkontrolle (z.B. Blitzschutz, ständiger Erdung, Spritzschutz beim Befüllen durch Eintauchen der Zuführungsleitung in die Flüssigkeit im Behälter, Durchßlußbschränkung, Bodenzulauf)
3. Auslegung des Behälters, daß er maximal möglichem Druck standhält
4. Lagerung unterhalb der Zündtemperatur
5. Nutzung geeigneter Instrumente (z.B. Füllstandsmessung über Radar)
aktive Maßnahmen:
1. Exposionsdruckentlastung (z.B. Dach mit Sollbruchstellen statt fester Konstruktion, Ex.klappen, etc.)
2. Lagerung der Materialien durch Kühlung unterhalb ihres Flammpunktes
3. Überwachung des Dampfraumes auf brennbare Atmosphäre
4. Inertisierung des Dampfraumes
5. Flammendurchschlagssperre in der Zu- und Ableitung
6. Notspülung bei Ansprechen der Überwachungseinrichtung in der Dampfphase
organisatorische Maßnahmen:
2. Anweisungen zur Befüllung des Behälters bei unterem Grenzwert mit Zuleitung unterhalb des Füllstandes als Spritzschutz
3. Keine Befüllung während eines Gewitters
<<
>>
OK


SafeCAD:Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Reaktor
Wertespeicher_Behälter
Ausgabe
Reaktor
Rührkesselreaktor
Ebene Sicherheit
Unterdruck/Vakuum
4. Kann eine zu hohe Ausflußrate bzw. ein Leerlaufen des Behälters zu unzulässigem Unterdruck führen?
Nein!
Ja!
passive Maßnahmen:
1. Auslegung des Behälters so, daß er größtmöglich zu erwartendenm Unterdruck standhält
2. Ablauf nur bei offenem Ventil (Druckausgleich) möglich.
3. Genau festgelegte Ausflußrate
aktive Maßnahmen:
1. Nutzung eines umfassenden Gasdruckkontrolsystems zur Minderung des Vakuums
2. Unterdruckentspannungseinrichtung
organisatorische Maßnahmen:
1. Prozeßtechnische Begrenzung der maximalen Ausflußrate
Alarm bei zu Unterdruck mit Anweisungen zur Vermeidung eines Vakuums!
<<
>>
OK


SafeCAD/Unbenannt*
Datei Ansicht
Teilsystem
FEI
Kolonne
Reaktor
Behälter
Wertespeicher_Behälter
Ausgabe
Ausgabe
In welcher Form wünschen Sie die Ergebnis-Ausgabe?
HTML
RI-Fließbild
Teilsysteme
<<
>>
OK