Sicherheitstechnische Gesamtbetrachtungen als Ziel der Weiterentwicklung technischer Regelwerke

F. Mayinger

Moderne Anlagen in der Kraftwerkstechnik und in der Chemie weisen als komplexe Systeme nicht zuletzt auch aufgrund einer äußerst leistungsfähigen Leittechnik hohen Vernetzungsgrad zwischen den Komponenten - Apparaten und Maschinen - auf. Zukünftige technische Regelwerke müssen deshalb stärker als bisher von Gesamtbetrachtungen ausgehen. Dies beginnt bereits bei einer integrierten Qualitätssicherung der Anlagenteile, die eine wesentliche Voraussetzung für optimalen Sicherheitsstandard ist.

In der Chemie und in der Energietechnik, aber auch in zahlreichen anderen technischen Bereichen, werden seit langem wichtige Grundregeln für die Gewährleistung optimaler Qualität und Sicherheit befolgt. Zu diesen Grundregeln gehören auch Wartungsstrategien für Schutz- und Sicherheitseinrichtungen, sowie die zunehmende Einführung von Redundanzen, die in der Leittechnik moderner, großer Anlagen zum Standard gehören.

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.

Mit zunehmender Leistungsfähigkeit der Computer und wachsenden Kenntnissen des dynamischen Verhaltens eines Prozesses, nicht nur bei bestimmungsgemäßem 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.

Die Automatisierung hat in der Anlagentechnik heute einen hohen Perfektionsgrad erreicht. Aber immer noch 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. Der Mensch muß aus den Informationen, die ihm die Instrumente liefern, geeignete eindeutig sicherheitsgerichtete Handlungen initiieren oder bei automatischen Schutzsystemen erkennen, daß die eingeleiteten Prozeduren angesichts des Zustandes der Anlage, notwendig und geeignet sind, Schaden zu verhindern. In dem System Prozeß, Information, Leittechnik und Mensch, kommt dem Wissen und Können der Betriebsmannschaft entscheidende Bedeutung zu. Es ist deshalb wünschenswert, daß in zunehmendem Maße Rechenprogramme entwickelt werden, anhand derer es möglich ist, das sicherheitsgerichtete Reaktionsvermögen von Betriebsmannschaften für ein möglichst breites Spektrum denkbarer Störfall-Sequenzen realitätsnah zu trainieren.

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 aber spricht die Tatsache, daß ein großer Prozentsatz an Störfällen - nicht nur in der Chemie - auf menschliche Fehlhandlungen zurückgeht.

Störungen 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 Unfall-Sequenzen entwickeln. Deshalb halte ich es für sicherheitstechnisch äußerst förderlich und notwendig, daß Wissen und Erfahrungen über Ereignisse beim Betrieb von 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.

München, 11. Juli 1994