SYSTEM-SICHERHEITSANALYSE

G. MIEZE,

Technische und physikalische Abteilungen,
Brown Boveri/Krupp Reaktorbau GmbH, Mannheim, Germany

ABSTRACT

An attempt will be made to describe the general decision making process in system safety assessment. In this context the criteria necessary and the problem of adequate data generation, handling and retrieval will be discussed. A system safety programme to support that effort and to assure the achievement of the safety objectives will be discussed. Analysis techniques as a part of that system safety programme will be identified and explained to some extent.

Emphasis will be placed on the status of reliability in the framework of system safety programme. Special attention will be given to the implementation of analysis techniques to mechanical systems.

1. ZIEL UND ZWECK DER SYSTEM-SICHERHEITSANALYSE

In fast allen Bereichen der Technik treten immer wieder große Störfälle auf. Oft führen unerwartete Ereigniskombinationen zu schweren Sach- und Personenschäden. Die Erfahrung lehrt, daß Störfälle nicht mit absoluter Sicherheit verhindert werden können. Wir müssen uns also mit dem Phänomen des Versagens technischer Systeme auseinandersetzen.

Ausfall, Versagen, Fehler sind Synonyme für unkontrollierte Funktionsänderungen von Systemen, Untersystemen und Bauteilen. Eine solche unkontrollierte Funktionsänderung kann zu einem Schaden im System selbst und in angrenzenden Systemen führen. In der chemischen Technik und in der Kerntechnik z.B. brauchen diese Schäden nicht auf angrenzende Systeme begrenzt zu bleiben, sondern können sich auch auf nicht unmittelbar beteiligte in der Umgebung ausdehnen.

Bei der Erstellung technischer Systeme werden wir nun vor die Entscheidung gestellt, ob wir in genügender Weise dem Versagen vorgebeugt haben und ob die Schäden, verursacht durch eventuelle Störfälle, in akzeptierten Grenzen bleiben. Wir haben zu entscheiden, ob das zu erstellende System sicher ist. Diese Entscheidung fällt für viele Systeme aufgrund von begrenztem Wissen über diese schwer.

Die System-Sicherheitsanalyse soll einen Teil der für die Entscheidung über die Sicherheit des Systems notwendigen Daten liefern. Das Ziel aller dieser Anstrengungen muß letztlich die Verbesserung des Systems sein, damit es gesetzten Normen genügt. Wir wollen einige Methoden diskutieren, die Informationen für solche Verbesserungen liefern. Bevor wir jedoch das Thema "System-Sicherheitsanalyse" angehen, sollen die Begriffe Ausfall und System geklärt werden.

2. WAS IST EIN SYSTEM?

In der modernen Technik versteht man unter einem System nicht nur eine Zusammenschaltung von Maschinen, Apparaten, Armaturen u.a. (Hardware), sondern dazu gehören auch Betriebs- und Wartungsvorschriften, Reserveteilhaltung u.a. (Procedures) und die in das System integrierten Menschen (Personal) 1 .

Ein solches technisches System ist durch eine Anzahl Charakteristika gekennzeichnet.

1. Jedes System muß eine Aufgabe (Funktion) erfüllen. Dafür ist es konstruiert.

2. Ein System besteht aus diskreten Elementen. Diese Elemente können wieder Systeme auf einer niedrigeren Ebene sein.

3. Eine Änderung der Funktion eines dieser Elemente erzeugt eine geänderte Systemfunktion.

4. Eine unkontrolliert geänderte Systemfunktion ist ein Versager und kann durch Freisetzung von Energie oder gefährlicher Stoffe zu Schäden an Eigentum und Personen führen.

Von einem sicheren System muß man die folgenden drei Eigenschaften erwarten:

1. Das System soll funktionstüchtig sein,

2. es soll seine Funktion zuverlässig über eine geforderte Zeit erfüllen und

3. das System soll bei Versagern nur einen in akzeptierbaren Grenzen liegenden Schaden verursachen.

Einige Mühe bereitet die Einordnung von Bauteilen in die obigen Festlegungen. Wir treffen daher die folgende Vereinbarung: Systeme sind aus diskreten Elementen zusammengesetzt. Diese Elemente sind wiederum Systeme auf einer niedrigeren Ebene. Bauteile eines Systems sind solche Systeme auf einer niedrigeren Ebene. Sie sind jedoch häufig nicht aus diskreten Elementen aufgebaut. Diese Elemente sind oft so miteinander verbunden, daß ihre Grenzen nicht mehr erkennbar sind (so ist z.B. ein Kreiselpumpengehäuse und der Lagerbock für die Pumpenwelle miteinander vergossen). Oftmals haben einzelne Elemente auch eine Vielzahl von Funktionen. Aus diesen Gründen gestaltet sich eine Entdeckung von Ausfallursachen und die Erforschung der Versagermechanismen äußerst schwierig.

Aus den Überlegungen wird klar, daß das Versagen für die Sicherheit technischer Systeme eine Schlüsselrolle spielt. Wir wollen daher den Versagensmechanismus näher betrachten.

3. WAS IST EIN VERSAGER?

Ein Systemversager liegt immer vor, wenn die vom System erwartete Funktion nicht mehr erbracht werden kann. Das tritt ein, wenn der Systemoutput aus dem vorgeschriebenen Toleranzband herauswandert.

Da die Systemfunktion aus den Funktionen der Elemente erzeugt wird, kann ein Systemversager nur durch das Versagen von einem oder mehreren Elementen hervorgerufen werden.

Wie verhalten sich nun diese Elemente? Wir wollen das am Beispiel eines Bauteils erläutern (Abb. 1). Jedes Bauteil unterliegt einer zeitlich sich ändernden Beanspruchung B. Es ist so konstruiert, daß es dieser Beanspruchung standhält. Es besitzt eine Standfestigkeit S, die größer als die Beanspruchung ist. Die Standfestigkeit gleicher Bauteile ist aufgrund von Herstellungstoleranzen unterschiedlich. Im Mittel haben die betrachteten Bauteilsorten die Standfestigkeit S_2. Im allgemeinen hängt die Standfestigkeit von Bauteilen auch noch vom Alter der Bauteile ab. Durch Abnutzungserscheinungen fällt sie zum Ende der Lebensdauer hin ab (Abb. 1).

Die Beanspruchung B ist über die Betriebszeit statistisch verteilt. Erreicht eine Beanspruchungsspitze die Standfestigkeit eines Bauteils dann fällt es aus (z.B. zur Zeit t_2 in Abb. 1). Liegt die Standfestigkeit hoch genug, dann werden die Beanspruchungsspitzen sie nicht erreichen. Erst ein Abfallen durch Abnutzung macht den Ausfall möglich (z.B. zur Zeit t_1 in Abb.1). Trägt man die Beanspruchung B und die Standfestigkeit S als Häufigkeitskurven auf, so erhält man Abb. 2. Die schraffierte Fläche, die beiden Kurven gemeinsam ist, stellt ein Maß für die Wahrscheinlichkeit des Auftretens einer die Standfestigkeit eines Bauteils übersteigenden Beanspruchung dar. Der Abstand der beiden Mittelwerte ist als Sicherheitsabstand bekannt.

Aufgrund von Beobachtungen lassen sich die Ursachen für Bauteilversager nach 2 in drei Kategorien einordnen:

1. Verschlechterung der Standfestigkeit des Bauteils vor Inbetriebnahme durch schlechte Konstruktion, schlechte Herstellung, schlechte Installation, schlechte Qualitätskontrolle u.a.,

2. Beanspruchung von an sich guten Bauteilen bei höheren, als vorgesehenen Einsatzbedingungen. Dazu gehören Transport, Handhabung, Prüfungen, Betriebs- und Umgebungsbedingungen u.a.,

3. Abnutzungsabhängige Verschlechterungen der Standfestigkeit durch zeitabhängige Abnutzungsmechanismen wie Korrosion, Verschleiß, Ermüdung, Abtragung u.a.

Aus Erfahrung weiß man, daß die Ursachenkategorie 1 doppelt so häufig zum Versagen von Bauteilen führt, wie Ursachenkategorie 3. Die Kategorien 1 und 2 stellen den größten Anteil der Ausfallursachen.

Wir stellen also fest, daß die Zuverlässigkeit von Bauteilen neben den Ermüdungsprozessen im besonderem Maße von den Einflüssen der Produktion und von den Einsatzbedingungen abhängt.

4. SICHERHEIT, RISIKO, ZUVERLÄSSIGKEIT

Nachdem wir uns über den statistischen Charakter des Auftretens von Versagern klar geworden sind, können wir den Zusammenhang zu den Begriffen Zuverlässigkeit, Risiko und Sicherheit herstellen.

Die Zuverlässigkeit ist das Maß für die Häufigkeit von Versagern in einem System, Untersystem oder Bauteil. Sie kann als Wahrscheinlichkeit für das spezifizierte Funktionieren einer Betrachtungseinheit in einer vorgesehenen Zeit ohne Versager aufgefaßt werden.

Das Risiko ist ein Maß für den zu erwartenden Schadensumfang durch das Versagen eines Bauteils, Untersystems oder Systems innerhalb eines betrachteten Zeitintervalls, z.B. ein Kalenderjahr. Mathematisch ist das Risiko eine Schadenserwartung. Sie ist gleich dem Produkt aus Eintrittswahrscheinlichkeit und Schadensumfang eines Versagers.

Sicherheit ist nach 3 die Abwesenheit von gefährlichen Zuständen und Ereignissen in dem betrachteten System. Gemeint sind hiermit Zustände oder Ereignisse, die alleine oder durch anregende Ereignisse zu Versagern mit großen Schäden führen.

Diese Definition eignet sich nur zusammen mit einer weiteren Festlegung darüber was gefährliche Zustände und Ereignisse sind und wieviele man zulassen will zur Beurteilung der Sicherheit eines Systems, Untersystems oder

Bauteils. Trotzdem ist diese Definition sehr nützlich, da sie uns zeigt, wo wir bei der Verbesserung der Sicherheit ansetzen müssen.

Zur Entscheidung über die Sicherheit eines Systems, Untersystems oder Bauteils eignet sich die folgende Definition: Ein System, Untersystem oder Bauteil ist sicher, wenn die zugehörige Schadenserwartung gleich oder kleiner als ein zulässiger Wert ist.

5. SYSTEM-SICHERHEITSANALYSE

Die Sicherheit ist, wie wir gesehen haben, eine abgeleitete Größe. Wir können sie bestimmen über die Schadenserwartung, d.h. über Versagenshäufigkeit und Schadensumfang der Versager.

Informationen über die Schadenshäufigkeiten und den Schadensumfängen eines betrachteten Systems können aus vier verschiedenen Quellen gewonnen werden:

1. Betriebserfahrungen an gleichen oder ähnlichen Systemen,
2. Tests,
3. Analysen,
4. Annahmen.

Natürlich sind Betriebserfahrungen die besten Informationen über das Betriebsverhalten. Tests und Analysen können einmal zum Ziel haben, nachzuweisen, daß keine Probleme mehr vorhanden sind, zum anderen, um neue Probleme zu entdecken (Experimente). Dadurch hängt der Vertrauensgrad für diese Informationen sehr wesentlich von den Testbedingungen bzw. von den benutzten Modellen und von den zugrundeliegenden Absichten und Annahmen ab.

Den geringsten Vertrauensgrad haben Annahmen. Dieser Vertrauensgrad wird praktisch Null, wenn hinter den Annahmen nicht Erfahrungen in der Praxis stehen (die ja wieder Betriebserfahrungen, Testergebnisse oder Analysenergebnisse sein müssen). Trotzdem kommt man in der modernen Technik ohne die Benutzung von Annahmen nicht aus. Sie sollten jedoch nur dann benutzt werden, wenn das unumgänglich ist.

Im folgenden wollen wir uns auf die Diskussion der System-Sicherheitsanalyse beschränken, deren Eingangsdaten natürlich Ergebnisse aus allen vier Informationsquellen sein können. Wir wollen auch auf die beiden Anwendungszwecke

- Nachweis einer vorhandenen Sicherheit und
- Verbesserung der Sicherheit

eingehen. Außerdem wollen wir die Diskussion der Anwendung auf Bauteile beschränken.

5.1 ERHÖHUNG DER SICHERHEIT

Das Ziel der Analyse ist die Verbesserung der Bauteilsicherheit für spezifische Einsatzbedingungen bei möglichst geringem Aufwand. Außerdem sollen gefährliche Ausfallarten konstruktiv beseitigt werden. Wir formulieren die erwarteten Ergebnisse wie folgt:

1. Identifizierung aller möglichen Ausfallarten eines Bauteils,
2. Identifizierung der zu den Ausfallsarten gehörenden Ausfallursachen und Erforschung der Mechanismen, die die Ausfälle erzeugen,
3. Beseitigen der Ausfallarten durch eliminieren der Ursachen oder durch kontrollieren des Ausfallmechanismus.

Je sicherer ein Bauteil sein soll, umso mehr Aufwand muß für die drei Ergebnisse getrieben werden.

Zur Erzeugung der im letzten Abschnitt aufgezählten Resultate kann man verschiedene Techniken anwenden:

1. Durchführung einer reinen Analyse, d.h. aufgrund von Informationen von vergleichbaren Bauteilen gelingt es, die gewünschten Resultate abzuleiten.
2. Anwendung einer kombinierten Test/Analysentechnik, die es gestattet, die Ausfallarten durch Tests zu gewinnen, um dann die Ausfallursachen und -mechanismen zu erforschen. Diese Technik ist jedoch nur mit Hilfe von Tests unter erheblich verschärften Einsatzbedingungen möglich.
3. Durchführung von Massentests über eine lange Zeit unter normalen Einsatzbedingungen. Beseitigung auftretender Mängel und Durchführung neuer Tests.

Die Diskussion dieser Techniken läßt uns sofort die schwerwiegenden Nachteile von 1. und 3. erkennen. Die Technik 1. führt zwangsläufig dazu, daß man bei neuen Bauteilen Ausfallarten übersieht, die gravierende Folgen haben können. Die Technik 3. ist mit enormen Kosten und großem Zeitaufwand verbunden. Am erfolgversprechendsten erscheint uns die zweite Technik zu sein. Sie kommt aus den USA und heißt "Zuverlässigkeitsphysik" (Reliability Physics). Sie löst die Probleme der Zuverlässigkeitsverbesserung von Bauteilen nach 4 in der folgenden Weise:

1. Schaffung von Modellgesetzen, die die Umrechnung von Testergebnissen unter verschärften Einsatzbedingungen des betrachteten Bauteils auf normale Einsatzbedingungen gestattet.

Experimenteller und/oder analytischer Nachweis der Gültigkeit dieser Modellgesetze.

2. Testen der betrachteten Komponenten unter verschärften Einsatzbedingungen, Erzeugung von Ausfällen, Untersuchung der Ausfallursachen, Ausfallmechanismen und Ausfallarten.

3. Detaillierte Untersuchung von neuen, ungewöhnlichen oder unerklärten Ausfallmechanismen.

4. Eliminieren der Ausfallarten der Bauteile mit schwerwiegenden Einfluß auf das vorgesehene System.

Mit Hilfe dieser Technik gelingt es uns, die Zuverlässigkeit von Bauteilen radikal zu erhöhen ohne die Massentests , die andernfalls notwendig wären, um eine hohe Zuverlässigkeit unter vorgesehenen Einsatzbedingungen nachzuweisen und sicherzustellen.

5.2 NACHWEIS DER ERFORDERLICHEN SICHERHEIT

Zum Nachweis der erforderlichen Sicherheit von Bauteilen ist das folgende Ergebnis zu erbringen:

Die Eintrittswahrscheinlichkeiten der Ausfallarten des Bauteils liegen unter den geforderten Werten.

Durch die System-Sicherheitsanalyse des zugehörigen Systems werden die Ausfallarten des Bauteils identifiziert, die zu schweren Schäden am Bauteil oder System führen. Ihnen werden aufgrund der Schadensumfänge die ihrem Eintreten folgen, maximale Eintrittswahrscheinlichkeiten zugewiesen.

Die Sicherheit eines Bauteils kann also nicht allgemeingültig formuliert werden, sondern hängt von der jeweiligen Verwendung des Bauteils in einem System ab.

Für Bauteile ist es üblich, nicht die Eintrittswahrscheinlichkeiten, sondern die Ausfallraten für die einzelnen Ausfallarten zu bestimmen.

Zur Führung dieses Nachweises kann man verschiedene

Analysentechniken oder

Testtechniken

benutzen. Analysen setzen ein zutreffendes Modell des Ausfallmechanismus (z.B. Bruchmechanik) voraus, das dann analysiert wird. Ein solches Analysenmodell muß jedoch durch Tests gesichert sein.

Tests zum Nachweis der Ausfallrate eines Bauteils können als Massentests unter Betriebsbedingungen oder als Tests unter verschärften Einsatzbe-

dingungen ist jedoch die Kenntnis der Modellgesetze, die die Übertragung der Testergebnisse auf Betriebsbedingungen gestatten. Diese Modellgesetze müssen experimentell gesichert sein.

6. INFORMATIONSSYSTEM

Wie eingangs bereits erwähnt wurde, sind eine große Anzahl von Daten, die in die System-Sicherheitsanalyse eingegeben werden, erforderlich.

Neben den Daten für die Konstruktion und Funktion des Bauteils selbst interessieren die Ergebnisse aus Betriebsbeobachtungen, Tests und Analysen an ähnlichen und gleichen Bauteilen. Für die Analysen sind die folgenden Daten besonders wichtig:

1. Ausfallarten und deren Ursachen
2. Ausfallraten für die Ausfallarten
3. Störfälle an gleichen und ähnlichen Bauteilen im Betrieb
4. Ausfallraten der Konstruktionselemente des Bauteils für deren Ausfallarten
5. Maßnahmen zur Beseitigung von Ausfallarten oder zu deren Kontrolle.

Alle diese Daten sollten in Dateien gesammelt werden und für die Analysen zur Verfügung stehen.

7. SYSTEM-SICHERHEITSPROGRAMM

Bisher wurden die Sicherheitseigenschaften der Bauteile, Untersysteme und Systeme als gegeben angenommen. Diese Annahme ist jedoch unbegründet und nicht haltbar, da auch die Bauteile, Untersysteme und Systeme konzipiert, detailliert, produziert, transportiert, montiert und in Betrieb genommen werden. Nur eine strenge Kontrolle aller dieser Phasen in Bezug auf die Einhaltung der sicherheitstechnischen Forderungen macht ein Endprodukt wahrscheinlich, wie wir es geplant haben. Im Qulitätswesen sind solche Kontrollen seit langem Gang und Gäbe.

Wir müssen daher ein System-Sicherheitsprogramm fordern, daß die Herstellung von Erzeugnissen entsprechend den Sicherheitsforderungen sicherstellt. Dieses System-Sicherheitsprogramm muß in das Gesamtprojekt integriert werden. Nur so wird es uns gelingen, unserem Sicherheitsziel mit großer Wahrscheinlichkeit nahe zu kommen.

Zur Durchführung des System-Sicherheitsprogrammes ist es notwendig, einen Plan aufzustellen. Dieser Plan sollte im einzelnen die folgenden Punkte enthalten:

1. Beschreibung der für die Systemsicherheit verantwortlichen Organisation. Insbesondere sollten die Kompetenzen und Verantwortlichkeiten der Mitglieder dieser Organisation festgelegt werden.

2. Terminplan für die Systemsicherheit. Er sollte u.a. Termine für Programmüberprüfungen, Forderungs- und Konstruktionsüberprüfungen, für die Fertigstellung von Analysen, für Tests und Rechenschaftsberichte enthalten.

3. Eins der wichtigsten Kapitel des Plans muß die anzuwendenden Maßstäbe für die Sicherheit enthalten, wie z.B. Gesetze, Richtlinien, Verordnungen, Vorschriften, Spezifikationen u.a.

4. Sehr wichtig erscheint ebenfalls, die für den Nachweis der Sicherheit anzuwendenden Analysentechniken anzugeben. Hier sollten Analysentechniken benannt werden, die den genannten Bereichen des Systemlebens überdecken und die gemeinsam eine gute Siebwirkung für gefährliche Elemente und Zustände haben.

5. Der Plan muß einen Datendienst enthalten, der die Forderungen nach Daten, Berichten usw. erfüllen kann. Hierzu gehört das Sammeln, speichern und auswerten von Daten wie Betriebsdaten, Konstruktionsdaten, Vorschriften, Berichte usw.

6. Der Plan sollte ebenfalls Bestimmungen für die Ausbildung, für das Training und für die Qualifikation von Personal enthalten.

7. Besondere Beachtung verdienen im System-Sicherheitsprogrammplan die Sicherheitstests, ob im Labor, am Modell oder am fertigen System. Hierbei ist auch die Sicherheit des Tests selbst zu beachten.

8. Der Plan sollte genaue Bestimmungen über die Durchführung von Programmüberprüfungen, Rechenschaftsablegungen und den Informationsfluß enthalten.

In den USA sind solche System-Sicherheitsprogramme seit langem in Anwendung. Ein Beispiel hierfür sei der Military Standard MIL-STD 882. Er ist für alle vom Department of Defense vergebenen Aufträge bindend.

8. SCHLUßFOLGERUNGEN

Wir gehen bei den folgenden Betrachtungen davon aus, daß Sicherheit die Abwesenheit von gefährlichen Zuständen und gefährlichen Ereignissen im betrachteten System bedeutet.

Durch die in der konventionellen Technik übliche Ursachenermittlung nach Störfällen versuchte man anfangs diese Ursachen zu eliminieren. Man ver-

suchte das System sicherer zu machen, ohne es gänzlich zu verstehen.

Die Nachteile dieses Verfahrens, nämlich daß Störfälle erst auftreten müssen, versuchte man durch das MCA-Konzept in der Kerntechnik zu umgehen. Man untersuchte mögliche Störfälle vor der Errichtung des Systems, obwohl man dieses System nicht in allen Einzelheiten verstand. Dadurch verlor man jedoch die Möglichkeit, gefährliche Zustände und Ereignisse im System direkt zu finden. Die Beurteilung des Systems gründete sich auf eine ganze Reihe von Annahmen. Die schwerwiegendste ist die, daß man einen Störfall als größten anzunehmenden Unfall festlegte.

Den Nachteil, einen GaU festlegen zu müssen, will man nun durch die Anwendung des Risikokonzeptes beseitigen. Dadurch kommen wir unserer Aufgabe, das System frei von gefährlichen Zuständen und Ereignissen zu machen, jedoch nicht näher. Die Anwendung des Risikokonzeptes ist nämlich gleichbedeutend mit der Frage: Wie wahrscheinlich ist ein Störfall und welche Auswirkungen hat er? Die einzige Schlußfolgerung hieraus kann nur sein: Wie mache ich den Störfall unwahrscheinlicher? Es muß deshalb bezweifelt werden, ob das Risikokonzept, wie es sich heute darstellt, in der Lage ist, unsere Sicherheitsprobleme zu lösen.

Es ist ganz offensichtlich notwendig, zum Ausgangspunkt der Diskussion zurückzukehren. Sicherheit, d.h. Freiheit von gefährlichen Zuständen und Ereignissen, kann nur erzielt werden, wenn man konsequent und systematisch mit effektiven Methoden diese Zustände und Ereignisse aufdeckt und eliminiert. Ist das nicht möglich, so ist die nächst schlechtere Lösung eine wirksame Kontrolle dieser Ereignisse und Zustände. Die letzte und bei weitem die schlechteste Lösung wäre, die gefährlichen Zustände und Ereignisse so unwahrscheinlich in ihrem Auftreten zu machen, daß man die Schadenserwartung daraus möglicherweise resultierender Störfälle akzeptieren kann. Das Unbehagen über diese letzte Lösungsmöglichkeit verspürt man auf Schritt und Tritt, wenn man die Auseinandersetzung um das Bersten eines Reaktordruckbehälters verfolgt. Dieses Unbehagen konnte auch durch das ins Feld geführte Risikokonzept aus den oben diskutierten Gründen nicht beseitigt werden. Vielmehr diskutiert man zur Zeit die Möglichkeit, das potentielle gefährliche Ereignis des Druckbehälterberstens durch eine Sollbruchstelle zu kontrollieren.

Wir kommen in unseren Bemühungen sicherlich einen großen Schritt voran, wenn wir neben den starren Systemmodellen, die im GaU- und Risikokonzept enthalten sind, auch andere, flexiblere zulassen. Bevor wir jedoch in die Diskussion über Modelle eintreten, ist es notwendig, das System, von dem wir ein Modell erstellen wollen, genau zu kennen und möglichst gut zu verstehen. Diese Kenntnisse lassen sich durch die Anwendung einer Systemanalyse erwerben. Die Systemanalyse sollte folgende Punkte enthalten:

1. Ziele des Gesamtsystems und Maßstäbe für die Leistung des Systems,

2. zwingende Umweltbedingungen,

3. Hilfsquellen des Systems,

4. Komponenten des Systems, ihre Funktionen, Ziele und Leistungsmaßstäbe und

5. das Managementsystem.

Mit dieser detaillierten Kenntnis des Systems versuchen wir nun ein Modell des Systems zu entwerfen, dessen Auswertung eine gleich gute Chance für die Auffindung von gefährlichen Zuständen und Ereignissen in allen Bereichen des Systems (Konstruktion, Produktion, Transport, Installierung, Tests, Prüfungen, Koordination, Betrieb usw.) bietet. In den meisten Fällen wird diese Siebwirkung jedoch nur mit Hilfe mehrerer verschiedener Modelle zu verwirklichen sein. Einige dieser möglichen Modelle sind im vorliegenden Bericht diskutiert worden.

Die Effektivität dieser Modelle hängt wesentlich von den zur Verfügung stehenden Informationen aus Betriebsbeobachtungen, Tests und vorhergehenden Analysen ab. Es ist deshalb dringend notwendig, alle diese Informationen schnell greifbar aufzubewahren. Insbesondere müssen die bisher kaum genutzten Betriebsbeobachtungen aktiviert werden, da sie die wertvollsten Informationen für die Beurteilung der Sicherheit von Systemen darstellen.

LITERATUR

1 WEST CHURCHMANN,C., "Einführung in die Systemanalyse" Verlag Moderne Industrie, 1970.

2 WRIGHT,L.W., "An Overview of Electronic Part Failure Analysis Experience IEEE Trans. on Reliability", Vol. R-17, No. 1, March 1968.

3 Military Standard Requirements for System Safety Program for Systems and Associated Subsystems and Equipment SIXTH DRAFT PROPOSED MIL-STD-882.

4 JACOBI,G.T., "Reliability Physics, IEEE Trans on Reliability" Vol. R-17, March 1968

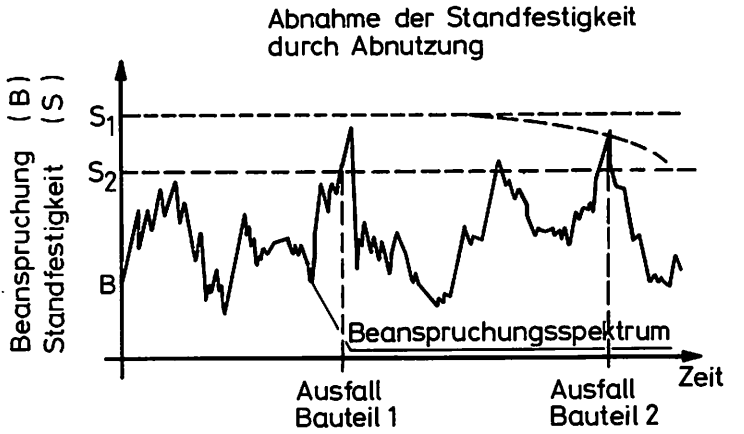

Abb. 1

Ausfallwahr-
scheinlichkeit

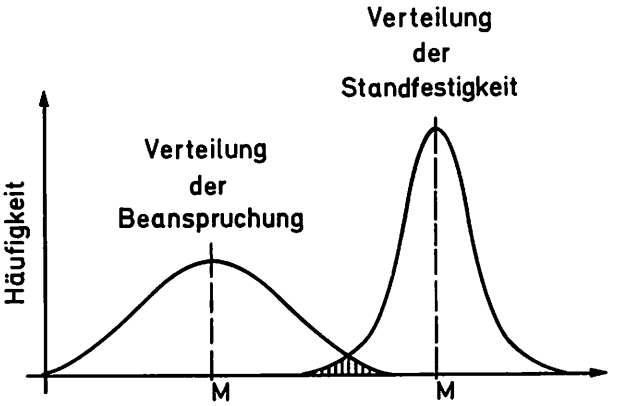

Abb. 2

Beanspruchung (B)
Standfestigkeit (S)

Ausfallwahr=
scheinlichkeit

DISCUSSION

Q Z. J. DORON, Belgium

Have you tested the two types of valves discussed and verified the improved reliability ? It would be interesting to have the experimental confirmation which would "close the loop".

A G. MIEZE, Germany

The first valve has been tested. If the redesigned valve is accepted to replace the original valve it certainly also will be tested.