Systemanalyse und Automatisierung

Elemente des Sicherheitsstandards chemischer Anlagen

F. Mayinger

1. Der Begriff "System" in sicherheitstechnischem Sinne

Mit dem Begriff System verbinden sich sehr unterschiedliche Vorstellungen, und die Frage nach einer Definition dieses Begriffes würde eine Vielzahl, in ihrer Aussage unterschiedliche Antworten ergeben. In meinem Fach, der Thermodynamik, versteht man darunter einfach einen abgegrenzten Raum, über den man Energie- oder auch Stoffströme bilanziert, und in dessen Innerem ein zu betrachtender Prozeß abläuft. Gegenüber dieser einfachen, fachspezifischen Definition verbinden sich mit dem Begriff Biosystem wesentlich unklarere Vorstellungen, angefangen von einer Wasserpfütze über den Regenwald bis zur gesamten Biosphäre des Erdballs. Die einseitigste und verwaschenste Vorstellung zum Begriff System hatte vermutlich die Studentenbewegung der Außerparlamentarischen Opposition Ende der sechziger und Anfang der siebziger Jahre, die zu System sofort das Wort herrschend addierte, wobei einzig darüber Einigkeit bestand, daß dieses herrschende System - gleichgültig welches auch immer - zu beseitigen sei.

Für eine bessere Begriffsbestimmung - auch im technischen Sinn - scheint es zweckmäßig zu sein, auf den Wortstamm zurückzugehen. Ursprung ist das griechische Verbum hystemi, das "setzen, stellen, legen" bedeutet. Ergänzt um das Adverb "syn", das, wie wir aus vielen Fremdworten wissen, mit "zusammen" zu übersetzen ist, kann man System dem Wortstamm nach als eine Zusammenstellung von Dingen und damit im Technischen als eine Zusammenstellung von Komponenten - also Apparaten und Maschinen - interpretieren, die zusammen in Wechselwirkung stehen und auch nach außen - also mit anderen Systemen - Energie-, Stoff- und Informations-Austausch betreiben können. Ein technisches System kann damit z.B. ein Behälter sein, in dem eine chemische Reaktion abläuft, der Wärme- und Stoffströme mit Nachbarsystemen - Kühl- oder Heizsysteme, Vorratsbehälter für Edukte und Speicher für Produkte - austauscht. dieser Behälter kann über in ihm angebrachte Sensoren Informationen nach außen

liefern, die in weiteren Systemen - Regel- und Überwachungseinrichtungen - interpretiert werden, wobei die Regelung dann Steuerungs- oder Schutzsignale an die vorher erwähnten Nachbarsysteme und an das unter Betrachtung stehende System, den chemischen Reaktor, abgibt. Man kann aber auch die Systemgrenze wesentlich weiterziehen, sie nämlich über die gesamte Anlage legen und Reaktor, Heizung, Kühlung, Stoffver- und -entsorgung sowie Steuerung und Regelung als Teilsysteme dieses Hauptsystems betrachten. Die Festlegung der Systemgrenzen und damit die Definition des Systems wird in der Technik so vorgenommen, wie es für die beabsichtigte Analyse am zweckmäßigsten und am besten überschaubar erscheint. Die Analyse selbst kann unter verschiedenen Gesichtspunkten durchgeführt werden, so z.B. unter den Gesichtspunkten der Qualitätsverbesserung, der Energieeinsparung, der Wirtschaftlichkeitsoptimierung oder auch der Gewährleistung eines hohen Sicherheitsstandards.

Sicherheitstechnische Systemüberlegungen können z.B. danach fragen, welches Fehlverhalten jeder einzelnen Komponente im System ist denkbar? Wie überträgt sich dieses Fehlverhalten auf andere Komponenten und ist zu erwarten, daß ein zunächst unbedeutendes "Ereignis" durch Wechselwirkungen mit anderen Komponenten und deren Fehlverhalten zu einer Störung des gesamten Systems oder gar zu einem Unfall eskaliert? Oder ist aufgrund der Wirksamkeit von Steuer- und schließlich auch Schutzvorrichtungen nach menschlichem Ermessen sicher davon auszugehen, daß das Gesamtsystem wieder in den bestimmungsgemäßen Betrieb zurückgeführt oder sicher abgeschaltet und ohne schädliche Auswirkungen auf die Umgebung oder auch auf Nachbarsysteme sicher im Ruhezustand gehalten werden kann? Für sicherheitstechnische Betrachtungen eines Systems interessieren also vor allem die Qualität seiner Komponenten, deren Ausfall- oder Störungsmöglichkeiten, die dabei entstehenden Störfallsequenzen und die Wirksamkeit der vorhandenen oder auch von außen bereitstellbaren Steuer- und Schutzvorrichtungen.

Damit ist bereits eine Staffelung der Sicherheitsmaßnahmen angesprochen, nämlich dahingehend, daß man zunächst auf eine möglichst hohe Qualität der Komponenten achtet, um Fehlverhalten zu minimieren, durch ein möglichst leistungsfähiges Steuer- und Regelsystem gewährleistet gestörte Betriebszustände wieder in den bestimmungsgemäßen Betrieb zu überführen und, wenn dies nicht mehr möglich sein sollte, schließlich die Anlage mittels zuverlässiger Schutzsysteme abschaltet und in einem sicheren Ruhezustand hält. Damit kann man auch ein völlig anderes "System" definieren, nämlich ein System, das zum großen Teil aus Software-Maßnahmen besteht und das bei der Qualitätssicherung beginnt und über ausgewogene Automatisierung zur Vermeidung menschlicher Fehleingriffe bis zur Redundanz und Diversität der Steuer- und Schutzeinrichtungen reicht. Betrachtungen dieses Systems können nicht nur die Si-

cherheit der Anlage erheblich verbessern, sie erlauben auch wirtschaftliche Aspekte bei der Abwägung verschiedener sicherheitstechnischer Maßnahmen zu berücksichtigen und den in den verschiedenen Verteidigungsebenen erzielbaren Sicherheitsgewinn dem Aufwand gegenüberzustellen.

Schließlich könnte man noch einen dritten Systembegriff definieren, den man in dem Bereich der qualitäts- und sicherheitsorientierten Unternehmensführung ansiedeln kann und der aus den Komponenten Planung, Managementverpflichtung, Organisation, Training, Kommunikation und Anerkennung sicherheitstechnischer Verbesserungsvorschläge besteht. Auch diese, dem unternehmerischen Bereich zuzuordnenden Faktoren bilden ein System, dessen sicherheitstechnische Relevanz durchaus bekannt ist, das aber meiner Meinung nach bei Planung, Fertigung und Betrieb noch nicht in der notwendigen Konsequenz angewandt wird.

Systemsicherheit kann also aus unterschiedlichen Perspektiven und Dimensionen betrachtet werden.

Es würde den Zeitrahmen weit überschreiten, wollte man alle diese Systemvarianten diskutieren, und die Betrachtungen sollen deshalb zunächst auf technische Systeme, also auf das Zusammenwirken der verschiedenen Komponenten - verfahrens- wie regeltechnischer Art - konzentriert und zum Schluß noch kurz auf das System Anlage - Leittechnik - Mensch ausgedehnt werden.

2. Systemtechnische Aspekte bei der Auslegung komplexer Systeme

Die auf Sicherheit und Qualität gerichtete Auslegung beginnt bei der "Integrierten Qualitätssicherung". Die heute noch großenteils traditionelle Trennung der Aufgabenbereiche führt zu abteilungsbezogenem Denken, verbunden mit zahlreichen Schnittstellen und beinhaltet die Gefahr, daß der Mitarbeiter die Übersicht über das Gesamtsystem verliert. Problemlösungen werden deshalb häufig unter dem Inselaspekt des eigenen, eingeschränkten Bereiches gesehen, oder noch lieber wird die Schuld an dem Problem anderen Bereichen zugeschoben. Dies führt leicht dazu, daß die Lösung des Problems auf Kosten anderer Bereiche und nicht im Sinne der Optimierung des Gesamtsystems erfolgt.

Integrierte Qualitätssicherung ist eine wesentliche Voraussetzung für optimalen Sicherheitsstandard. Die Motivation dazu sollte Bestandteil der Unternehmenspolitik sein. Qualität muß systematisch gesichert werden, was am besten gelingt, wenn alle Unternehmensbereiche dies als ihre Angelegenheit sehen.

Beim systematischen Vorgehen zur Verbesserung von Qualität, Zuverlässigkeit und Sicherheit kann man drei Regelkreise zur Vermeidung von

- Planungsfehlern,
- Fertigungsfehlern,
- Anlagenfehlern

nutzen. Zunächst müssen Systementwicklung, -planung und -konstruktion enge Rückkopplung mit Zuverlässigkeits- und Sicherheitsanalysen haben, die dann ihrerseits Vorgaben und Verbesserungsvorschläge für die Systemplanung machen. Ein zweiter sicherheitstechnischer Regelkreis resultiert aus dem Herstellungsprozeß, aus dem mögliche oder tatsächliche Fertigungsfehler an die Zuverlässigkeits- und Qualitätssteuerung gemeldet werden, wobei von dort wieder Verbesserungsvorschläge nicht nur an die Systemherstellung, sondern auch an die Systementwicklung und -planung gehen. Der dritte und meiner Meinung nach besonders wertvolle und wichtige Regelkreis zur Verbesserung von Qualität und Sicherheit geht vom Betrieb aus. Ungewollte Transienten im Prozeß, Störungen und erkannte Anlagenfehler müssen uneingeschränkt der Zuverlässigkeits- und Qualitätssteuerung zur Kenntnis gegeben werden, damit diese wiederum rückkoppelnd Vorschläge für Verbesserungsmaßnahmen an die Systemplanung und -entwicklung, an die Systemherstellung und auch an den Betrieb weiterleitet.

In der Chemie, aber auch in zahlreichen anderen technischen Bereichen werden seit langem wichtige Grundregeln für die Gewährleistung optimaler Qualität und Sicherheit befolgt wie

- Auslegung hinsichtlich thermischer, mechanischer und elektrischer Belastungen in sicherem Abstand zur Grenzbelastung,

- Verwendung qualitativ hochwertiger Materialien und Bauteile,

- Vereinfachung von Entwurf und Konstruktion,

- umfassende Qualitätsprüfungen.

Ebenfalls in Anwendung befinden sich

- systematische Analysen zur Verbesserung der Sicherheit der Anlage und

- das Hinzufügen von Redundanz.

Die Diskussion der verschiedenen Möglichkeiten von Sicherheitsanalysen ist Gegenstand von späteren Erörterungen. Hier soll zunächst kurz auf den Gedanken der Redundanz eingegangen werden. Redundanz bedeutet, daß eine Komponente im Übermaß, also überzählig für den Anforderungsfall vorhanden ist. Zugrunde liegt dabei der Gedanke der sogenannten gestaffelten Verteidigung gegen Unfälle. Diese besteht aus drei bis vier Ebenen, nämlich

- der Qualitätssicherung,
- dem Regel- und Schutzsystem,
- den Sicherheitseinrichtungen und
- gegebenenfalls Notfallschutzmaßnahmen oder dem Accident Management, wie es im angelsächsischen Sprachgebrauch heißt.

Schutz- und Sicherheitsvorrichtungen werden bei technischen Systemen, bei denen auf besondere Sorgfalt zu achten ist, zwei- oder mehrfach redundant ausgeführt. Man unterstellt dabei, daß im Anforderungsfall die erste Vorrichtung nicht wirksam wird oder sich im Augenblick der Störfalleinleitung in routinemäßiger Inspektion befindet.

Strenggenommen darf man sich aber auf Redundanz nur dann verlassen, wenn die redundanten Komponenten unterschiedliche Konstruktion haben oder zumindest von unterschiedlichen Herstellern stammen. Es besteht sonst die Gefahr, daß ein Konstruktions- oder Materialfehler, der allen Komponenten zueigen ist, zum Versagen im Anforderungsfall führt. Im Angelsächsischen nennt man einen solchen Konstruktions- oder Materialfehler, der allen redundant angeordneten Komponenten zueigen ist, einen "common mode"-Fehler. Es gibt dafür durchaus Beispiele aus der Praxis. Redundante Komponenten sollten deshalb in gewißem Maße auch diversität sein.

Aus systemtechnischer Sicht müssen Redundanz und Diversität in einem vernünftigen Verhältnis stehen. Auch noch so hohe Redundanz bringt wenig Sicherheitsgewinn, wenn die Gefahr von "common-mode"-Fehlern besteht, und auf der anderen Seite kann zu hohe Diversität auch wieder zusätzliche Fehlerquellen verursachen.

Wartungsstrategien für Schutz- und Sicherheitseinrichtungen können ebenfalls entscheidende Auswirkung auf die Zuverlässigkeit, bzw. auf die Nichtverfügbarkeit haben. Betrachten wir ein System, in dem vier parallel geschaltete Kühlwasserpumpen arbeiten und von denen mindestens zwei benötigt werden. Nehmen wir weiter an, es seien viermonatige Wartungsintervalle vorgesehen, so kann man dabei so vorgehen, daß man alle vier Monate die Anlage kurz stillegt und dabei für einige Stunden die Wartungsarbeiten an allen vier Pumpen und deren Antrieben vornimmt. Man kann aber auch unter Beachtung dieser viermonatigen Wartungsintervalle monatlich einmal jeweils nur eine Pumpe warten, ohne die Anlage außer Betrieb zu nehmen, da ja zwei Pumpen für den Betrieb genügen und immer noch eine Pumpe als Redundanz mitläuft. Diese zweitgenannte Wartungsstrategie verringert die Erwartung für den Ausfall des gesamten Kühlsystems um den Faktor 5 - vorausgesetzt die Wartungszeiten sind sehr kurz gegenüber den Wartungsintervallen. Bei sehr teueren Produktionsanlagen, insbesondere dann, wenn der Preis einer Kühlwasserpumpe gering ist im Vergleich zu den Kosten des Gesamtsystems, hat damit vernünftige Redundanz zusammen mit einer optimierten Wartungsstrategie auch wirtschaftliche Vorteile, da Wartungsarbeiten am Kühlwassersystem den Betrieb der Produktionsanlage und damit deren Jahresausstoß nicht mehr beeinträchtigen.

Redundanzen werden in der Chemie heute schon häufig in der Steuerungs- und Leittechnik angewandt. Man spricht dort von sogenannten 2 von 3 Systemen. Das bedeutet, daß 3 voneinander unabhängige Sensoren Signale an die Steuerung liefern, die vergleicht, ob alle drei Signale innerhalb einer gewissen Fehlertoleranz identisch sind. Ist dies nicht der Fall, so muß die Steuerung ein Kriterium verfügbar haben, nachdem sie entscheidet, ob eine tatsächliche Stö-

rung im Betrieb vorliegt, oder ob die Sensoren fehlerhaft arbeiten. Dieses Kriterium ist die genannte 2 von 3-Auswahl, d.h. wenn zwei Sensoren den Sollwert des Prozesses melden, wird die Anzeige des dritten Sensors als fehlerhaft eingestuft, und die Anlage bleibt in Betrieb.

Man kann dieses 2 von 3-System selbstverständlich über den eigentlichen Bereich der Sensoren hinaus erweitern und kann auch die Datenverarbeitung und Teile der Leittechnik dreisträngig aufbauen. Am Ende dieser Kette muß jedoch eine zentrale Einheit stehen, welche einen wohldefinierten Befehl an den Prozeß gibt. Diese letzte "Einheit" kann der Mensch sein, der dann schließendlich zu entscheiden hat; es wird aber heute auch hier überwiegend auf den Computer zurückgegriffen. Bei besonderen Anforderungen, wie zum Beispiel in der Raumfahrt oder in der Kerntechnik wird dieser zentrale Computer nochmals von einem zweiten Computer überwacht, der bei Verdacht auf Fehlmeldungen oder falsche Befehle die Anlage unabhängig abschalten und in einen sicheren Ruhezustand überführen kann.

Mit zunehmender Leistungsfähigkeit der Computer und wachsenden Kenntnissen des dynamischen Verhaltens eines Prozesses, nicht nur bei bestimmungsgemäßen Betrieb und der darin vorgesehenen Regel- und Anfahrvorgänge, sondern auch in Störfallsituationen, bietet sich eine weitere neue Möglichkeit der Zuverlässigkeitsverbesserung von großen chemischen Anlagen an, nämlich durch Prozeßmodelle, welche das Betriebs- und Störfallverhalten der Anlage vorausberechnen und auch während des Betriebes vergleichend analysieren lassen. Solche Computermodelle müssen selbstverständlich auf soliden und umfassenden theoretischen Kenntnissen der Verfahrensabläufe in der Anlage und der Verfügbarkeit mathematischer Beschreibungen aufbauen. Sie benötigen in der Regel mehrere Entwicklungs- und Erprobungsphasen bis zu ihrem routinemäßigen Einsatz.

In der ersten Phase wird das Modell als solches entwickelt und erstellt, wobei man auf Stabilitäts- und Sensitivitätsanalysen aufbaut. Mathematische Basis ist dabei häufig die Theorie der Bifurkationen und der Oszillationen. Es folgt dann die Entwicklung modellgestützter Regelverfahren, wobei die dafür notwendigen physikalischen oder chemischen Modelle auf gutem menschlichen Wissen aufbauen, das in der Regel nicht rein theoretischer Natur ist, sondern aus Beobachtungen, also aus Experiment und Erfahrung stammt. Einfache Regelalgorithmen kann man aus Kennzahlen der Thermo- und Fluiddynamik, der Wärme- und Stoffübertragung und der Reaktionskinetik entwickeln. Häufig sind auch adaptive Regelmethoden im Einsatz.

Im dritten Schritt werden dann optimale Steuerungen durch Simulation erprobt. Hier muß auf Datendokumentation aus dem Betrieb von Pilotanlagen oder aus konstruktiv und in der Prozeßführung ähnlichen Anlagen zurückgegriffen werden. Die Ermittlung optimaler Steuerungen erfolgt zunächst für den stationären Betrieb und wird dann auf dynamisches Betriebsverhalten ausgeweitet. Der letzte Schritt ist dann die Anwendung auf die Produktionsanlage, wobei hier nochmals Parameterschätzungen und eine Überprüfung der Stoffdaten vorgenommen werden müssen. Ziel ist schließlich die Vorhersage einer optimierten Fahrweise der Produktionsanlage nicht nur im bestimmungsgemäßen Betrieb, sondern auch bei unvorhergesehenen Transienten, so daß für den Betrieb der Produktionsanlage im Ernstfall genügend vorausschauendes Wissen vorhanden ist, und diese - per Computer oder von Hand - zuverlässig wieder in den optimalen Betriebszustand zurückgeführt oder in einen sicheren Ruhezustand übergeführt werden kann.

In der Regel dienen solche Prozeßmodelle nicht nur zur Optimierung und Parameteranpassung einzelner Fahrweisen, sondern auch zur Simulation von Störungen. Prozeßmodelle bieten darüber hinaus die Möglichkeiten, das chemische Verfahren durch Kombination von Experiment und Simulation weiterzuentwickeln und die Bedienungsmannschaft für Störfälle an der Anlage zu schulen. Für die zuletztgenannte Aufgabe müssen die Prozeßmodelle in Echtzeit arbeiten, um nicht nur das Wissen der Mannschaft über möglichst viele Störfallpfade der Anlage zu erweitern, sondern auch deren Reaktionsvermögen für Notfallmaßnahmen zu verbessern.

3. Systemtechnische Möglichkeiten zur Verbesserung des Sicherheitsstandards

Selbst in der Fachwelt findet man häufig die Meinung, systemtechnische Analysemöglichkeiten zur Verbesserung des Sicherheitsstandards würden überwiegend nur in der Luft- und Raumfahrt, in der Computertechnik und in der Kerntechnik genutzt, seien aber in der Chemie noch kaum in Anwendung. Dies entspricht nicht der Wirklichkeit, nur die Methoden der systemtechnischen Sicherheitsanalysen sind für chemische Anlagen teilweise anders als für die zuvor genannten technischen Systeme. Dies liegt sowohl an der konstruktiven Gestaltung als auch an der verfahrenstechnischen Prozeßführung. Jede chemische Anlage ist weitgehend ein Unikat, das sicherheitstechnisch nur sehr beschränkt mit anderen Anlagen zu vergleichen ist, auch wenn deren Verfahrensablauf und Fließbild ähnlich sind. In der Luft- und Raumfahrt, in der Computertechnik und in der Kerntechnik existieren Klassen von Systemen, deren Konstruktion und deren Prozeßschaltungen in großem Umfang zeichnungsgleich sind. Erfahrungen an einer Anlage können deshalb voll auf andere Anlagen übertragen werden, was in der Chemie nicht ohne weiteres möglich ist. In der Regel sind dort auch die Verfahrens- und Prozeßabläufe besser überschaubar, oder zumindest innerhalb einer Anlagenkategorie einheitlicher, als bei den sehr unterschiedlich geplanten chemischen Anlagen, ganz abgesehen von deren äußerst vielfältigen und breiten Produktpalette.

In der Literatur spricht man von induktiven und von deduktiven Analyseverfahren, von Analyseverfahren nach Markovschen Prozessen und schließlich von quantitativen Risikoanalysen. Im allgemeinen Sprachgebrauch versteht man unter Induktion oder induktivem Vorgehen im logischen Sinne den Schluß vom besonderen auf das allgemeine, oder anders ausgedrückt, in der Methodenlehre das Ausgehen von empirischen Einzelbeobachtungen mit dem Ziel, zu allgemein gültigen Aussagen zu kommen. Nach der strengen Logik - zunächst nicht bezogen auf Sicherheitsanalysen - sind induktive wissenschaftliche Verfahren, die von empirischen Sätzen - empirischen Einzelbeobachtungen - zu sicheren allgemein gültigen Aussagen gelangen wollen, nicht möglich. Aus besonderen Beobachtungen lassen sich umfassende und abdeckende allgemeine Gesetze nur ableiten, wenn alle Einzelfälle gegeben sind, man spricht dann von vollständiger Induktion. Sind sie nichtgegeben - also im Falle unvollständiger Induktion -, so ist der Schluß nur wahrscheinlich. Auf sicherheitstechnische Analysen übertragen heißt dies, daß ihnen im Falle von Bemühungen um quantitative Aussagen immer eine mehr oder weniger große Wahrscheinlichkeit anhaftet. Zahlen für Eintrittswahrscheinlichkeiten von Störfällen können daher immer in Frage gestellt werden.

Im Gegensatz dazu bedeutet das deduktive Verfahren die Ableitung besonderer Erkenntnisse oder naturwissenschaftlicher Aussagen, aus allgemeinen Gesetzen. In der Logistik geht man von Axiomen mit Hilfe von Deduktionen zu beweisbaren Theoremen und verfährt dabei nach mathematischen Methoden mit dem Ziel, die Logik selbst deduktiv aufzubauen. In der Sicherheitsanalyse ist strenggenommen für quantitative Aussagen auch diese Methode nicht möglich oder mit großen Unsicherheiten behaftet. Bei deduktiven sicherheitstechnischen Analyseverfahren benützt man sogenannte Fehler- oder Gefährdungsbäume, die wiederum individuelle Zuverlässigkeitsdaten für jede Komponente benötigen. Eine solche quantitative Analyse setzt deshalb große Mengen Erfahrungsdaten aus dem Betrieb zeichnungsgleicher oder zumindest konstruktiv sehr ähnlicher Anlagen voraus.

Beide Methoden der Sicherheitsanalyse, die induktive und die deduktive, arbeiten heute noch mehr reflektierend als prognostizierend, d.h. sie sind bevorzugt anwendbar für die sicherheitstechnische Beurteilung existierender Anlagen, können aber selbstverständlich wertvolle Aussagen machen, welche sicherheitstechnischen Gewinne bei konstruktiven Änderungen oder bei Ersatz einzelner Anlagenteile zu erwarten sind. Sie sind prädestiniert, eine evolutionäre, quasi-statische Anlagenentwicklung zu verfolgen, wie sie zum Beispiel in der Kerntechnik oder auch in der Luft- und Raumfahrt zu beobachten ist.

Die chemische Industrie weist demgegenüber ein hohes Maß an spontaner Innovation auf und dies nicht nur hinsichtlich neuer Produkte, sondern auch im Hinblick auf Produktionsverfahren, also verfahrenstechnischer Prozesse und folglich der Anlagen, in denen diese Prozesse betrieben werden. Deshalb ging die chemische Industrie ihre eigenen Wege bei der Entwicklung von Analyseverfahren zur Optimierung der Sicherheit ihrer Anlagen. Angefangen von den ersten Überlegungen bereits bei der Forschung nach einem neuen Produkt und dem Entwurf einer ersten Versuchsanlage, über die Pilotanlage, die Planung und den Bau der Produktionsanlage bis zum laufenden Betrieb der Produktionsanlage wird die sicherheitstechnische Analyse als ein fortwährender und ineinandergreifender Prozeß gesehen. Im Sinne einer umfassenden und systematischen Durcharbeitung des Projektes werden dabei die wesentlichen sicherheitstechnischen Überlegungen und Ergebnisse von Zeit zu Zeit neu überdacht und in einem Fachgremium diskutiert. Bei der Planung und dem Bau einer neuen Produktionsanlage unterscheidet man verschiedene Phasen und sicherheitstechnische Schwerpunkte wie

- Darlegung und Entscheidung, daß das gewählte Verfahren an dem vorgesehenen Standort aus sicherheitstechnischer Sicht durchgeführt werden kann,

- Erarbeitung des sicherheitstechnischen Konzepts und Darlegung für eine Begutachtung durch Fachleute mit Betriebserfahrung ohne projektspezifische Kenntnisse,

- Überprüfung der Planungsunterlagen auf sicherheitstechnische Konsistenz im Sinne einer sicherheitstechnischen Selbstkontrolle.

Die dabei erzielten Arbeitsergebnisse werden Sicherheitsbetrachtungen genannt und wiederum in Stufen eingeteilt. Es handelt sich also hier bewußt nicht um eine Sicherheitsanalyse im Sinne der Störfall-Verordnung. Entsprechend dem zeitlichen Bedarf sind die Sicherheitsbetrachtungen in den Planungsablauf so eingeordnet, daß die erste Stufe vor der Ausarbeitungsfreigabe, die zweite vor der Behördenbesprechung und die dritte kurz nach der Projektgenehmigung vorliegt.

Die erste Stufe der Sicherheitsbetrachtung hat zum Ziel, die wesentlichen Gefährdungsmöglichkeiten des Verfahrens und die Gefahrenquellen der Anlage aufzuzeigen sowie die Aufgaben für die sicherheitstechnische Grundkonzeption zu formulieren.

Die Stufe 2 der Sicherheitsbetrachtung beinhaltet das Sicherheitskonzept zur Beherrschung der Gefährdungsmöglichkeit der Produktionsanlage und deren Verfahren.

Schließlich ist es Ziel der dritten Stufe, bereits erarbeitete Planungsunterlagen, z. B. Fließbilder auf sicherheitstechnische Konsistenz zu überprüfen. Diese Prüfung wird von der Planungsgruppe nach vorgegebenen Regeln durchgeführt. Diese vorgegebenen Regeln sind weitgehend einheitlich in der chemischen Industrie und lehnen sich an die sogenannte PAAG-Methode an. Diese Bezeichnung entstand aus den Anfangsbuchstaben der Ziele und Aufgabe dieser Methode, nämlich aus

- **P**rognose,
- **A**uffinden der Ursachen,
- **A**bschätzen der Auswirkungen,
- **G**egenmaßnahmen.

Diese Methode wurde ursprünglich von ICI entwickelt und nennt sich im Englischen "Hazard and Operability Studies" (HAZOP-Verfahren).

Der Berufsgenossenschaft der chemischen Industrie, und hier insbesondere der deutschen Internationalen Sektion der Internationalen Vereinigung für Soziale Sicherheit kommt dabei großes Verdienst bei der Einführung dieser Methode in der Chemie zu. Sie machte dadurch ein systematisches Verfahren verfügbar, um Gefährdungen aus chemischen Anlagen zu identifizieren und Risiken in der Chemie zu minimieren. Das PAAG-Verfahren wurde im deutschsprachigen Raum zum ersten Mal 1978 veröffentlicht. Es hat sich inzwischen zu einem wichtigen Standardverfahren für die Sicherheitsanalysen nicht nur geplanter, sondern auch bestehender Chemieanlagen entwickelt.

Das PAAG-Verfahren ist, wie gesagt, eine systematische Vorgehensweise zum Auffinden nicht offensichtlicher Störungs- und Gefahrenquellen in Systemen aller Art. Solche Systeme können technische Anlagen und organisatorische Abläufe, z.B. Produktionsbetriebe, Lager, Transportsysteme, aber auch Betriebsvorschriften sein. Das PAAG-Verfahren kann auf bestehende und auf geplante Systeme angewandt werden. Ziel des Verfahrens ist es, die Vorstellungskraft der Planer, Konstrukteure, Sicherheitsingenieure und der Betreiber von Anlagen systematisch so anzuregen, daß sie potentielle Gefahren in Anlagen frühzeitig erkennen können. Nach Bewertung der Gefahren schließt sich dann die Entwicklung von Maßnahmen zur Gewährleistung der Arbeits- und Betriebssicherheit, des Umweltschutzes und der Verfügbarkeit der Systeme an. Dank seiner Flexibilität kann das Verfahren sehr vielseitig angewandt werden, angefangen von kontinuierlichen Prozessen in der chemischen oder petrochemischen Industrie über diskontinuierlich arbeitende Einheiten bis hin zu Einzelaggregaten.

Das PAAG-Verfahren hat den großen Vorteil einer kognitiven Methode, nämlich in dem Sinne, daß durch Einbindung von Betriebsleitern, Betriebsingenieuren, Meistern sowie Meß- und Regeltechnikern bei der Planung von Anlagen sehr früh das Wissen um Störfallpfade und mögliche Gegenmaßnahmen gefördert wird und bei der Analyse bestehender Anlagen die Betriebsmannschaft ihre Anlage hinsichtlich möglichen Störfallverhaltens besser kennenlernt.

Schließlich ist noch kurz die auf Fehlerbaumbetrachtungen basierende probalistische Risikoanalyse zu erläutern. Sie geht von denkbaren auslösenden Ereignissen und Ausfällen von Komponeten aus, die entweder in Betriebserfahrungen beobachtet wurden oder die durch systematisches Nachdenken, ähnlich wie in dem vorher erwähnten PAAG-Verfahren oder auch in Mo-

dellüberlegungen ermittelt wurden. In der Fehlerbaumanalyse werden dann die Ereignisketten verfolgt und geprüft, ob und wie Regel- bzw. Schutzvorrichtungen wirksam werden. Sowohl das auslösende Ereignis selbst, als auch die sachgerechte Wirkung der Komponenten in den Regel- und Schutzsystemen sind hinsichtlich Auftreten und Verfolgen eines weiteren Ereignispfades mit Unsicherheiten behaftet, die durch Wahrscheinlichkeitsverteilungen beschrieben werden, durch welche wiederum die mögliche Variation der Größen ausgedrückt wird. Hier liegt das große Problem solcher probabilistischer Risikostudien, da auch für scheinbar einfache Komponenten, wie Ventile oder Pumpen heute noch große Kenntnisunsicherheiten hinsichtlich Fehlaktionen oder Ausfallwahrscheinlichkeiten existieren und man dann auf subjektive, also der Schätzung des Bearbeiters unterliegende Wahrscheinlichkeitsbegriffe und -zahlen zurückgreifen muß. Die probabilistische Risikoanalyse ist sicher ein gutes Werkzeug bei hinreichender Kenntnis der Zuverlässigkeit der sicherheitstechnisch wichtigen Komponenten in einer Anlage, Schwachstellen des Systems zu finden, die durch konstruktive Verbesserung oder durch Redundanz beseitigt werden können. Sie sollten aber nicht dazu herangezogen werden, quantitative Zahlen für die Wahrscheinlichkeit eines Störfalles angeben zu wollen.

4. Automatisierung und Schnittstellen zwischen technischem System und Mensch

Die Automatisierung hat in der Anlagentechnik heute einen hohen Perfektionsgrad erreicht. Innerhalb des bestimmungsgemäßen Betriebes werden nicht nur stationäre Betriebszustände, sondern auch An- und Abfahrvorgänge sowie Transienten vollautomatisch geregelt. Teilweise übernimmt die Regelung auch Schutzaufgaben, nämlich dadurch, daß sie bei Störfällen die Anlage sicher abschaltet und in einen Zustand überführt, der minimale Auswirkungen auf die Umgebung gewährleistet. Regel- und Schutzsysteme müssen dabei ein hohes Maß an "Wissen" über das dynamische Verhalten der Anlage besitzen. Solche Regelalgorithmen sind meist schutzzielorientiert, d.h. sie steuern die Anlage in einen für die Umgebung ungefährlichen Zustand, z.B. durch Unterbrechung der chemischen Reaktion, durch Druckentlastung oder durch massive Kühlung. Sie versuchen also nicht primär das Ereignis im Detail zu analysieren, sind aber auf Signale des Ereignisses oder der Ereigniskette angewiesen. Solche Signale sind z.B. Temperaturanstieg bei durchgehender Reaktion, bei Ausfall der Kühlung oder Druckabfall bei Leckage.

Für moderne Anlagen werden höhere Regelalgorithmen angewandt, und die Optimierung der Steuerung erfolgt durch rechnergestützte Simulation des Prozesses. Gerade angesichts der sehr fortgeschrittenen Prozeßleittechnik stellt sich häufig die Frage, ob eine weitere Perfektionierung und Automatisierung bei der Steuerung und Regelung von energie- und verfahrenstechnischen Anlagen sicherheitstechnisch nicht eher kontraproduktiv als fördernd wäre. Argumente, die man dabei immer wieder hört, sind Mangel an Herausforderungen an eine für die Resttätigkeit überqualifizierte Betriebsmannschaft, daraus resultierende Langeweile, Gleichgültigkeit und damit Schwierigkeiten, engagierte Mitarbeiter für die Tätigkeit auf der Leitwarte zu gewinnen.

Für die Automatisierung von Schutzmaßnahmen bei Störfällen spricht die Tatsache, daß ein großer Prozentsatz an Störfällen - nicht nur in der Chemie - auf menschliche Fehlhandlungen zurückgeht. So sagen Statistiken, daß 60 bis 80 Prozent der Flugunfälle, die sich in den letzten Jahrzehnten in der westlichen Welt ereigneten, ihre Ursachen in menschlichem Versagen haben. In der Kerntechnik wurde deshalb bei den Anlagen westlicher Bauweise ein Kompromiß zwischen Automatisierung und menschlichem Eingreifen bei Störfällen dahingehend beschritten, daß während der ersten halben Stunde nach Eintritt eines Ereignisses oder einer Störung die automatische Leittechnik die Schutzmaßnahmen voll übernimmt, und während dieser Zeit

ein menschlicher Eingriff nur mit ganz bestimmten, wohlüberlegten Handlungsprozeduren möglich ist. So müßte das automatische System von zwei Personen durch gleichzeitige Schalthandlungen in zwei verschiedenen Räumen entriegelt werden. Man will dadurch unüberlegte Kurzschlußhandlungen ausschließen und unterstellt, daß der durch die Störung ausgelöste Stress die Wahrscheinlichkeit für Fehlhandlungen besonders in den ersten 30 Minuten erhöht.

Bei den Reaktionen der Betriebsmannschaft auf Störungen muß man zwischen

- fertigkeitsbedingtem,
- regelbedingtem und
- kenntnisbedingtem

Verhalten unterscheiden.

Unter fertigkeitsbedingtem Verhalten versteht man ein häufig geübtes Verhalten, das nach Wahrnehmung der Eingangsinformation aufgrund der vorhandenen Erfahrung bzw. Übung quasi automatische Verhaltensweisen auslöst, ein Verhalten also das Routinecharakter hat. Beim regelbedingten Verhalten wird nach Erkennen der Eingangsinformation aufgrund vorhandener Regeln die Zuordnung des vorliegenden Zustandes zu entsprechenden vorgeplanten Aktionen vorgenommen. Unter kenntnisbedingtem Verhalten wird schließlich ein Verhalten in neuartigen Situationen verstanden, in denen eine Problemlösung durch die Bedienungsmannschaft erwartet wird. Nach Identifizierung der Merkmale der Störung muß die Betriebsmannschaft aus generellen Zielen Handlungsnotwendigkeiten ableiten, und die zu ihrer Ausführung nötigen Schritte planen.

Menschliches Versagen besteht nicht nur darin, daß menschliche Fehlhandlungen als Störfallauslöser fungieren, sondern auch in solchen Aktionen, die einen vorliegenden Störfall verschlimmeren. Natürlich erwartet man, daß eine gutgeschulte und bestens trainierte Betriebsmannschaft in der Lage ist, durch geplante oder auch durch improvisierte Handlungen den Störfall zu beherrschen.

Ursächlich für Störfälle können aber auch menschliche Fehlhandlungen sein, die zeitlich weit vor Eintritt des Ereignisses liegen. Solche Fehlhandlungen können bei routinemäßigen Überprüfungen oder auch bei Wartungsarbeiten entstehen, die sich erst dann auswirken, wenn die falsch gewartete Komponente, z.B. bei einer Betriebstransiente vom automatischen Leitsystem angefordert wird.

In der Regel sind es die Schnittstellen in der Informations- und Aktionskette, also zwischen Prozeß und Information, zwischen Information und Mensch und schließlich zwischen Mensch und Prozeß, welche zu Mißverständnissen und Fehlhandlungen führen können. Für eine reibungsfreie Übertragung vom Prozeß auf die Informationsebene muß die Instrumentierung sachgerecht ausgelegt sein, und sie muß die für Störmeldungen repräsentativen Signale vollständig erfassen, um sicherheitsgerichtete Prozeduren einleiten zu können. Signale und Prozeduren müssen an der Schnittstelle zwischen Information und Mensch von der Betriebsmannschaft nicht nur ausreichend wahrgenommen, sondern auch richtig verstanden werden. Störmeldungen dürfen nicht aus nichtigen Gründen auftreten, da sonst die Betriebsmannschaft dagegen abstumpft und sie für irrelevant hält. Durch das Leitsystem verursachte Fehlmeldungen müssen klar und eindeutig erkannt werden.

Schließlich muß der Mensch aus den Informationen, die ihm die Instrumente liefern, geeignete, eindeutig sicherheitsgerichtete Handlungen initiieren oder bei automatischen Schutzsystemen zumindest erkennen, daß die eingeleiteten Prozeduren angesichts des Zustandes der Anlage notwendig und geeignet sind, Schaden zu verhindern. In dem System verfahrenstechnischer Prozeß, Informations- und Leitsystem und Mensch kommt deshalb dem Wissen und Können der Betriebsmannschaft entscheidende Bedeutung zu. Dabei muß man berücksichtigen, daß der Mensch unter Streßsituationen, insbesondere wenn rasches Handeln gefordert ist, nur einen Teil seiner tatsächlichen Fähigkeiten parat hat.

Das in der Streßsituation verbliebene Können liegt überwiegend auf dem Gebiet des fertigkeitsbedingten Verhaltens, also einer Verhaltensweise, in der häufige Übung und gründliche Erfahrung ihre Ursache haben. Damit kommt der Aus- und Fortbildung sowie dem laufenden Training der Mannschaft große Bedeutung zu. Für eine Optimierung des Sicherheitsstandards reicht es nicht aus, diese Aus- und Fortbildung auf mehr oder weniger theoretische Analysen und Erläuterungen in Seminaren und Kursen zu beschränken. Die Betriebsmannschaft muß ihre Fähigkeiten, Betriebstransienten und Störungen unter Kontrolle zu bringen, in praktischen Übungen trainieren. Selbstverständlich kann dies nicht an der realen Anlage erfolgen. Der heutige Stand der Computer-Technik und das moderne, in theoretischen Analysen und auch experimentell an Versuchs- oder Pilotanlagen erworbene Wissen über das dynamische Verhalten verfahrens- und energietechnischer Anlagen erlauben es, den Prozeß so realitätsnah auf elektronischen Rechnern - Workstations oder auch Personal Computers - nachzubilden, daß dort auch Störfallsequenzen studiert werden können. Es wäre meiner Meinung nach wünschens-

wert, daß in zunehmendem Maße Rechenprogramme entwickelt werden, die es erlauben, das sicherheitsgerichtete Reaktionsvermögen von Betriebsmannschaften für ein möglichst breites Spektrum denkbarer Störfallfrequenzen realitätsnah zu trainieren.

Störfallsequenzen entstehen häufig aus zunächst harmlosen Betriebstransienten oder für sich allein gesehen unbedeutenden Ereignissen. Tritt aber zufällig oder kausal eine zeitliche Koinzidenz von zwei oder mehreren Ereignissen ein, so können sich daraus sehr rasch eskalierende Störfallsequenzen entwickeln. Deshalb halte ich es für sicherheitstechnisch äußerst förderlich und notwendig, daß Wissen und Erfahrungen über Ereignisse beim Betrieb von chemischen Anlagen systematisch gesammelt und soweit aufgearbeitet werden, daß Betreiber und Hersteller bei Kenntnisnahme Schlüsse und Lehren für eine Verbesserung ihrer Sicherheits- und Anlagentechnik ziehen können. Eine breite Kenntnisnahme ist nur dann möglich, wenn diese Ereignis-Erfahrungen von kompetenter Seite analysiert und - selbstverständlich in anonymer Form - den daran interessierten Betreibern und Herstellern zugeleitet werden.

Erfahrung sammeln heißt Fehler machen und daraus lernen. Das Lehrgeld für das Erfahrungssammeln kann man erheblich reduzieren, wenn man nicht nur aus den eigenen Fehlern, sondern auch aus denen der anderen lernt. Voraussetzung für eine Bereitschaft zur Sammlung solcher Daten ist aber, daß solche Ereignismeldungen - gleichgültig von welcher Seite auch immer - nicht zu Horrorszenarien, möglichst noch unter Einbeziehung der Öffentlichkeit hochgespielt werden, um daraus politisch motivierte, der Sicherheit nicht immer dienliche, neue Vorschriften zu erfassen.