KfK 2999
August 1980

Methoden der Systemplanung bei gefordertem Langzeitbetriebsverhalten

Bericht über ein zweitägiges Seminar am 26. und 27. Februar 1980 in Karlsruhe, Bundesrepublik Deutschland

F. Fischer, W. Haußmann, G. Weber
Institut für Datenverarbeitung in der Technik
Projekt Wiederaufarbeitung und Abfallbehandlung
Projekt Nukleare Sicherheit

Kernforschungszentrum Karlsruhe

KERNFORSCHUNGSZENTRUM KARLSRUHE

Institut für Datenverarbeitung in der Technik

Projekt Wiederaufarbeitung und Abfallbehandlung
Projekt Nukleare Sicherheit

KfK 2999

"Methoden der Systemplanung bei gefordertem Langzeitbetriebsverhalten"

Bericht über ein zweitägiges Seminar
am 26. und 27. Februar 1980 in Karlsruhe,
Bundesrepublik Deutschland

Herausgeber: F. Fischer
W. Haußmann
G. Weber

Kernforschungszentrum Karlsruhe GmbH, Karlsruhe

Kernforschungszentrum Karlsruhe GmbH
ISSN 0303-4003

Zusammenfassung

Im Rahmen der zweitägigen Diskussionssitzung "Methoden der Systemplanung bei gefordertem Langzeitbetriebsverhalten" (am 26. und 27. Februar 1980) im Institut für Datenverarbeitung in der Technik (IDT) des Kernforschungszentrums Karlsruhe (KfK), Bundesrepublik Deutschland, wurden in acht Übersichtsvorträgen und darauf folgenden Diskussionen folgende Schwerpunkte behandelt:

- der heutige Stand der Zuverlässigkeits-Praxis,
- die Bedürfnisse der Praxis nach verbesserter Methodik und/oder verbesserten Daten,
- der Stand der Theorie heute sowie der Informationsbedarf aus der Praxis.

Die Systemplanung bei gefordertem Langzeitbetriebsverhalten stützt sich auf die Methoden der Zuverlässigkeit, Sicherheit, Verfügbarkeit und Instandhaltung. Weiterhin ist es sehr wichtig, den Lebenszyklus eines Systems - also die Phasen des Entwurfs, der Entwicklung, der Prüfung, Konstruktion und die Phasen des Betriebs - zu verfolgen. Mit wachsender Komplexität von Systemen müssen häufig neue Methoden für den Entwurf und die Analyse entwickelt werden. Die Datenverarbeitung ist hierbei oft selbst ein wichtiger Systembestandteil, zum anderen dient sie aber auch als ein notwendiges Hilfsmittel der Analyse. Beide Aspekte der Datenverarbeitung wurden in der Diskussionssitzung angesprochen. Der vorliegende Bericht gibt alle Übersichtsvorträge und Diskussionen wieder.

Methods for System Planning under a Specified Long Term Operation Behavior

Abstract

In the two days workshop on 'Methods for System Planning under a Specified Long Term Operation Behavior' (February 26-27, 1980) in the Institut für Datenverarbeitung in der Technik (IDT) of the Kernforschungszentrum Karlsruhe (KfK), Federal Republic of Germany, the following questions have been emphasized in eight review papers and subsequent discussions:

- Approaches and Methods in reliability as used by practitioners.
- Need for improved methods and/or improved data from practitioners.
- Theory today compared to the requirements for information from practitioners.

System planning under a specified longterm operation behavior is based on methods of reliability, safety, availability, and maintainability. Thus it is very important to follow the life cycle of a system, i.e. the phases of design, development, tests and contruction as well as the phases of operation. With the increasing complexity of systems it is often required to develop new methods for design and analysis. Here data processing is on the one hand itself an important part of the system, on the other hand it is a crucial step in many types of analysis. Both aspects of data processing have been emphasized in this workshop. This report contains all papers presented and also the subsequent discussions.

I n h a l t

Seite

Einführung

zum zweitägigen Seminar

"Methoden der Systemplanung bei gefordertem Langzeitbetriebsverhalten"

von

R. Avenhaus und H. Trauboth

Das Institut für Datenverarbeitung in der Technik des Kernforschungszentrums Karlsruhe nimmt eine Stellung zwischen Industrie und Hochschule ein: Seine Mitarbeiter bearbeiten reale Probleme der Kerntechnik und der Datenverarbeitung, und sie entwickeln Methoden und Werkzeuge zur Lösung dieser Probleme. Mit dieser Stellung und dieser Arbeitsweise wird ein Brückenschlag zur Überwindung der oft nicht unerheblichen Kluft zwischen Theorie und Praxis angestrebt.

Seit mehreren Jahren werden im Institut für Datenverarbeitung in der Technik Zuverlässigkeits- und Verfügbarkeitsanalysen technischer Systeme durchgeführt. Im Rahmen dieser Tätigkeiten wurden im Sinne der genannten Ausrichtung des Institutes sowohl methodologische Arbeiten erstellt als auch praktische Anwendungen im Bereich der Kerntechnik behandelt. Da es sich zeigte, daß einerseits die Methodenentwicklung schon sehr weit, aber nicht immer in eine die Praxis interessierende Richtung fortgeschritten ist, und daß andererseits in der Industrie konkrete Probleme bei der Systemplanung häufig ohne zureichende Kenntnis der verfügbaren Methoden gelöst werden, erschien es sinnvoll und nützlich, in einem Arbeitskreis einmal zu diskutieren,

- in welchem Umfang Praktiker heute von den verfügbaren Methoden Gebrauch machen,
- inwieweit von der Praxis her ein Bedürfnis nach erweiterten, verfeinerten bzw. vereinfachten Methoden besteht, und
- wo die Methodenentwicklung heute steht bzw. welche Daten und Informationen aus der Praxis für sie wichtig wären.

Aus diesem Grunde wurde im Sommer 1979 geplant, im Institut für Datenverarbeitung in der Technik ein zweitägiges Seminar zu diesen Fragen zu veran-

stalten, wobei acht Übersichtsvorträge zu den folgenden Gebieten vorgesehen wurden:

- Einführung

  1. "Beitrag der Qualitäts- und Zuverlässigkeitssicherung zur Systemwirksamkeit"

     . Grundbegriffe, insbesondere Langzeitbetriebsverhalten
     . Unternehmerische Zielsetzung
     . Qualitäts- und Zuverlässigkeitssicherung

- Erfahrungen aus verschiedenen Bereichen der Technik

  2. "Nutzung von Schadens- und Zuverlässigkeitsdaten in Zuverlässigkeitsmodellen zur Systemplanung von Kraftwerksanlagen"

     . Betriebs- und Ausfalldatenerfassung
     . Verwendung von derartigen Daten beim Bau neuer Kraftwerke
     . Komplexität, Großkomponenten, Organisatorische Fragen, Instandhaltung im Rahmen der Systemplanung

  3. "Praktische Zuverlässigkeitsrechnung und Qualitätssicherung"

     . Zuverlässigkeit langlebiger Systeme am Beispiel der Satellitentechnik
     . Ausfallart- und Effektanalyse als Hilfsmittel der Produktsicherung
     . Vorgehen bei Systemen, die sehr komplex und nicht wartbar sind

  4. "Zuverlässigkeitsanalysen im Rahmen der Begutachtung von Kernenergieanlagen"

     . Anforderungen und Spezifikation
     . Formale Einbindung von Zuverlässigkeitsanalysen bei der Erstellung von Gutachten
     . Nachweis und Dokumentation der Zuverlässigkeit

- Methoden für verschiedene Bereiche der Technik

  5. "Verfügbarkeits- und Kapazitätsplanung für Prozeßsysteme mit Zwischenlagern"

     . Untersuchung der Verfügbarkeit und
       Effektivität bei in der Planung befindlichen Systemen

. Anwendung von analytischen Verfahren und von Simulationsprogrammen

6. "Analytische Modelle für Zuverlässigkeitsuntersuchungen von Kraftwerkssystemen"

   . Untersuchung komplexer EVU-Systeme

   . Planung im Kurz-, Mittel- und Langzeitbereich beim Einsatz von EVU-Systemen

7. "Analytische und simulative Verfahren zur Berechnung der Zuverlässigkeitsmerkmale komplexer Systeme"

   . Auswertung von Fehlerbäumen mit analytischen bzw. Monte Carlo Methoden

   . Vergleich der Leistungsfähigkeit dieser Methoden

8. "Software-Zuverlässigkeit"

   . Gemeinsamkeiten und Unterschiede bei Hardware- und Software-Zuverlässigkeit

   . Erhöhung der Zuverlässigkeit durch Methoden der Softwareredundanz

   . Wartung der Software für Langzeitbetriebsverhalten

Im Sommer und Herbst gelang es den mit der Organisation des Seminars betrauten Mitarbeitern des Institutes, den Herren Dr. F. Fischer, Dipl.Wi.-Ing. W. Haußmann und Dr. G. Weber, kompetente Persönlichkeiten aus Forschung und Technik für Vorträge und Diskussionen zu gewinnen. Das Seminar fand am 26. und 27. Februar 1980 in den Institutsräumen statt; ohne Übertreibung läßt sich sagen, daß im Laufe dieser zwei Tage in ausgezeichneter Arbeitsatmosphäre ein hohes Maß von gegenseitiger Information erreicht wurde.

Im folgenden sind die schriftlichen Fassungen der Vorträge und der im Anschluß an die Vorträge erfolgten Diskussionen wiedergegeben.

BBC BROWN BOVERI

Seminar "Methoden der Systemplanung bei gefordertem Langzeitbetriebsverhalten"

26./27. Februar 1980 im
Institut für Datenarbeitung
in der Technik,
Kernforschungszentrum Karlsruhe

DER BEITRAG DER QUALITAETS- UND ZUVERLAESSIGKEITSSICHERUNG ZUR SYSTEMWIRKSAMKEIT

DR. HEINZ H. FREY

BROWN BOVERI & CIE

BADEN, SCHWEIZ

1. EINFUEHRUNG

In den meisten Lebensbereichen des Menschen, aber speziell in der Technik, haben Begriffe wie Qualität, Zuverlässigkeit, Sicherheit und Verfügbarkeit vergleichsweise bereits einen hohen Stellenwert erhalten und ihre Bedeutung dürfte auch in Zukunft weiterhin zunehmen. Die Erfahrung mag gezeigt haben, wie ärgerlich es ist, wenn z.B. das Auto nicht anspringen will oder sich in der Reparaturgarage befindet (d.h. nicht verfügbar ist), wenn während einer Fahrt eine Panne passiert (d.h. die Zuverlässigkeit zu wünschen übrig lässt), wenn die Bremsen versagen (d.h. neben der Zuverlässigkeit auch die Sicherheit ungenügend ist) oder wenn zB. Innenverkleidungen lose werden (d.h. die Ausführungsqualität Wünsche offen lässt.) Manch einer hat sich in solchen Situationen schon gefragt, ob der Aufwand bzw. die Gesamtkosten seines Autos irgendwie im Verhältnis zum Nutzeffekt stehen (d.h. die Systemwirksamkeit seines Autos befriedigend ist). [1]

2. UNTERNEHMERISCHE ZIELSETZUNG UND SYSTEMWIRKSAMKEIT

Verminderte Qualität, Zuverlässigkeit, Sicherheit und Verfügbarkeit bedeuten Reklamationen, Umtriebe, Ausfälle, Gefährdung von Personen, Sachen und Umwelt, Unfälle, Schäden, Zeitverlust, verminderte Nutzung und somit Unkosten und Verluste. Anderseits bedeutet eine Forderung nach zu hoher Qualität, Zuverlässigkeit, Sicherheit und Verfügbarkeit unnötigen Aufwand bzw. erhöhte Herstellungs-, Betriebs- und Instandhaltungskosten. Das Ziel eines Unternehmens ist es folglich, Anlagen, Geräte und deren Komponenten so zu planen, zu entwickeln, zu fabrizieren und zu betreiben bis zur Ausserbetriebsetzung, dass der Gesamtnutzen maximal und der erforderliche Aufwand minimal wird.
Für den Hersteller bedeutet diese Zielsetzung die Planung und Realisierung eines Produktes oder Systems in der Weise, dass neben der Erfüllung der Forderungen des Kunden, des Marktes und des Gesetzes ein wirtschaftlicher Betrieb sowie die Instandhaltung und die logistische Unterstützung bis zur

Ausserbetriebsetzung gewährleistet sind. Dabei übernimmt der Betreiber die Verantwortung für die korrekte, sichere Betriebsführung des Systems und dessen ordnungsgemässe Instandhaltung, damit die Leistungsfähigkeit (performance) über der gesamten Nutzungsphase bei minimalem Aufwand erhalten bleibt. Fig. 1. Die Beurteilung und Bewertung des Nutzeffektes und Aufwandes eines technischen Systems über den gesamten Lebenszyklus geschieht zweckmässigerweise mittels des Begriffes der Systemwirksamkeit. Die Unterbegriffe der Systemwirksamkeit und deren gegenseitige Beziehung sind in Fig. 2 dargestellt. (Für Details siehe [2]). Der Nutzeffekt wird mittels der operationellen Wirksamkeit und der Aufwand oder wirtschaftliche Aspekt mittels der Lebenszykluskosten erfasst. Man erkennt aus Fig. 2 dass die Verfügbarkeit, Zuverlässigkeit, Instandhaltung, logistische Unterstützung und die Sicherheit, welche normalerweise als Kenngrössen spezifiziert sind, einen wesentlichen Beitrag zur operationellen Wirksamkeit beitragen. Die 'performance' kann als Momentaufnahme aufgefasst werden, und die Kenngrössen, Verfügbarkeit, Zuverlässigkeit usw. erfassen die zeitliche Entwicklung der Performance-Parameter (Langzeitbetriebsverhalten). [2]
Die Sicherung der Systemwirksameit erfordert eine sich über den gesamten Lebenszyklus erstreckende Organisation, die 'Qualitätssicherung', mit dem eindeutig festgelegten Verantwortungsbereich der Festlegung der Massnahmen und Wahrnehmung der daraus resultierenden Aufgaben. D.h., das Massnahmenpaket zur Spezifizierung. Planung, Erzeugung und Aufrechterhaltung einer bestimmten Systemzuverlässigkeit, Systemsicherheit und Systemverfügbarkeit sowie der Ausführungsqualität (Güte) bildet einen integrierenden Bestandteil der Planungs-, Realisierungs- und Nutzungsphase.
Neben anderen technischen Systemen kommt der Qualitätssicherung von elektronischen und leistungselektronischen Systemen und Anlagen eine besondere Bedeutung zu, da diese oftmals zentrale Funktionen (Steuern, Regeln, Datenübertragung, Datenerfassung und -verarbeitung usw.) in hierarchisch aufgebauten Systemen versehen.
Die eher neuen Marktforderungen verlangen von jedem Hersteller komplexer (Elektronik) Systeme und -anlagen während der Konzeptions-, Entwicklungs-

und Fabrikationsphase die Durchführung von zusätzlichen Massnahmen zur Sicherstellung der geforderten Leistungsfähigkeit, Sicherheit, Zuverlässigkeit und Verfügbarkeit. Die Sicherung dieser Eigenschaften wird mittels des Qualitäts-Sicherungssystems des Herstellers erreicht. Dagegen ist die Erhaltung dieser Eigenschaften während der Einsatzphase meistens Sache des Betreibers, wobei dieser auf die logistische Unterstützung (Service, etc.) des Herstellers baut. (Begriffe und Definitionen siehe Anhang).

3. QUALITAETSANFORDERUNGEN DER PRODUKTE

Die Qualitätsanforderungen bzw. das geforderte Langzeitbetriebsverhalten (Zuverlässigkeit, Sicherheit, Verfügbarkeit), sowie Forderungen bezüglich Instandhaltung und logistische Unterstützung über die Nutzungsdauer sind, abhängig vom Einsatzgebiet von Elektroniksystemen, recht verschieden.

Die Qualitätsanforderungen an Elektronikprodukte für den Einsatz in Sicherheitssystemen von Kernkraftwerken zählen zu den strengsten. Die Anforderungen sind weitgehend durch ein internationales und nationales Normenwerk und gesetzliche Vorschriften festgelegt; z.B. [3]. Die geforderte Nutzungsdauer beträgt dabei meist 40 Jahre während deren die spezifizierten Systemeigenschaften (Leistungsfähigkeit, Sicherheit, Zuverlässigkeit, Verfügbarkeit) erhalten bleiben, bzw. erhaltbar (Instandhaltung, Logistik) sein müssen.

Die Forderungen an das zu erwartende Langzeitbetriebsverhalten eines Systems werden durch 'Systemanalysen' (z.B. [4]-[6], Fig. 3 und 4) und 'Qualifikationsprüfungen', welche in internationalen Normen und projektspezifischen Vorschriften festgelegt sind, überprüft (z.B. IEEE Std 323 und 381, [3]).

In technischen Systemspezifikationen erscheinen die Zuverlässigkeit, Systemausfallrate, mittlere ausfallfreie Betriebszeit (MTBF), die Sicherheit, die Verfügbarkeit und ihre begleitenden Kanngrössen wie minimales Wartungsintervall, max. Wartungs- und Reparaturdauer, etc, als quantitative Kenngrössen für die Spezifikation des Langzeitbetriebsverhaltens eines

Systems. Diese Kenngrössen auferlegen den Systemplanern und Entwicklern bestimmte Grenzen in der Wahl und Ausnutzung der Systemkomponenten, Bauteile und Materialien und erfordern möglicherweise strukturelle Massnahmen (Redundanz, Ueberwachung, etc.). Sie bedeuten somit je nach Spezifikation harte Bedingungen. [4] - [6].

Daraus ist zu ersehen, dass bei hohen Qualitätsanforderungen, aufgrund des Einsatzes von hochzuverlässigen Komponenten, redundanten Funktionspfaden, etc. sowie des höheren Entwicklungs-, Fabrikations- und Prüfaufwandes, entsprechend hohe Beschaffungskosten erwachsen. Zudem ist die Erhaltung einer hohen Zuverlässigkeit, Sicherheit oder Verfügbarkeit zumeist mit entsprechend hohen Instandhaltungskosten verbunden.

4. QUALITAETSSICHERUNGSSYSTEM

Wie vorgängig bereits erwähnt, sind für Produkte mit hohen Zuverlässigkeits- und Qualitätsanforderungen über eine blosse Endprüfung eines Produktes hinaus, zusätzliche zuverlässigkeits-, sicherheits- und gütesichernde Massnahmen vom Hersteller zu treffen (Dokumentation, Qualitätssteuerung, Fehlerverhütung). Dies ist einerseits zur Sicherstellung der geforderten Leistungsfähigkeit und des Langzeitbetriebsverhaltens eines Produktes notwendig und andererseits, um Vertragspartnern, gesetzlichen Körperschaften und gegebenenfalls Benutzern und Umwelt das notwendige Vertrauen bzw. den Nachweis für die Befolgung der notwendingen Sorgfaltspflicht und Vorschriften auf einer wirtschaftlichen Basis zu erbringen.

Die Struktur eines Qualitätssicherungssystems ist wiegehend, einigermassen einheitlich in internationalen Normen festgelegt [7] [8]. Alle diese QS-Systeme basieren auf grundsätzlich 16 QS-Systemfunktionen, welche einzelne Massnahmenpakete zur Sicherung der Qualität umfassen. Einige der QS-Systemfunktionen bzw. Massnahmen sind direkt einzelnen Projektphasen zuzuordnen (projektphasenabhängig). Jedoch sind die meisten der Massnahmen bzw. Aktivitäten von grundlegendem Charakter und gelten gleichsweise für verschiedene Projektphasen (projektphasenunabhängig).

Als Beispiel sind die Systemfunktionen einiger QS-Systeme aufgeführt Tabelle I :

CSA Z 299.1:	10 CFR 50, Appendix B:	BBC - QS - Handbuch:
1. Contract Review	(1. Organization)	1. Vertrag, Pflichtenheft, Bestellung
2. Design Control	2. Quality Assurance Program	2. Entwicklung
3. Document Control	3. Design Control	3. Technische Stammunterlagen
4. Measuring and Testing Equipment	4. Procurement Document Control	4. Beschaffungsunterlagen
5. Purchasing	5. Instructions, Procedures and Drawings	5. Zulieferungen und Dienstleistungen
6. Incoming Inspection	6. Document Control	6. Identifizierung
7. Inprocess Inspection	7. Control of Purchased Material, Equipment and Services	7. Spezielle Fertigungsverfahren
8. Final Inspection	8. Identification and Control of Materials, Parts and Components	8. Fertigung
9. Inspection Status	9. Control of Spezial Processes	9. Endprodukt
10. Identification and Traceability of Items	10. Inspection	10. Mess- und Prüfmittel
11. Handling and Storing Items	11. Test Control	11. Lagerung, Transport, Versand
12. Manufacturing and Construction	12. Control of Measuring and Test Equipment	12. Prüfstatus
13. Special Processes	13. Handling, Storage and Shipping	13. Fehlerhafte Einheiten
14. Preservation, Packaging and Shipping	14. Inspection, Test and Operating Status	14. Korrekturmassnahmen
15. Quality Records	15. Nonconforming Materials, Parts or Components	15. Qualitätsnachweise
16. Nonconforming Items	16. Corrective Action	16. Qualitätsberichterstattung
17. Customer Supplied Items	17. Quality Assurance Records	
18. Corrective Action	(18. Audits)	

Tabelle I: QS-Systemfunktionen verschiedener QS-Systemnormen

Diese Systemfunktionen bedürfen in einer bestimmten Firmenorganisation und für ein gewisses Produktesortiment einer näheren Definition in der Form von Qualitätssicherungsverfahren (QSV) und Ausführungsvorschriften (Qualitätshandbücher).

Die Wirksamkeit eines Qualitätsicherungssystems wird periodisch auf dessen Vollständigkeit, Wirtschaftlichkeit und Implementationsgrad mittels eines 'Q-Audits' überprüft. Die Wirksamkeit der getroffenen QS-Massnahmen zeigt sich aufgrund der Qualitätskosten während der Herstellphase und den erfassten Betriebs- und Ausfalldaten sowie -kosten während der Nutzungsphase (Optimierung des Nutzen/Aufwandverhältnisses bzw. der Systemwirksamkeit).

Ein QS-System umfasst somit folgende grundsätzliche Elemente:

- QS-Organisation (QS-System)
- QS-Systemfunktionen (Ablauforganisation, QSV)
- Q-Audit
- QS-Dokumentation (QS-Handbücher, etc.).

5. QUALITAETSSICHERUNGSMASSNAHMEN FUER ELEKTRONIKPRODUKTE

Schliesslich stellen sich die Fragen, welche QS-Massnahmen werden zu welchem Projektzeitpunkt und mit welcher Intensität für die Zuverlässigkeits- und Qualitätssicherung von Elektronikprodukten angewendet. Bei der Beantwortung dieser Fragen müssendie spezifischen Merkmale, Anwendungsgebiete und Einsatzbedingungen der Elektronik berücksichtigt werden.

Wesentliche Merkmale von informations- und leistungselektronischen Systemen sind z.B. die Komplexität (Hardware, Software),die Vielzahl der Bauteile und Verbindungen, sowie die Beeinflussbarkeit durch äussere Einwirking (EMC, etc.). Diesen Merkmalen muss bereits bei der Systemplanung und dem Schaltungsentwurf Rechnung getragen (Zuverlässigkeits- und Sicherheitsplanung [4] - [6], Fig. 4, sowie in der Fabrikations- und Prüfphasen geeignete Qualitätssicherungsmassnahmen vorgesehen werden.

Figur 5 gibt eine vereinfachte Darstellung der Zusammenhänge zwischen Lebenszyklusphasen eines Elektronikproduktes und Art und Intensität der Zuverlässigkeits- und Qualitätssicherungsmassnahmen über den gesamten Lebenszyklus. Dabei sind die wichtigsten (projektphasenabhängigen) QS-Massnahmen in etwa chronologischer Reihenfolge aufgeführt. Die Markierungen in der QS-Matrix stellen die Intensität oder das relative Gewicht in der betreffenden Lebenszyklusphase dar.

Die projektphasenunabhängigen QS-Massnahmen sind vertikal zu den projektphasenabhängigen QS-Massnahmen mit der relativen Gewichtung aufgezeichnet (vertikale Systemfunktionen). Z.B., ist die 'Dokumentation' und die daraus hervorgehenden 'Qualitätsnachweise' in jeder Projektphase sowie der Nutzungsphase von grundlegender Wichtigkeit. In der Entwicklungsphase kann es beispielsweise das Resultat einer Zuverlässigkeits- oder Sicherheitsanalyse

(Entwurfsüberprüfung) sein, in der Fabrikationsphase Kontrollkarten und Prüfrapporte und in der Nutzungsphase die Betriebs- und Ausfalldaten-statistik, etc.

D.h. in jeder Projektphase bzw. einem bestimmten Zeitpunkt sind spezifische produkt- oder prozessbezogenen Aufgaben wahrzunehmen (z.B. Erstmuster-prüfung), welche durch die vertikalen Systemfunktionen jeweils ergänzt werden (z.B. Dokumentation und periodische Kalibrierung und Wartung der Mess- und Prüfmittel, etc.). Aufgrund der Signifikanz der QS-Funktion 'Prüfung' (Tabelle I) in der Herstellung von Elektroniksystemen (wegen Komplexität, Beeinflussbarkeit, etc) bestimmt diese den grundsätzlichen ablauf der projektspezifischen Qualitätssicherung (Fig. 5). Die einzelnen Prüfverfahren sind die Vertrags- und Spezifikationsüberprüfung, Arten der Entwurfsüberprüfung, Bauteil-, Prototyp-, Erstmuster-, Zwischen-, End- und Abnahmeprüfungen, etc. sowie periodische Funktionsprüfung und Wartung in der Nutzungsphase (vergl. [6], [9].)

Aus Figur 5 erkennt man ferner, dass ein QS-System mit seinen Systemfunktionen allgemeine Gültigkeit besitzt, dass aber für eine wirksame Qualitätssiche-rung eines bestimmten Produktesortiments wie die Elektronik, gewisse QS-Massnahmen ein besonderes Gewicht und einen bestimmten Platz im Projekt-ablauf, neben allen anderen Qualitätssicherungsaktivitäten, erhalten. Dies schliesst auch ein, dass zur Erfüllung bestimmter Qualitätsanforderungen eines Produktes, nur bestimmte QS-Massnahmen (produktespezifisches Z- und Q-Sicherungsprogramm) von der Gesamtheit aller QS-Systemfunktionen (Tabelle I) notwendig sind (QS-Systemanforderungsstufen, z.B. CSA Z299.1-Z299.4).

Damit ist auch der Zielsetzung genüge getan, Qualität und Zuverlässigkeit wirtschaftlich zu erzeugen und zu erhalten. (Optimierung der Systemwirksam-keit.)

LITERATURVERZEICHNIS

[1] H. Frey: Safety and Reliability - Their Terms and Models of Complex Systems. IFAC Workshop Safecomp'79, Stuttgart, May 16-18, 1979.

[2] H. Frey: System Effectiveness, a comprehensive characteristic for assessing complex system performance throughout the life cycle. Internat. Management System Assoc., 6th Internat Congress, 24./28.9.79.

[3] IEEE-Standards betreffend die elektrische Ausrüstung von Kernkraftwerken. IEEE-Std 279, 308, 323, 344, 379, 381, etc.

[4] H. Frey: Zuverlässigkeitsplanung von Elektroniksystemen, E und M Elektronik und Maschinenbau, 1978 (6/7).

[5] H. Frey: Computerorientierte Methodik der Systemzuverlässigkeits- und Sicherheitsanalyse. Diss. Nr. 5244, ETH Zürich, 1973.

[6] H. Frey, K. Roth: On the Relationship between Redundancy, Maintenance and Safety Margins for Testing Thyristor Valves. Proc. Int. Conf. on Large High Voltage Electric Systems (CIGRE), Study Committee No. 14, August 1978, Paris.

[7] DGQ 22 und DGQ/SAQ 23: Organisation der Qualitätssicherung im Unternehmen. Deutsche Gesellschaft für Qualität/Schweiz. Arbeitsgemeinschaft für Qualität.

[8] Th. Stumpf: Anforderung an Qualitätssicherungssysteme - eine Uebersicht. Qualität und Zuverlässigkeit, 1979 (1).

[9] H. Erni, H. Frey, G. Köppl, Impact and Effectiveness of Quality Assurance and Testing on the Reliability of Circuit-Breakers. Proc. Int. Conf. on Large High Voltage Electric Systems (CIGRE), Paper 13-04, August 1978, Paris.

ANHANG: BEGRIFFE UND DEFINITIONEN

Systemwirksamkeit:	Ein Mass für die Fähigkeit eines Systems, den vorgegebenen Aufgabenkomplex mit dem bestmöglichen Verhältnis Nutzen zu Aufwand über den gesamten Lebenszyklus zu erfüllen.
Nutzen	Nutzeffekt, Nutzwert. Wertschätzung einer Handlung, Massnahme, Funktion, Dienstleistung, technischen Leistung, eines Programmes etc. bezogen auf den Grad der jeweiligen situationsbezogenen Zielerreichung (Merkmale oder Parameter zur Erfassung der Wertschätzung über eine bestimmte Zeitdauer).
Aufwand	Gesamtheit der Kosten für die Mittel und Aufwendungen für das Erreichen eines Zieles oder zum Erbringen eines bestimmten Nutzens (Beschaffungskosten, Betriebskosten, Instandhaltungskosten etc.).
Lebenszyklus	Betrachtungsdauer des Systems umfassend Konzept-, Planungs-, Entwicklungs-, Konstruktions-, Fabrikations-, Prüf-, Betriebs- bzw. Nutzungs- und Ausserbetriebssetzungsphase.
Verfügbarkeit	Fähigkeit eines Systems, seine Funktion im Augenblick der Betrachtung zu erfüllen. (Berücksichtigung der Einwirkung der Zuverlässigkeit, Instandhaltbarkeit, logistische Unterstützung und menschliche Faktoren.)

Zuverlässigkeit : Die Fähigkeit eines Systems, innerhalb der vorgegebenen Grenzen denjenigen durch den Verwendungszweck bedingten Anforderungen zu genügen, die an das Verhalten ihrer Eigenschaften während einer gegebenen Zeitdauer gestellt sind.

Sicherheit ; Fähigkeit eines Systems, innerhalb der vorgegebenen Grenzen und während einer gegebenen Zeitdauer keine Gefährdung für Menschen, Sachen oder Umwelt darzustellen.

Oder:

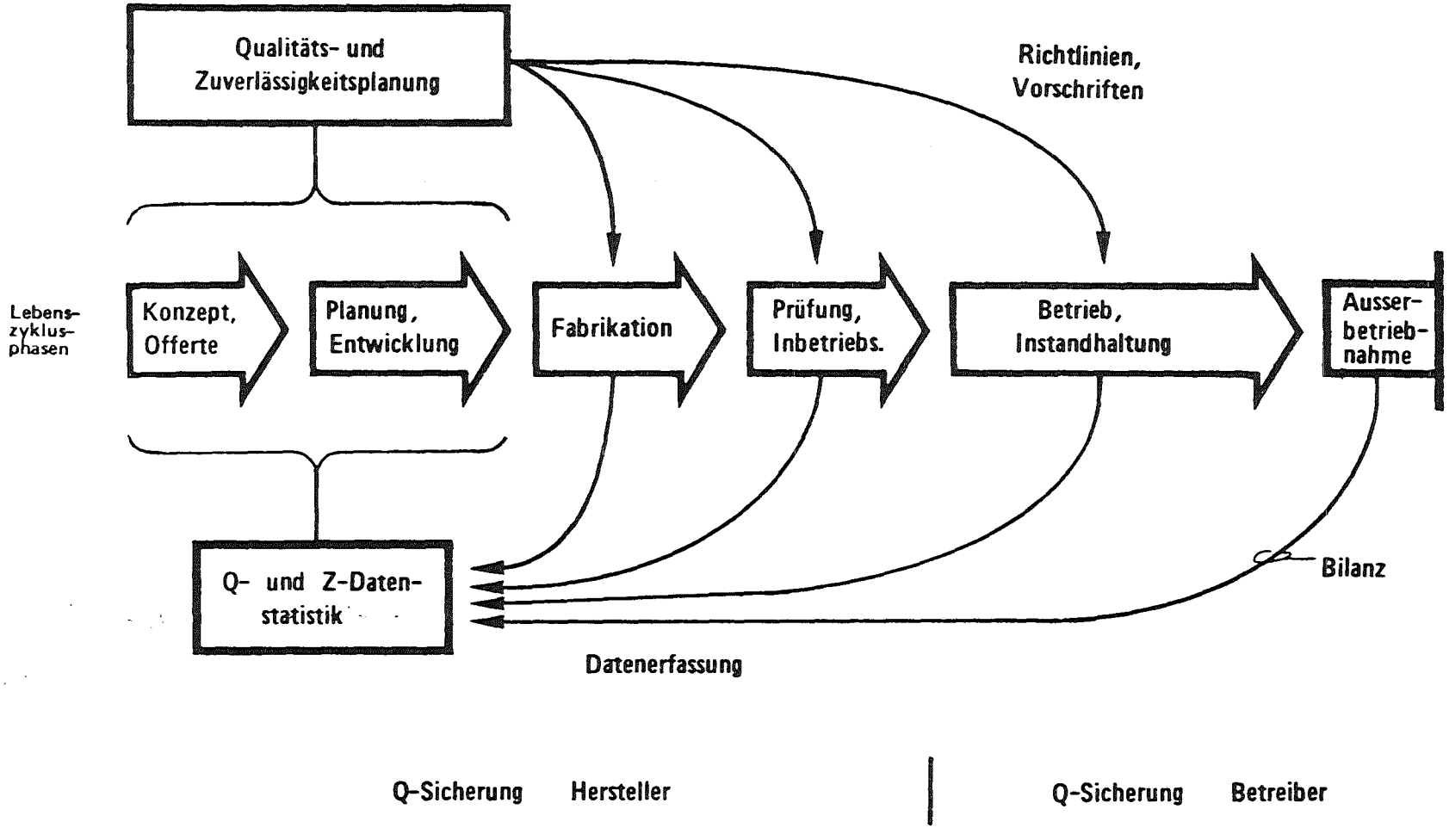
Ein System wird als "sicher" bezeichnet, wenn es mit einer durch den Verwendungszweck gegebenen, angemessen hohen Wahrscheinlichkeit gefährliche Auswirkungen - verursacht durch Systemausfälle - auf die Umwelt ausschliesst.

Ausfall; Unzulässige Abweichung von einem Merkmal oder Parameter.

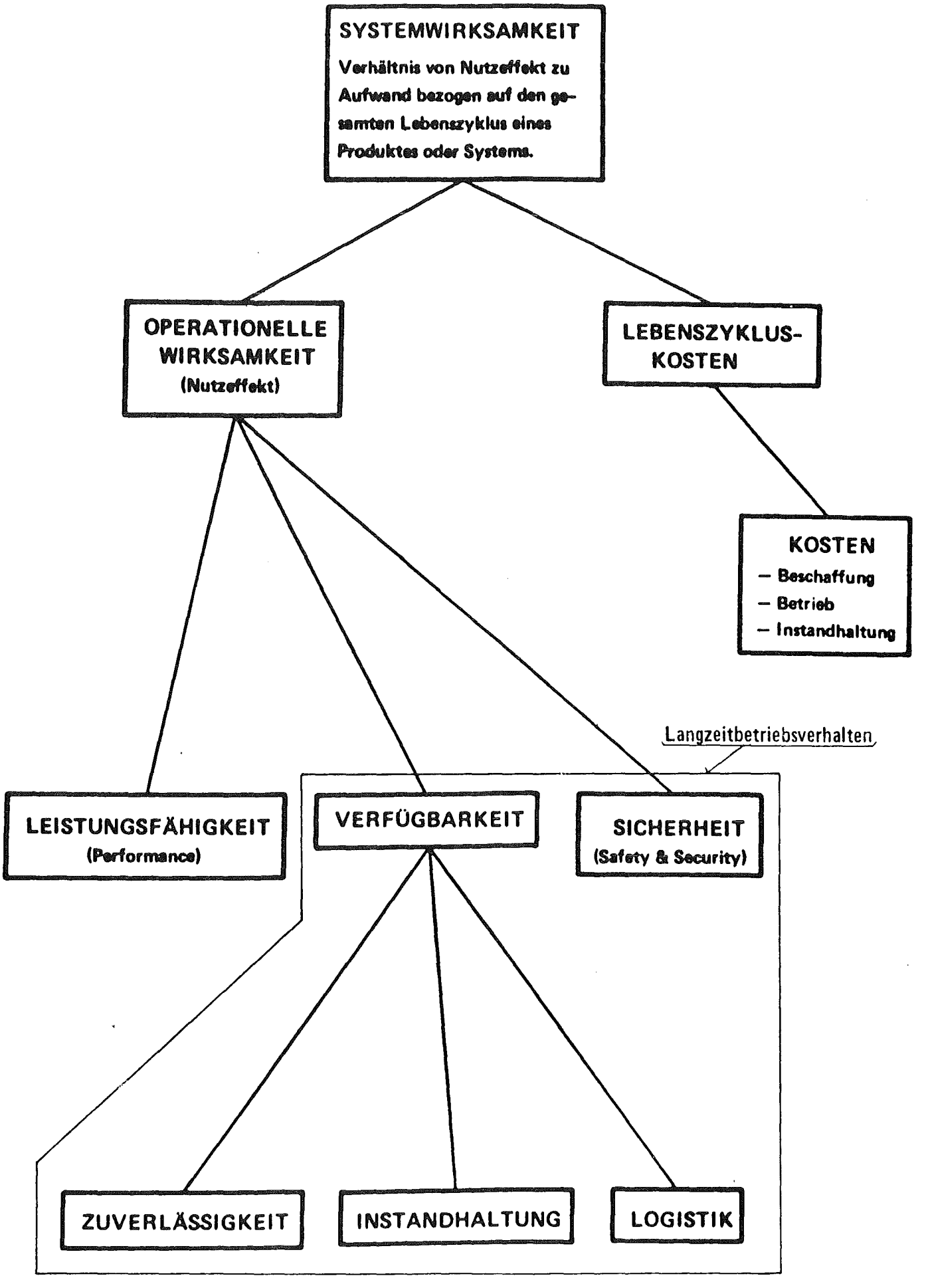
Instandhaltung; Alle nötigen Massnahmen und Arbeiten, um spezifizierte Eigenschaften eines Systems erhalten oder neu geben zu können.

Logistische Unterstützung; Gesamtheit der Aktivitäten, ausgeführt mit dem Ziel, eine wirksame und wirtschaftliche Verwendung des ausgelieferten Systems während seiner ganzen Nutzungsphase zu ermöglichen (Nachschub der Ersatzteile etc.).

Menschliche Faktoren:	Sammelbegriff für die Faktoren, die den Einfluss des Menschen auf die Verfügbarkeit eines Systems umfassen (Aspekte der Ergonomie (Man-Machine Interface), Auswahl, Motivierung und Schulung des Betriebs- und Instandhaltungspersonals, Zuverlässigkeit des Menschen etc.).
Qualität:	Die Gesamtheit aller Merkmale und Eigenschaften, die ein Produkt, System oder eine Dienstleistung zur Erfüllung vorgegebener Forderungen geeignet macht.
Qualitätssicherung:	Massnahmen zur Spezifizierung, Planung, Erzeugung und Aufrechterhaltung einer bestimmten Ausführungsqualität, Zuverlässigkeit, Sicherheit und Verfügbarkeit als integrierender Bestandteil der Planungs-, Realisierungs- bzw. Einsatzphase eines Systems (übergeordneter Qualitätsbegriff und Bestandteil der Systemwirksamkeit).
Ausführungsqualität:	Der Grad der Uebereinstimmung zwischen Ausführungsvorschriften und Ausführung in der Fertigung (Güte).

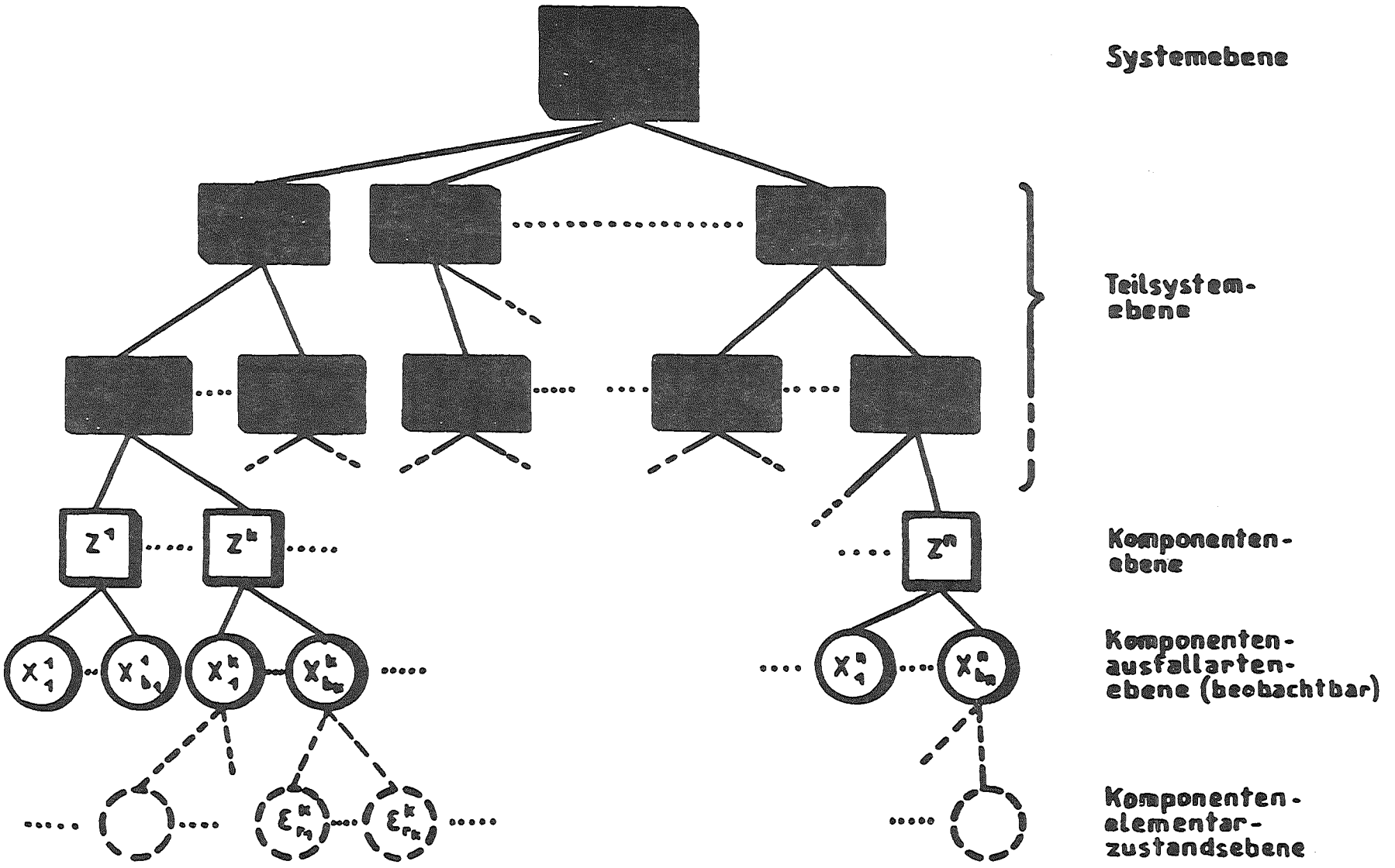

Qualitäts- und Zuverlässigkeitsplanung
Richtlinien, Vorschriften
Lebens-zyklus-phasen
Konzept, Offerte
Planung, Entwicklung
Fabrikation
Prüfung, Inbetriebs.
Betrieb, Instandhaltung
Ausser-betrieb-nahme
Q- und Z-Daten-statistik
Bilanz
Datenerfassung
Q-Sicherung Hersteller
Q-Sicherung Betreiber

Figur 1


SYSTEMWIRKSAMKEIT
Verhältnis von Nutzeffekt zu Aufwand bezogen auf den gesamten Lebenszyklus eines Produktes oder Systems.
OPERATIONELLE WIRKSAMKEIT
(Nutzeffekt)
LEBENSZYKLUS-KOSTEN
KOSTEN
– Beschaffung
– Betrieb
– Instandhaltung
Langzeitbetriebsverhalten
LEISTUNGSFÄHIGKEIT
(Performance)
VERFÜGBARKEIT
SICHERHEIT
(Safety & Security)
ZUVERLÄSSIGKEIT
INSTANDHALTUNG
LOGISTIK

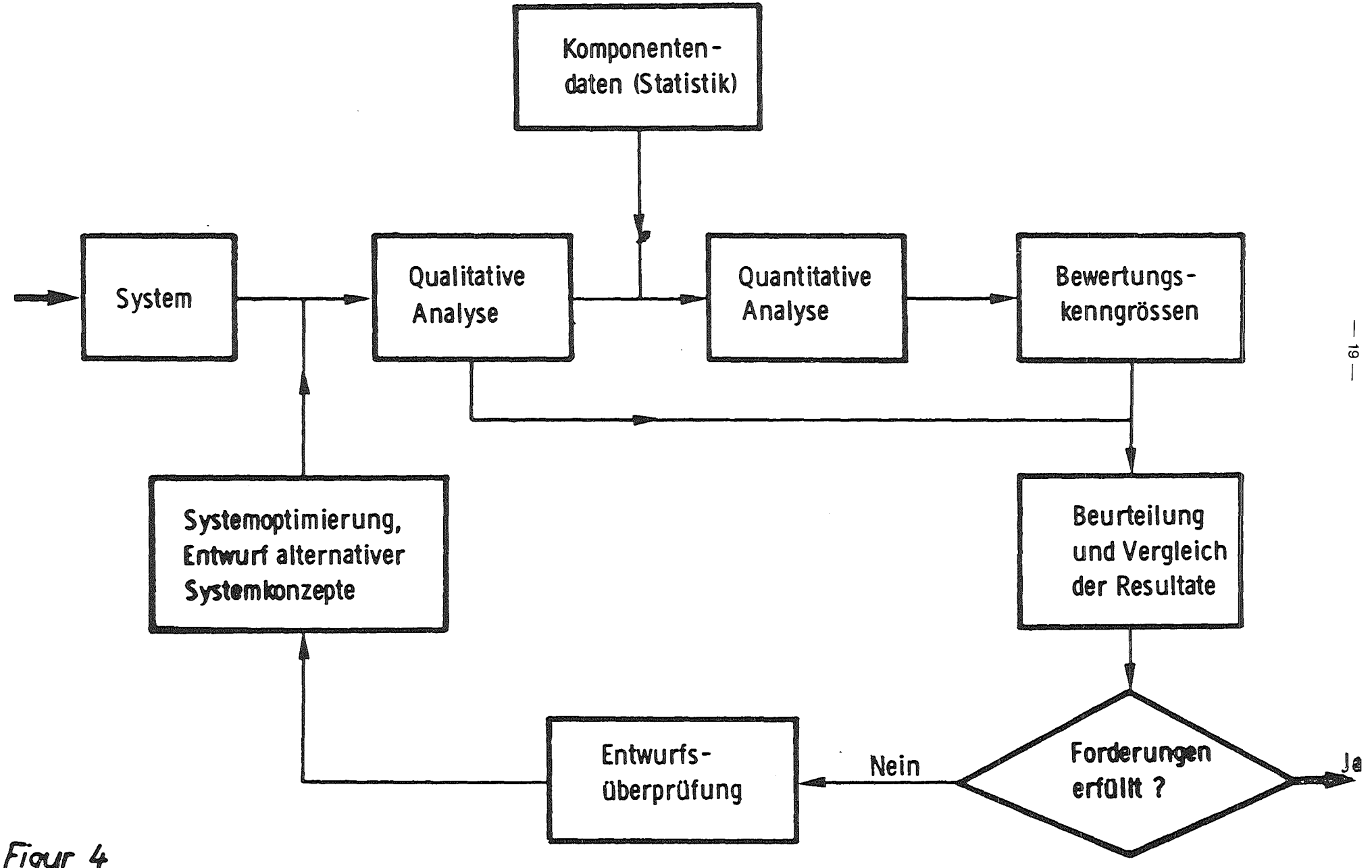
Figur 2

System - Dekomposition



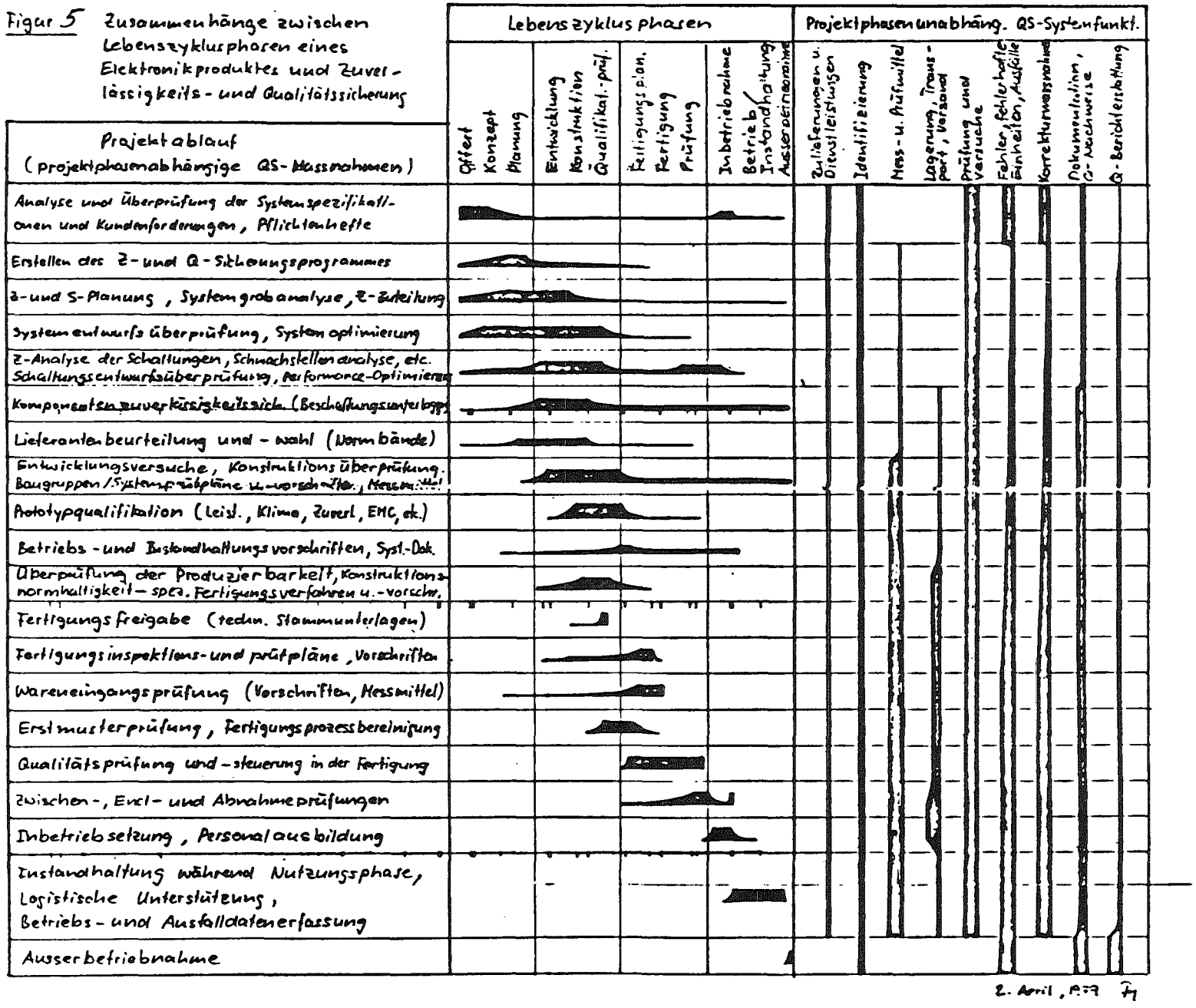
Figur 3

SYSTEMZUVERLAESSIGKEITSANALYSE



Figur 4

Figur 5 Zusammenhänge zwischen Lebenszyklusphasen eines Elektronikproduktes und Zuverlässigkeits- und Qualitätssicherung



2. April, 79 Fy

Diskussion

Frage: Die Schwierigkeit bei der Analyse von Rechnersystemen mit IC's ist nicht nur die Berücksichtigung verschiedener Ausfallarten und deren prozentualer Anteil sondern im allgemeinen die Bestimmung von Ausfallraten. Die Angaben in der Literatur zeigen große Abweichungen auf. Wie weit ist es zweckmäßig, in Analysen überhaupt die verschiedenen Ausfallarten von IC's zu berücksichtigen?

Wie realistische Resultate gibt MIL-HDBK-217C?

Antwort: Grundsätzlich müssen für Sicherheitsanalysen alle Ausfallarten bekannt sein und auf ihre Auswirkung evaluiert werden. Da bei IC's diese Angaben normalerweise nicht verfügbar sind, werden für Schaltungen deren Sicherheit nachgewiesen werden muß (z.B. Bahnen) nur (technologisch übersehbare) diskrete Komponenten verwendet. Für die detaillierte Z-Analyse (Feinanalyse) sind die Ausfallarten der Komponenten ebenfalls notwendig.

Das MIL-HDBK-217C ist nach unserer Erfahrung eher konservativ (gemessene λ-Werte (Ausfallrate) zu berechneten λ-Werten, vielleicht 1:3 ÷ 5). Man muß aber immerhin berücksichtigen, daß für die Berechnungen meistens Auslegungsgrenzwerte (Temperatur, Streß, etc.) gewählt werden, welche im Betrieb selten erreicht werden, so daß folglich auch eine geringere Ausfallrate statistisch erfaßt werden müßte. Diese Tatsache wird auch durch andere Quellen in diesem Rahmen bestätigt (RAC, etc.).

Frage: In welchem Umfang wird auf statistische Erfahrungen zurückgegriffen, um Fehlersuchzeiten konkret zu minimieren?

Antwort: Die Ausfallerkennung und Lokalisierung hängt von vielen Faktoren ab, nämlich von der Systemstruktur (funktioneller Transparenz) bzw. Komplexität des Systems, der Prüfbarkeit, Ausfallüberwachungsmethode und -anzeige, Zugänglichkeit während dem Betrieb, der Konstruktion des Systems (Modularität, ...), der Reparatur-, Personalausbildungs- und Schwierigkeitsgrad des Diagnostikprozesses (Reparatur), Standort des Systems etc.

Die Evaluation und Optimierung des Diagnostikprozesses basiert auf gewissen system- bzw. projektbezogenen Grunddaten die bekannt sein müssen bzw. abgeschätzt werden müssen (Erfahrung mit ähnlichen Systemen) um Fehlersuchzeiten zu minimieren.

Frage: Wie kann man subjektive Bewertungen (etwa "public acceptance" bei Kernenergie) in die Quantifizierung des Nutzens einbeziehen? Hier liegen die Gewichte bei Kernenergie und anderen Technologien sehr verschieden.

Antwort: Das Problem der objektiven Bewertung des Nutzens stellt sich in grundsätzlicher Art, da die Aussage ja produkt-, projekt- bzw. dienstleistungsgebunden sein soll.

Die Bewertungsmaßstäbe für jeden einzelnen Bewertungsparameter des Nutzens müssen festgelegt werden. Die eine Möglichkeit ist aufgrund von Erfahrung (Referenzsystem $E_o(T_i)$ bzw. Parameter), andernfalls andere zweckmäßige Maßgaben.

Der Wert der ermittelten Systemwirksamkeit $E(T_i)$ liegt nun offenbar hauptsächlich im Vergleich von alternativen Systemen und Systemkonzepten (siehe [2]):

$$\frac{E(T_i)}{E_o(T_i)} = \frac{U(T_i)/c(T_i)}{E_o(T_i)} = c_e(T_i)$$

$E_o(T_i)$: Referenzwert

$c_e(T_i)$: relativer "cost effectiveness" Faktor

Frage: Die zu Beginn gegebene Definition der unternehmerischen Zielsetzung scheint primär am "Produkt"erzeugenden Unternehmen orientiert. Etwas anders - möglicherweise nun erweiternd - scheint sich die Frage für Dienstleistungsunternehmen zu stellen, deren Unternehmensziel die sichere Bereitstellung der Leistung ist, weil auch die Prognose des Bedarfs der Leistung Einfluß auf die Qualität der Dienstleistung (Sicherheit der Versorgung) hat.

Antwort: Eine Dienstleistung zu erbringen ist grundsätzlich auch eine Funk-

tion zu erfüllen. Das Mittel dabei kann wiederum ein "System" bestehend aus den Elementen "Mensch", "Hardware", "Software" und/oder Information sein, also gilt grundsätzlich dieselbe unternehmerische Zielsetzung. Jedoch wäre eine allgemeinere Formulierung der bestehenden U-Zielsetzung zweckmäßig bei allgemeineren Betrachtungen.

Frage: Bei der Definition der unternehmerischen Zielsetzung haben Sie die Sicherheit der Anlage nicht erwähnt. Ich bin der Meinung, daß die Sicherheit der Anlage eine entscheidende Rolle (besonders bei Kernkraftwerken) spielt und darum in der Definition der Zielsetzung nicht vernachlässigt werden kann.

Antwort: Die Sicherheit ist ein wichtiger Aspekt und darf nicht vernachlässigt werden. Der Aufwand für Erzeugung der Sicherheit bzw. einer sicheren Funktion und der Aufwand für die Erhaltung derselben kann eindeutig erfaßt werden.

Der Nutzen der Sicherheit könnte z.B. damit bewertet werden (Kraftwerk, Bahn, Flugzeug, etc.) daß dadurch gewisse Leistungen (im Rahmen des Gesetzes und der Vorschriften, etc.) möglich sind. Z.B. Erzeugung von Energie durch Ausnutzung von Uran, etc., Fliegen von A bis B (in kurzer Zeit!), erhöhtes Bruttosozialprodukt, ... Grundsätzlich gilt aber, daß ohne die verlangte Sicherheit die betreffende Funktion bzw. Leistung nicht möglich wäre; das würde heißen, daß die Sicherheit nicht explizit als Bewertungskenngröße erscheint wie Leistung, Verfügbarkeit, etc. Aber falls die Sicherheit nicht mehr gegeben ist und z.B. ein Unfall passiert, so erscheint diese in zusätzlichem Aufwand (Kosten) und vermindert damit die Systemwirksamkeit.

Frage: Wie geht man vor, um die unterschiedlichen Fehlerarten großintegrierter Bausteine festzulegen?

Wie kann man die entsprechenden Fehlerraten abschätzen?

Antwort: - Ermittlung der Technologie (Physik) und deren Defekte (Fehlerarten) (Bonding, Oxyd failure, leakage, Material aging and decay, etc.)

- aufgrund der technologischen Defekte Ermittlung der resultierenden elektrischen oder funktionellen Ausfallarten (Statistik).

  Bedingung: Verfügbarkeit der entsprechenden, teueren Testmittel (µ-Processor Tester, etc.) und der Spezialisten (Halbleitertechnologe).

- Betriebsstatistik, Lebensdauerprüfungen (Hersteller), beschleunigte Lebensdauerprüfung. (Ermittlung der dominanten Ausfallarten bei beschleunigter Prüfung und der Beschleunigungsfaktoren wie erhöhte Temperatur, stress cycling, etc.) Extrapolation zu Normaltemperatur bzw. Belastung.

- Ausfallanalyse ausgefallener Komponenten.

Dr. D. Vetterkind *)

Die Nutzung der Schadens- und Zuverlässigkeitsdaten in Zuverlässigkeitsmodellen zur Systemplanung von Kraftwerksanlagen

1. Die Komplexität der Kraftwerksanlage und der zuverlässigkeitsrelevanten Information

1.1 Die Kraftwerksanlage und ihr Zielsystem

Jede thermische Kraftwerksanlage kann ohne größere Abgrenzungsschwierigkeiten als aus Betriebssystemen und aus Sicherheitssystemen bestehend aufgefaßt werden. In den Betriebssystemen finden die Prozesse der Energieumformungen statt. Wichtige Eigenschaft der Betriebssysteme ist ihre Leistungsfähigkeit (z.B. Dampfleistung in t/h oder elektrische Leistung in MW). Wichtigste Eigenschaften der Sicherheitssysteme sind die Erkennung von gefährlichen Anomaliezuständen von Betriebssystemen und das Treffen von Gegenmaßnahmen,um unzulässige Auswirkungen von Betriebsanomalien zu verhindern. Nachfolgend werden unter Kraftwerksanlagen ausschließlich Braunkohlen-gefeuerte und Kernkraftwerksanlagen verstanden.
Bezüglich der technischen Ausführung dieser Anlagen wird auf die Literatur verwiesen /1, 2, 3, 4/.

*) in Rheinisch-Westfälisches Elektrizitätswerk AG, Hauptverwaltung, Kruppstr. 5, 4300 Essen 1

Die Darstellung der Komplexität der Kraftwerksanlage könnte im Prinzip auf verschiedene Weisen geschehen. So läßt sich entsprechend der Vorgehensweise in der Nutzwertanalyse /5/ ein Zielsystem der Kraftwerksanlage aufstellen (siehe Bild 1) mit den Oberzielen Verfügbarkeit, Wirtschaftlichkeit und Sicherheit sowie den zugehörigen Unterzielebenen. Die zentrale Bedeutung der Zuverlässigkeit ergibt sich aus ihrem Einfluß auf die Verfügbarkeit der Kraftwerksanlage, auf die wirtschaftliche Energieerzeugung und auf die drei Sicherheitskategorien, nämlich Sicherheit außerhalb des Kraftwerkes, Sicherheit des Personals und die Sicherung der Anlage gegen Beschädigung (Anlagenschutz).

Ebenfalls in Bild 1 dargestellt sind die Einflußgrößen auf die Zuverlässigkeit in Form von geplanten und realisierten Anlagenmerkmalen: Konzept- bzw. Entwurfsneuheiten, erhöhte Anlagengröße, geeignete Auslegung und Güte, Redundanz, Automatisierung, Instandhaltbarkeit, Planungs- und Realisierungsdauer. Mit Hilfe von gegensteuernden Maßnahmen während der Verwendung, d.h. mit Hilfe der Durchführung von Instandhaltungs- und Änderungsmaßnahmen, wird die Zuverlässigkeit auch während der Betriebsphase in den erwünschten Grenzen gehalten.

1.2 Zuverlässigkeitsprobleme und zu deren Lösung benötigte Informationen

Die Komplexität der Zuverlässigkeitseigenschaften von Kraftwerksanlagen ergibt sich insbesondere aus folgenden Gründen:

- Die Kraftwerksanlage besteht aus einer sehr großen Zahl von Komponenten.

- Diese Komponenten sind teils mechanischer, elektrischer, elektronischer Natur und miteinander vermascht.

- Es werden in der Kraftwerksanlage mechanische Großkomponenten verwendet, die nur in geringer Stückzahl gebaut werden.

- Während der Planungs-, Herstellungs- und Montagephase der Kraftwerksanlage muß eine Zusammenarbeit von Auftraggeber, Auftragnehmer, Unterauftragnehmer und unabhängiger Überwachungsstelle erfolgen bezüglich Qualitätssicherung, Zuverlässigkeitsplanung und bezüglich der Zusammenarbeit im Genehmigungsverfahren.

- Es sind Entscheidungshilfen für die Instandhaltung zu erarbeiten.

Eine stichwortartige Übersicht über die Lösungswege für diese Themen und die für die Lösung benötigten Informationen gibt Tabelle 1; in der zweiten bzw. vierten Spalte dieser Tabelle wird bezüglich einiger wichtiger Punkte auf entsprechendes Schrifttum (jeweils nur Beispiele) hingewiesen.

Weitere wichtige bei der Zuverlässigkeit zu beachtende Punkte sind die Bedienungsfehler, die common-mode-failures, das Fehlansprechen von Schutz- und Automatisierungseinrichtungen sowie der Einsatz der Zuverlässigkeitsanalyse zur quantitativen Bestimmung des Risikos. Eine stichwortartige Übersicht über diese Punkte samt der zugehörigen Lösungswege und benötigten Informationen gibt Tabelle 2.

2. Gewinnung und Verarbeitung von Zuverlässigkeitsdaten

2.1 Die RWE-Schadensstatistik

Seit Mitte der 60er Jahre erfolgt in den Kraftwerken des RWE eine Schadenserfassung, die systematisch an das Auftragswesen der Instandhaltung gekoppelt ist. Über diese Schadensstatistik ist bereits mehrfach berichtet worden, z.B. in//6,17,18,19/.

Ihre wesentlichsten Erfassungsmerkmale und Ziele sind aus Tabelle 3 zu ersehen.

2.2 Die RWE-GRS-Modellfälle

Der RWE-GRS-Modellfall Neurath, bei dem die Anlagenmerkmale und die Ausfall- und Instandhaltungsdaten von einem neuen Braunkohlenkraftwerksblock erfaßt wurden (siehe Tabelle 3), stellt einen Test für eine mehr zuverlässigkeitsorientierte Schadenserfassung an Kraftwerksanlagen dar. Der Modellfall Neurath /20/ arbeitete mit 5 Dateien (Bauteilerfassung; Standorterfassung mit Betriebsdaten; Umgebungsbedingungen; Schadenserfassung; Betriebsstunden- bzw. Schaltspielerfassung) und lieferte gesicherte Ausfallraten von wichtigen konventionellen Komponenten mit Angabe des Vertrauensbereiches.

Eine Fortsetzung in Richtung Erfassung von Zuverlässigkeitsdaten von Komponenten stellt der nun angelaufene Modellfall Biblis Block B dar. Diese Datensammlung steht im Zusammenhang mit der in Arbeit befindlichen Deutschen Risikostudie für Leichtwasserreaktor-Kernkraftwerke. Die wichtigsten Erfassungsmerkmale dieses Modellfalles sind ebenfalls in Tabelle 3 dargestellt.

Darüberhinaus läuft derzeit eine von der GRS in Zusammenarbeit mit dem RWE durchgeführte Auswertung von Betriebserfahrungen, Biblis, Block A, die insbesondere das Ziel hat, Zuverlässigkeitsdaten von Teilsystemen oder Teilsträngen direkt zu gewinnen. Hierzu ist u.a. die Auswertung der Ergebnisse von Wiederholungsprüfungen notwendig. Bei dieser Auswertung von Betriebserfahrungen soll versucht werden, auch Aussagen über das Auftreten unerwünschter Transienten sowie über die Operator-Zuverlässigkeit zu gewinnen.

Bei der Auswertung bzw. bei der Vorbereitung der RWE-GRS-Modellfälle zur Zuverlässigkeitsdatensammlung waren bezüglich der Datenqualität und -anwendung u.a. folgende Punkte zu betrachten:

- Definition der Ausfälle entsprechend den Funktionsanforderungen.

- Widerspruchsfreiheit der Ausfallarten

- Ausfallraten, in den ersten Betriebsjahren ermittelt, enthalten Frühausfälle; daher Extrapolation nicht ohne weiteres auf 30 Jahre möglich

- Können geschätzte Versagenswahrscheinlichkeiten (auf Anforderung) sinnvoll auch als Ausfallrate in (1/h) angegeben werden?

- Sofern man die Ausfallrate einer Komponentenart als stochastische Größe auffaßt: Gehorcht die Ausfallrate dann einer log-n-Verteilung (der Median dieser Verteilung liegt vergleichsweise hoch)?

- Einflüsse von Qualitätsmerkmalen auf die Zuverlässigkeit

- Einflüsse von Wartung/Inspektion auf die Zuverlässigkeit

- Nicht-auslegungsgemäßer Betrieb einer Komponente

- Testen von Funktionselementen während Wiederholungsprüfungen, die im Betrieb und auch im Störfall nicht angefordert werden, erscheint nicht sinnvoll.

3. Nutzung der Schadens- und Zuverlässigkeitsdaten zur Verfügbarkeits- und Sicherheitsplanung

3.1. Nutzung der Daten zur Planung der Systemverfügbarkeit (Beispiele)

3.1.1. Verfügbarkeitsprognose von braunkohlengefeuerten Dampferzeugern.

Zur mittelfristigen Verfügbarkeitsprognose bereits in Betrieb befindlicher braunkohlengefeuerter Dampferzeuger wurde ein heuristisches Verfahren /15/ angewendet, bei dem unter anderem die Ausfalltrends von Komponenten, die zeitliche Parallelität von Komponentenreparaturen und der technisch abschätzbare Revisionserfolg verwendet wurden. Die hier verwendeten Schadens- und Verfügbarkeitsinformationen der Komponenten des Dampferzeugers bzw. des Systems Dampferzeuger sind in Bild 2 dargestellt. Mit diesem Modell können z.B. brauchbare Aussagen über Erfolg und Zweckmäßigkeit von Umbaumaßnahmen gewonnen werden.

Die im Bild 2 verwerteten Informationen sind dem Ausfall- und Reparaturverhalten des Dampferzeugers entnommen, das in Bild 3 dargestellt ist in Form des Zeitverlaufs der kummulierten Nichtverfügbarkeit.

3.1.2. Verteilung der Betriebs- und Nichtverfügbarkeitszeiten von braunkohlengefeuerten Kraftwerksblöcken

Die Verteilung der Betriebs- und Nichtverfügbarkeitszeiten von braunkohlengefeuerten Kraftwerksblöcken wurden in /23/ und /25/ untersucht. Für das Beispiel des in Bild 3 gezeigten Dampferzeugers sind in Bild 4 die Verteilung der Betriebszeiten vor und nach Revision bzw. Umbau sowie in Bild 5 die Verteilung der Nichtverfügbarkeitszeiten in den entsprechenden Intervallen dargestellt. Bei der Verteilung der Betriebszeiten ergibt sich ein starker Einfluß des Umbaues. Die Kenntnis der Betriebs- und Nichtverfügbarkeitszeiten ist wichtig, um mit Hilfe von Erneuerungsmodellen (z.B. überlagerter Erneuerungsprozeß) die Verfügbarkeit von Kraftwerksblöcken bzw. eines Systems von mehreren Kraftwerksblöcken für Planungszwecke, z.B. der Reservehaltung an Kraftwerkskapazität, im voraus abzuschätzen.

3.1.3. Zeitabhängige Ausfallraten von Komponenten und Dampfzeugern

Bei deutlich verschleißanfälligen Komponenten oder Hauptaggregaten kann die zeitabhängige Ausfallrate unter Verwendung des zeitabhängigen Poissonprozesses aus den (zwischen den Ausfällen) aufeinanderfolgenden Betriebszeiten abgeschätzt werden /23/; das Ergebnis einer solchen Abschätzung über mehrere Revisionsintervalle hinweg (langfristiger Anstieg) zeigt Bild 6 für vier zeichnerisch gleiche Halblast-Braunkohlenkessel. Man sieht, daß die vier Kessel einerseits trotz Zeichnungsgleichheit unterschiedlich schnell ansteigende Ausfallraten aufweisen, diese andererseits jedoch wesentlich enger zusammenliegen als z.B. der 95% - Vertrauensbereich für die Ausfallrate eines einzigen Kessels.

Zusätzlich sind in Bild 6 die Oszillationen einer Ausfallraten-Grobschätzung entsprechend dem n- fachen Kehrwert der Summe aus n aufeinanderfolgenden Betriebszeiten für einen Kessel dargestellt; dies zeigt, daß die einfache Grobschätzung für die Extrapolation der Ausfallrate viel weniger geeignet ist als die verfeinerte Schätzung über den zeitabhängigen Poissonprozeß.

3.1.4. Verwendung parametrischer Fehlermodelle (Beispiel: Verschleiß von Eco-Rohrbögen)

Beim Sandverschleiß von Rohren und Rohrbögen der Berührungsheizflächen von Braunkohlenkesseln handelt es sich um stochastische Prozesse, deren Zufälligkeiten mit den Schwankungen einiger Merkmale, insbesondere der Kohlequalität (Sandgehalt), der Strömungsverhältnisse des Rauchgases, der Heizflächenverschmutzung und der Erosionsbedingung der Rohrbögen, zusammenhängen. Einige wichtige deterministisch formulierte Zusammenhänge des Sandverschleißes wurden unter Versuchsbedingungen von Fehndrich /26/ erarbeitet. Die Verschmutzungsneigung wurde von Schöddert /27/ untersucht. Dies sind wichtige Erkenntnisse, die für die Auslegung eines Kessels benutzt werden.

Für die Beschreibung des Verschleißverhaltens von Rohren und Rohrbögen bereits in Betrieb befindlicher Kessel bringt eine probabilistische Betrachtungsweise weitere Vorteile.

Anhand des zeitlich-stochastischen Verschleißverhaltens, welches z.B. durch die mit Hilfe der Ultraschallprüfung bestimmten Minimalwandstärke wiedergegeben werden kann, ist eine Voraus-schätzung des Ausfallverhaltens der betroffenen Rohre und Rohrbögen möglich.

In Bild 7 sind für eine Gruppe verschleißbehafteter Eco-Rohrbögen Minimalwandstärken für die Revision nach 16 bzw. 18 Betriebsjahren wiedergegeben. Man erkennt die Verschiebung des Mittelwertes der Minimalwandstärken (von 3,1 abfallend auf 2,4 mm) während der beiden dazwischen liegenden Betriebsjahre. Auf die zugehörige Rechenmethode wird hier nicht weiter eingegangen /23/.

3.2. Nutzung der Daten zur Planung der Systemsicherheit (Beispiele)

3.2.1. Komponenten-Ausfallraten und deren Streubereich

Bekanntlich streuen die Schätzwerte der Ausfallraten der verschiedensten mechanischen und elektrischen Komponenten über viele Zehnerpotenzen. Darüber hinaus streut aber die aus einem Kollektiv gleichartiger Komponenten bestimmte Ausfallrate noch erheblich, insbesondere dann, wenn die Komponenten aus verschiedenen Anlagen stammen. Bild 8 gibt das Beispiel der Ausfallraten von Absperrschiebern, bestimmt aus den Angaben von /20/. Hierbei ergibt sich für die drei verschiedenen genannten Ausfallarten ein systematischer Unterschied der Ausfallraten.

3.2.2. Verteilung des Schätzwertes der Ausfallraten gleichartiger Komponenten

Wie sich zeigt, sind die Schätzwerte der Ausfallraten gleichartiger Komponenten (Komponenten aus unterschiedlichen Anlagen und/oder Komponenten etwas unterschiedlicher Konstruktion) verteilt. Für diese Verteilung wurde in /28/ eine logarithmische Verteilung angenommen, was sich in /29/ einigermaßen gut bestätigt hat. Es ist jedoch derzeit noch die Frage, ob hier noch eine andere Art von Verteilung angesetzt werden könnte im Gegensatz zur logarithmischen Normalverteilung, welche einen vergleichsweise hohen Median-Wert besitzt.

3.2.3. Beispiel des zweigeteilten Haupt-Netzanschlusses

In Bild 9 ist die Schaltung eines zweifach redundanten Haupt-Netzanschlusses eines einzelnen Kraftwerksblocks gezeigt. Zur Vereinfachung sind die beiden zugehörigen Eigenbedarfsschienen des Kraftwerksblocks und die Notstromaggregate nicht eingezeichnet. Der Notstromfall ist dann eingetreten, wenn die Eigenbedarfsschienen weder vom Blockgenerator noch vom äußeren Netz weiter versorgt werden können; es werden die Notstromaggregate angefordert. Je nach Höhe der Eintrittswahrscheinlichkeit des Notstromfalles pro Jahr ist eine entsprechende Anzahl von Redundanzen der Notstromaggregate vorzusehen.

In Bild 10 sind die Fehlerbäume für den Eintritt des Notstromfalles nach Netzausfall bzw. nach Ausfall des Blockgenerators, d.h. für die beiden wichtigsten Fälle, dargestellt. Hierbei erscheinen die Komponenten der Eigenbedarfsschiene und der Eigenbedarfsumschaltung nicht im Fehlerbaum, da deren Zuverlässigkeit gleich Eins gesetzt wird und nachstehend insbesondere der Einfluß der Netzausfallrate, der Wahrscheinlichkeit des Nichtabfangens des Blockgenerators auf Eigenbedarf und der Ausfallwahrscheinlichkeiten von Generator- und Leistungsschaltern auf die Eintrittswahrscheinlichkeit des Notstromfalles demonstriert werden soll.

Die Zuverlässigkeit der beiden Maschinentransformatoren, die jeweils zwischen Leistungs- und Generatorschalter liegen, geht bezüglich der beiden betrachteten Notstrom-Eintrittsfälle nicht in die Fehlerbäume ein. Alle weiteren Notstromfälle, bei denen weder Netzausfall noch Generatorausfall vorliegen, liefern vergleichbar geringe Wahrscheinlichkeitsbeiträge und werden hier nicht betrachtet.

Die Ergebnisse der Fehlerbaumberechnung zeigt Bild 11. Beim Notstromfall nach Netzausfall (parametrierte Kurven A, B, C) hängt die Eintrittswahrscheinlichkeit des Notstromfalles praktisch von der Ausfallrate des Netzes und von der Nichtabfangwahrscheinlichkeit des Blockgenerators ab.

Für diese beiden Kenngrößen gibt es derzeit noch keine fest eingegrenzten Daten, jedoch Vorstellungen über die obere Grenze der Zahlenwerte. Vergleichende Betrachtungen verschiedener Schaltungsvarianten /24/ des Netzanschlusses des Blockgenerators haben hierbei ihre Bedeutung.

Beim Notstromfall nach Ausfall des Blockgenerators (z.B. nach Reaktorschnellabschaltung) ist die zu erwartende Eintrittswahrscheinlichkeit des Notstromfalles entsprechend Bild 11 stark abhängig sowohl von der Ausfallrate des Blockgenerators als auch von den Versagenwahrscheinlichkeiten der Generator- und Leistungsschalter bei Anforderung (siehe Kurven D, E, F, G). Hierbei stehen sowohl für die Ausfallrate des Blockgenerators als auch für die Versagenswahrscheinlichkeiten der Generator- und Leistungsschalter aus der RWE-Schadensstatistik gesicherte Daten zur Verfügung.

4. Verwendung und Aussagekraft von Schadens- und Zuverlässigkeitsdaten

Bei der Gewinnung und Verwendung von Schadens- und Zuverlässigkeitsdaten ist sowohl bezüglich der Verfügbarkeitsplanung als auch bei der Sicherheitsplanung von Kraftwerksanlagen bereits ein erheblicher Stand erreicht worden. Es erscheint aber auch wichtig, danach zu fragen, welche Bedürfnisse in der Praxis nach verbesserter Datenmethodik bzw. nach verbesserten Daten bestehen und auch welcher Stand der Theorie hierzu heute erreicht worden ist bzw. welchen Informationsbedarf die Theorie aus der Praxis in Zukunft erhalten sollte. In Tabelle 4 ist in Form einer Matrix dargestellt, was bezüglich der Komponentenauswahl, Datenrückführung, Verfügbarkeitsprognose und -optimierung, Zuverlässigkeitsanalyse, bezüglich der common-mode-failures, der menschlichen Zuverlässigkeit und bezüglich der Inspektionsabstände aus heutiger undkünftiger Sicht bereits erreicht wurde bzw. noch angestrebt werden sollte. Diese Matrix-Darstellung soll eine Grobinformation geben und sollte zur weiteren Diskussion anregen.

5. Schrifttum

/1/ W.E.Fuchs: Kraftwerks- und Anlagentechnik
(Steinmüller-Taschenbuch, Vulkan-Verlag)

/2/ K. Schröder: Große Dampfkraftwerke, Bände I, II, III
(Springer-Verlag)

/3/ W. Oldekop: Druckwasserreaktoren für Kernkraftwerke
(Verlag Karl Thiemig, 1974)

/4/ D. Smidt: Reaktortechnik, Bde. 1 u. 2
(G. Braun-Verlag, 1971)

/5/ C. Zangemeister: Nutzwertanalyse in der Systemtechnik
(Verlag Wittemann, 1971)

/6/ W. Fehndrich, W. Kutsch, D. Vetterkind: Die Daten- und Erfahrungsrückführung zur Erhaltung und Verbesserung der Zuverlässigkeit und Ertragsfähigkeit von Kraftwerksanlagen.
Tü 16 (1975), Nr. 7/8, S. 216-221

/7/ Technische Regeln Dampfkessel (TRD), 14. Änderung Mai 1976
(Carl Heymanns Verlag, Köln; Beuth-Verlag, Berlin)

/8/ ASME boiler and pressure vessel code, 1977

/9/ P.E. Becher, A. Pedersen:
2nd SMIRT Conf., Berlin (1973), Paper M 6/4

/10/ F.-J. Adamsky, H.D. Teichmann: Betriebserfahrungen mit Speisewasserbehältern.
VGB Kraftwerkstechnik 57 (1977), H. 11, S. 759-773

/11/ Entwurf KTA-Regel 1401: Allgemeine Anforderung an die Qualitätssicherung.-Fassung 6/78

/12/ VDI-Richtlinie 4007, Blatt 2: Organisation und Zusammenarbeit der Zuverlässigkeitsstellen bei Auftraggeber und Auftragnehmer.
VDI-Richtlinie 4007, Blatt 4: Berichtswesen in der Zuverlässigkeit

/13/ H. Effenberger, W. Schäfer: Ein mathematisches Modell zur Bestimmung einer optimalen Verfügbarkeit für einen Kraftwerksblock bzw. für ein Kraftwerk.
Energietechnik 21 (1971), H. 1, S. 9-14

/14/ W.Fehndrich, W. Hinterthan: Wartbarkeit von Kraftwerksanlagen. Symposium des TÜV Rheinland, Bad Neuenahr, 1974

/15/ D. Vetterkind: Ein Voraussagemodell für die Nichtverfügbarkeit von Dampferzeugern.
VGB Kraftwerkstechnik 52 (1972), H. 5, S. 435-446

/16/ KTA-Regel 3501: Reaktorschutzsystem und Überwachung von Sicherheitseinrichtungen.

/17/ H. Vetter: Einheitliche Schadenserfassung als Grundlage für Zuverlässigkeitsanalysen. - Tü 11 (1970), H. 3, S. 75-78

/18/ K. Neuroth: Auswertung der Schadensstatistik mit Beispielen. -Mitt. VGB 50 (1970), H. 5, S. 429-435

/19/ W. Fehndrich, W. Hlubek, D. Vetterkind: Zuverlässigkeitsprobleme von der Planung bis zum Betrieb thermischer Kraftwerke.
Energie 25 (1973), H. 7/8, S. 190-198

/20/ P. Hömke, H. Krause: Der Modellfall IRS-RWE zur Ermittlung von Zuverlässigkeitskenngrößen im Betrieb.
-Bericht IRS-W-16 (Nov. 1975)

/21/ VDEW: Richtlinien zur Erfassung von Schäden und Stillstandszeiten in Wärmekraftwerken; mit Anhang A: Schadensschlüssel für Dampfkraftwerke mit fossilen Brennstoffen. (VDEW-Verlag).

/22/ Kraftwerk-Kennzeichen-System (KKS)
Arbeitskreis RWE/Steag/IRS/KEG/BBC/HRB/KWU

/23/ D. Vetterkind: Graphentheoretische Modelle zur Berechnung der Zuverlässigkeit und Verfügbarkeit von Kraftwerksanlagen.
Dissertation RWTH Aachen, 1977

/24/ KTA-Regelentwurf 3701.1: Übergeordnete Anforderungen an die elektrische Energieversorgung des Sicherheitssystems in Kernkraftwerken

/25/ K.W. Edwin, J. Nachtkamp: Ein Beitrag zur statistischen Ermittlung des Betriebsverhaltens wichtiger Komponenten der elektrischen Energieversorgung.
ETZ-A 96 (1975), H. 12, S. 543-548

/26/ W. Fehndrich: Verschleißuntersuchungen an Kesselrohren
(Dissertationsarbeit, T.H. Karlsruhe, 1968)

/27/ G. Schöddert: Untersuchungen über die Verschmutzung der rauchgasumströmten Heizflächen von Dampferzeugern bei Verbrennung rheinischer Braunkohle
(Dissertationsarbeit T.U. Karlsruhe, 1969)

/28/ Wash 1400, Reactor Safety Study, USNRC, 1975

/29/ P. Hömke, E. Lindauer, G. Meinlschmidt:
Data Collection in a Nuclear Power Plant and a Pilot Collection System in a Lignite-Powered Station
(Aus: Inservice Data Reporting and Analysis; The American Society of Mechanical Engineers; Dez. 1978)

Tabelle 1: Zuverlässigkeitsprobleme und benötigte Informationen

Zuverlässigkeitsproblem	Lösungsweg	für die Lösung benötigte Information: welche Information	wie erhalten
große Zahl und Vermaschung von mechanischen, elektrischen u. elektronischen Komponenten	Auswahl zuverlässiger Komponenten	Verfügbarkeit, Funktionszuverlässigkeit	Schadensstatistik-Auswertungen nach Komponenten, Hauptaggregaten und Herstellern /6/
	Redundanz von Komponenten oder Teilsystemen; z.B. /16/	Systeminformation u. zugehörige Entscheidung	Systemanalyse; Zuverlässigkeitsabschätzung
	Zuverlässigkeitsoptimierung	Alternativen des Systemaufbaus	aus technischer Sicht mögliche Alternativen der Zuverlässigkeitsabschätzung unterwerfen
mechanische Großkomponenten in geringer Stückzahl	determinist. Vorschriften über Werkstoff, Form u. Beanspruchungen; z.B./7,8/	Fehlerbegrenzung	Ermittlung von Standzeiten im Test und im Betrieb; Vorgabe von Grenzbeanspruchungen
	Wiederholungsprüfung	Komponentenzustand	Prüfung meßbarer Parameter (z.B. Rißanzahl,-tiefe,-wachstum); zeitliche Extrapolation
	stochast. physikalische Fehlermodelle	Fehlermechanismus	stochastische Bruchmechanik; stochastische Erdbebenbetrachtung; Extremwertverteilungen; z.B. /9/
	Komponenten-Auswahl	Verringerung des Verfügbarkeitsrisikos	computergestützte Analyse der mechanischen Spannungen und der Plastizität; Eignung von Form und Material; /10/
Zusammenarbeit von Auftraggeber, Auftragnehmer, Unterauftragnehmer und Überwacher während der Planungs-, Herstellungs- u. Montagephasen	Qualitätssicherung /11/	Material, Fertigung, Prüfwesen, Nachweise	Materialprüfung; Herstellungs- und Montageüberwachung
	Zuverlässigkeitsplanung /12/	Zuv. von Komponenten, Redundanz, Automatisierung	Zuverlässigkeitsdaten von Komponenten; Zuverlässigkeitsanalyse; Hersteller-Vergleich /6/
	Zusammenarbeit im Genehmigungsverfahren	Genehmigungsschritte, Vorschriften, Dokumentation	Einzelnachweise; Auflagen; Betriebsvorschriften; Zuverlässigkeitsanalyse; EVA-Auslegung; etc.
Erarbeitung von Entscheidungshilfen für die Instandhaltung	Zeitabstände, Dauer u. Umfang von Revisionen	Maßnahmen-Bündelung, Revisionserfolg	Schadensstatistik-Auswertungen; Analyse von Verschleiß- u. Abnutzungsschäden; Schätzung von zeitabhängigen Ausfallraten u. des Revisionserfolges/13,15/
	Wartungs- und Inspektionsaufwand	welche Komponente wird wann gewartet bzw. inspiziert	Vorgaben von Zeitabständen und geeigneter Maßnahmen durch Hersteller und aus Bewährungsdaten; Checklisten; /14/
	Verfügbarkeitsprognose	Verfügbarkeit mehrerer oder eines Blockes oder Hauptaggregates	heurist. Extrapolation aufgrund von Ergebnissen der Schadensstatistik; Zerlegung in Zeitintervalle vor/nach Revision und Schätzung ; /15/

Tabelle 2: Weitere Zuverlässigkeitsprobleme und benötigte Informationen

Zuverlässigkeits-problem	Lösungsweg	für die Lösung benötigte Information: welche Information	wie erhalten
Bedienungsfehler	Schulung und Training des Bedienungspersonals	Handlungs- u. Verhaltensinformation	Handbücher für Betriebs- und Störfälle, Kurse; Einweisung durch Anlagenhersteller
	ergonomische Anlagengestaltung	Gestaltung von Hardware u. Info.- flüssen	wissenschaftliche Untersuchungen; technische Erfahrungen; Zuverlässigkeitsabschätzung
	Automatisierung	Modellinformation	Studien über stochast. Signale u. Ansprechwerte; Systemanalyse; Bewährungsdaten
Fehlanregung von Schutz- und Automatisierungseinrichtungen	optimale Einstellung	Praxisinformation	Einstellteste unter Betriebs- oder Prüfbedingungen; Funktionstests
	Mehrheitsentscheidungssystem	Schaltungslogik	Entwicklung; Bewährungsdaten; Zuverlässigkeitsanalyse
weitere Verbesserung von automatisierten Schutzeinrichtungen	detaillierte Systemanalyse	Zustandsübergänge, unbeabsichtigte Zustände	Systembetrachtung; Zeitabhängigkeit von Parametern; Zuverlässigkeitsanalyse; Einführung von Diversität
	fail-safe-Schaltung	Schaltungslogik, logische Barrieren	Entwicklung; Auslegungsgesichtspunkte
common-mode-failure	Herausfinden der common-modes	Information über redundanzvermindernde Fehlfunktionen	detaillierte und fachkundige Systemanalyse; Bedienungsanalyse; Instandhaltungsanalyse; Einbeziehung von Material, Konstruktion und Fertigung
	Diversität; räumliche Redundanz	technische Funktionen, bauliche Gegebenheiten	technische Betrachtung; Auslegung gegen EVA
quantitative Bestimmung des Risikos von KKW	Erstellung von Risiko-Studien	Ergebnisse von WASH-1400, AIPA, deutscher LWR-Studie	Untersuchung von Anlagen-Störfällen, EVA, Freisetzung und Ausbreitung radioaktiver Stoffe, biologischer Wirkung, Evakuierung; Zuverlässigkeitsdaten von Komponenten

Tabelle 3: Erfassungsmerkmale und Ziele der Datensammlungen

erfaßte Merkmale	RWE-Schadens-statistik	Modellfall Neurath	Modellfall Biblis B
Anlagenerfassung:			
- nach VDEW /21/	bisher	-	-
- Vorstufe KKS	-	ja	-
- KKS /22/ (Funktion/ Aggregat/Betriebs-mittel)	es erfolgt Umstellung	-	ja
technische Angaben über Betrachtungseinheit (Konstruktion, Nennwerte, Prinzip)	ja	ja	ja
Bauteil auch nach Wechsel des Einbauortes identifizierbar?	nur in Sonderfällen	ja	ja
Anzahl Bestriebsstunden oder Schaltspiele	nein	ja	ja
Umgebungsbedingungen der Betrachtungseinheit	bisher nicht, demnächst i. Sonderf.	ja	ja
Schadensbild (explizit)	bisher nicht, demnächst	nein	ja
Schadensbeschreibung (Text)	ja	ja	ja
Schadensursache	ja	ja	ja
Ausfallart, Fkts.-Element	nein	ja	ja
Zeitpunkte von Ereignissen	ja	ja	ja
Dringlichkeit d. Stillstands	ja	ja	ja
Schadensklasse	ja	ja	ja
Startgruppe f. Reparatur	ja	ja	ja
Intensität d. Personaleinsatzes	ja	ja	ja
Nichtverfügbarkeitszeiten	ja	ja	ja
Art der Fehlerentdeckung	nein	nein	ja
Zustand bei Ausfall	nein	nein	ja
Art der Ausfallwirkung	nein	nein	ja
Ziele:			
- Verfügbarkeitssteuerung	ja	nein	nein
- Schwachstellenforschung	ja	nein	möglich
- Zuverlässigkeitskenngrößen	bedingt	ja	ja

Tabelle 4: Verwendung und Aussagekraft von Schadens- und Zuverlässigkeitsdaten

Problem/ Tätigkeit	heutiger Stand der Praxis (allgem./Beispiele)	Bedürfnisse der Praxis nach verbesserter Methodik bzw. nach verbesserten Daten	Theorie heute sowie Informationsbedarf der Theorie aus der Praxis
Verfügbarkeitsplanung			
Komponentenauswahl	Dokumentation von Schadensschwerpunkten (Listen, Histogramme) je Komponente über mehrere Anlagen; Herstellervergleich der Verfügbarkeitsergebnisse	Streubereich der Daten (λ, μ) sehr groß, daher Bildung von Teilkollektiven besser vergleichbarer Komponenten und Bauteile bzw. zusätzliche Ingenieurbewertung	Entscheidungskriterien bilden trotz großer Ausfallratenstreuung; Berücksichtigung physikalischer Parameter
Daten- und Erfahrungsrückführung	Rückführung der aufbereiteten Schadensdaten in die Planung und an den Hersteller (sowie in die Instandhaltung)	zumeist problemorientierter Informationsrückfluß; Ausschöpfung des Datenmaterials könnte verbreitert werden	Möglichkeiten der Datenbanken voll einsetzen (speichern, sortieren, geeignete Datensätze abrufen; ggf. Zuv.-Formeln bilden)
Verfügbarkeitsprognose	Formeln zur Berechnung der System- aus der Komponenten-Verfügbarkeit; Beurteilung und Extrapolation der Verfügbarkeitsabhängigkeit von Anlagengröße und -generation	da oftzwei oder mehr verschiedene Verhaltensvarianten auftreten können, sind Prognosen entsprechend zu strukturieren	zeitabhängige Ausfallraten (Früh- bzw. Spätausfälle) und ggf. zeitabh. Erneuerungsraten benutzen; Berücksichtigung von Parallelreparaturen
Verfügbarkeitsoptimierung	Beurteilung von Mono- bzw. Duo-Bauweise (von Dampferzeugern), von Redundanzen (z.B. Speisewasserpumpen) und von Umbau-Investitionen	Die Optimierung beschränkt sich auf die Beurteilung und Auswahl der möglichen Varianten; Analyse von Abnutzungsvorgängen	Erfolge von Voll- bzw. Teilreparaturen (mathematisch) formalisieren bzw. abschätzen; Verfügbarkeitsbewertung geänderter Konstruktionen und neuer Materialien ist problematisch
Sicherheitsplanung			
Zuverlässigkeitsanalyse	ausgedehnte Anwendung der Zuverlässigkeitsanalyse für spezielle Teilsysteme; Annahme konstanter Ausfallraten; auch deterministische Vorgaben (Einzelfehler, Reparatur)	Gewinnung von mehr Zuverlässigkeitsdaten (Einbeziehung weiterer Anlagen); ad-hoc-Bestimmung von Ausfallraten spezieller Komponenten	Einbeziehung zeitveränderlicher und regelungstechnischer Vorgänge in die Zuverlässigkeitsanalyse
common-mode-failures	gewisses Datenmaterial vorhanden; relativer Anteil von c.m.f. an allen Ausfällen je Ausfallart und Komponente gebildet	weiteres Datenmaterial wird die vorhandenen Zahlen und Faktoren weiter erhärten	entsprechende Systemanalyse (Einbeziehung auch der Entwicklungs- und Herstellphasen der Anlage) heute bereits praktiziert
menschliche Zuverlässigkeit	einige Daten vorhanden, weiteres Datenmaterial in Erarbeitung (z.B. Auswertung Betriebserfahrungen)	Datenauswertung (z.B. aus Betriebserfahrungen) ist komplex aber machbar; im allg. nur wenige Ereignisse	Weiterentwicklung von Modellen zur menschlichen Zuverlässigkeit;
Inspektionsabstände und -tiefe	Wahrscheinlichkeit des unbemerkten Ausfalles ist auch bei konstanter Ausfallrate zeitlich ansteigend, daher Vorgabe für Abstände von Inspektionen und Wiederholungsprüfungen möglich	noch bessere Abstimmung der Prüftermine mit den betrieblichen Erfordernissen (z.B. Revisionsintervalle, Zugänglichkeit)	Einbeziehung von Daten (Parameter und deren Verläufe) aus der Maschinendiagnostik

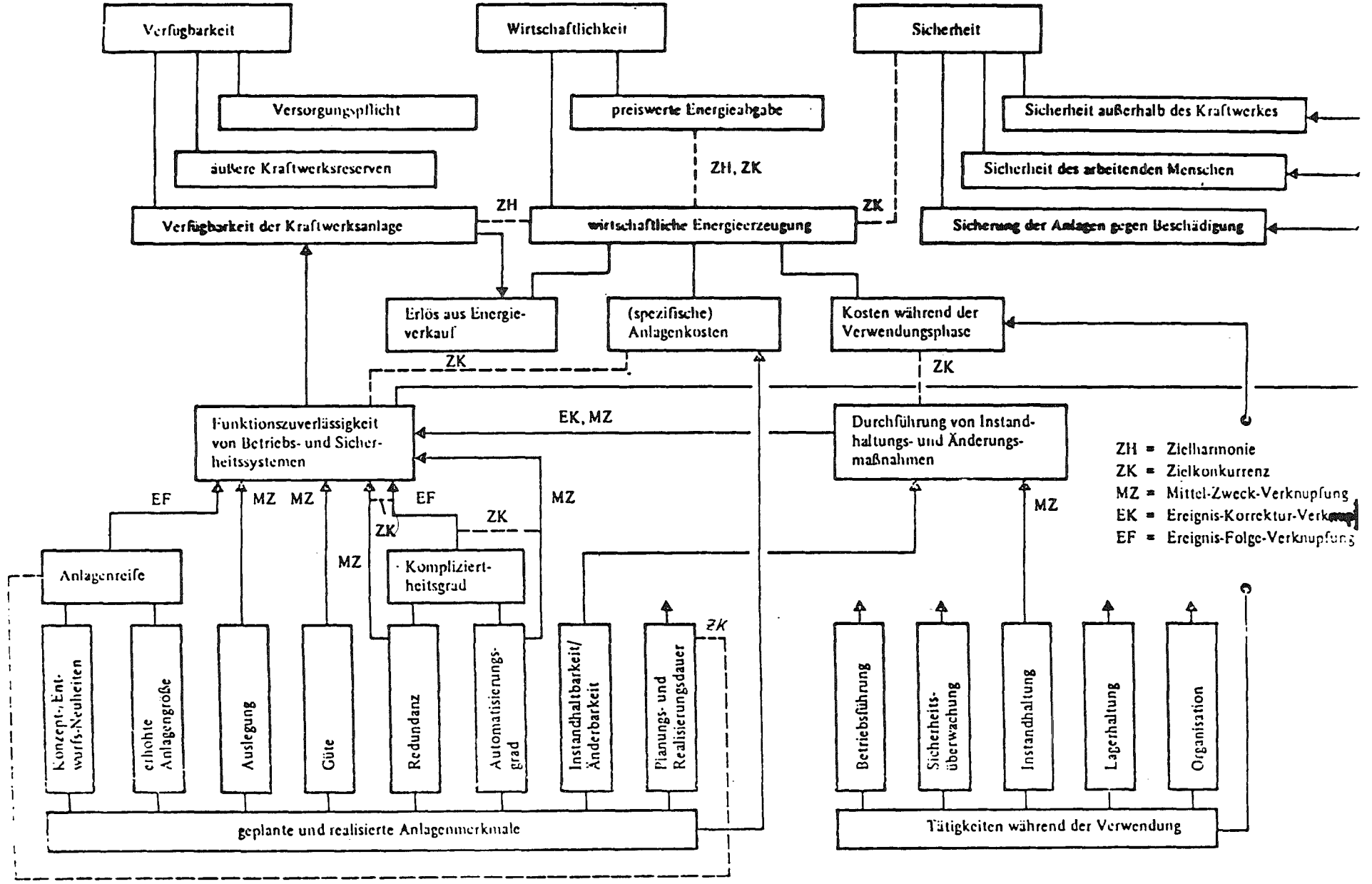


Bild 1: Die zentrale Bedeutung der Zuverlässigkeit im Zielsystem der Kraftwerksanlage.

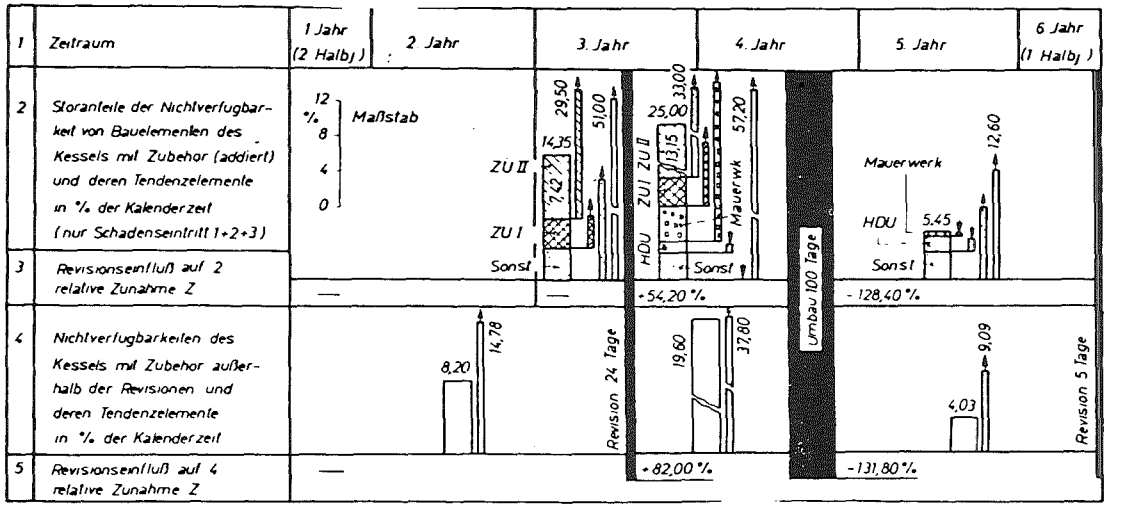


Bild 2 : Nichtverfügbarkeiten von Kessel 2 außerhalb der Revisionen

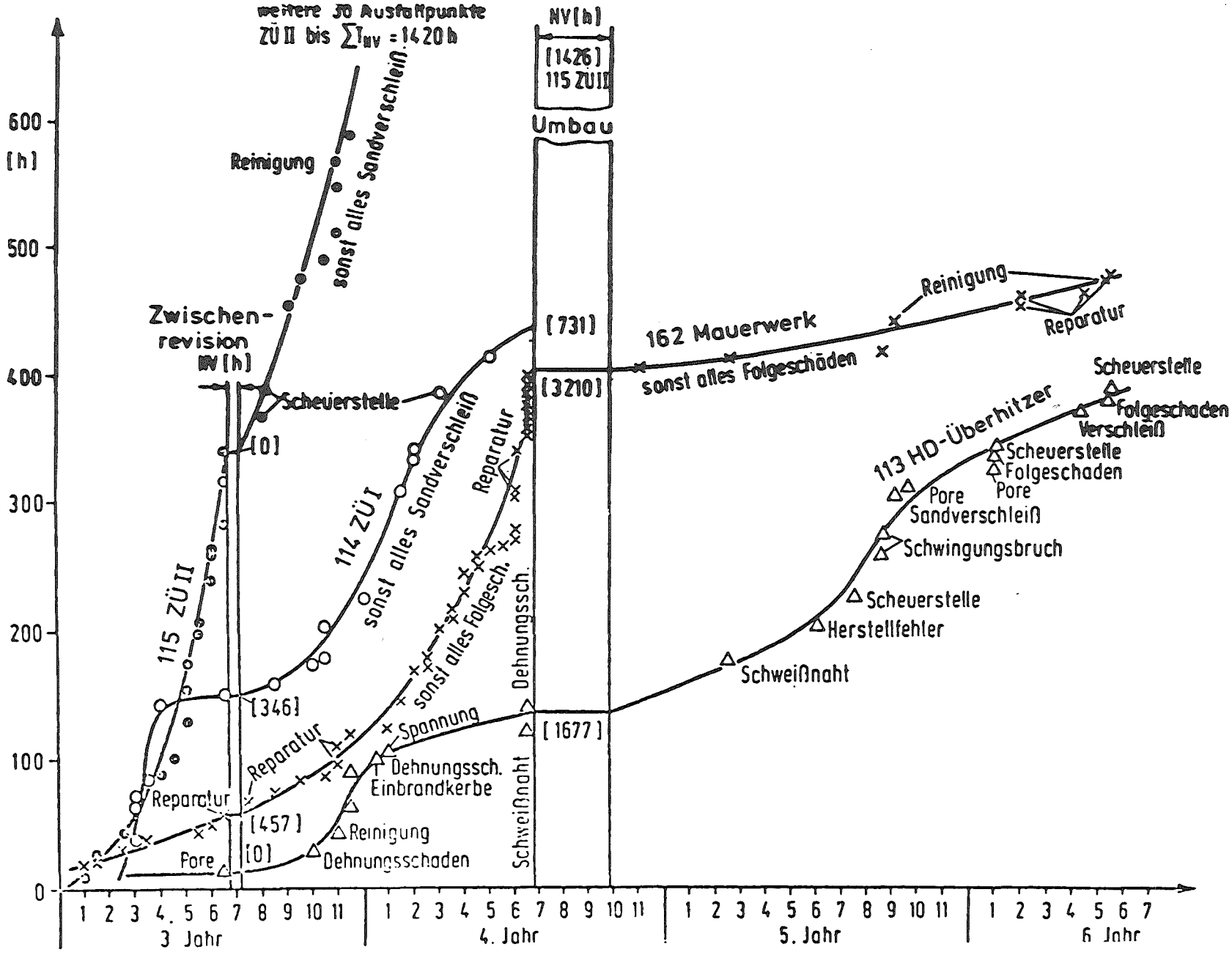


Bild 3: Zeitverlauf der kumulierten NV-Zeit.

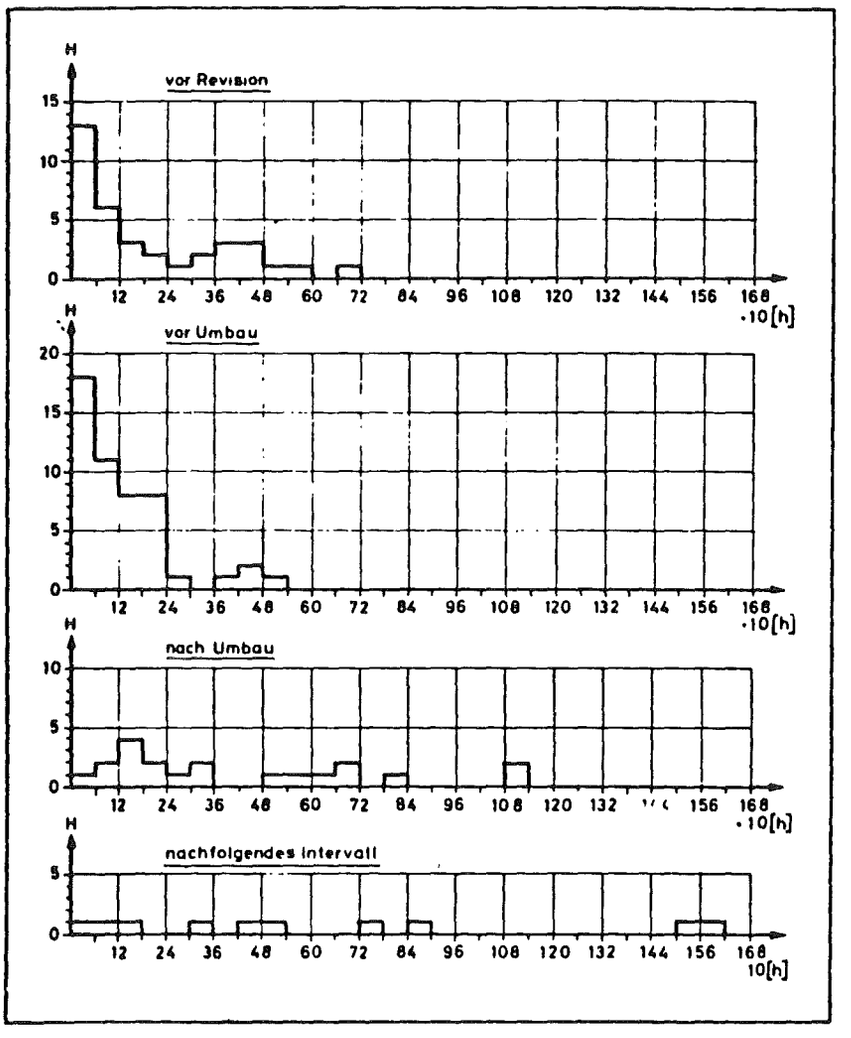


Bild 4: Histogramme der Betriebszeiten von Block 2 für die beiden Zeitintervalle vor dem Umbau und die beiden Zeitintervalle nach dem Umbau

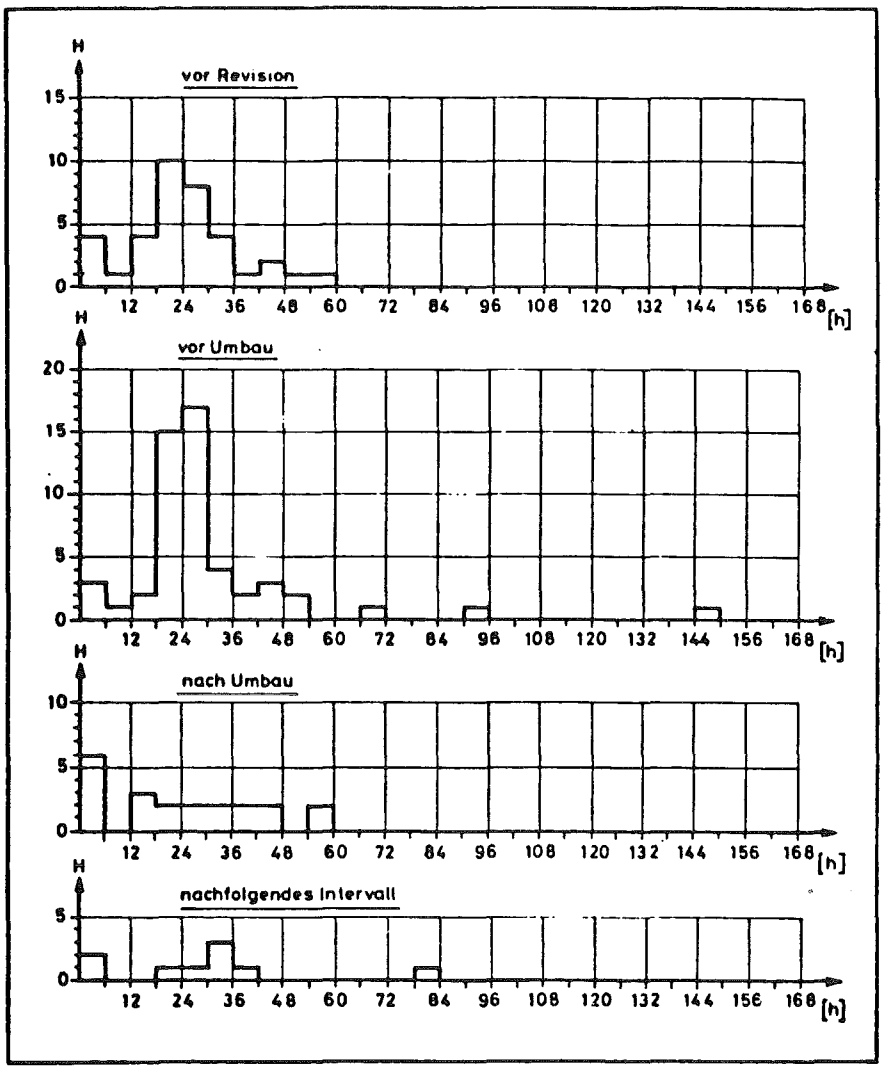
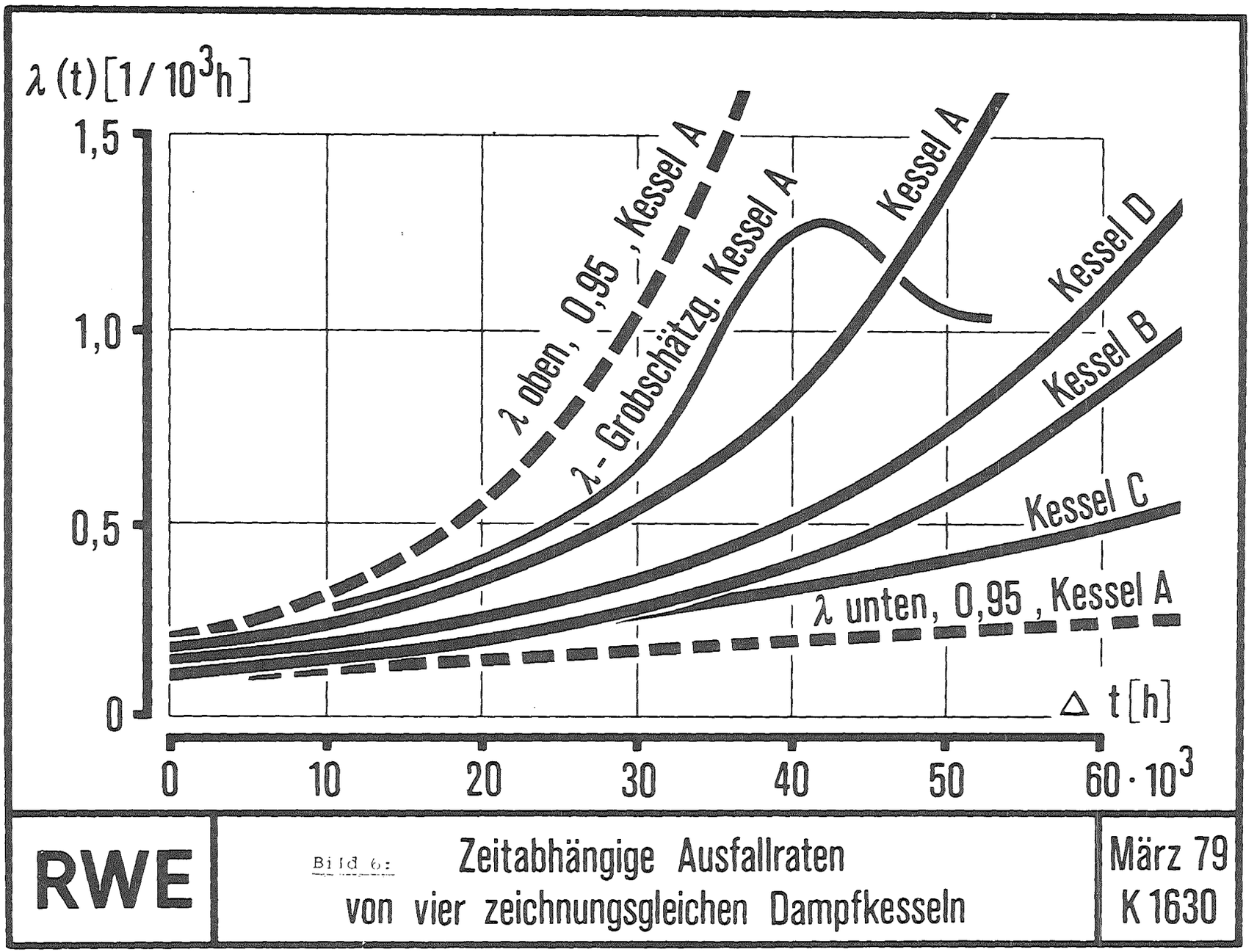
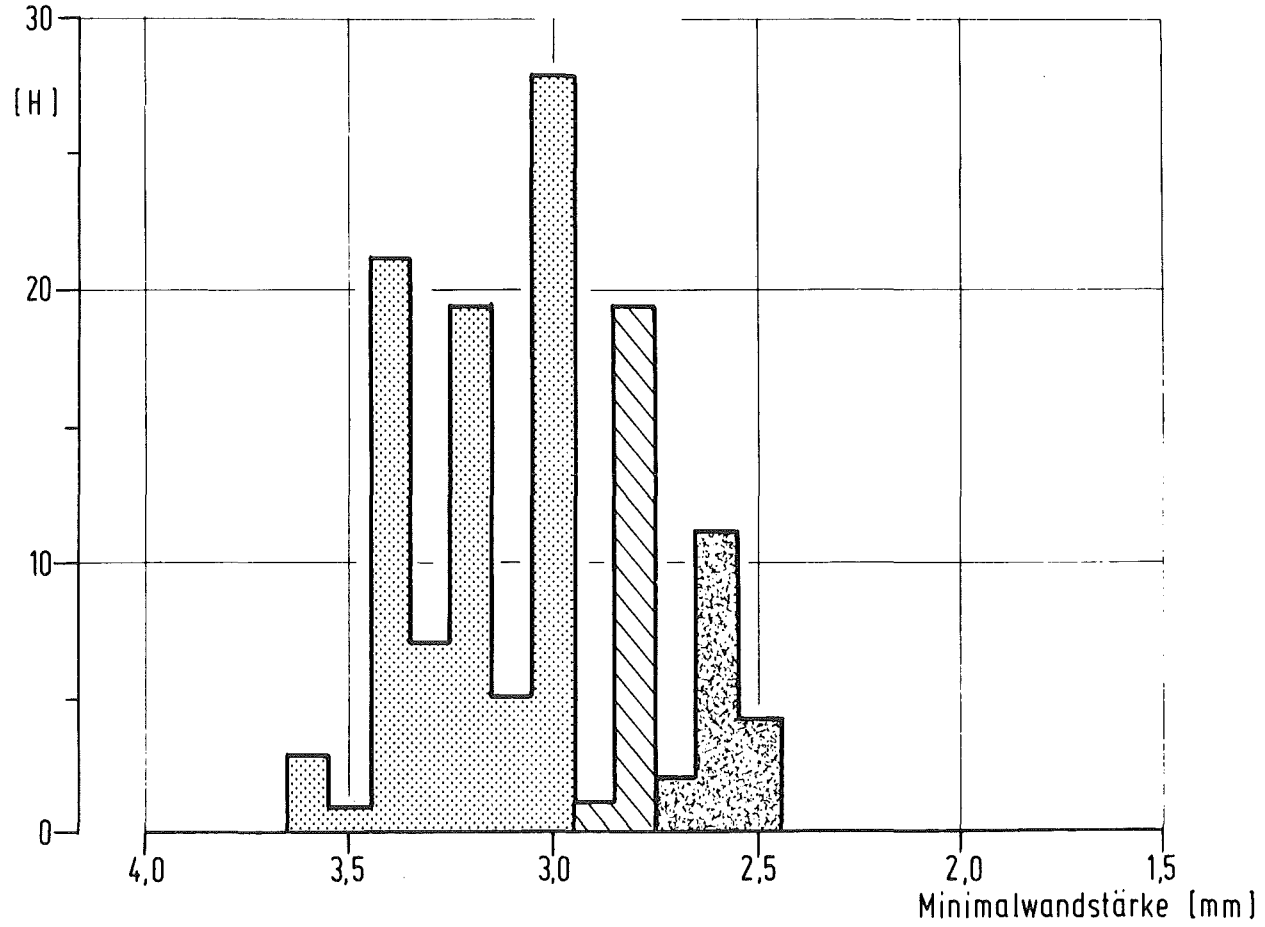


Bild 5 : Histogramme der NV-Zeiten von Block 2 für die beiden Zeitintervalle vor dem Umbau und für die beiden Zeitintervalle nach dem Umbau



RWE	Bild 6: Zeitabhängige Ausfallraten von vier zeichnungsgleichen Dampfkesseln	März 79 K 1630



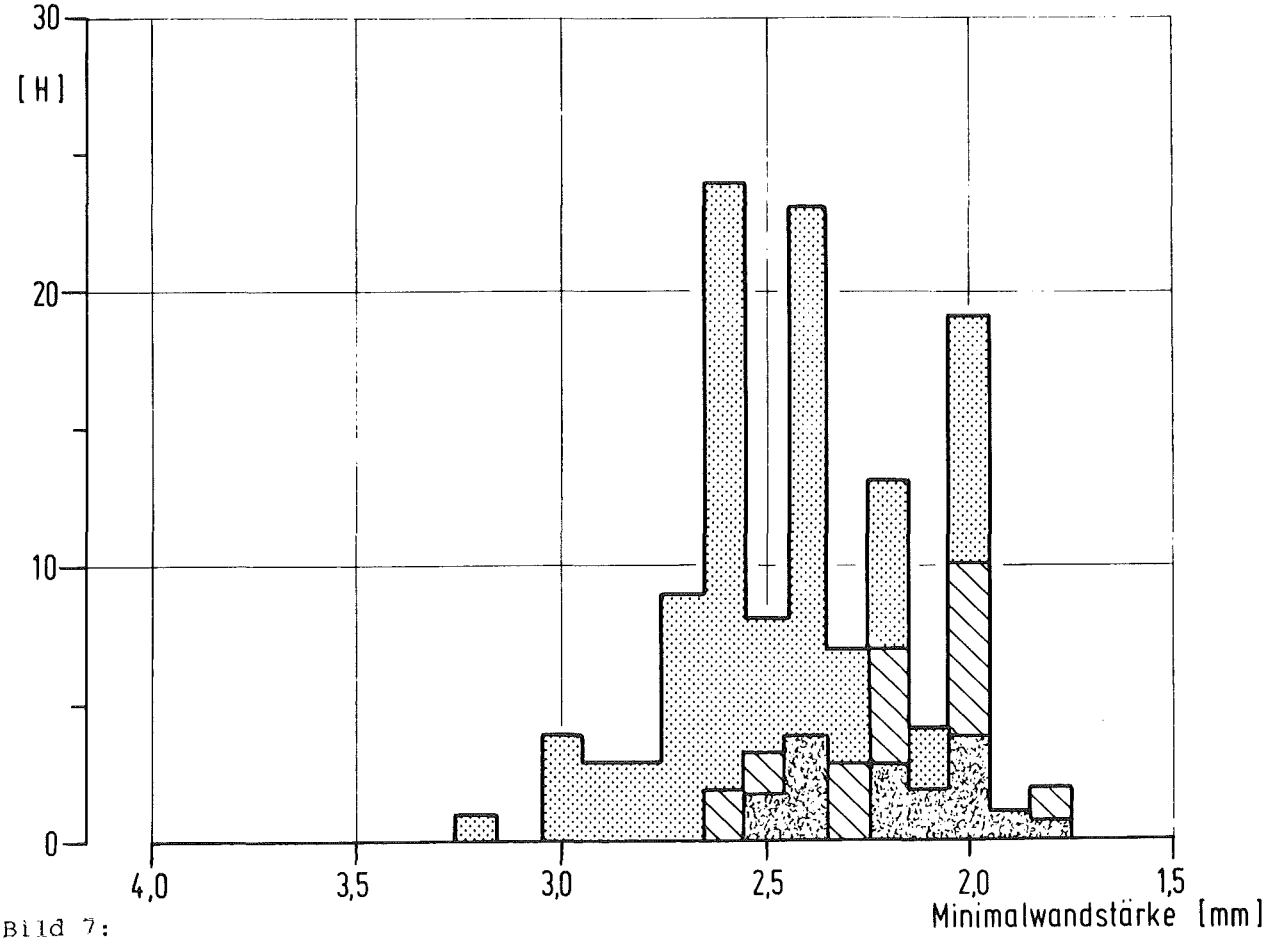


Bild 7:

Zeitliche Abnahme der Minimalwandstärke von Eco-Rohrbögen

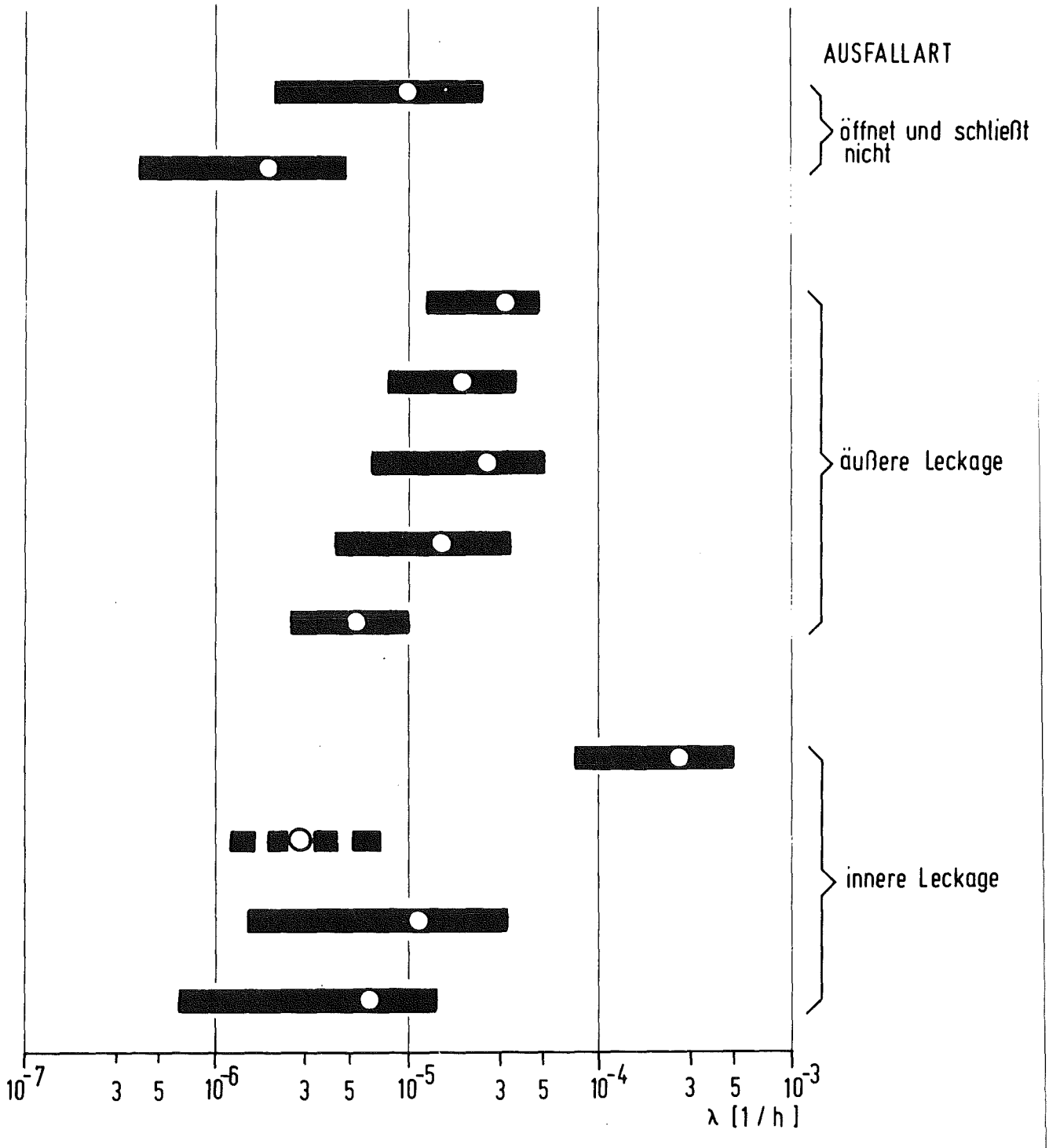
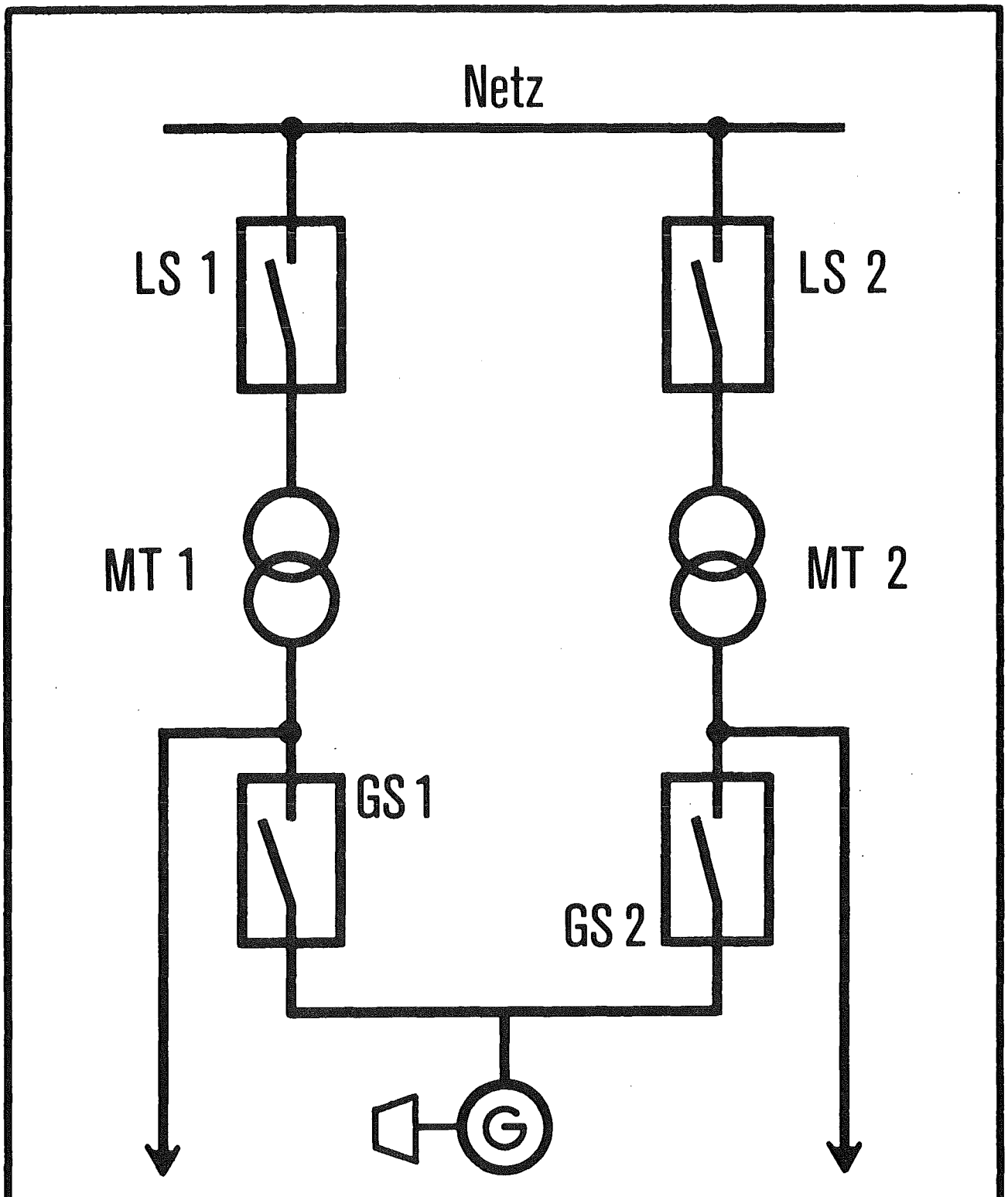


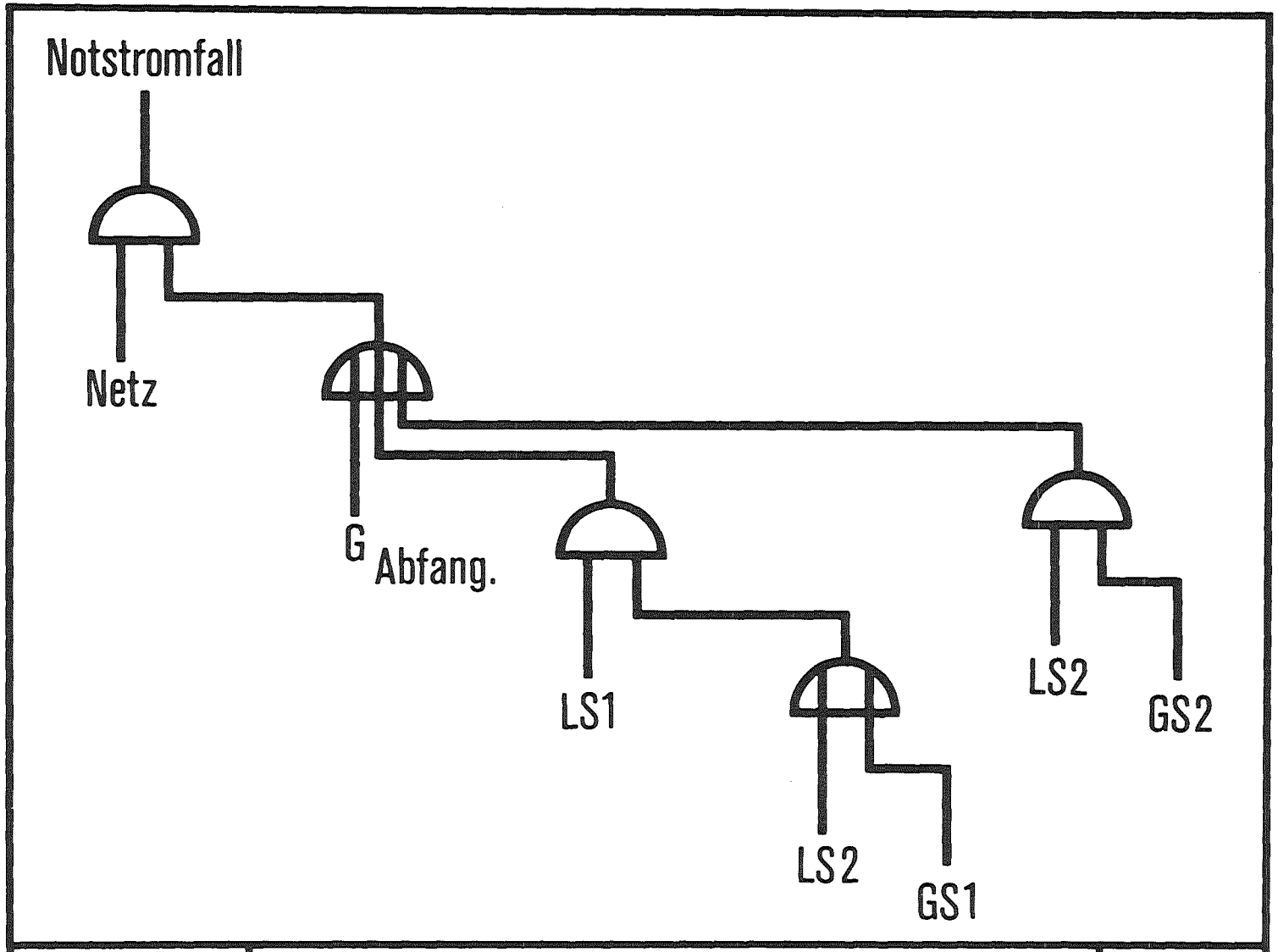
Bild 8: Streuung der Ausfallraten von Absperrschiebern



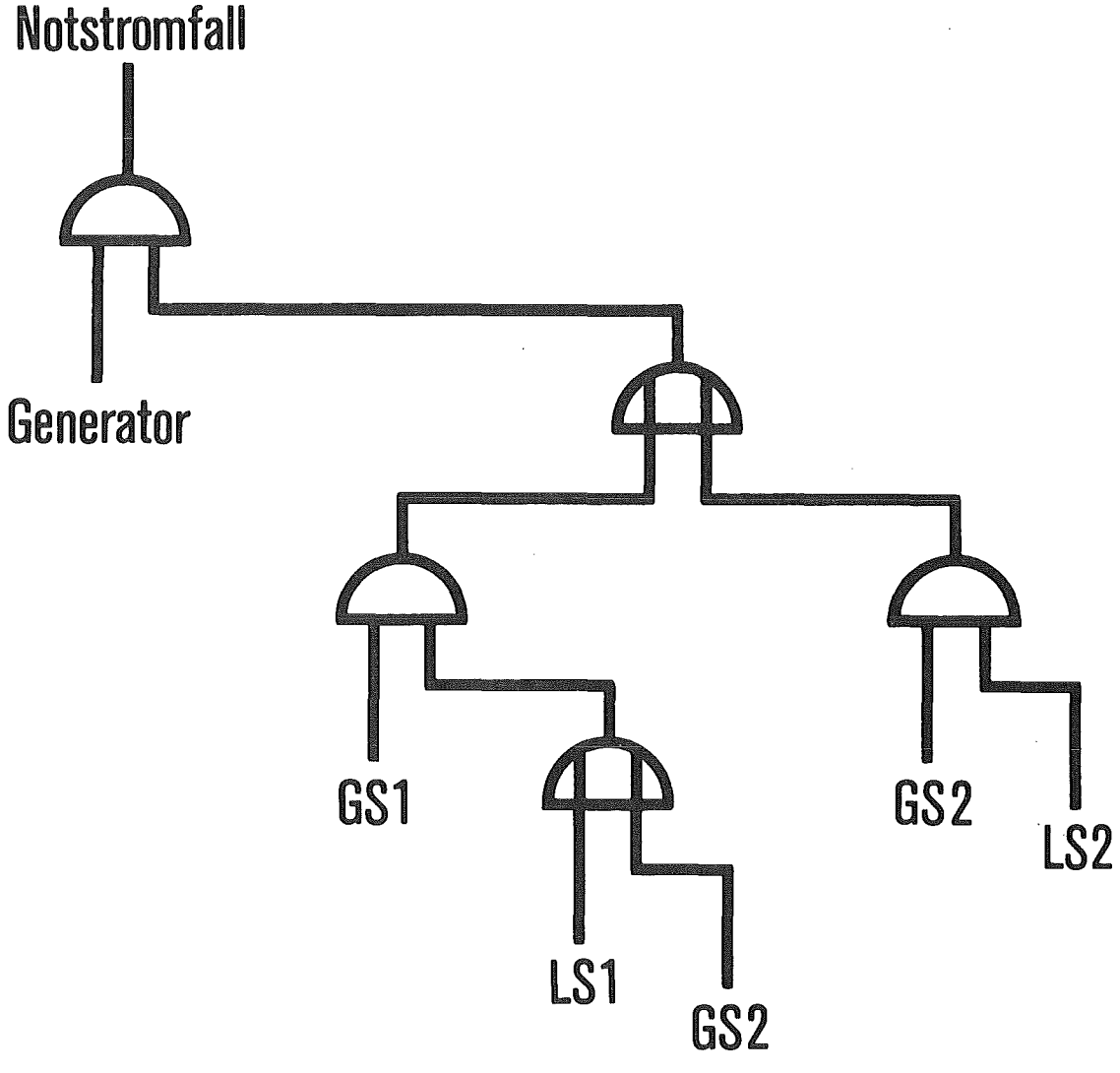
RWE

Bild 9: Zweigeteilter Haupt - Netzanschluß

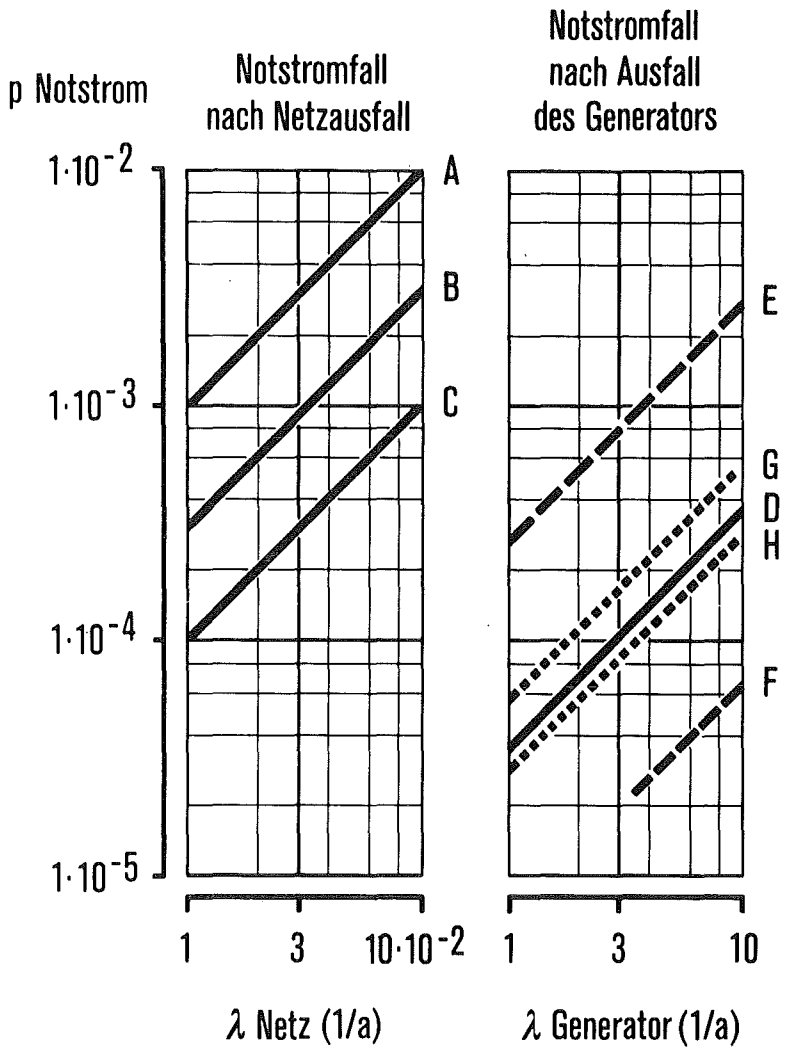
März 79
E 1631



RWE	Bild 10a: Fehlerbaum des Notstromfalles nach Netzausfall	März 79 E 1632



RWE	Bild 10b: Fehlerbaum des Notstromfalles nach Generatorausfall	März 79 E 1633



Legende:

Kurve	p (G_{NA})	p (GS)	p (LS)
A	$1 \cdot 10^{-1}$		
B	$3 \cdot 10^{-2}$		
C	$1 \cdot 10^{-2}$		
D		$5 \cdot 10^{-3}$	$1 \cdot 10^{-3}$
E		$1{,}5 \cdot 10^{-2}$	$1 \cdot 10^{-3}$
F		$1{,}7 \cdot 10^{-3}$	$1 \cdot 10^{-3}$
G		$5 \cdot 10^{-3}$	$3 \cdot 10^{-3}$
H		$5 \cdot 10^{-3}$	$3{,}3 \cdot 10^{-4}$

p (G_{NA}) ≡ Wahrsch. Nichtabfangen Generator

p (GS) ≡ Wahrsch. Versagen Generatorschalter

p (LS) ≡ Wahrsch. Versagen Leistungsschalter

RWE

Bild 11:

Wahrscheinlichkeit des Notstromfalles

März 79
E 1634

D i s k u s s i o n

Frage: Zur Beurteilung einer sinnvollen Leistungssteigerung haben Sie von Verfügbarkeitsanalysen für Braunkohlenblöcke verschiedener Leistungsgrößen gesprochen. Sind diese Untersuchungen auch für Kernkraftwerke verschiedener Leistungen durchgeführt worden?

Stellen hierbei längere Nichtverfügbarkeitszeiten durch Störungen in KKW dabei ein Einschränkung dar?

Antwort: Mit Hilfe von Daten aus den jährlichen Berichten der IAEA über das Betriebsverhalten von Kernkraftwerken habe ich die Zeitabhängigkeit der Verfügbarkeit der amerikanischen DWR- und SWR-Kernkraftwerke für aufeinanderfolgende Generationen in Kurvenform dargestellt (siehe zitierte Dissertation). Wie bei den Untersuchungen des Herrn Vetter über die Braunkohlenblöcke ergibt sich, soweit aus den Daten erkennbar, auch für die Kernkraftwerke keine abnehmende Verfügbarkeitstendenz mit steigender Blockgröße.

Eine Untersuchung mit Hilfe nur technischer (und nicht schadensstatistischer) Daten im Hinblick auf die Blockgrößen-Abhängigkeit der Verfügbarkeit von Kernkraftwerken ist mir nicht bekannt.

Frage: Wann wird vom Modellfall Biblis ein Ergebnis veröffentlicht?

Antwort: Vom RWE-GRS-Modellfall Biblis Block B zur Erfassung von Zuverlässigkeitsdaten wird 1981 ein Bericht erscheinen.

Frage: Sie haben über die Schadensstatistiken berichtet, die vom RWE aufgrund eigener Erfahrungen erstellt wurden. Nun gibt es aber Aufgaben im Bereich der Planung von z.B. neuartigen Anlagen, bei denen man nicht auf eigene Ausfalldaten zurückgreifen kann, sondern vielmehr auf Erfahrungen anderer Arbeitsgruppen bzw. auf Datenbanken zurückgreifen muß. Waren Sie selbst mit diesem Problem konfrontiert und wenn ja, haben Sie z.B. mit Datenbanken gearbeitet?

Antwort: Das Datenmaterial der RWE-Kraftwerksschadensstatistik ist wegen der großen Anzahl der Braunkohlen-Kraftwerkblöcke und wegen der bis-

herigen langen Erfassungszeit für den Bereich der konventionellen Kraftwerke ausreichend. Darüber hinaus läuft derzeit der RWE-GRS-Modellfall Biblis Block B zur Erfassung von Zuverlässigkeitsdaten von Kernkraftwerkskomponenten.

Darüber hinaus beteiligt sich das RWE mit seiner Schadensstatistik an der VGB-Kraftwerks-Schadensstatistik, in die auch die anderen deutschen Kraftwerksbetreiber einspeisen. Eine übernationale Beteiligung des RWE an Schadensdatenbanken, z.B. an der englischen Syrel-Datenbank, findet nicht statt.

Frage: Betrifft Tabelle 3 Erfassungsmerkmale und Ziele der Datensammlung.

Warum wurden gerade die für die Zuverlässigkeitsanalyse wichtigen Merkmale (Kolonne RWE, teilweise Neurath)

- Anzahl Betriebsstunden
- Ausfallart
- Art der Fehlerentdeckung
- Art der Ausfallwirkung

weggelassen ("Nein")?

Antwort: Die von Ihnen genannten und aus der Tabelle 3 ersichtlichen Merkmale sind in der bisherigen Form der RWE-Kraftwerksschadensstatistik nicht enthalten, da diese Schadensstatistik ja zum Zwecke der Verfügbarkeitsdokumentation und -kontrolle, nicht aber direkt zur Gewinnung von Zuverlässigkeitsdaten ins Leben gerufen wurde. Trotzdem hat diese Schadensstatistik bisher wichtige Aussagen über die Zuverlässigkeit spezieller Komponenten hergegeben.

Die RWE-GRS-Modellfälle Neurath bzw. Biblis Block B sind dagegen von ihrer Zielrichtung her zur Gewinnung von Zuverlässigkeitsdaten eingerichtet worden.

Zuverlässigkeit langlebiger Systeme am Beispiel der Satellitentechnik

Dr.rer.nat. H.W. von Guérard
Freier Berater
bei der
INDUSTRIEANLAGEN-BETRIEBSGESELLSCHAFT m.b.H.
8012 Ottobrunn

Referat zu T O P 4,

Praktische Zuverlässigkeitsrechnung und Qualitätssicherung

- Methoden und Algorithmen
- spezielle Probleme der Raumfahrt

des Seminars

"Methoden der Systemplanung bei geforderten Langzeitbetriebsverhalten"

am 26./27. Februar 1980 beim

Kernforschungszentrum Karlsruhe

Vorbemerkung:

Dieses Referat fällt in zweifacher Hinsicht aus dem Themenkreis des Seminars heraus: Zunächst steht hierbei nicht Zuverlässigkeit aus der Sicht der Kraftwerkstechnik im Mittelpunkt der Betrachtung, sondern Produktsicherung als Anliegen der Satellitentechnik. Dabei folgt derjenige Teil des Referats, der sich vorwiegend mit Tests beschäftigt, im wesentlichen einem im Vorjahr gehaltenen Referat, das im 2. Teil dieser Niederschrift als Nachdruck wiedergegeben ist.

Weiterhin ist festzustellen, daß der 1. Teil dieser Niederschrift nicht etwa ein Bericht über eine wissenschaftlich-technische Untersuchung ist, sondern ein persönlicher Erfahrungsbericht über die Entwicklung von Sicherheits- und Zuverlässigkeitsrechnung, der auf jahrzehntelanger Tätigkeit, davon großenteils in den USA, beruht. Verf. wünscht vorweg klarzustellen, daß eine solche Regelung in Vereinbarung und auf Befürwortung der Veranstalter getroffen wurde.

Erfahrungsbericht

1. Die Kunst der Primitiven

Langlebigkeit technischer Systeme ist ein Begriff, der in Relation zur erreichbaren Lebensdauer gesetzt werden muß. Für einen Nutzsatelliten sind im allgemeinen 5 bis 7 Jahre bereits eine beachtliche Lebenszeit, insbesondere, da es sich dabei um ein nicht-wartbares, nicht-reparierbares System handelt; siehe dazu die Einleitung des 2. Teils dieser Niederschrift, hier als /1/ referiert. Wir werden heute mit den speziellen analytischen Problemen der Zuverlässigkeit von Satelliten zufriedenstellend fertig, - dabei kann man nicht einmal sagen, daß von dieser Seite aus eine besondere Befruchtung der Theorie eingesetzt hätte. Aber gegen Ende der fünfziger Jahre, als bereits die Vorarbeiten zum Apollo-Programm voll im Gang waren, sah unser Werkzeugkasten wesentlich dürftiger aus.

Lassen Sie mich aus dieser Zeit berichten: Von einem etablierten Wissenszweig "Technische Zuverlässigkeit" war damals noch keine Rede, und als ich mit diesem Thema für das Lockheed (California Division)-Angebot für Apollo beauftragt wurde, standen mir zwar Kenntnisse aus einigen verwandten Gebieten zur Verfügung (Statik und Festigkeit; Biostatistik, statistische Qualitätskontrolle), aber die erforderliche Synthese zur Zuverlässigkeits-Analyse war damit nicht verbunden. Die Projektleitung drückte mir ein "paperback" /2/ in die Hand, in dem auf 11 Seiten "Reliability and Maintainability" /3/ sehr überschlägig abgehandelt war, - im Vergleich zum heutigen Stand wirklich noch die Kunst der Primitiven! Der Lockheed-Entwurf landete als "runner-up", und damit war für mich die erste Lektion in Zuverlässigkeitstechnik überstanden. Immerhin hatte ich dabei auch erfahren, wie optimistisch die Elektroniker waren: "Alle 5 Jahre bekommen wir eine neue 9 hinter dem Komma" hieß es hoffnungsvoll, und sie haben bis heute im wesentlichen Recht behalten. Das war die Vorwegnahme des Duane- oder anderer logarithmischer Modelle für "reliability growth".

Man möge aber nicht denken, es hätten damals dort, wo sie unbedingt gebraucht wurden, noch keine soliden Kenntnisse der Zuverlässigkeitsmathematik vorgelegen; nur die Veröffentlichungen waren noch nicht so weit: 1963 erschien das bemerkenswerte Buch von Pieruschka (ebenfalls bei Lockheed), siehe /4/, und erst 1965 wurde mit dem inzwischen klassischen Buch von Barlow-Proschan-Hunter /5/ eine wirkliche Systematik der technischen Zuverlässigkeit vorgelegt.

Pieruschka, der aus der Peenemünder "Schule" kam, arbeitete auf dem Gebiet der Raketentechnik und hatte von Robert Lusser, dem (selbsternannten) Vater der technischen Zuverlässigkeit, frühzeitig gelernt, daß es "inhärente" Fehler komplexer Systeme gibt, die sich innerhalb der gegebenen Grenzen von Technologie, Zeit und Budget nicht vermeiden lassen, und mit denen weitgehend so gerechnet werden kann, als ob sie unabhängig-zufällig auftreten würden. Zu den besten (sehr kurzen) Zeiten der V1- und V2-Rakete war ohnehin kein "trade-off" zwischen Aufwand und Erfolgswahrscheinlichkeit mehr möglich, der letztere über etwa 60 v.H. gebracht hätte (siehe /4/). Heute mögen es für Satelliten (nach erfolgreichem Abschuß) 95 v.H. sein, für ihre Träger (Raketen) vielleicht 85 v.H.; ob der Rest des Risikos im strengen Sinn "inhärent" ist, läßt sich schwer sagen.

Robert Lusser's Zuverlässigkeits-Pessimismus war allgemein bekannt: Er prophezeite die Unmöglichkeit bemannten Raumflugs, weil einfache Systeme per se, und komplexe Systeme wegen Schaltungs- und anderen Unsicherheiten unzuverlässig sein müßten. Das ist längst widerlegt, aber seine Theorie der inhärenten Fehler hat schließlich zur heutigen Zuverlässigkeitsanalysis geführt, die wir Koryphäen wie Shannon, Eisenhart, Epstein, Shooman (alle USA) und vielen anderen verdanken.

Die Zuverlässigkeitsmathematik kann zum großen Teil als mathematische Theorie elektrischer und elektronischer Redundanzen bezeichnet werden. Bis wenigstens die Basis dieser Theorien Allgemeingut geworden war, behalfen wir uns mit heuristischen Modellen für Redundanz, wobei wir Anleihen bei anderen, uns besser vertrauten Gebieten der angewandten Mathematik machten. So erinnere ich mich aus meiner Zeit bei Lockheed, optimale Allozierung kalter Redundanzen durch das mir aus der kommunalen Statistik bekannte d'Hondt'sche Verfahren asymptotisch approximiert zu haben. Das d'Hondt'sche Verfahren leistet die "möglichst proportionale" Zuteilung von Mandaten auf Wählerstimmen. Für den mir vorliegenden Zweck waren je Untersystem identische Elemente so zu allozieren, daß die Kette aus diesen Untersystemen für gegebene Missionszeit möglichst zuverlässig war; heute sind dafür bessere, exakte Algorithmen bekannt.

2. Kritik an Routinen

Die Organisation der Produktsicherung in der Raumfahrt konnte im wesentlichen von der Luftfahrtindustrie übernommen werden. Es ist fast schon Standard, folgenden Aufbau einzuhalten:

a) parts, materials and processes
b) reliability apportionment and prediction
c) manufacture inspection and tests.

In diesem Rahmen haben sich eine Reihe von weitgehend genormten Routinen entwickelt, die der Produktsicherung im weitesten Sinne dienen, so z. B. auch "configuration management and control"; Fehlerbaumanalyse und die (in entgegengesetzter Richtung arbeitende) Störfallablaufanalyse werden in der Raumfahrt angewandt wie auch sonst überall. Über die wichtige Störmeldeverfolgung bliebe einiges zu sagen, - und das steht, in engem Zusammenhang mit den Erfahrungen bei den Satelliten AEROS (A und B) und AZUR, in einer bemerkenswerten Kritik /6/, die sich fast wie ein Kriminalroman liest, nämlich, wie (gelinde gesagt) unkritisch häufig verfahren wurde!

In diesem Zusammenhang ist die FMECA (failure modes, effects and criticality analysis; Ausfallarten- und Auswirkungsanalyse) zu erwähnen, die von den Komponenten an aufwärts durch alle Stufen der Systemintegration bis zum Satelliten als Ganzes durchzuführen ist. Sie ist nur quantitativ zu verstehen, - zu einer Revision der Zuverlässigkeits-Hochrechnung aus Komponenten käme sie ohnehin zu spät.

Was mir bei diesem Verfahren unverständlich bleibt, ist der immer wieder betonte Aspekt, das ein "single failure point" (s.f.p.) besonders gefährlich sein müsse und deshalb möglichst zu eliminieren sei. Eine seriell geschaltete "black box" mit innerer Redundanz ist sicher eine solche singuläre Fehlerstelle, - wenn man sich die "black box" als Rahmen entfernt denkt, aber offenbar nicht mehr! Nach der Theorie, daß komplexe Baueinheiten immer ein zusätzliches Risiko enthalten, sollten singuläre Fehlerstellen sogar begrüßt werden!

Maßgeblich ist, ganz im Gegensatz zu diesen stereotypen Warnungen vor s.f.p., das Zuverlässigkeits-Profil über Zeit, das in Verbindung mit einer Betrachtung zum Nutzwert der Zielerfüllung als Funktion der Zeit zu beurteilen ist: Nur selten ist nichts anderes als ein genauer Zeitpunkt der Missionserfüllung zu bewerten, - mitunter aber doch, so bei Forschungssatelliten mit sehr speziellem Auftrag; häufiger ist es so, daß entweder Untererfüllung, etwa 5 Jahre Lebensdauer eines Nutzsatelliten statt vorgesehener 7, oder auch Übererfüllung, mit bestimmten Werten belegt werden können. Relativ hohe Bewertung von Untererfüllung zielt auf einen steilen Durchgang der Zuverlässigkeits-Charakteristik durch den spezifizierten Punkt R_m, t_m (Index m für Mission) und damit auf möglichst hohe Redundanz, - und umgekehrt bei hoher Bewertung von Übererfüllung. Man sollte aber nicht übersehen, daß die Allozierung von Redundanzen oft ein technisches Problem ist, das wenig oder keine Freiheitsgrade zur Berücksichtigung von zusätzlichen Forderungen in der R_m, t_m-Ebene läßt.

Die Allozierung und Auswertung von Redundanzen stellt heute kein Problem mehr dar, weder konzeptionell noch rechnerisch. In der neueren Entwicklung kommt auch eine spezielle Art der Betrachtung auf, die die Importanz von Baueinheiten unter dem Aspekt der Systemzuverlässigkeit quantifiziert; dazu wird, in unterschiedlichen Ansätzen (nach Birnbaum bzw. nach Barlow und Proschan), die Wahrscheinlichkeit der Beteiligung einer Komponente am Systemausfall bestimmt (siehe z. B. /7/); vor allem dürfte damit das fragwürdige Konzept von der besonderen Kritikalität der sogenannten sigulären Fehlerstellen endgültig ausgeräumt werden.

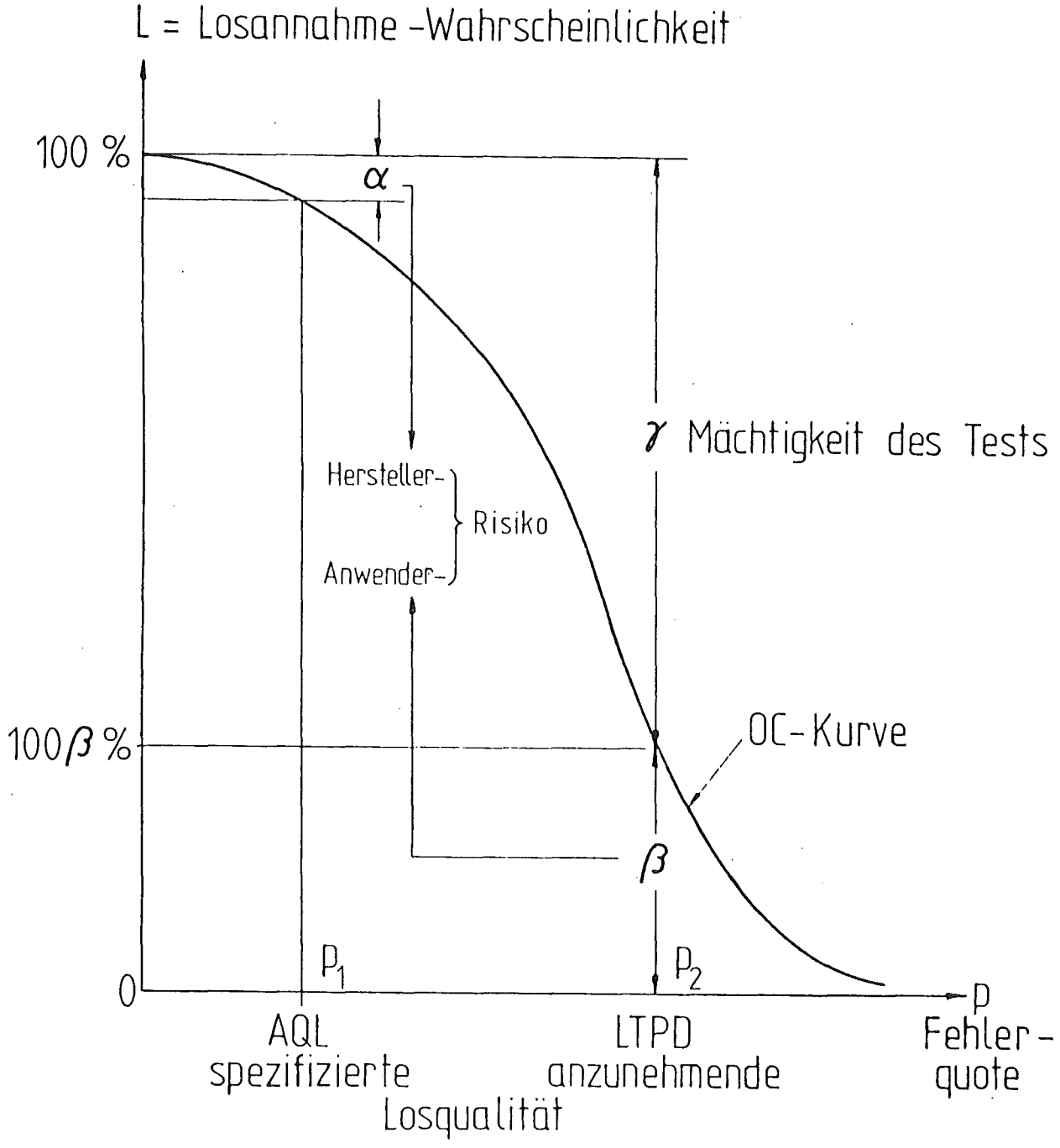


BILD 1: OPERATIONS-CHARAKTERISTIK

3. Bauteilequalität und Systemzuverlässigkeit

Bei allem Zutrauen in die Zuverlässigkeitsmathematik hat mich im Laufe der letzten Jahre immer wieder ein Zweifel beunruhigt, der eigentlich vor aller Analysis bereits behoben sein sollte: Was ist der Zusammenhang von Bauteilequalität und Systemzuverlässigkeit? Die Zuverlässigkeitsmathematik leistet schließlich nur eine "Hochrechnung von Ausfallraten" durch alle Stufen der Systemintegration, - wie es aber mit der Vertrauenswürdigkeit der Ausgangsdaten aussieht, darüber sagt sie nichts. Es ist sicher interessant, einmal in die statistischen Schlußweisen hineinzuleuchten, die dem Zusammenhang von Zuverlässigkeit und Qualität zugrunde liegen.

Die Bauteileprüfung wird zum Teil auf Stichprobenbasis durchgeführt, nämlich soweit es Umgebungs- und Lebensdauertests betrifft. Hierbei gilt selbstverständlich "test items don't fly" (siehe /1/). Es wäre ein Repräsentationsschluß durchzuführen, aber das ist im allgemeinen umständlich; durch die Anwendung des Kunstgriffs der OC-Kurve (Operations Characteristic) wird nun dieser Schluß auf die Form des Inklusionsschlusses von der Grundgesamtheit auf die Stichprobe zurückgeführt. Die Grundlagen dazu wurden beim National Bureau of Standards (USA) entwickelt; siehe /8/. Das ist in Bild 1 veranschaulicht; LTPD ist dabei die rechnerisch anzunehmende Qualität - und nicht etwa die Losannahmequalität! α und β sind wie üblich die Risiken 1. und 2. Art.

Von besonderer Wichtigkeit erscheint mir, wie von Qualitätsmessungen an Bauteilen, die günstigenfalls zur Losannahme führen, auf Lebenserwartung unter Betriebslast geschlossen wird. Dazu müssen zwei streng auseinander zu haltende statistische Schlüsse herangezogen werden:

(1) Zwischen einer Kombination gewisser Meßdaten einerseits und der zu erwartenden Ausfallrate andererseits wird, auf der Basis kumulativer Ausfallraten, ein Korrelationszusammenhang postuliert.

(2) Zwischen dem ersten oder Prototyp-Los und den Nachbaulosen aus kontrollierter Fertigung wird eine Homogenität postuliert, die die Übertragung der Korrelation auf diese späteren Lose erst gestattet.

Das Schema ist demnach

Schluß	Substitution	Transponierung
Mengen	dieselben	verschieden
Merkmale	verschieden	dieselben
Kriterium	Korrelation	Homogenität
Testgröße	r^2	χ^2

Substitution: Qualität für Lebensdauer;
Transponierung: vom Prototyp- auf Nachbaulose.

Man vergleiche dazu Bild 2, das einer früheren Arbeit entnommen ist /9/, bei der ich einem anderen Gedankengang folgte, nämlich, daß die Information aus dem Prototyp-Los als Priori-Information mit Test-Information aus dem Nachbaulos gekoppelt wird, und daß dieser Prozeß im Laufe weiterer Tests iteriert werden kann; dabei wird konsekutiv immer wieder die letzte Posteriori- zur nächsten Priori-Information. Davon bin ich aber wieder abgekommen und berufe mich darauf, daß wohl jeder Statistiker, der auf sich hält, einmal in seinem Leben Bayesianer gewesen ist, - und dann nie wieder.

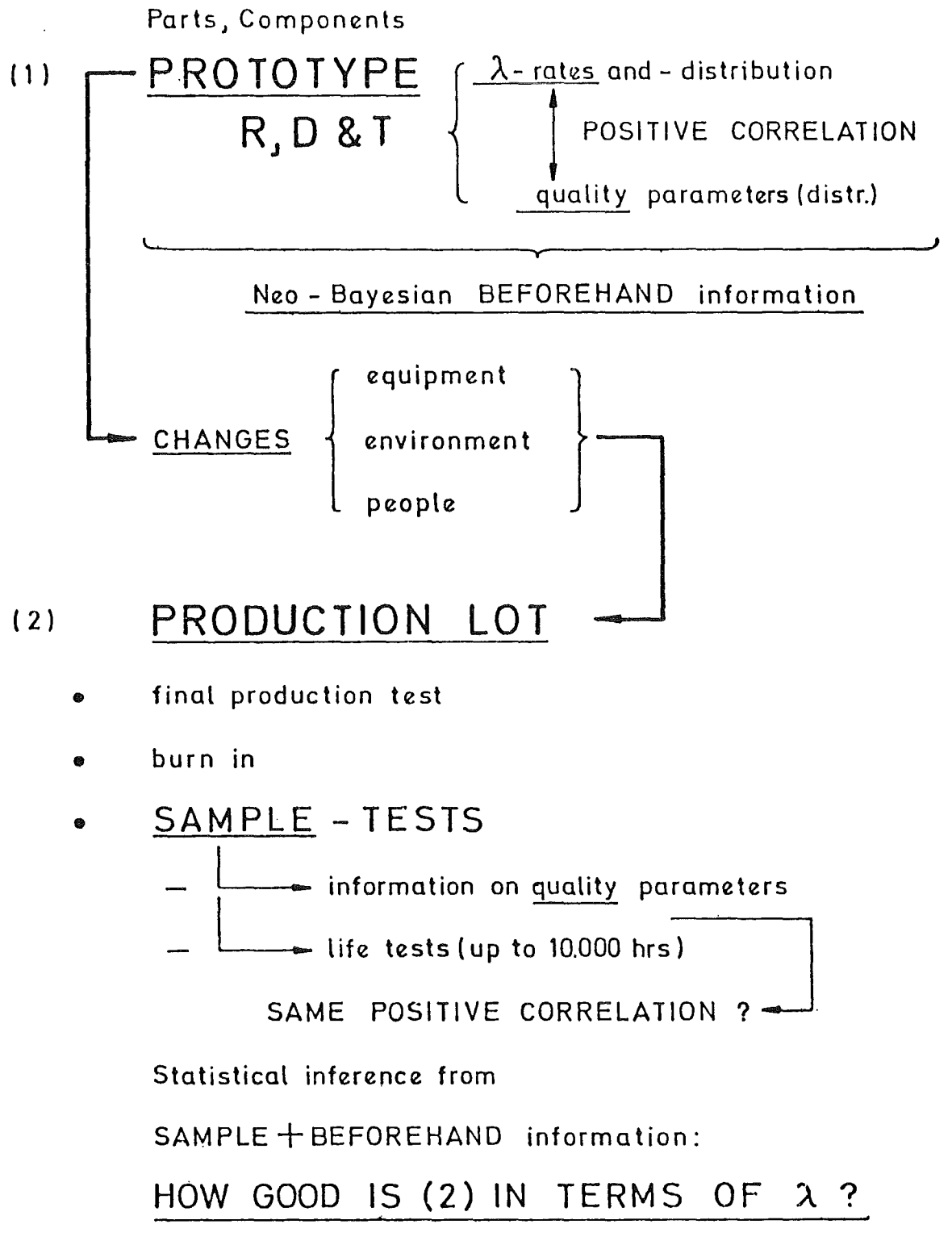


BILD 2: NEO BAYESIAN AND CORRELATION ANALYSIS

Der Boden, auf dem Zuverlässigkeitsrechnungen und -vorhersagen durchgeführt werden ist demnach dünnes Eis. Die von den Amerikanern Bean, Bloomquist und Finkelstein durchgeführten Vergleiche von Vorhersage und Erfahrung bei Satelliten zeigen zwar über die letzten Jahrzehnte einen beträchtlichen Lernerfolg, aber die Streuung der Quotienten von gerechneter zu wahrer nützlicher Lebensdauer ist immer noch beträchtlich /9/.

4. Up the Learning Curve

Wie wenig über Einzelheiten, insbesondere bei Schnittstellen und Wechselwirkungsproblemen bekannt ist, wurde uns klar, als Dr. Winkler (DFVLR) und ich Korrelationsprobleme bei den Sonnensatelliten HELIOS A und B untersuchten; siehe /10/. Diese Rechnungen beruhen auf der Auswertung von Daten, die Jet Propulsion Laboratory in Pasadena (Calif.) aufbereitet hatte. Einzelheiten sind:

(1) Die Untersysteme Energieversorgung und Thermohaushalt waren in der Bodensimulation unkorreliert, in der Umlaufbahn jedoch mit $r = +0.27$ deutlich korreliert.

(2) 8 von 10 funktionierenden (von 11 beabsichtigten) Experimenten hingen nur von den Untersystemen Energieversorgung und Datenverarbeitung ab. Jedoch zwei Experimente, betreffend Radiowellen bzw. Plasma, waren von der High-Gain-Antenna abhängig, und zwar zeigten sie, wenn diese aktiviert war, bis zu 50 v.H. Datenverlust ($r = -0.5$). Mit zunehmender Zeit verminderte sich dieser Fehler beträchtlich und konnte als Frühfehler eingestuft werden.

(3) Wenn der Memory-Read-Out Mode angeschaltet war, wurde eine Störung (Übersprechen) anderer Stromkreise beobachtet. Es war das bereits zu $r = 0.25$ am Boden festgestellt worden, während in der Umlaufbahn $r = 1$ stattfand. Hier zeigte sich die Nutzlosigkeit von Bodentests, wenn die Diagnose versagt und der Fehler fortbesteht und sich noch verstärkt, weil seine Ursache unerkannt und damit unbehoben bleibt.

Trotz aller Anstrengungen auf dem Gebiet der Satellitenzuverlässigkeit und trotz aller Erfolge, kann man noch nicht von glaubwürdiger Vorhersage sprechen. Die USA-Satelliten zeigen das deutlich; siehe dazu /11/, woraus ich hier die Feststellung wiederhole, daß

(1) die Satelliten der Serie RANGER sechs glatte Mißerfolge aufwiesen, ehe schließlich 1 Teilerfolg gelang;

(2) die Satelliten der Serie LUNAR ORBITER trotz unüberhörbarer Warnungen seitens der Zuverlässigkeitsingenieure fünf Erfolge buchten und keinen Fall von Versagen aufwiesen.

Trotzdem muß man sich fragen, was wohl ohne Zuverlässigkeitsanalyse geschehen würde; da wäre wohl schwärzester Pessimismus angebracht. Der Projektmanager von HELIOS nannte zwar Zuverlässigkeitsrechnungen ein NUMBER GAME, - in den USA eine illegale Lotterie im Unternehmensbereich der MAFIA, - aber diese Einstufung wäre doch ein großes Unrecht. Viele Erfolge, insbesondere aber das APOLLO-Programm, zeigen, daß es sich bei der Produktsicherung in der Raumfahrt, von der die Zuverlässigkeitsanalyse ein notwendiger Teil ist, im ganzen gesehen wohl um eine großartige Success Story handelt!

Man kann dieses Thema nicht verlassen, ohne auf Zuverlässigkeit von Information einzugehen. Hierzu zwei Hinweise (aus /11/) wiederholt:

(1) 1964 verfehlte eine (USSR) VENUS PROBE relativ spät ihre Flugbahn, die dann vom Boden aus korrigiert wurde, was in den USA damals (noch mit Computern der 2. Generation) prima facie als unmöglich galt. Man vermutete die Anwendung eines zahlentheoretischen Tricks, nämlich sogenannter modularer Algebra, - die dann plötzlich hochgespielt wurde. Das beruhigte sich aber schnell, als EDV-Hardware der 3. Generation zur Verfügung stand.

(2) Wenig später versagte ein (USA) MARS MARINER Launch Vehicle durch einen elementaren Programmierfehler, der durch alle Kontrollen durchgeschlüpft war; also Vorsicht hinsichtlich Zuverlässigkeit von Software!

Abschließend kann dazu gesagt werden, daß hinsichtlich der einschlägigen Verfahren betreffend Zuverlässigkeit von Information, z. B. Error Protected Names und Self Correcting Codes außerhalb des Kreises spezialisierter Informatiker leider nur wenig bekannt ist. Der Trend geht, wie einer Mitteilung des IEEE /12/ zu entnehmen ist, daß man sich zunehmend auch mit komplexer Hardware an Bord von Satelliten wagt und nicht mehr so viel wie bisher der EDV - Anlage bei den Bodenstationen überlassen will. Auch das dürfte eine Erhöhung von Zuverlässigkeit beim Betrieb von Satelliten bedeuten.

Der folgende Teil berichtet über die zugehörige "Testphilosophie", die zwar im Vortrag integriert war, aber hier zur Vermeidung von Doppelarbeit getrennt dargestellt wird.

Schrifttumsverzeichnis

/1/ H.W. von Guérard: Das Protoflight-Konzept der Satellitentechnik
Ref. 10. Tagung "Technische Zuverlässigkeit", Nürnberg 1979

/2/ Operations Research Center, M.I.T.: Notes on Operations Research 1959
Technology Press, 1959

/3/ G.E. Kombell: Reliability and Maintenance in /2/

/4/ E. Pieruschka: Principles of Reliability
Hall publ., 1963

/5/ Barlow/Proschau/(u. Hunter): Mathematical Theory of Reliability
SIAM Series, Wiley publ., 1965

/6/ W. Meier: Berichte über Störmeldungen beim Projekt AEROS,
DFVLR/OP, 1971 - 1973;
Berichte über Störmeldungen beim Projekt AZUR,
DFVLR/OP, 1969 - 1970

/7/ Koslow/Uschakow/(u. Reinschke): Handbuch der Berechnung der Zuverlässigkeit für Ingenieure
Hanser-Verl.: 1979

/8/ Eisenhart/Hastay/Wallis: Techniques of Statistical Analysis
McGraw-Hill publ., 1947

/9/ Bean/Bloomquist/Finkelstein: More Reliability Data from Inflight Spacecraft
Annual Symp. Rel. 1973 , Philadelphia

/10/ von Guérard/Winkler: Correlation Analysis of Spacecraft Interface Problems
Re. COSTRONICS, Budapest 1976

/11/ H.W. von Guérard: Spacecraft Reliability, - Over Here and over There: Past and Future
ESA Product Assurance Symp., Frascati, 1976

/12/ I. Doshay: Report on IEEE Joint - Computer/Reliability Meeting
IEEE Reliability Society Newsletter XXV/4, 1979

Das Protoflight-Konzept der Satelliten-Technik

von Dr. H.W. von Guérard

Industrieanlagen-Betriebsgesellschaft mbH

8012 Ottobrunn

Vortrag auf der 10. Tagung

T e c h n i s c h e Z u v e r l ä s s i g k e i t

29. und 30. März 1979

Nürnberg

Übersicht:

Es wird, unter dem Gesichtspunkt der Produktsicherung, das Protoflight-Konzept der Satelliten-Technik vorgestellt, demzufolge das integrierte Qualifikations-Modell als Flugeinheit Verwendung findet. Dagegen erhobene Bedenken, bei denen Test- gegen Modell-"Philosophie" stehen, werden erörtert. Das Niedrig-Kosten-Konzept für Satelliten, das sowohl von NASA als auch von ESA befürwortet wird, spricht neben der Modellfolge auch die äußerst kritische Frage der Bauteile-Qualifikation an, die aber unabhängig vom Protoflight-Konzept beantwortet werden sollte.

Abschließend wird auf zwei (Papier-) Simulationen eingegangen, die eine Rechtfertigung des Protoflight-Konzepts erbracht haben, und zwar für einen Forschungssatelliten in einem Falle und für einen Satz von Raumflug-Experimenten im anderen.

Abstract:

This paper presents, under the aspect of product assurance, the Protoflight concept for Satellites, according to which the integrated qualification model serves as the flight unit. Objections to that, confronting model-vs. qualification-philosophy, are discussed. The Low Cost Satellite-concept, as favoured by NASA as well as by ESA, refers to the sequence of models as well as to the most crucial question of parts qualification level which, however, should be considered as independent of the protoflight-concept. Finally, two (paper-) simulations are discussed which justify the protoflight concept, one for a research satellite and for an assembly of space experiments the other.

1. Der Weg zum Protoflight-Modell

Der Aufbau und die Technik der Produktsicherung bei der Entwicklung und beim Bau von Satelliten, wie sie im Bereich der ESA (= European Space Agency) angewandt werden, wurden im wesentlichen schon in den USA von bzw. im Auftrage der NASA entwikkelt. Dabei konnte auf den Erfahrungen der Luftfahrttechnik aufgebaut werden, wenn auch Unterschiede zu dieser bestehen, die die Aufgaben der Produktsicherung in der Raumfahrt von Beginn an erschwerten. Die Gründe dafür sind vornehmlich

a) der große Anteil technischer Innovation

b) die Anwendung auf nicht-wartbare und vorwiegend nicht-steuerbare Systeme

c) ein empfindlicher Mangel an Information über die Ursachen von Störfällen im Betrieb.

Mit dem Serienbau von Nutzsatelliten in den USA verliert a) an Allgemeingültigkeit. Zu b) ist zu bemerken, daß zwar z. B. Bahnkorrekturen oder das Einschalten einer funktionalen Redundanz durch Bodenkommandos geschehen können, daß aber ein Satellit vergleichsweise zu anderen Systemen ein im wesentlichen sich selbst überlassenes System ist. Zu c) ist zweierlei zu sagen: zunächst, daß ein Satellit im Betrieb nicht mehr für physikalische Analysen zur Verfügung steht; weiterhin, daß das Telekommunikations-System ein Funktions-Engpaß ist, bei dessen Versagen keine Information mehr über das Verhalten anderer Funktionseinheiten oder deren Komponenten zu erhalten ist.

Unter diesen Umständen war anfänglich ein Aufwand an Produktsicherung geboten, der nach kostspieligen Lehrjahren vorsichtig abgebaut werden konnte. Nachdem die Erfahrung aus vielen erfolgreichen Projekten vorlag, hat man verständlicherweise begonnen, nach einer Rationalisierung der Produktsicherung zu suchen, damit trotz erhöhter Komplexität der Produkte die Kosten zur Sicherung ihrer

Funktionstüchtigkeit nicht auch noch ständig wüchsen. Das dabei entwickelte Protoflight-Konzept steht in den USA seit etwa 10 Jahren zur Debatte und wird nicht nur dort zunehmend praktiziert; es wäre zu dieser Zeit nichts mehr darüber zu sagen, wenn nicht sowohl die Gründe als auch die Grenzen dieses Erfolgs für fast jedes derartige Projekt wieder zu prüfen wären.

Das konventionelle Programm der Produkticherung in der Satellitentechnik ist in Bild 1 dargestellt. Das Strukturmodell ist bereits flug-repräsentativ für Abmessungen, Trägheit und Gewicht, und es dient mitunter schon der Qualifikation des Untersystems "Struktur". Das Thermo-Modell dient der Simulation des Wärmehaushalts sowie der Prüfung von Vorhersagen auf diesem Gebiet; die elektrischen und elektronischen Labor- und Werkstattmodelle für Schaltung und Verdrahtung werden als "bread boards" zusammengefaßt. Anschließend wird das "Ingenieur"-Modell integriert, wenn auch noch nicht auf HiRel-(= Hochzuverlässigkeits-) Ebene und noch ohne identische Redundanzen. Schnittstellen-(interface-) Probleme sollten bereits hier erkenntlich und lösbar sein. Von da wird zum Qualifikations-Modell fortgeschritten, das auf HiRel-Ebene, mit oder auch noch ohne identische Redundanzen erstellt wird und so vollständig sein muß, daß alle induzierten Umgebungs-(interference-) Probleme erkenntlich und lösbar sind. Dieses Modell dient dem Austesten bei überhöhten Lasten und mindestens bis zu Missions-Dauern.

In der Regel geben diese Tests zu einer großen Anzahl von Änderungen, Nachbesserungen und Nachqualifikationen Anlaß. Dabei gilt grundsätzlich, daß auf keiner Stufe der Systemintegration eine Störmeldung anfallen sollte, die schon vorher hätte anfallen können. Das läßt sich jedoch nur unvollkommen realisieren, und zudem läßt sich das durch die zahlreichen Störfälle, die erst durch Tests, falsches Testgerät und menschliches Versagen beim Testen verursacht werden, nur schlecht verfolgen.

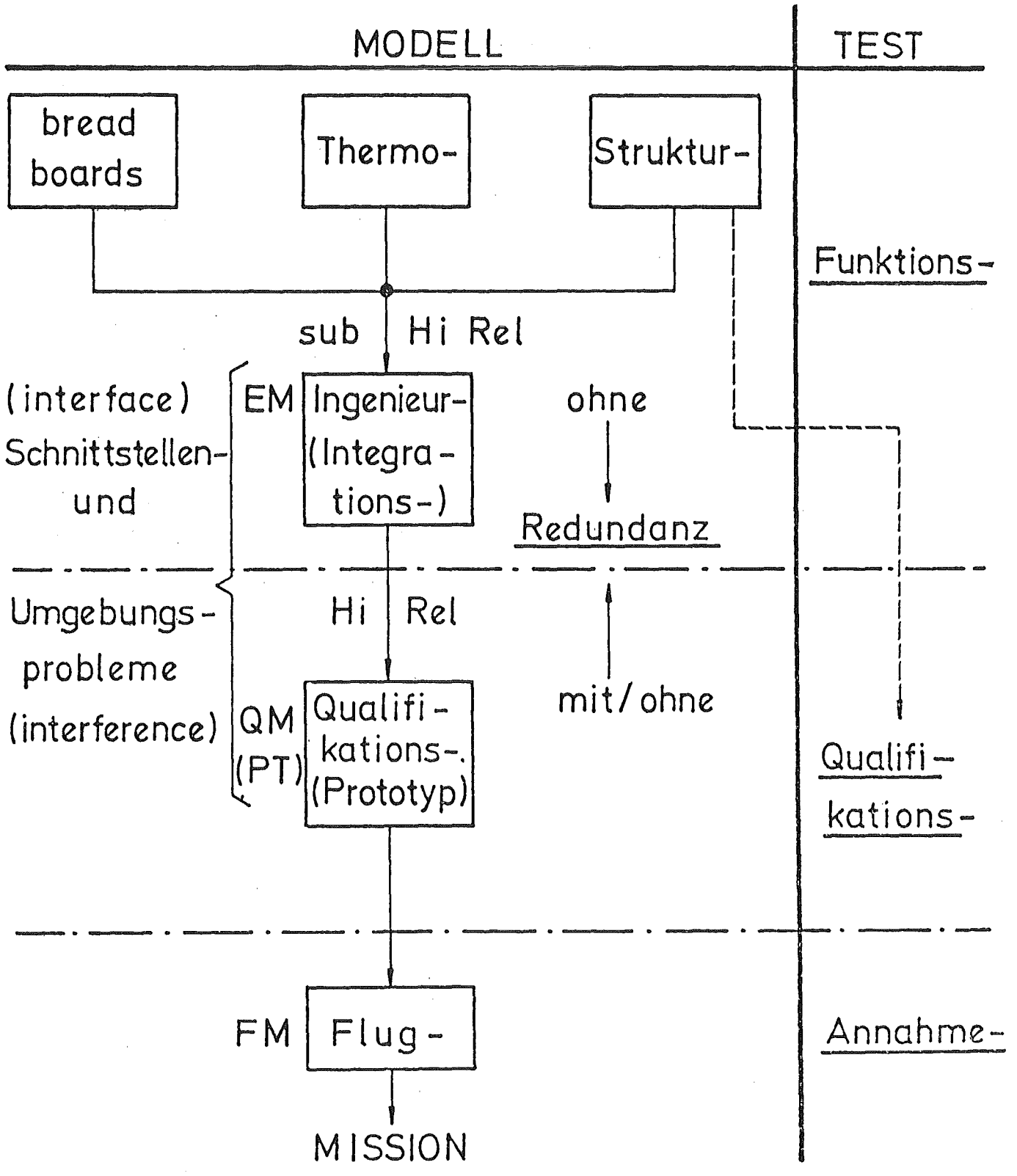


Bild 1: MODELL-Entwicklung und TEST-Programm

Nachdem man sich soweit der Raumfahrttauglichkeit des Satelliten vergewissert hat, wird ein identischer Zwilling des Qualifikationsmodells gebaut, der aber auch dort vollständig ist, wo beim Qualifikationsmodell noch Redundanzen ausgelassen waren. Dieses Flugmodell wird einem vergleichsweise milden Annahmetest unterworfen, der in keinem Fall die postulierten Missionsbeanspruchungen bzw. -dauern überschreiten soll.

Man war schon früher dazu übergegangen, das Qualifikationsmodell (QM) als Flugreserve zu verwenden, wenn z. B. das Flugmodell (FM) einem fehlerhaften Abschuß zum Opfer gefallen war. Die Erfahrungen damit waren so vorzüglich, daß man das Q-Modell sehr bald als dem F-Modell gleichwertig betrachtete, wenn auch in einem repräsentativen Programm, nach /1/, im Qualifikationstest ca. 40 v. H. mehr Störmeldungen anfielen als im Annahmetest. Jedenfalls wurde hier durch Eliminierung eines vollständigen Satelliten die Chance zu einer echten Kostensenkung wahrgenommen.

Dazu s. Bild 2. Soweit das Q-Modell voll flug-repräsentativ war, wurde es als Prototyp (PT) bezeichnet. Dieser konnte dann auch als F-Modell dienen, und so entstand der Begriff des Protoflight-Modells (PF). Schließlich legte man den Werdegang eines Satelliten gleich auf diese reduzierte Version an und sprach dann vom Protoflight-Konzept. Bei seiner Verwirklichung rechnete man ein, daß das Ingenieurmodell (EM) bereits Funktionstests unter allen Umgebungsbedingungen unterworfen würde, da sonst das PF-Modell mit Aufgaben überlastet worden wäre.

Im Anfangsstadium der Satellitentechnik bot die sogenannte Modellphilosophie ein noch vollständigeres Bild: Die Qualifikation fand zunächst auf der Ebene von Baueinheiten (box level) statt und diese zusammen wurden als QM bezeichnet. Der integrierte Satellit, als Prototyp bezeichnet, wurde wiederum qualifiziert und danach bestenfalls noch als Reserve für das Flugmodell angesehen.

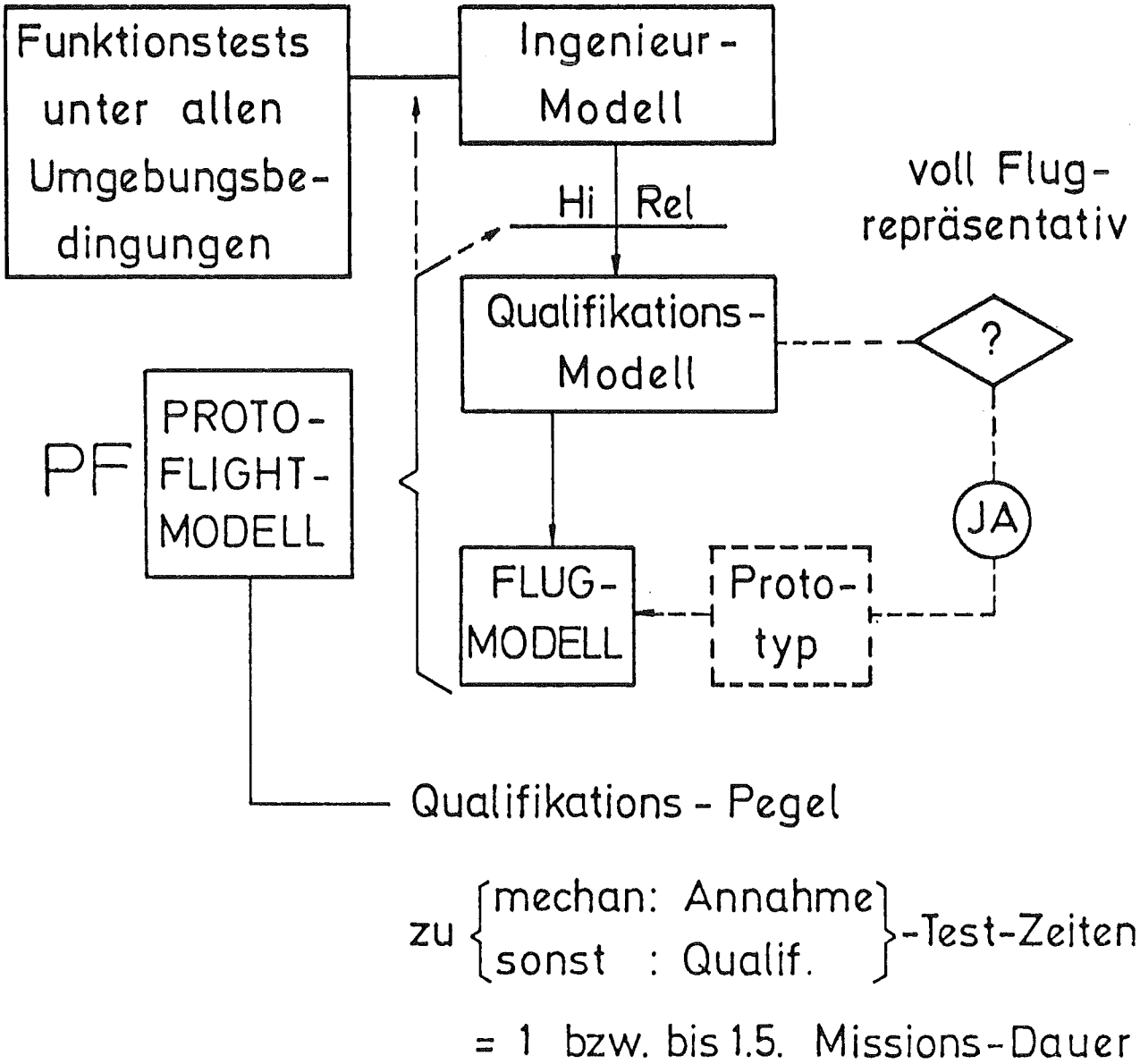


Bild 2: Der Weg zum PROTOFLIGHT - Modell

2. Einwände, Bedenken und Spekulationen

Dem einschlägigen USA-Schrifttum, insbesondere soweit es vom Goddard Space Flight Center (GSFC) stammt, ist zu entnehmen, daß seitens der Test-Ingenieure schon frühzeitig gewisse Bedenken gegen das PF-Konzept erhoben wurden; diese Kritik verstummte erst, als seitens der Autoren maßgeblicher Untersuchungen über Satelliten-Tests zugegeben werden mußte, daß sich über den Erfolg nicht streiten lasse und daß das PF-Konzept für alle Nutzsatelliten-Programme ernsthaft in Betracht zu ziehen sei. Man darf solche anfänglichen Bedenken nicht als Fakultäts-Egoismus abtun; sie entspringen vielmehr dem Gedanken, daß man eher unter Beibehaltung vollständiger Modell-Sätze (also E+Q+F-Modelle) die Testdauern reduzieren solle als bei festen Testspezifikationen die Modellfolge; als Gründe wurden angeführt:

- mangelhaftes Training des technischen Personals, weil an zu wenig Modellen geprüft werde;
- das Fehlen eines Prototyps, an dem Probleme, die während der Mission auftreten, am Boden simuliert werden könnten;
- erhöhtes Risiko, weil nicht immer konsequent bis zu den Belastungspegeln der Entwurfs- und Konstruktions-Spezifikationen ausgetestet würde;
- die Tendenz, Qualifikationstests zu frühzeitig an Teilmodellen auszuführen und daher den Kontakt mit den im Laufe der Entwicklung möglicherweise wiederholt revidierten Spezifikationen zu verlieren.

Es wurde ferner geltend gemacht, daß

- die Beschaffungszeit für kritische HiRel-Bauteile sowie
- die Neigung, für den Mangel an Modellen durch ein Übermaß an Analysis zu kompensieren

einen Zeitgewinn des PF-Konzepts ohnehin weitgehend illusorisch machten.

Nicht zuletzt scheint es die Sorge von Experten wie R.E. Heuser, H.P. Norris und A.R. Timmins (deren einschlägige Veröffentlichungen z. T. im Schrifttumsverzeichnis von /2/ aufgeführt sind) gewesen zu sein, daß mit dem PF-Konzept nicht genügend Test-Daten gewonnen werden, um aus ihnen Schlüsse für optimale Testprogramme ziehen zu können. Es gibt in dieser Richtung zwei Ansätze, die zudem logisch nicht scharf von einander zu trennen sind, und zwar

- die Definition der Wirksamkeit von Tests,
- die Bestimmung des Grenznutzens von Tests.

Vergleicht man die umfangreichen Statistiken aus einer Reihe von Veröffentlichungen (darunter /1/ und /3/)über Testprogramme, so kommt man zu folgenden Schlüssen:

- die Gefahr, daß bei Testbeanspruchungen bis an die Grenzen der Spezifikation latente Fehler in den Satelliten hineingetestet werden, ist als vernachlässigbar gering zu veranschlagen;
- es besteht positive Korrelation zwischen den Häufigkeiten der Störmeldungen während der Tests und denjenigen während der Mission; daraus folgt, daß gut konzipierte und einwandfrei gefertigte Satelliten nicht tot getestet werden,und daß weniger leistungsfähige Satelliten trotz reichlicher Mängelbehebungen weniger leistungsfähig bleiben;
- es gibt zu Bedenken Anlaß, daß die vereinte Wirkung von
  Los- und Teilequalifikation
  Zuverlässigkeitsforderungen
  Sicherheits-(K-)Faktoren
  derating (= Lastdrosselung)
  Vertrauensbereichen (z. B. für MTTF = $^1/\lambda$)

es bis heute nicht vermocht hat, den ungewöhnlich hohen Ausfallanteil elektrischen und elektronischen Versagens weiter herabzusetzen.

Es ist besonders seitens GSFC versucht worden, durch statistische Analyse die Schwachstellen von Testprogrammen einzukreisen; s. dazu die Formeltafel Bild 3: $\eta_i(M)$ ist dabei das Verhältnis der Häufigkeit spezifischer Störmeldungen in einer Testfolge zur Häufigkeit aller, also auch späterer Störmeldungen, auf die der i^{te} Test spezifisch angesetzt wurde. Damit ist in der Terminologie der Stochastik die "Mächtigkeit" eines Tests gekennzeichnet. Wird die Fehlerzahl bezüglich i hingegen auf alle späteren Fehler, nicht nur der Klasse i, bezogen, so wird auch noch der relative Anteil der in Rede stehenden Störfälle wirksam, und man kann von der "Wichtigkeit" $\eta_i(W)$ der Test-spezifischen Klasse i sprechen, wobei diese Bewertung wiederum statistisch, nicht jedoch funktionell zu verstehen ist. Dieses System ist nicht frei von logischen Diskrepanzen, schon weil die Testfolge Einfluß auf das Ergebnis hat; wegen Einzelheiten s. /3/. In den dortigen Formeltafeln bezieht sich i (von 1 bis 22) sowohl auf einzelne Tests als auch auf Gruppen davon.

Die Auswertung solcher statistischen Fehlermodelle sollte u. a. ein Kriterium liefern, wonach jeder Test unmittelbar bei Erreichen seines "Grenznutzens" abgebrochen würde, sobald nämlich weiteres Testen nicht mehr kostenwirksam wäre. Das ist aber schwer zu definieren; um einiges realistischer dürfte die Frage sein, ob man eine Testdauer unterhalb der Missionszeit festlegen kann, bei der die Test-spezifische Ausfallrate konstant wird.

Um diese Verhältnisse beurteilen zu können, müßte man zunächst einmal Einigkeit über die Ursache der hohen Störfalldichte in den ersten Tagen eines Satelliten in seiner Umlaufbahn erreichen. Ein spekulatives Modell dazu, über das aber die bisherigen Feststellungen über Störfälle noch nicht zu entscheiden gestatten, ist im Bild 4 dargestellt. Demzufolge wäre anzunehmen, daß kritische Abschußbelastungen neue Frühfehler in den Satelliten induzieren,

1. Spezifisches η_i (Mächtigkeit eines Tests)

$$\eta_i\,(D) = \frac{\text{Störfälle v. Typ } i \text{ (System-Ebene)}}{\text{spätere* Störfälle v. Typ } i + \text{Zähler}}$$

---

2. Generelles η_i (Wichtigkeit eines Tests)

$$\eta_i\,(W) = \frac{\text{Störfälle v. Typ } i \text{ (System-Ebene)}}{\text{alle späteren * Störfälle} + \text{Zähler}}$$

* Abschuß, Akquisitions-Phase (u. Mission)

---

3. Vorschlag GSFC
Testdauer bis Grenznutzen $N_i = 0$

Kriterium: { $(MTBF)_i$ = const
Verbesserung vs. Schädigung
Testkosten vs. Wert der Information } ?

Bild 3: Definitionen zur Wirksamkeit von Tests

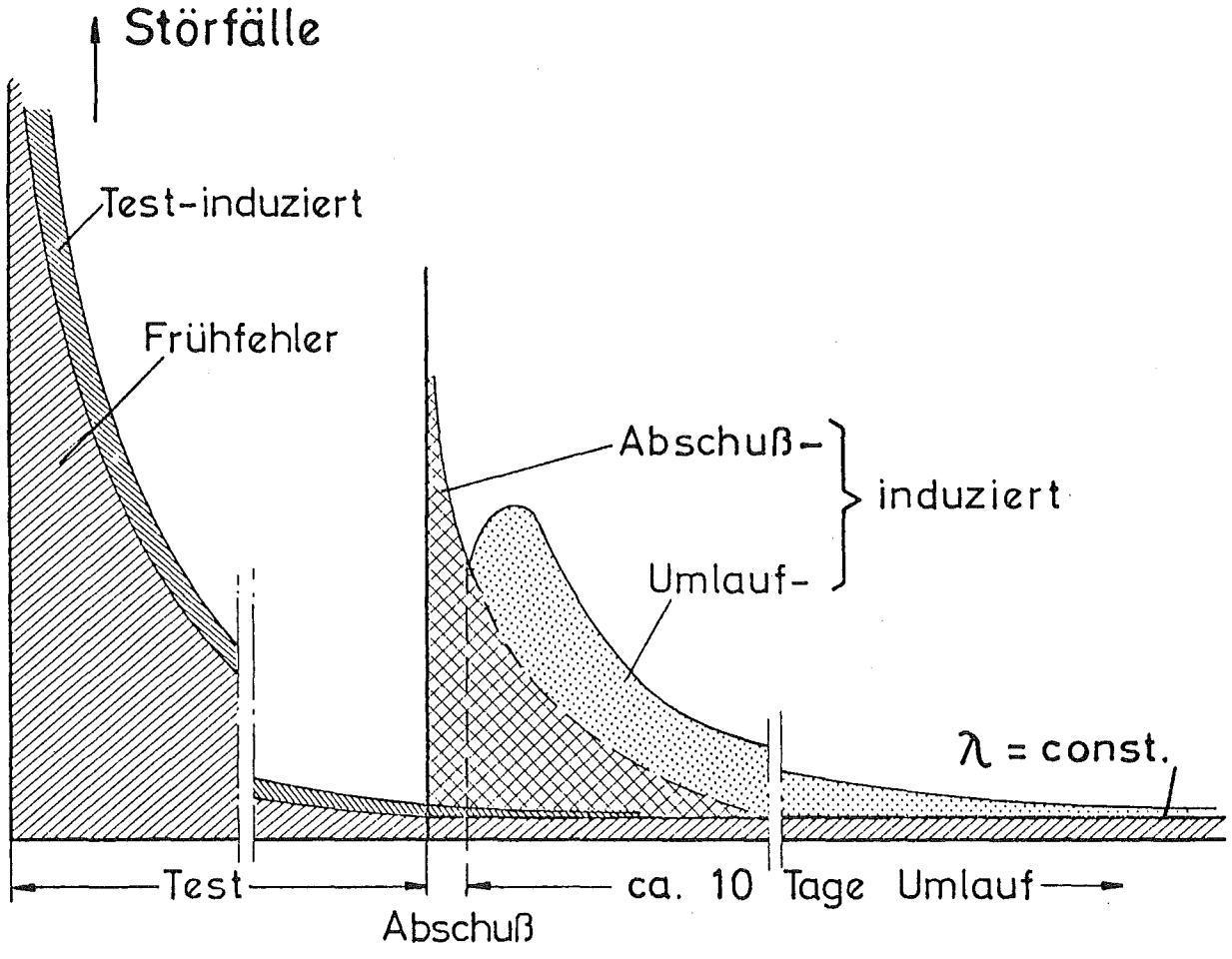


Bild 4: Annahme über die Zurechnung von Störfällen

die sich in etwa den ersten 10 Tagen auswirken und sich mit nicht-konstanter Fehlerdichte den echten Zufallsfehlern konstanter Dichte überlagern. Von anderer Seite wird die Meinung vertreten, daß es hauptsächlich Störfälle infolge thermischer Zyklen im Vakuum seien, die Frühfehler der Mission verursachen.

So lange über diese Dinge Unklarheit besteht, können Testprogramme nicht optimiert werden, und so lange wird es auch Einwände gegen die Abkürzung des gesamten Testvorgangs durch Befolgen des Protoflight-Konzepts geben. Man kann heute aber feststellen, daß die Analyse umfangreicher Teststatistiken zwar zu einer Überprüfung der Spezifikationen führen mag, daß sie aber auf die fast durchgängige Anwendung des Protoflight-Konzepts keinen Einfluß mehr haben wird.

3. Protoflight- und Niedrig-Kosten-Konzept

Bei Serien von Nutzsatelliten, wie sie in den USA erstellt werden, hat man so gut wie regelmäßig den qualifizierten Prototyp, nach dem die Serie gebaut wurde, ebenfalls als Flugmodell eingereiht; so weit bekannt ist, war das nach gelungenem Abschuß immer erfolgreich. Bei dem Annahmetest, der dabei als "Bestätigung der Qualifikation" verstanden sein mag, zeigten sich oft Schwächen gerade des letzten Exemplars, - eine Art "last come, worst served"-Phänomen, das verschiedene Ursachen haben kann. In kritischen Fällen hatte man keine Bedenken, auch noch auf das E-Modell zurückzugreifen und, nach Ausstattung mit HiRel-Bauteilen, dieses auf Mission zu schicken (s. Bild 5).

Diese Betrachtung zeigt, daß die Dinge auch nach grundsätzlicher Einführung des PF-Konzepts noch im Fluß sind. Der Trend dürfte heute in zwei Richtungen gehen, s. dazu Bild 6: in Teil A ist angegeben, daß im Falle eines erhöhten Risikos, z. B. des Sicherheits-Risikos bei militärischen Satelliten, wenigstens die kri-

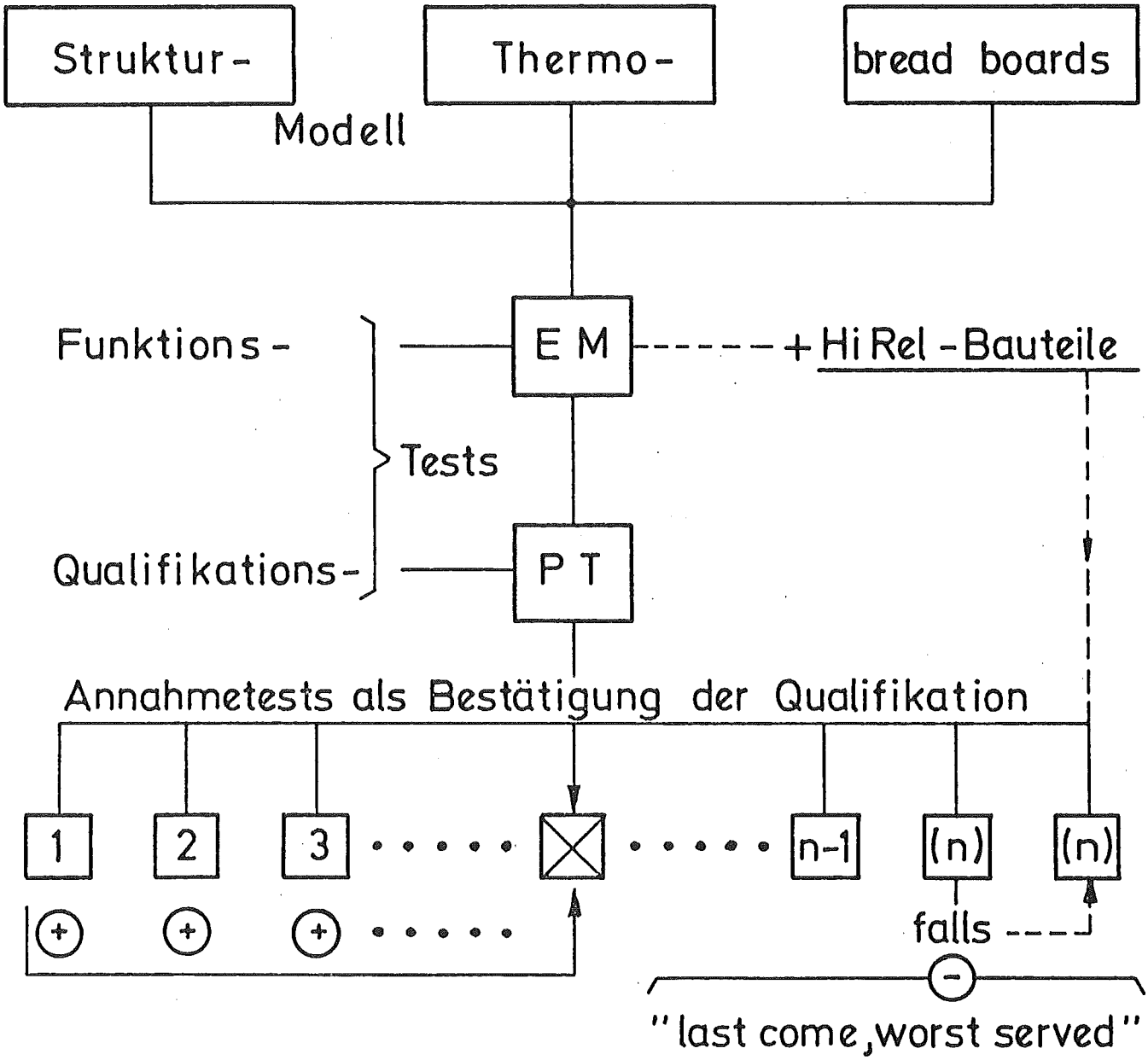


Bild 5: Schematische Darstellung eines Qualifikations- und Einsatz-Plans für Satelliten-Serie

A. HYBRID - KONZEPT

als Lockerung des PF - Konzepts

Im Falle
- weitgehender technologischer Neuerung
- von Zuverlässigkeits - engpässen (single points of failure)
- sonst. erhöhten Risikos (z.B. milit. Sicherheit)

} QM unterhalb Systemebene, sonst PF

B. NIEDRIG - KOSTEN - KONZEPT

als Verschärfung des PF - Konzepts

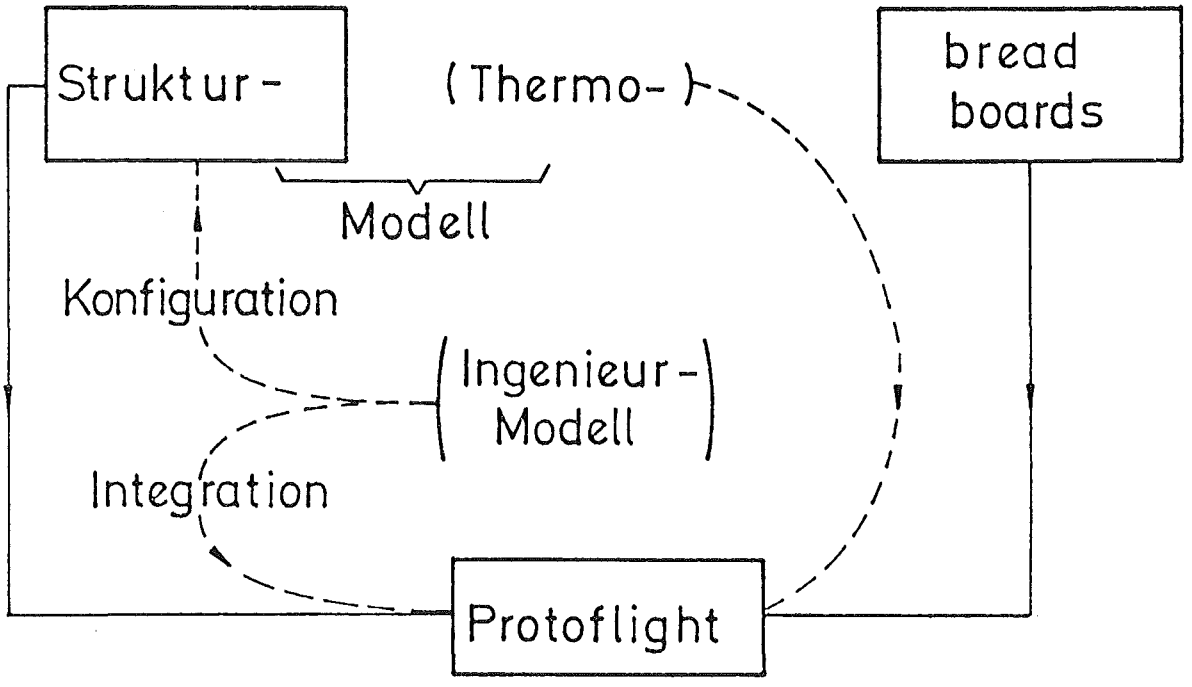


Bild 6: Lockerung bzw. Verschärfung des Protoflight - Konzepts

tischen Baueinheiten und Untersysteme einer besonderen Qualifikation derart unterworfen werden, daß dafür immer noch die klassische Regel der Qualitätssicherung für Raumflug gilt, "test items don't fly".

Liegen dagegen solche Bedenken nicht vor, so folgt man dem in den USA für die NASA zunächst von der General Electric Corporation praktizierten Konzept, sowohl das Thermo- als auch das gesamte Ingenieur-Modell ausfallen zu lassen und deren Aufgaben, wie in Teil B von Bild 6 angezeigt, auf die verbleibenden Modelle zu verteilen. Das ist ein Niedrig-Kosten-Konzept, wie es sich ein Auftraggeber nur wünschen kann.

Es ist sicher zutreffend, daß der Zwang zur Sparsamkeit erfinderisch macht, und in Verbindung mit dem Protoflight- als Teil eines umfassenden Niedrig-Kosten-Konzepts tritt die Frage auf, welches der nächste Schritt sei. Die größte Versuchung liegt darin, das Niveau der Bauteile-Qualifikation herabzusetzen; aber gerade dabei würden niedrige Kosten mit überproportional erhöhtem Risiko erkauft. Über die Vorsicht, die in dieser Hinsicht zu walten hat, kann an Hand eines Dokuments über den Aeronomie-Satelliten AEROS B berichtet werden, s. /4/: Als für das thermische Experiment GSA (= Gegenspannungs-Analysator) HiRel-Transistoren fehlten, wurde vergeblich versucht, durch Eigenscreening von Normalbauteilen HiRel-qualifizierte zu gewinnen. Schließlich mußten bei deutschen Parallelprojekten auf Lager befindliche HiRel-Transistoren verwandter Typen genommen werden, obwohl dadurch eine Reihe von Modifikationen bedingt und mit erheblichen Schwierigkeiten für Fertigung und Produktsicherung verbunden waren.

Die USA-Luft- und Raumfahrt-Behörde NASA unterhält ein besonderes "Low Cost Systems Office", und ein in dessen Auftrag erstellter Bericht über Niedrig-Kosten-Satelliten, s. /5/, präzisiert ab-

schließend 9 Empfehlungen, von denen keine die HiRel Bauteile-Qualifikation in Frage stellt, obwohl der damit zusammenhängende Fragenkreis keineswegs übergangen wird. 3 Empfehlungen beziehen sich auf Vollständigkeit der Qualitätssicherung; 3 weitere unterstreichen die Forderung nach möglichst geringer Komplexität, deretwegen auch Zugeständnisse hinsichtlich des sonst so kritischen Gewichtsproblems bei Satelliten gemacht werden müßten, und 1 Forderung bezieht sich ausdrücklich auf die Befolgung des PF-Konzepts sowie auf die Ablehnung eines PT-Tests. Die beiden restlichen Forderungen, Projekt-Management betreffend, sind hier nicht von Interesse.

Zur Würdigung der Ergebnisse muß gesagt werden, daß dieser Studie 12 USA-Satelliten-Programme von insgesamt 8 verschiedenen Kontraktoren zugrunde lagen. Davon waren 4 NASA-Programme; 4 militärische Programme betrafen Träger/Nutzlast-integrierte Satelliten und 4 weitere bezogen sich auf experimentelle Nutzlasten, die, mit ablösbarem Trägermodul oder nicht, auf anderen Satelliten angebracht waren ("piggyback"-Konfiguration).

4. Beispiele für technische Konzept-Simulation

So stark auch bei Forschungssatelliten der Trend zum PF-Modell ist, so ist doch der Tatbestand der Übertragbarkeit von Erfahrungen keineswegs eindeutig gegeben, und es muß von Fall zu Fall eine schwierige Entscheidung getroffen werden. Für den ESA-Satelliten EXOSAT (zur Erforschung kosmischer Röntgen-Signale) wurde vom Hauptauftragnehmer MBB eine Studie durchgeführt, die, bereits ohne thermisches Untermodell, die drei in Bild 7 aufgeführten Konzepte vergleicht; s. /6/. Dazu wurden 6 "Verzweigungspunkte" des Entwicklungs- und Fertigungsprogramms gewählt, in denen wesentliche Test-, Entwurfs- und Beschaffungsprobleme auftreten und je nach Modellkonzept Kosten- bzw. Risikoerhöhungen verursachen.

1. konversativ EM + PT + FM
2. alternativ (EM = PT) + FM
3. Protoflight EM + (PT = FM)

1. 26.4 MAU + 5.04 vH = 27.73 MAU
2. 23.3 MAU + 10.59 vH = 25.77 MAU
3. 21.1 MAU + 5.57 vH = 22.28 MAU

(MAU = 10^6 Rechnungseinheiten)

Bild 7: Kostenvergleich gemäß EXOSAT - Simulation

Die 6 "branching points" sind:

3 unterschiedliche Fehler, die jeweils eine Verletzung der elektrischen oder elektromagnetischen Verträglichkeit zwischen Baueinheiten (z. B. Sternsensor, Datensystem, Experimente) zur Folge haben;

1 Fehler durch strukturelle Resonanz;

1 thermischer Fehler durch Überhitzen des Antriebsmotors für die Solarzellenflächen;

1 18-Wochen-Verzögerung in der Beschaffung eines HiRel-Bauteils.

Die Kostenerhöhungen durch diese erheblichen Störungen, die unabhängig voneinander und gemeinsam auftretend angenommen werden konnten, wurden abgeschätzt und sind in Bild 7 angeführt.

Es geht hier nicht nur um das Ergebnis, das deutlich für das PF-Konzept spricht, sondern auch um den erstaunlich sicheren Beitrag, den eine "Papier-Simulation" zu wichtigen Entscheidungen über ein Satellitenprojekt leisten kann. Die gezielte Auswahl der Verzweigungspunkte, deren Kombination möglichst repräsentativ für kritische Vorkommnisse in dem betreffenden Satellitenprojekt sein sollte, ist sicher eine nicht eindeutig zu lösende Aufgabe. Bei allen Einwänden ist aber nicht zu übersehen, daß bei dieser Untersuchung die Signifikanz des Ergebnisses noch durch eine bemerkenswerte Ausdehnung der Analyse auf Vertrauensbereiche für die Schätzwerte sowie durch Anwendung auf unterschiedliche Missionsdauern beträchtlich abgesichert würde.

In den Bereich solcher spekulativen Untersuchungen, die für die Praxis wertvolle Entscheidungshilfen bereitstellen, gehört auch eine Studie, s. /7/, die im Auftrag des BMFT angefertigt wurde. Dabei wurde ein Modell für die Kostenwirksamkeit von Modellfolgen bei Satelliten erstellt, wobei sich

hier jedoch Zähler (= Nutzwert) wie Nenner (= Aufwand) nur auf Experimente beziehen. Die dabei getrennt für SPACELAB- und Satelliten-Experimente errechneten Werte empfehlen übereinstimmend das Protoflight-Konzept.

Es kann nicht unerwähnt bleiben, daß dabei aufgestellte Untersuchungen über das erforderliche Niveau von Bauteile-Qualifikation zu etwas milderen Aussagen führen als zuvor an dieser Stelle erwähnt; man darf aber Konzessionen für einzelne Experimente nicht auf einen Satelliten als den "single point of failure" für alle ihm anvertrauten Experimente übertragen. Eine der Resultatzeilen in diesen Analysen läßt sich bemerkenswerter Weise so interpretieren, daß der Beitrag der Produktsicherung zum Nutzwert der Experimente im praktisch nutzbaren Bereich annähernd proportional zum Aufwand für eben diese Produktsicherung ist; jedenfalls sind errechnete Abweichungen davon nicht signifikant.

Es erhebt sich die Frage, ob die Methodik dieser interessanten Untersuchung auch von Experimenten auf Satelliten ausgedehnt werden kann. Man würde dadurch sog. Modellphilosophie und Fragen der Bauteilequalifikation miteinander verbinden; die zuvor geäußerten Bedenken wegen einer Risiko-Erhöhung bleiben aber bestehen. Es kann bei diesen Betrachtungen ein Umstand nicht übersehen werden, der die Einsparung von Zwischenmodellen ohne Zweifel unterstützt; gemeint ist das Bestreben, die Qualifikation für Raumflug mehr und mehr auch auf höherer als Bauteile-Ebene durchzuführen, also für Instrumente, Geräte, Baugruppen und Systemkomponenten (die Terminologie ist hier wohl nicht einheitlich). Dadurch werden im Endergebnis alle Qualifikationsprobleme eines Satelliten weitgehend zu Integrationsproblemen.

Dadurch, daß mehr und mehr Zwischenstufen von Modellen ausgeschaltet werden, gewinnen die Zuverlässigkeit von Nachbesserungen und die Ausführung von Änderungen sowie die Nachqualifikation mehr

und mehr an Gewicht, und es hat den Anschein, als habe man früher doch zu viele Bedenken in dieser Richtung gehabt. Damit wird die Frage aufgeworfen, warum das Protoflight-Konzept so lange auf seine Verwirklichung hat warten lassen, wenn es doch eine gleichermaßen sichere wie kostensparende Variante einer ursprünglich viel vollständigeren Modellfolge ist. Zunächst ist dazu zu sagen, daß sich die Technik der Nutzsatelliten inzwischen weitgehend etabliert hat, so daß der Netto-Satellit als Träger von Kommunikations- oder Erkennungssystemen trotz aller Komplexität verhältnismäßig unproblematisch geworden ist. Aber wenn auch früher Qualifikationsmodelle bereits raumflugtauglich gewesen sein sollten, so bleibt vom Standpunkt der statistischen Entscheidungstheorie folgendes festzustellen: Selbst bei Zubilligung großzügiger Irrtumswahrscheinlichkeiten bestand nicht genügend Information, um die Hypothese abzulehnen, Qualifikationssatelliten seien durch Übertesten, Änderungen, Nachbesserungen und Nachqualifikation signifikant geschädigt.

Es liegt demnach inzwischen nicht nur eine weiter entwickelte Technologie vor, sondern auch signifikante statistische Information darüber, was geschieht, wenn der Auftraggeber unter Kostendruck postuliert "test items do fly".

Schrifttum:

/1/ General Technology Systems Ltd.: Final Report on a Study of Guidelines Applicable to European Protoflight Satellites and the Orbiting of Qualification Model Hardware (Vol. I) - ESTEC No. 2937/76/NL SW (1977)

/2/ IABG: Literature Survey on the Trade-Off between System Testing and in-Orbit Reliability of Spacecraft - ESTEC No. 3291/NL/HP (SC) (1978)

/3/ Hughes Aircraft Co.: Test Effectiveness Study Report NASA-CR-15312 (1979)

/4/ Dornier System GmbH: Abschlußbericht über den Bau des Aeronomie-Satelliten AEROS B - TN-B 600-000529, i. A. d. BMFT, vertreten durch GfW

/5/ The Aerospace Corp.: Standardization and Program Practices Analysis - Report No. ATR-78 (7659)-1, Vol. I: Executive Summary (1977)

/6/ MBB: EXOSAT Study-C, Optimisation of Planning, Final Report. ESRO Tender AO/557

/7/ Dornier System GmbH: Studie zur Aufwandsoptimierung bei Satelliten- und SPACELAB-Experimenten, i. A. d. BMFT, vertreten durch DFVLR/BPT (1978)

Diskussion

Frage: Sie bemerkten in Ihrem Vortrag, daß jeder Statistiker einmal Bayesianer ist und dann wieder davon abkommt. Wenn ich annehmen darf, daß Sie diese Aussage auch auf sich selbst bezogen haben, möchte ich fragen, welches Ihre persönlichen Erfahrungen waren, die Sie wieder von Bayes'scher Theorie abkommen ließen?

Antwort: Zu dieser Feststellung komme ich hauptsächlich durch zwei Erfahrungen:

a) Im Rahmen des Großprojekts "Humanisierung der Arbeitswelt", Teilprojekt "Streß in Arbeitssystemen", besuchte ich 1976-1978 Tagungen der deutschen Sektion der Internationalen Biometrischen Gesellschaft. Dabei ist mir die weit überwiegend und sehr deutlich ablehnende Haltung der Vertreter dieses Faches, in dem das Bayes-Verfahren lange angewandt und hochgelobt wurde, aufgefallen.

b) Bei eigenen Untersuchungen in der statistischen Qualitätskontrolle ist mir aufgefallen: Entweder arbeitet man mit im wesentlichen homogenen Mengen, und dann besagt das Bayes'sche Verfahren nicht mehr als es die Verwendung kumulativer Daten ohnehin tut; oder, die in Verbindung gebrachten Mengen sind inhomogen, so ist der Bayes'sche Schluß illusorisch. Mit andern Worten und zugegebenermaßen überspitzt: wenn Bayes nichts neues bringt, braucht man ihn nicht, und wenn er was neues bringt, stimmt er nicht.

Frage: Sie erwähnten in Ihrem Vortrag, daß Sie zu einem bestimmten Zeitpunkt per Management-Entscheidung zum Zuverlässigkeitsexperten ernannt wurden, daß Sie sehr wenig spezielle Vorkenntnisse einbringen konnten, und daß es zum damaligen Zeitpunkt sehr wenig Speziallitteratur gab? Haben Sie damals unter großem Mangel an Methoden gelitten, oder gelang es Ihnen in den meisten Fällen, Ihre Probleme mit dem Ihnen verfügbaren Handwerkszeug zu lösen?

Antwort: Die Bücher von Barlow/Proschan/Hunter, von Pieruschka, und von Shoomann, erschienen erst später. Jeder versuchte, mit dem ihm zur

Verfügung stehenden Werkzeug die notwendigen Modelle, z.B. für funktionsverteilte Redundanz, zu erstellen. Einiges davon erschien dann in Zeitschriften, z.B. Journal of Operations Research, in der diese Anfänge spärlich und wenig überzeugend waren. Sicher gab es schon mehr auf diesem Gebiet, aber es war nicht allgemein zugänglich; unter Zeitdruck, wie bei dem zitierten Lockhaed-Angebot für APOLLO, hat man auch keine Zeit für Literatursuche, sonder verläßt sich lieber auf die eigene Findigkeit. Später, besonders mit den IEEE Transactions on Reliability, änderte sich das gründlich.

Technischer Überwachungs-Verein Norddeutschland e.V.

Abteilung Kerntechnik und Strahlenschutz

TÜV Norddeutschland

Zuverlässigkeitsanalysen im Rahmen der Begutachtung von Kernenergieanlagen

H.P. Balfanz, H. Ohlmeyer

Vortragsmanuskript zum Seminar "Methoden der Systemplanung bei geforderterm Langzeitbetriebsverhalten" am 26/27. Febr. 1980 im Kernforschungszentrum Karlsruhe

Hamburg, Jan. 1980

TÜV Norddeutschland

Inhaltsverzeichnis

TÜV Norddeutschland

Einleitung

Zuverlässigkeitsanalysen von Sicherheitssystemen in Kernenergieanlagen finden heute ein breites Anwendungsgebiet.
Es werden die Arbeiten, die auf diesem Gebiet vom TÜV Norddeutschland e. V. im Rahmen der Begutachtung durchgeführt werden, vorgestellt. Dabei steht die formale Einbindung der Zuverlässigkeitsanalysen bei der Erarbeitung von Gutachten - abgeleitet aus den vorliegenden Sicherheitskriterien und Regelwerken - im Vordergrund. In diesem Zusammenhang werden die Bewertungsmaßstäbe der Zuverlässigkeitsergebnisse sowie ihre Vereinbarkeit mit deterministischen Kriterien aufgezeigt.
Die Darstellung der für Druck- und Siedewasserreaktoren durchgeführten Zuverlässigkeitsanalysen liefert allgemeine Grundsätze zum Verfahren und ausgesuchte Analysenergebnisse. Auf detaillierte Analysenergebnisse und methodische Gesichtspunkte wurde zur Begrenzung dieses Beitrages verzichtet.
Die Gewinnung von Zuverlässigkeitsdaten als die Eingangsgrößen für probabilistische Analysen wird aufgezeigt.
Auf die Notwendigkeit der Auswertung von Betriebserfahrungen wird dabei hingewiesen.

1. Anwendungsbereich

1.1 Allgemeines

Zuverlässigkeitsanalysen, übernommen aus der amerikanischen Luft- und Raumfahrttechnik, sind für Sicherheitssysteme von Kernkraftwerken seit ca. 10 Jahren in der Bundesrepublik fortentwickelt worden und zunehmend zur Anwendung gekommen.
Die Analysen lieferten gegenüber der bisherigen ingeneurmäßigen Beurteilung zusätzliche Systeminformationen, so z.B. ob Systemschwachstellen vorhanden sind und Aussagen über optimale Reparatur- und Inspektionsintervalle.

Parallel zu dieser Entwicklung wurden zwei DIN-Normen

- Störfallablaufanalyse /1/ und
- Fehlerbaumanalyse /2/,

erstellt. Für die Systemanalyse hat sich die Fehlerbaumanalyse durchgesetzt. Die Zuverlässigkeitsanalyse ist damit als ein eigenständiges Prüfverfahren bei der Begutachtung der Systemtechnik in Kernenergieanlagen entwickelt worden, ohne daß hierfür die Notwendigkeit einer Risikoquantifizierung bestand.
Die amerikanische und die deutsche Risikostudie /3,4/ zeigen, daß die Zuverlässigkeitsanalysen auch hierfür ein geeignetes Instrumentarium sind. In der amerikanischen Reaktorsicherheitsstudie - Wash 1400 - /3/ wurde der Anwendungsbereich der Störfallablaufanalyse stark herausgearbeitet (vergl. auch /5/).

Aufgrund der aufgezeigten Entwicklung wird heute in verschiedenen Regelwerken der Kerntechnik der Nachweis der Zuverlässigkeit von sicherheitstechnischen Einrichtungen gefordert.

Grundsätzliche Aussagen werden in diesem Zusammenhang in den "Sicherheitskriterien für Kernkraftwerke" (verabschiedet im Länderausschuß für Atomkernenergie am 12. Oktober 1977) /6/ gemacht, wo es zum Thema Zuverlässigkeit von Systemen im Abschnitt 1, "Grundsätze der Sicherheitsvorsorge" unter anderem heißt:

"....Diese Systeme sind so auszulegen, daß Störfälle als Folge von anomalen Betriebszuständen mit ausreichender Zuverlässigkeit[1)] vermieden werden.

1) Anmerkung zur Methodik:

Zur Überprüfung der Ausgewogenheit des Sicherheitskonzeptes sind - in Ergänzung der Gesamtbeurteilung der Sicherheit des Kernkraftwerkes aufgrund deterministischer Methoden - die Zuverlässigkeiten sicherheitstechnisch wichtiger Systeme und Anlagenteile mit Hilfe probabilistischer Methoden zu bestimmen, soweit dieses nach dem Stand von Wissenschaft und Technik mit der erforderlichen Genauigkeit möglich ist".

Im Weisungsbeschluß 13 der TÜV-Leitstelle Kerntechnik, Thema: "Standardgliederung mit Merkposten für TÜV/GRS-Gutachten für Kernkraftwerke mit Druck- oder Siedewasserreaktoren"/7/, wird für verschiedene Sicherheitssysteme die Zuverlässigkeit als ein Bewertungskriterium genannt.

Die KTA-Regel 3701.1 - Übergeordnete Anforderung an die elektrische Energieversorgung des Sicherheitssystems in KKW, Teil 1: Einblockanlagen - /8/ fordert in Abschnitt 3.1 - Zuverlässigkeit - u.a.:

> "Die Energieversorgung des Sicherheitssystems ist so zuverlässig auszulegen, daß sie die Nichtverfügbarkeit der zu versorgenden Systeme nicht bestimmt. .....
> Eine ausreichende Zuverlässigkeit für den bestimmungsgemäßen Betrieb und die zu betrachtenden Störfälle ist nachzuweisen".

Durch die Festschreibung der Zuverlässigkeitsanalyse für Sicherheitssysteme von Kernenergieanlagen durch wesentliche Regelwerke ist diese auch ein Bestandteil des Genehmigungsverfahrens.

Aufgrund des bis heute gültigen Sicherheitskonzeptes, der Analyse des größten anzunehmenden Unfalls (GaU-Konzept), sind bereits für verschiedene KKW Zuverlässigkeitsanalysen für Notkühlsysteme im Hinblick auf den größten Bruch der Primärkühlmittelleitung durchgeführt worden.
Nicht zuletzt durch die erwähnten Risikoanalysen wurde gezeigt, daß mit dem GaU-Konzept nicht alle anderen Störfälle abgedeckt sind und daß ein kleines Leck in einer Primärkreisleitung, der Notstromfall sowie Transienten zu Störfallauswirkungen führen können, die denen eines 2F-Bruches entsprechen. Diese Störfälle haben höhere Eintrittswahrscheinlichkeiten und stellen verschiedene Anforderungen an die Systeme, so

daß sich für die einzelnen Störfälle verschiedene Zuverlässigkeiten ergeben. Die Begutachtung von Kernkraftwerken im Rahmen der Genehmigungsverfahren hat sich an dieser Stelle fortentwickelt, so daß heute eine breite Palette an Störfällen einer systematischen Analyse unterzogen wird.

1.2 Untersuchte Systeme

Art und Umfang der im Genehmigungsverfahren durchzuführenden Zuverlässigkeitsanalysen sind in erster Linie aus den bestehenden Regelwerken und Sicherheitskriterien der Kerntechnik abzuleiten. Dennoch ist der Analysenumfang für eine Gesamtanlage heute noch nicht eindeutig festgelegt.

Nach den "Sicherheitskriterien für Kernkraftwerke" sind für sicherheitstechnisch wichtige Systeme und Anlagenteile Zuverlässigkeitsanalysen mittels probabilistischer Methoden durchzuführen.

Im einzelnen sind dies:

- Notkühlsysteme
- Sicherheitsbehälterabschlußsystem
- Notstromsystem
- Reaktorschutzsystem
- Abschaltsysteme

Der im Weisungsbeschluß 13 geforderte Nachweis der Zuverlässigkeit bezieht sich auf eine größere Anzahl von Einzelsystemen. Die Art der Nachweisführung und die

Beurteilungsmaßstäbe sind hier nicht angegeben. In Kapitel 2 wird weiteres zur Methodik der Zuverlässigkeitsanalysen dargestellt.

1.3 Bewertungsmaßstäbe

Die Ziele der Zuverlässigkeitsanalysen sind

- der Nachweis einer geringen Ausfallwahrscheinlichkeit der Sicherheitseinrichtungen (äquivalent zu einer hohen Zuverlässigkeit),
- das Aufzeigen von möglichen Schwachstellen in den Sicherheitssystemen,
- Aussagen über die Ausgewogenheit der Gesamtheit der Sicherheitsmaßnahmen im Hinblick auf die sicherheitstechnische Bedeutung der einzelnen zu beherrschenden Störfälle,
- Festlegung von Prüfhäufigkeiten und zulässigen Reparaturzeiten der Systemkomponenten oder Systemstränge und
- vergleichende Untersuchungen alternativer Auslegungskonzepte.

Die Höhe der Ausfallwahrscheinlichkeit des Sicherheitssystems muß sich an der Häufigkeit für den Eintritt des Störfalls und an den Auswirkungen bei Versagen der Sicherheitseinrichtung orientieren. D.h. die Wahrscheinlichkeit für ein Schadensereignis - Produkt aus der Häufigkeit des Störfalles und der Ausfallwahrscheinlichkeit des Sicherheitssystems - ist die sicher-

heitstechnisch relevante Bewertungsgröße. Da gegenwärtig keine verbindlichen Wahrscheinlichkeitsgrößen festliegen, gilt als Bewertungsmaßstab der heute praktizierte und anerkannte Auslegungsstand von Sicherheitseinrichtungen.
Die Ereigniskette Kühlmittelverluststörfall (kleines oder großes Leck im Primärkreis mit einer Eintrittswahrscheinlichkeit von ca. 10^{-3} - 10^{-4} pro Jahr) und Versagen des Notkühlsystems (Ausfallwahrscheinlichkeit im Anforderungsfall von ca. 10^{-3} - 10^{-4}) wird in diesem Zusammenhang als repräsentativ angesehen.

Andere Sicherheitseinrichtungen, die ebenfalls zur Erhaltung der Kühlung des Reaktorkerns - jedoch bei anderen Einleitungsstörfällen - erforderlich sind, können hinsichtlich ihrer Ausfallwahrscheinlichkeit in Verbindung mit der Eintrittswahrscheinlichkeit des Störfalls unmittelbar mit der erstgenannten Ereigniskette verglichen werden. Die Ausgewogenheit der verschiedenen Sicherheitsmaßnahmen ist damit überprüfbar.

Die Systemüberprüfung auf mögliche Schwachstellen leitet sich aus den Einzelbeiträgen von Komponenten und Teilsystemen im Verhältnis zu der Ausfallwahrscheinlichkeit des Gesamtsystems ab. Dieses ergibt sich unmittelbar aus der Fehlerbaumberechnung.

Von einer ausgewogenen Systemauslegung kann beispielsweise gesprochen werden, wenn das Gesamtergebnis durch die Vielzahl der Systemkomponenten mehr oder weniger gleichmäßig bestimmt wird.

Das Verfahren zur Bestimmung zulässiger Reparaturzeiten und Ausführungsvorschläge zur Festlegung zulässiger Reparaturzeiten für Sicherheitssysteme wird z.Z. in einem TÜV-Arbeitskreis erarbeitet (vergl. auch /9/).

In der Interpretation zu den Sicherheitskriterien des BMI zum Einzelfehlerkonzept /10/ heißt es in Abschnitt 5 in diesem Zusammenhang

> "Die Inspektionsintervalle sowie die ohne besondere Maßnahmen zulässigen Wartungs- und Instandsetzungszeiten.... sind unter Verwendung der für die redundanten Systeme durchgeführten Zuverlässigkeitsanalysen so festzulegen, daß die Zuverlässigkeiten dieser Systeme durch die Instandhaltungsarbeiten nicht unter die zur Störfallbeherrschung erforderlichen Zuverlässigkeiten herabgesetzt werden".

1.4 Vereinbarkeit von deterministischen und probabilistischen Kriterien

Deterministische Kriterien, wie

- Redundanz (abgeleitet aus dem Einzelfehlerkonzept /10/)
- Diversität (Komponenten mit gleicher Funktion jedoch verschiedener Bauart in redundanten Systemen)
- Unabhängigkeit redundanter Systemstränge (Verzicht auf Vermaschung, räumliche Trennung),

stellen für die Systemauslegung konkrete Forderungen dar, die unmittelbar umgesetzt und leicht überprüft werden können. Sie liefern damit sichere Aussagen über das Vorhandensein von Sicherheitsmaßnahmen.
Die probabilistische Methode quantifiziert die in einem Systementwurf "installierte" und damit erreichbare Systemzuverlässigkeit. Unterschiede zwischen gleichermaßen redundanten Systemen mit jedoch sehr unterschiedlichen Zuverlässigkeiten können aufgezeigt werden, z.B. ein System mit nur wenigen und im wesentlichen passiven Komponenten gegenüber einem System mit einer Vielzahl von aktiven Komponenten in den einzelnen redundanten Strängen.
In der gemeinsamen Anwendung beider Prinzipien und unter Ausnutzung der dargestellten Eigenschaften sehen wir die besten Voraussetzungen um bei der Systemauslegung ein hohes Zuverlässigkeitsziel zu erreichen. Die deterministischen Kriterien stellen in diesem Zusammenhang Mindestanforderungen dar. Ein Abrücken von dieser Forderung ist zulässig für Komponenten mit unverhältnismäßig geringer Versagenswahrscheinlichkeit, z.B. bei bestimmten passiven Komponenten (vergl. /10/).

TÜV Norddeutschland

2. Zuverlässigkeitsanalyse

2.1 Verfahren

Zuverlässigkeitsanalysen werden im Rahmen der Begutachtung nach folgenden Einzelschritten durchgeführt:

1. Festlegung und Spezifizierung der durch die Sicherheitssysteme zu beherrschenden Störfälle
2. Zusammenstellung der erforderlichen Systeme einschließlich der Hilfssysteme
3. Einarbeitung in die Wirkungsweise der Systeme (Systemspezifikation und Schaltpläne).
4. Festlegung der Wirksamkeitsbedingungen der Sicherheitssysteme (Redundanzgrad einzelner Stränge) bei verschiedenen Anforderungsstörfällen
5. Durchführung bzw. Überprüfung der vom Hersteller vorgelegten Fehlerbaumanalyse
6. Festlegung der Zuverlässigkeitsdaten (Ausfallraten, Inspektionszeiten, Reparaturzeiten)
7. Berechnung des Fehlerbaums (Ausfallwahrscheinlichkeit des Gesamtsystems und einzelner Komponenten und Teilsysteme, Ermittlung zulässiger Reparaturzeiten)
8. Abschätzung der Eintrittswahrscheinlichkeiten der Störfälle
9. Bewertung der Zuverlässigkeitsergebnisse
10. Abfassung der Gutachtensbeiträge
11. Festschreibung der in der Analyse zugrunde liegenden Betriebsstrategie (Inspektionszeiten, zul. Reparaturzeiten, Armaturengrundstellungen, Schaltmaßnahmen, Pumpenfahrweisen) z.B. im Betriebshandbuch der Anlage.

1: Ausgangspunkt für die Zuverlässigkeitsanalysen ist die Ermittlung der relevanten Störfälle einer Anlage, die durch die hier zu untersuchenden Sicherheitssysteme beherrscht werden müssen.
Die "Sicherheitskriterien für Kernkraftwerke" geben hierfür die sicherheitstechnisch wichtigen Systeme vor (vergl. Abschn. 1.2).
Für die Analyse der Not- und Nachkühlsysteme der Druck- und Siedewasserreaktoren sind hier folgende Ausgangsstörfälle relevant:

Nachkühlsysteme:	kleines Leck
	mittleres Leck
	großer Rohrbruch
Notspeisesystem:	Notstromfall
	Ausfall der Hauptwärmesenke
	Rohrbruch im Sekundärkreis
	kleines Leck im Primärkreis
	Einwirkungen von außen (allgemein)

In den Fehlerbaumanalysen werden diese Störfälle durch die Definition des unerwünschten Ereignisses jeweils berücksichtigt.
Bei der Analyse des Reaktorschutzsystems ist die Gesamtheit der Störfälle zu erfassen. Da in diesem System die Anrege- und Abschaltketten jedoch im wesentlichen gleichartig aufgebaut sind, genügt hier die Auswahl repräsentativer Störfälle. Die Auswahl erfolgt hinsichtlich der minimalen Redundanz im Reaktorschutzsystem und hinsichtlich der Komplexität von Anregeketten. Die Zuverlässigkeitsergebnisse sind dann auch auf

andere Anforderungsfälle übertragbar.

2: Der zweite Schritt beinhaltet die Ermittlung der Systeme, die für die Beherrschung der einzelnen Störfälle notwendig sind.

3: Vor Erstellung oder Überprüfung der Fehlerbäume ist eine detaillierte Einarbeitung in die Wirkungsweise der Systeme anhand von Schaltplänen und Systemspezifikationen erforderlich.
Die Ermittlung der einzelnen Ausfallarten der Systemkomponenten, die damit verbundenen Ausfallwirkungen und die Fehlererkennbarkeit sind ebenfalls wesentliche Voraussetzungen für die Zuverlässigkeitsanalyse. Dieser Punkt kann mit der speziell hierfür entwickelten DIN-Norm: Ausfalleffektanalyse /11/ erarbeitet werden. Hierbei erfolgt auch die Beurteilung der Prüfmöglichkeiten und der zugehörigen Prüfintervalle und -strategien.

Die Genauigkeit der erzielten Ergebnisse ist neben gesicherten Zuverlässigkeitsdaten wesentlich von einer richtigen Umsetzung des Systems und des Systemverhaltens unter Störfallbedingungen in das Zuverlässigkeitsmodell (Fehlerbaum) abhängig. Dieses setzt eine enge Zusammenarbeit zwischen den Bearbeitern der Zuverlässigkeit mit denen der Systemtechnik und Störfallanalyse voraus.
Dieser Analysenabschnitt erfordert erfahrungsgemäß den größten Bearbeitungsaufwand und beinhaltet eine Vielzahl von Abstimmungsgesprächen zwischen den betroffenen Parteien.

4: Der Punkt 4 erfordert die Durchführung detaillierter Wirksamkeitsanalysen für die einzelnen Systeme. Ergebnis ist die Festlegung der Anzahl der Stränge eines Systems, die zur Störfallbeherrschung erforderlich sind, z.B.:

Notstromfall bei DWR:	1v4 Stränge des Notspeisesystems
2F-Bruch bei DWR: (Standardanlage)	5v8 Druckspeichereinspeisungen 2v4 ND-Einspeisungen etc.

5: Kernpunkt der Fehlerbaumanalyse ist, daß alle zur Beherrschung eines Störfalles notwendigen Systeme analysiert werden und daß das TOP-Ereignis des Fehlerbaums die Gesamtheit der möglichen Ausfallkombinationen der Sicherheitssysteme darstellt. Dieses erfolgt nach dem deduktiven Prinzip der Fehlerbaumanalyse und wird in DIN 25424 /2/ ausführlich beschrieben (vergl. auch /3 (App II), 12, 13/, Bild 1).
Damit wird ebenfalls der Zuverlässigkeitsnachweis für verschiedene Einzelsysteme (Weisungsbeschluß 13) geliefert.
Eine nach verschiedenen Einzelsystemen getrennt durchgeführte Zuverlässigkeitsanalyse würde dagegen im Hinblick auf die zu untersuchenden Sicherheitsfunktionen, wie Notkühlung oder Abschaltung, verfälschte Ergebnisse liefern.

6: Für die Berechnung des Fehlerbaums ist die Festlegung von Ausfallraten, Inspektions- und Reparaturzeiten der Komponenten erforderlich. Nachfolgende Tabelle zeigt beispielhaft die bei der Begutachtung verschie-

dener Kernkraftwerke verwendeten Ausfallraten:

Komponente	Ausfallart	Ausfallrate 1/h
Pumpe	startet nicht	$1{,}5 \cdot 10^{-5}$
Motorschieber	öffnet nicht, schließt nicht	$1 \cdot 10^{-5}$
Rückschlagklappe	öffnet nicht	$5 \cdot 10^{-7}$
Rückschlagklappe	schließt nicht	$2{,}5 \cdot 10^{-6}$
Lüfter	startet nicht	$5 \cdot 10^{-6}$
Diesel	startet nicht	$4 \cdot 10^{-2}$/Anforderung

Diese Daten entstammen größtenteils der Literatur.

Im Kapitel 3 wird noch im einzelnen auf Gewinnung von Zuverlässigkeitsdaten aus Betriebserfahrungen in Kernkraftwerken eingegangen.

7-11: Das Berechnungsverfahren des Fehlerbaums kann hier nicht behandelt werden. Hierfür existieren eine Reihe von Rechenprogrammen /14/. Auf die weiteren Punkte wird in den folgenden Abschnitten sinngemäß eingegangen.

2.2 Zuverlässigkeitsanalysen für einen SWR

Für das Kernkraftwerk Krümmel wurden detaillierte Zuverlässigkeitsanalysen für

- das Schnellabschaltsystem
- die Notkühlsysteme
- das automatische Druckentlastungssystem

durchgeführt. Repräsentative Störfälle stellten die Ausgangsbedingungen für die unerwünschten Ereignisse der Fehlerbaumanalysen dar.

Im folgenden werden die Ergebnisse zum Druckentlastungssystem (DES) und Notkühlsystem dargestellt:

Für das Druckentlastungssystem wurden entsprechend seiner sicherheitstechnischen Aufgaben

a) Druckbegrenzung bei Ausfall der Hauptwärmesenke
b) Automatische Druckentlastung bei einem Kühlmittelverluststörfall (44 cm^2-Leck im RDB-Boden)

probabilistische Zuverlässigkeitsanalysen durchgeführt.

In den Analysen wurden die aktiven Komponenten des Druckentlastungssystems, wie Hauptventile, Vorsteuerventile, Magnetventile, Schalter, Gleichstromversorgung berücksichtigt.

Die Zuverlässigkeitsanalyse der Steuerungen der Sicherheitssysteme KKW Brunsbüttel zeigte, daß die Unverfügbarkeit der Funktionsgruppensteuerungen gegenüber der Maschinentechnik nicht zu vernachlässigen ist. Eine Zuverlässigkeitsanalyse für die Steuerungen der Sicherheitssysteme wird in einer späteren Analyse durchgeführt, um sicherstellen zu können, daß dieser Teil der Sicherheitssysteme keine Schwachstellen beinhaltet.

a) Analyse für den Störfall "Ausfall der Hauptwärmesenke":

Als Anforderungsfall an die automatische Druckbegrenzung wird ein Ausfall der Hauptwärmesenke, verursacht durch fehlangeregten Durchdringungsabschluß mit einer

Eintrittshäufigkeit von ca. 2 Ereignissen pro Jahr, zugrunde gelegt. Diese Transiente stellt die schärfste Anforderung an die Druckbegrenzung dar.
Der Analyse wurde als unerwünschtes Ereignis ein Versagen der Druckbegrenzung derart, daß der 1,1-fache Auslegungsdruck (96 bar) des Druckbehälters überschritten wird, zugrunde gelegt. Dieses Ereignis stellt im Sinne einer Risikoanalyse noch kein Schadensereignis (Bruch) für den Behälter dar; es beschreibt vielmehr ein unzulässiges Überschreiten des Auslegungswertes. Der verbleibende Abstand (Druckdifferenz) zwischen dem analysierten und einem Schadensereignis wurde jedoch nicht bestimmt. Wirksamkeitsrechnungen zeigen, daß ein Reaktordruck von 96 bar überschritten wird, wenn folgendes Ereignis eintritt:

"6 der 11 Hauptventile öffnen nicht bei Anforderung".

Die quantitative Auswertung des Fehlerbaums für dieses Ereignis ergibt eine maximale Unverfügbarkeit von

$$UV_{max} < 1 \cdot 10^{-7}$$

Dieser Wert ergibt sich aufgrund des hohen Redundanzgrades der Vorsteuer- und Hauptventile.
Der Einfluß gemeinsamer Versagensursachen der Komponenten wurde nicht quantifiziert, da für die hier verwendeten Komponenten aus Betriebserfahrungen keine diesbezüglichen Anhaltspunkte vorliegen.

b) Analyse für den Störfall "44 cm^2-Leck im RDB-Boden":

Eine detaillierte Zuverlässigkeitsanalyse für die Not- und Nachkühlsysteme erfolgte für den Störfall "Speisewasserleitungsbruch". Die Analyse für den maschinenbaulichen Teil ergab eine maximale Unverfügbarkeit von

$$UV_{max} = 5 \cdot 10^{-4}$$

Da sich beim kleinen Leck im RDB die Wirksamkeitsbedingungen für die Notkühlsysteme gegenüber dem Speisewasserleitungsbruch verbessern, ergibt sich auch für das kleine Leck eine etwas günstigere Gesamtunverfügbarkeit der maschinenbaulichen Komponenten.

Für die Beherrschung des Störfalls "44 cm^2-Leck im RDB-Boden" wird zusätzlich zu den Notkühlsystemen der Einsatz der automatischen Druckentlastung sowie des hydraulischen Offenhaltesystems notwendig.

Die oben genannten Systeme des DES wurden hinsichtlich ihres Beitrages zur Gesamtunverfügbarkeit der Notkühlsysteme bewertet. Aufgrund von Wirksamkeitsbetrachtungen wurde folgendes unerwünschtes Ereignis der Analyse zugrunde gelegt.

"Bei Anforderung der automatischen Druckentlastung öffnen weniger als 3 der 10 angeregten Hauptventile oder das Offenhaltesystem versagt".
Entsprechend dieser Bedingung wurde eine Fehlerbaumanalyse durchgeführt.
Der Unverfügbarkeitsbeitrag des Druckentlastungssystems beträgt

$$UV_{max} = 0,9 \cdot 10^{-4}$$

Die Unverfügbarkeit der Not- und Nachkühlsysteme einschließlich des Druckentlastungssystems für die betrachteten Kühlmittelverlust-Störfälle ergibt sich zu

$$UV_{max} \leqslant 5 \cdot 10^{-4}$$

2.3 Zuverlässigkeitsanalysen für einen DWR

Die Zuverlässigkeitsanalyse zu den Sicherheitssystemen des DWR (Standardanlage) umfaßt das gesamte Bruchspektrum der KMV-Störfälle

a)
- 2F-Bruch im heißen, kalten Strang
- mittleres Leck
- kleines Leck

Die Sicherheitssysteme wurden weiterhin für die Störfälle

b)
- Einwirkungen von außen

c)
- Notstromfall

einer Zuverlässigkeitsanalyse unterzogen.

Im einzelnen wurden folgende maschinenbauliche Systeme in der Analyse erfaßt:

- Nukleares Not- und Nachkühlsystem
- Nukleares Zwischenkühlsystem
- Nukleares Nebenkühlwassersystem
- Notspeisesystem
- Lüftung des Notspeisesystems
- Energieversorgungssysteme

Die Analysen zur Abblasestation auf der Sekundärseite (Druckabsenken zum Abfahren der Anlage) und zur Steuerung der Systeme erfolgen zu einem späteren Zeitpunkt.

a) Analyse der Kühlmittelverluststörfälle:

In den Analysen zu den Kühlmittelverluststörfällen wurden die Ausgangsstörfälle so gewählt, daß das gesamte Bruchspektrum abgedeckt werden konnte.

Grundlage der Analyse bilden Wirksamkeitsbedingungen des Genehmigungsverfahrens, die auf der Basis konservativer Randbedingungen ermittelt wurden. Bei großen und mittleren Brüchen wird das Überschreiten einer Hüllrohrtemperatur von 1200°C als Versagen der Notkühlung gewertet. Diese Auslegungsgrenzen wurden ebenfalls als unerwünschtes Ereignis für die Fehlerbaumanalyse gewählt. Schadensumfangsanalysen (Untersuchungen der GRS) auf der Basis von "best-estimate"-Bedingungen (wahrscheinlichste Störfallparameter) zeigen noch erhebliche Reserven auf bevor ein Kernschmelzen eintritt. Die Frage nach der Verwendung von realistischeren Daten befindet sich noch in der Diskussion. In der amerikanischen und deutscher Risikostudie wurde hiervon jedoch auch noch kein Kredit genommen.

Die in den Analysen angenommenen Wirksamkeitsbedingungen sind im folgenden aufgeführt[x]:

2F-Bruch, kalter bzw. heißer Strang:

Druckspeicher	: 5v8	beliebige Druckspeicher
ND-Einspeisung	: 2v4	heiß, 1v4 kalt bzw. 2v4 kalt,
	1v4	heiß
Nachwärmeabfuhr über	2v4	heiße Einspeisungen und
die Nachkühlkette	: 2v4	Nachkühlketten

x) Ergebnisse der Untersuchung der Gesellschaft für Reaktorsicherheit für die DWR-Standardanlage.

TÜV Norddeutschland

Mittleres Leck:

Druckspeicher	: <	5v8 beliebige Druckspeicher
HD-Einspeisung	:	2v4
ND-Einspeisung	: <	2v4
Nachwärmeabfuhr		2v4 heiße Einspeisungen und
über Nachkühlkette	:	2v4 Nachkühlketten
Sekundärseite	:	---

Kleines Leck:

Druckspeicher	:	---
HD-Einspeisung	: <	2 v 4
ND-Einspeisung	: <	2 v 4
Nachwärmeabfuhr		
über Nachkühlkette	:	2v4 Nachkühlketten
Sekundärseite	:	2v4 Dampferzeugerbespeisungen mittels Notspeisesystem

Die Randbedingungen für die Wirksamkeitsberechnungen basieren in erster Linie auf dem Einzelfehlerkriterium, d.h. ein Teilsystem befindet sich im Anforderungsfall in Reparatur, beim anderen tritt ein Fehler auf; das verbleibende System muß den Störfall beherrschen. Werden mit diesen Annahmen die zulässigen Störfallparameter eingehalten, wird der Wirksamkeitsnachweis als erfüllt angesehen.
Liegen die errechneten Parameter hinreichend weit unter den zulässigen, so ist es denkbar und bei den mit (<) gekennzeichneten Fällen wahrscheinlich, daß der weitere Ausfall eines Teilsystems noch zu keiner Überschreitung zulässiger Werte führt.
Wenn die Zuverlässigkeitsanalyse mit den gewählten Ausgangswerten ausreichende Ergebnisse liefert, so

wird keine weitere Wirksamkeitsanalyse durchgeführt.

Als Zuverlässigkeitskenngröße wurde die maximale Unverfügbarkeit errechnet, d.h., die Wahrscheinlichkeit dafür, daß die Systeme zum Ende des Inspektionsintervalls im Anforderungsfall versagen.

2F-Bruch	:	$UVmax = 1 \cdot 10^{-4}$
Mittleres Leck	:	$UVmax = 1{,}5 \cdot 10^{-4}$
kleines Leck	:	$UVmax = 10^{-2} - 1{,}3 \cdot 10^{-3}$

Für die einzelnen Bruchgrößen ergeben sich aufgrund der verschiedenartigen Anforderungen an die Systemtechnik unterschiedliche Werte für die Unverfügbarkeit. Zur Beherrschung des 2F-Bruches wird in der ersten Phase des Störfalles der Einsatz der Druckspeicher sowie der ND-Einspeisung notwendig. Nach Umschaltung auf Sumpfbetrieb ist zusätzlich der Einsatz der Zwischen- und Nebenkühlwassersysteme notwendig. Die Druckspeichereinspeisungen, die beim Nachweis der Notkühlwirksamkeit den höchsten Beitrag leisten, tragen zur maximalen Unverfügbarkeit der Notkühlsysteme nur mit einem geringen Anteil bei. Die ND-Einspeisung leistet einen Anteil von ca. 30%. Der Hauptbeitrag der Unverfügbarkeit (ca. 70%) wird durch die notwendige Nachwärmeabfuhr aus dem Containment hervorgerufen, was für den Störfallablauf positiv zu werten ist, da in dieser Phase der Reaktor bereits wieder geflutet ist und die maximalen Hüllrohrtemperaturen bereits das Maximum überschritten haben.

Für das mittlere Leck ergibt sich ein Unverfügbarkeitswert, vergleichbar zum Wert des großen Bruches. Der zusätzliche Einfluß der HD-Einspeisung auf das Zuverlässigkeitsergebnis ist nur gering. Der Hauptanteil wird ebenfalls durch den Ausfall der Nachwärmeabfuhr hervorgerufen.

Für die Beherrschung der kleinen Lecks wird zusätzlich zu dem Not- und Nachkühlsystem der Einsatz der Sekundärseite notwendig. Obwohl die Anforderung an die Kühlkapazität des Not- und Nachkühlsystems geringer ist, verringert sich die Unverfügbarkeit nicht erheblich, da auch in diesem Fall zwei Nachkühlketten zur Beherrschung des kleinen Lecks erforderlich sind, was ca. 70% der für den großen Bruch errechneten Unverfügbarkeit ausmacht.

Die hohe Unverfügbarkeit von UVmax = $1 \cdot 10^{-2} - 1{,}3 \cdot 10^{-3}$ wird durch das sekundärseitige Notspeisesystem der DWR-Standardanlage bestimmt. Die Werte - Differenz ergibt sich aus der Prüfhäufigkeit für die Dampferzeugerhöhenstandsregelung sowie für die Freilaufrückschlagventile, je nachdem, ob diese monatlich oder nur jährlich prüfbar sind.

Weiterhin ist zur Beherrschung des kleinen Lecks die Dampferzeuger-Abblasestation notwendig. Aufgrund der strangzugeordneten Bespeisung der Dampferzeuger durch das Notspeisesystem und der langen Inspektionsintervalle für die Abblaseeinrichtung wird hier zusätzlich noch ein wesentlicher Unverfügbarkeitsbeitrag erwartet. Dies konnte jedoch in der bisherigen Analyse noch nicht berücksichtigt werden.

b) Analyse der Einwirkungen von außen:

Beim Störfall infolge "Einwirkungen von außen" spielt das Notspeisesystem die zentrale Rolle. Die Wirksamkeitsbedingung bei totalem Verlust der nichtgesicherten Nachwärmeabfuhrsysteme einschließlich der Versorgungssysteme fordert zur Störfallbeherrschung:

" 2v4 Notspeisestränge"

Die maximale Unverfügbarkeit entspricht in etwa dem Wert für den Anforderungsfall kleines Leck.

Weiterhin sind zur Störfallbeherrschung der Einsatz der Sicherheitsventile der Dampferzeugerabblasestation und die Füllstandshaltung auf der Primärseite notwendig, die einen zusätzlichen Beitrag zur Unverfügbarkeit liefern.

c) Analyse des Notstromfalls:

Zur Beherrschung des Notstromfalls stehen bei der DWR-Standardanlage die beiden separaten Notstromsysteme Notnetz 1 und 2 zur Verfügung (Jeweils 4 Teilsysteme). Die Notstromdiesel von Netz 1 versorgen zusätzlich zu dem Not- und Nachkühlsystem sekundärseitig die An- und Abfahrpumpen. Die Diesel von Notnetz 2 versorgen die Notspeisestränge. Die Analyse des Notstromfalls unter Berücksichtigung aller verfügbaren Systeme ist gegenüber den vorgenannten Systemen am vielfältigsten und ist gegenwärtig noch nicht abschließend behandelt. Auf die Angabe von Ergebnissen wird hier verzichtet.

Da die Eintrittswahrscheinlichkeit des Notstromfalls vergleichsweise zu denen von Kühlmittelverluststörfällen groß ist, hat der Notstromfall sicherheitstechnisch hohe Relevanz.
Eine grobe Abschätzung von Notstromfällen aufgrund der Netzverfügbarkeit des deutschen (Fall 1) und des amerikanischen Verbundnetzes (Fall 2 u. 3) /15 - 18/ liefert folgende Werte:

Fall 1	$\leq$ 1 h	$H = 5 \cdot 10^{-2}$ 1/a
Fall 2	1-10 h	$H = 1 \cdot 10^{-2}$ 1/a
Fall 3	$>$ 10	$H = 1 \cdot 10^{-3}$ 1/a

Die Aussagesicherheit der angegebenen Häufigkeitswerte nimmt mit der Dauer des Netzausfalls erheblich ab, da längerfristige Netzausfälle nur durch großflächige Umweltkatastrophen vorstellbar sind und daher nur schwer prognostiziert werden können. Weiterhin wird die Wiederherstellung des Netzes stark durch die gegebenen Umstände beeinflußt.

Die Zuverlässigkeitsanalysen zur DWR-Standardanlage zeigen für einzelne Systeme vergleichbare Ergebnisse zur deutschen Risikostudie. Abweichungen ergeben sich durch teilweise unterschiedliche Systemausführungen, auf die hier im einzelnen jedoch nicht eingegangen werden kann. Auch für die DWR-Standardanlage führen die Störfälle "kleines Leck" und "Notstromfall" im Zusammenhang mit den Sicherheitssystemen zu den größten Wahrscheinlichkeitswerten vergleichsweise zu anderen Störfallkombinationen. Gegenüber der Referenzanlage der deutschen Risikostudie stehen bei der Standardanlage zwei Notstromsysteme (insgesamt 8 Diesel) zur Beherrschung von Störfällen mit Ausfall der Eigenbedarfsversorgung zur Verfügung. Die momentan vorliegenden Er-

gebnisse sind denen der deutschen Risikostudie vergleichbar, da nur Sicherheitssysteme analysiert wurden. Bei Berücksichtigung der vorhandenen Betriebssysteme ist eine erhebliche Reduzierung der Wahrscheinlichkeitsergebnisse zu erreichen.

2.4 Analysenaufwand

Der Bearbeitungsaufwand zur Durchführung der Analysen für die wesentlichen Sicherheitsfunktionen einer Anlage ist für sich genommen beträchtlich und kann bis zu ungefähr 1-2 Mannjahren betragen. Dieser Aufwand ist jedoch vergleichsweise zur kompletten Systembegutachtung nur ein geringer Teil. Für jede weitere systemtechnisch gleichartige Anlage sind die erarbeiteten Ergebnisse unmittelbar übertragbar. Der Aufwand besteht dann in der Gewährleistung der richtigen Übertragung der Ergebnisse.
Eine enge Zusammenarbeit zwischen den Bearbeitern der Zuverlässigkeitsanalyse und denen der Systemüberprüfung (letztere fällt in jedem Fall an) ist nicht nur aus sachbezogenen Gründen erforderlich, sondern deckt auch einen wesentlichen Bearbeitungsaufwand ab (vergl. Abschnitt 2.1).

TÜV Norddeutschland

3. Zuverlässigkeitsdaten

3.1 Benötigte Daten

Für die Berechnung des Fehlerbaums sind folgende Eingangsdaten für die erfaßten Komponenten erforderlich:

- Ausfallraten bzw. Ausfallwahrscheinlichkeiten pro Anforderung
- Inspektionszeiten
- Reparaturzeiten

Für die Sicherheitssysteme (wie in Abschnitt 2 erwähnt), die im wesentlichen im Stand by-Betrieb zur Reaktoranlage gefahren werden, gibt die Inspektionszeit (Zeit zwischen zwei Prüfungen) die maximale Fehlerentdeckungszeit ausgefallener Komponenten an. Für die meisten verfahrenstechnischen Systeme wird ein Monat als Inspektionszeit vorgegeben, um einerseits die Start- und Schalthäufigkeit der Komponenten zu begrenzen und andererseits die Fehlerentdeckungszeit möglichst klein zu halten. Die Nichtverfügbarkeit einer Komponente ergibt sich aus dem Produkt von Ausfallrate und Fehlerentdeckungszeit einschließlich der Instandsetzungszeit (Reparaturzeit). Eine Änderung der Inspektionszeit bewirkt unmittelbar eine Änderung der Nichtverfügbarkeit einer Komponente. Das Zuverlässigkeitsergebnis eines Stand by-Systems kann damit in einfacher Form verändert werden. Einer erstrebten Verbesserung durch Reduzierung der Inspektionszeiten sind jedoch Grenzen gesetzt, da dann mit einer Zunahme von Verschleiß zu rechnen ist.
Durch diese Betrachtung wird auch deutlich, daß die wiederkehrenden Prüfungen der Systeme ein ganz entscheidendes Instrument zur Gewährleistung einer ermit-

telten Systemzuverlässigkeit sind. Daraus ergeben sich folgende Forderungen an die Systemauslegung und an den Betrieb: Die Prüfung dieses Systems muß in der Form gestaltet werden, daß alle für die Systemfunktion erforderlichen Komponentenfunktionen abgefragt werden und diese dann auch zur Anzeige kommen. Bei erkanntem Ausfall einer Komponente wird die Instandsetzung durchgeführt.
Die Fragen der Prüfbarkeit und Reparierbarkeit von Komponenten stellen daher wesentliche Bearbeitungspunkte bei der System- und Zuverlässigkeitsprüfung dar.
Die Reparaturzeiten ergeben sich aus den Betriebserfahrungen. Je nach Art der Fehler streuen diese Zeiten sehr stark, diese liegen zwischen wenigen Minuten (Austausch einer Elektronikkarte) und einigen Wochen (Austausch einer großen verfahrenstechnischen Komponente). Die Obergrenze wird durch die Ersatzteilbeschaffung bestimmt.
Auch bei einem Fehler in der Steuerung können dem Austausch einer Elektronikkarte mehrere Stunden der Fehlersuche vorangehen.
Die in Wash 1400, App III / 3 / angegebenen Reparaturzeiten für verschiedene Komponenten können durch unsere Untersuchungen bestätigt werden.
Für Notstromdiesel haben wir eine mittlere Reparaturzeit von 12 Stunden ermittelt, die Verteilung ist in etwa log-normal und reicht von ca. 1 Stunde bis zu einigen Wochen. Ähnliche Ergebnisse ergeben sich für Pumpen und Armaturen.
Da die Nichtverfügbarkeit von Stand-by-Komponenten sich aus der Fehlerentdeckungszeit (max. 1 Monat) und der Reparaturzeit (im Mittel 10 Std.) ergibt, hat

die Genauigkeit der Reparaturzeitangabe keinen hohen Einfluß auf das Zuverlässigkeitsergebnis insgesamt. Die prinzipielle Reparierbarkeit einer Komponente auch nach einem Störfall, ist jedoch von wesentlicher Bedeutung. Ferner ist zu berücksichtigen, daß Reparatur- und Reparaturzeitbeschränkungen im Hinblick auf den Reaktorbetrieb durch Betriebsauflagen festgeschrieben sein können.
Zuverlässigkeitsdaten wie Ausfallraten und Ausfallwahrscheinlichkeiten bei Anforderung werden im allgemeinen aus Betriebserfahrungen gewonnen und finden ihren Niederschlag in der einschlägigen Literatur /3 (App. III), 19 - 24/.
Die Übertragbarkeit dieser Literaturwerte auf die Komponenten des betrachteten Systems ist jedoch häufig mit Unsicherheiten behaftet, wenn Literaturwerte nur wenig spezifiziert sind, z.B. im Hinblick auf

- die Art der betrachteten Komponente
- Stichprobenumfang
- Ausfallhäufigkeit
- Ausfallarten
- Ausfallursachen

Zur Erhöhung der Datensicherheit werden vom TÜV eigene Untersuchungen auf der Basis von Betriebsaufzeichnungen der im Betrieb befindlichen Anlagen durchgeführt.
In Einzelfällen, wie z.B. der Ermittlung der Absturzwahrscheinlichkeit einer schweren Last vom Hebezeug /25/, wurden zur Vergrößerung des Stichprobenumfanges auch vergleichbare konventionelle Anlagen herangezogen. Diese Arbeit wurde von mehreren TÜVen durchgeführt.

Ebenfalls wird z.Z. eine umfangreiche Auswertung über Notstromdieselaggregate erarbeitet.

3.2 Auswertung von Betriebserfahrungen

Im ersten Schritt der Ermittlung von Zuverlässigkeitsdaten werden Ausfallhäufigkeiten bestimmt.
Dafür wird die Anzahl der Ausfälle der Komponenten innerhalb eines Beobachtungszeitraumes ermittelt und ebenfalls die Anzahl der beobachteten Komponenten (z.B. die in einem System).
Der Beobachtungsraum (Zeit und Stichprobenumfang) ist dabei frei wählbar.
Die relative Häufigkeit "h" wird nach folgender Beziehung berechnet:

$$h_{ij} = \frac{\text{Anzahl der Ausfälle der Komponenten (i) einer Ausfallart (j)}}{\text{Anzahl der beobachteten Komponenten (i) x Beobachtungszeit}}$$

Für die Bestimmung der Ausfallhäufigkeit bei Anforderung wird statt der Beobachtungszeit, die Anzahl der Anforderungen (Schaltungen, Starts) angesetzt.
Die Anzahl der beobachteten Komponenten (z.B. einstufige Kreiselpumpen oder Absperrarmaturen einer bestimmten Größe) ist aus den Systemspezifikationen, Systemzeichnungen und Komponentenlisten zu entnehmen.
Komponentenausfälle werden in der betrieblichen Dokumentation einer Anlage geführt, wie:

- Schichtbücher
- Reparatur- und Arbeitsaufträge
- Monatsberichte
- Protokolle der wiederkehrenden Prüfungen
- Störungsmeldungen an die GRS

Die in der Dokumentation aufgeführten Störmeldungen müssen entsprechend ausgewertet werden. Dabei hat sich die Verwendung eines Formblattes als zweckmäßig erwiesen (Bild 2).

1. Kennzeichnung der Komponente (Anlagenkennzeichnung)
2. Zeitpunkt der Ausfallerkennung (bei einer Stand by-Komponente liegt der tatsächliche Ausfallzeitpunkt vor diesem Wert), Ermittlung der unbemerkten Ausfallzeit
3. Art der Fehlererkennung
4. Anlagenzustand bei Ausfall (z.B. gekennzeichnet durch die Höhe der Reaktorleistung)
5. Ausfallart der Komponente (wird aus der Störungsbeschreibung abgeleitet)
6. Störungsursache (wird aus der Reparaturmaßnahme abgeleitet)
7. Zeitpunkt der Störungsbehebung (Ende der Ausfallzeit, bzw. Nichtverfügbarkeitszeit der Komponente)
8. Angabe der Störungsauswirkung bei Eintritt der Störung und bei der Durchführung der Reparatur (der Komponentenausfall führt ggf. zum Teilsystem- oder Systemausfall, durch die Reparaturmaßnahme muß ggf. ein System freigeschaltet werden).
9. Angabe der verwendeten Unterlagen

Der Aufbau des Formblattes ist mit dem der Norm: Ausfalleffektanalyse /11/ sehr verwandt.

Die einzelnen Angaben im Formblatt werden codiert:

Spalte (3): "Störung erkannt durch"
- WP: Wiederholungsprüfung
- Md: Wartenmeldung
- Rg: Anlagenrundgang
- Af: Anforderung

Spalte (9): "Art der Störungsbeherrschung"
- R : Reparatur
- W : Wartung (allgemein)
- Öl: Ölwechsel, Wechsel von Schmiermittel
- K : Kontrollmaßnahme
- U : Komponentenumbau

Spalte (6): "Störungsart (Ausfallart)"

Armatur:
- fällt offen aus (bei Anforderung oder in Offenstellung)
- fällt geschlossen aus (bei Anforderung oder in Geschlossenstellung
- schließt nur teilweise
- öffnet nur teilweise
- innere Leckage (gering bzw. groß) bei Geschlossenstellung
- äußere Leckage (gering bzw. groß)

Schalter:
- fällt offen aus (bei Anforderung oder in Offenstellung)
- fällt geschlossen aus (bei Anforderung oder in Geschlossenstellung)

- öffnet unbeabsichtigt
- schließt unbeabsichtigt

Pumpe:
- läuft nicht an oder schaltet kurz nach Anlauf wieder ab
- fällt während des Betriebes aus
- äußere Leckage (gering bzw. groß)

Nach der Durcharbeitung der Störmeldungen, die innerhalb der festgelegten Beobachtungszeit vorliegen, werden diese in Teilmengen nach

- Komponentenklassen und
- Ausfallarten

eingeteilt. Die relative Ausfallhäufigkeit wird dann für jede Teilmenge berechnet.
Eine solche Teilmenge ist z.B.

- Absperrarmatur mit elektr. Stellantrieb (NW 100-400)
- Ausfallart: öffnet nicht.

Je nach Art der angefallenen Störmeldungen müssen die Teilmengen sinnvoll gewählt werden.
Traten z.B. die Ausfälle hauptsächlich in der Ansteuerung der Komponenten auf, so sind diese in erster Linie nach der Art der Ansteuerung einzuteilen. Andere komponentenspezifische Merkmale haben ggf. nur einen vernachlässigbar geringen Einfluß auf die Ausfallhäufigkeit (siehe Abschnitt 3.3).

TÜV Norddeutschland

3.3 Ergebnisse der Datenauswertung

In Abschnitt 2.1 wurde für verschiedene Komponenten Ausfallraten angegeben, die in Zuverlässigkeitsanalysen für mehrere Kernkraftwerke verwendet wurden. Diese Daten entstammen überwiegend der Literatur.

Die Auswertung der Betriebsdaten ergab für die aufgeführten Komponenten eine recht gute Übereinstimmung mit den Literaturdaten.

Ein hoher Anteil der erfaßten Ausfälle der Komponenten ist auf das Versagen von Hilfseinrichtungen und im besonderen auf die Steuer- und Überwachungseinrichtungen zurückzuführen. Mechanische Ausfälle der Hauptaggregate sind dagegen selten, diese bewirken dann jedoch den Anteil der längeren Reparaturzeiten.
Aufgrund der Vielfältigkeit der Ausfallursachen ist auch ein mehr oder weniger konstantes Ausfallverhalten festzustellen, d.h. die Ausfallzeitpunkte sind zufällig und zeitlich gleichverteilt.
Frühausfälle für die Komponenten sind zu beobachten, eine signifikante Ausprägung ist jedoch nicht ableitbar. Die ermittelten relativen Ausfallhäufigkeiten können daher als konstante Ausfallraten verwendet werden.
Ein ähnliches Bild über das Ausfallverhalten ergibt sich auch für die Notstromdiesel, da die Funktion des

Diesels von einer großen Anzahl von Komponenten der Hilfseinrichtungen abhängig ist. Die für die Notstromdiesel häufig verwendete Ausfallwahrscheinlichkeit pro Start ist für dieses Aggregat nicht charakteristisch, hier gilt auch die konstante Ausfallrate. Die Ausfallwahrscheinlichkeit des Diesels erhöht sich nicht mit der Anzahl der Starts innerhalb eines bestimmten Zeitabschnittes, sondern mit der Dauer der prüfungsfreien Zeit.

Auch bei Hebezeugen in Bezug auf die Absturzwahrscheinlichkeit der Last konnte ein ähnliches Verhalten festgestellt werden /25/. Für verschiedene Hebezeugklassen mit unterschiedlicher Lastspielzahl war diese nur von geringem Einfluß (Bild 3).

Die Auswertung der Betriebserfahrung zeigt, daß für die Zuverlässigkeitsanalyse repräsentative Daten ermittelt werden können. Die heute festgestellten Daten sind im allgemeinen Mittelwerte einer Wahrscheinlichkeitsverteilung. Erste Untersuchungen zeigen für die hier genannten Komponenten die Ausprägung einer log.-Normalverteilung. Die Unsicherheitsfaktoren der Daten für die einzelnen Komponenten liegen überwiegend innerhalb einer Größenordnung. Eine Quantifizierung dieser Werte erfolgte nicht, hierzu sind noch weitergehende Arbeiten notwendig.

Für die in den Abschnitten 1 und 2 beschriebene Aufgabenstellung der Zuverlässigkeitsanalyse (Relativbewertung der Analysenergebnisse) sind die verfügbaren Daten bereits hinreichend aussagekräftig.

Die weiter zu vertiefenden Punkte sind die Erfassung und ggf. die Quantifizierung von systematischen und gemeinsamen Versagensursachen sowie Einflüsse menschlicher Fehler. Die aus Betriebserfahrungen gewonnenen

Ausfalldaten für einzelne Komponenten schließen alle möglichen Fehlerursachen ein und damit auch menschliche Fehler. Aus diesem Grunde ist es bei der Datenermittlung auch immer zweckmäßig, möglichst große Komponenteneinheiten zu wählen, z.B. Notstromdieselaggregat einschließlich seiner Hilfseinrichtungen.
Für gemeinsame Versagensursachen gleichartiger Komponenten, sei es durch Auslegungsmängel, systematische Fertigungsfehler oder durch Fehlbedienung, zeichnet sich ein ähnliches Ausfallverhalten ab, wie für die Einzelkomponenten dargelegt wurde, nur auf einem geringeren Wahrscheinlichkeitsniveau. Die geschilderten Verfahren ermöglichen auch hier eine systematische Datenauswertung. Durch die Maßnahmen der wiederkehrenden Prüfungen der Komponenten und Systeme in der Anlage können auch derartige Versagensursachen begrenzt und ggf. reduziert werden.
Der Nutzen einer systematischen Auswertung von Betriebserfahrungen kann wie folgt zusammengefaßt werden:

1. Gewinnung empierisch gesicherter Zuverlässigkeitsdaten.
2. Lokalisierung von Schwachstellen und Identifizierung von systematischen Ausfallursachen, die sich auch im Verlauf der Lebensdauer einer Anlage einstellen können. (Vergleich mit den Eingangsparametern einer bereits durchgeführten Analyse)
3. Überprüfung der verwendeten Zuverlässigkeitsmodelle.
4. Informationsrückfluß über das Systemverhalten zur ingenieurmäßigen Systemüberprüfung.

Mit einer stärkeren Zuwendung zur Quantifizierung der Zuverlässigkeit von Sicherheitseinrichtungen in kerntechnischen Anlagen gewinnt dieser Bereich zunehmend an Bedeutung.

TÜV Norddeutschland

Literaturverzeichnis

/ 1/ DIN 25419, Störfallablaufanalyse; Störfallablaufdiagramm, Methode und Bildzeichen, 6.77
Störfallablaufanalyse; Auswertung des Störfallablaufdiagramms mit Hilfe der Wahrscheinlichkeitsberechnung, 2.79
Beuth Verlag, Berlin

/ 2/ DIN 25424, Fehlerbaumanalyse; Methode und Bildzeichen, 6.77
Beuth Verlag, Berlin

/ 3/ Reactor Safety Study - An Assessment of Accident Risks in US Commercial Nuclear Power Plants, USNRC, Wash 1400 (NUREG-75/014), October 1975

/ 4/ Gesellschaft für Reaktorsicherheit, Deutsche Risikostudie/Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko/
Verlag TÜV Rheinland, 1979

/ 5/ Kritischer Bericht zur Reaktorsicherheitsstudie (Wash-1400), IRS-I-87/MRR-I-65, April 1976,
Köln/Garching

/ 6/ Der Bundesminister des Innern, Sicherheitskriterien für Kernkraftwerke, verabschiedet vom Länderausschuß für Atomkernenergie am 12. Okt. 1977,
Der Bundesanzeiger Nr. 206, 1977

/ 7/ TÜV-Leitstelle Kerntechnik bei der VdTÜV, Weisungsbeschluß Nr. 13: Standardgliederung mit Merkposten für TÜV/GRS-Gutachten für Kernkraftwerke mit Druck- oder Siedewasserreaktoren, VdTÜV, Essen, Mai 1977

/ 8/ KTA-Regel 3701.1, Übergeordnete Anforderung an die elektrische Energieversorgung des Sicherheitssystems im KKW, Teil 1: Einblockanlagen, Aug. 78, KTA-Geschäftsstelle, Köln

/ 9/ B. Böhm, J. Blombach, W. Rosenhauer, Unverfügbarkeitsuntersuchungen an Notkühlsystemen, atw, Juli 1974

/10/ Der Bundesminister des Innern, Interpretation zu den Sicherheitskriterien für Kernkraftwerke Einzelfehlerkonzept - Grundsätze für die Anwendung des Einzelfehlerkriteriums - (Stand: 26. Okt. 1978)
Der Bundesanzeiger Nr. 38, 1978

/11/ DIN 25448, Ausfalleffektanalyse, Nov. 1979
Beuth Verlag, Berlin

/12/ E. Dressler et.al., Zuverlässigkeitsuntersuchung von Sicherheitssystemen des Kernkraftwerkes Biblis, Block A,
Kerntechnik 17. Jg. 1975/Nr. 4

/13/ H.-P. Balfanz, F.W. Heuser, W. Ullrich, Principles of Reliability Analysis Methods Applied to an Energency Core Cooling System, Nuclear Engineering and Design 29 (1974)

/14/ K. Kotthoff, W. Otto, Vergleich von Rechenprogrammen zur Zuverlässigkeitsanalyse von Kernkraftwerken, IRS, Febr./April 1976

/15/ R. Billinton, T.K.P. Medicherla, M.S. Sachdev, Common-Cause Outages in Multiple Circuit Transmission Lines, IEEE, Transactions on Reliability, Vol. R-27, No.2, June 1978

/16/ Loss of Electric Power Coincident with LOCA, Nuclear Safety, Vol 18 No. 1, January - February 1977

/17/ Stromausfall in Süddeutschland Der Maschinenschaden 49 (1976) Heft 5

/18/ H. Novak, Die Wärmekraftwerke beim süddeutsch-österreichischen Netzzusammenbruch von 1976, VGB Kraftwerkstechnik, 58. Jahrgang, Heft 11, Nov. 1978

/19/ H.-P. Balfanz, Ausfallratensammlung IRS-W-8 (Dez. 1973), Köln

/20/ H.D. Hager, U. Steimel, Zuverlässigkeit elektronischer Baugruppen beim Einsatz in der Kraftwerksleittechnik, Elektrizitätswirtschaft, Jg. 75 (1976), Heft 24

/21/ P. Sommer, K.-R. Hartung, H. Scholz, S. Wust, Ermittlung der Ausfallraten von Dieselaggregaten und Elektronikkarten zur Bestimmung der

Ausfallwahrscheinlichkeit von Sicherheitssystemen, Qualität und Zuverlässigkeit, Jg. 22, (1977), Heft 5

/22/ P. Hömke , H. Krause, Der Modellfall IRS - RWE zur Ermittlung von Zuverlässigkeitskenngrößen im praktischen Betrieb, IRS-W-16 (November 1975), Köln

/23/ E. Lindauer, Die Auswertung von Betriebserfahrungen für die deutsche Risikostudie, GRS-Fachgespräch (Nov. 1977), GRS-10, Köln

/24/ Nuclear Plant Reliability Data System 1976 Annual Reports of System and Component Reliability, Southwest Research Institute, San Antonio, Texas 78284, May 1977

/25/ Schwerlastkrane, Auslegung, Prüfung, Zuverlässigkeit Sicherheit, Schadensfälle; Tagungsheft, VdTÜV, Essen, 21.Nov. 1978

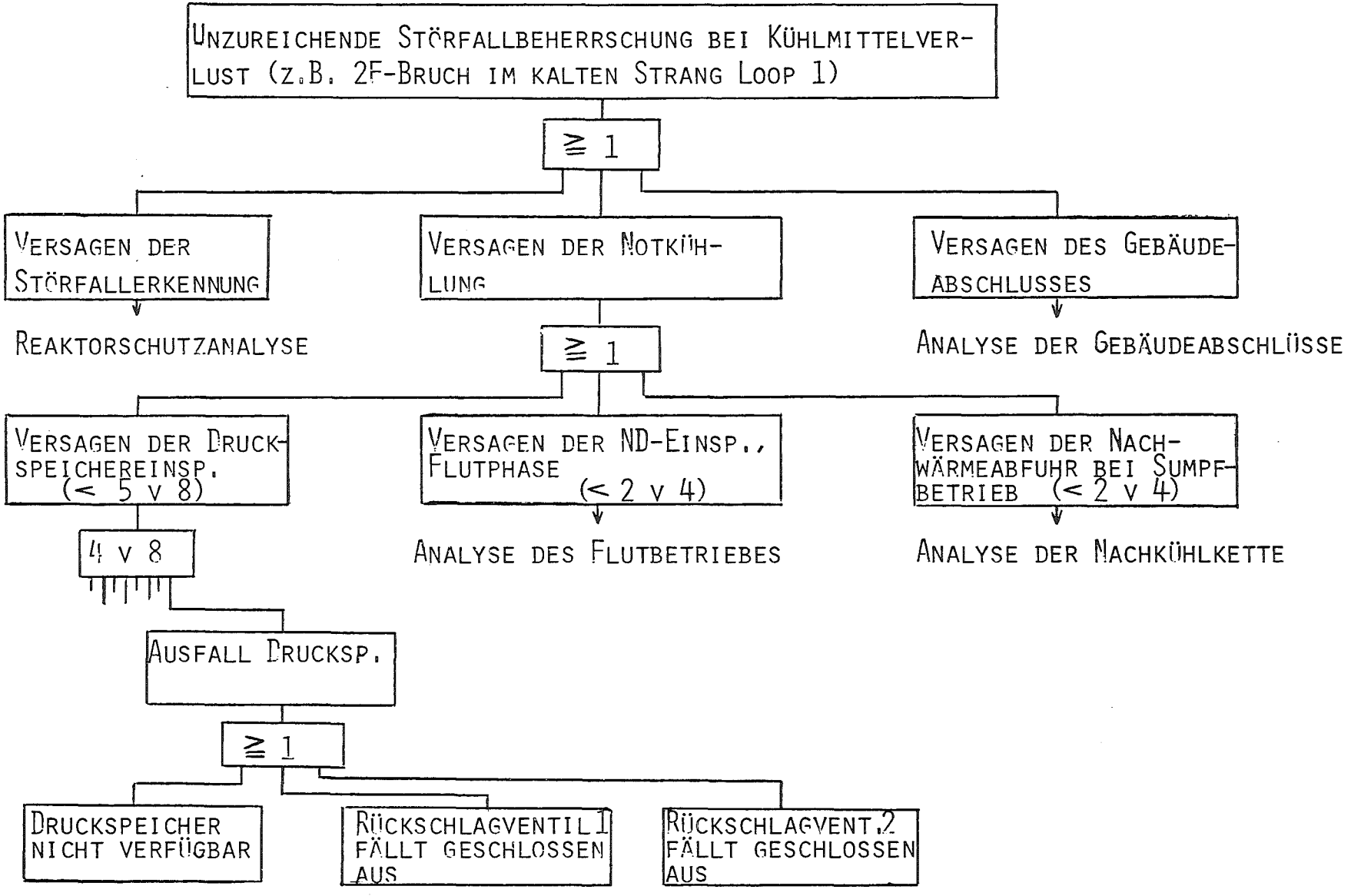


Bild 1: Beispiel für einen Fehlerbaum

Lfd. Nr.	1 Komponenten-bezeichnung	Störung erkannt 2 am	3 durch	4 Reakt.L.	5 Störungsart Störungsbeschreibung	Kod.	6 Art der Störungsbehebung Störungsursache	Kod.	Störung behoben 7 am	8 Störungsauswirkung	9 Reparat.-bericht
1	TC 01 S 102	24.6.76	Af	100	Armatur läßt sich nicht zufahren, Überstromauslösung		Spindel schwergängig, ausgetauscht	R	26.6.76		
8	TP 25 D 501	4.8.76	Rg	100	Pumpe macht Geräusche, Temperatur Lagergehäuse hoch		Lager gewechselt	R	11.8.76		
29	VF 43 D 101	30.9.76	-	100	--		Fett ausgewechselt	Öl	30.9.76		
63	TH 11 S 102	30.7.76	-	0	Vorbeugende Maßnahme, zu geringe Dimensionierung der Spindel		Spindel ausgetauscht	U	30.7.76		
103	RM 19 5402	6.12.76	Md	100	Armatur durchlässig, Druckausgleich		Dichtflächen neu eingeschliffen	R	6.12.76		
103	RM 29/39 S 402	6.12.76	-	100	--		Dichtflächen neu eingeschliffen	W	17.12.76		

Bild 2: Formblatt / Erfassung und Codierung von Störmeldungen

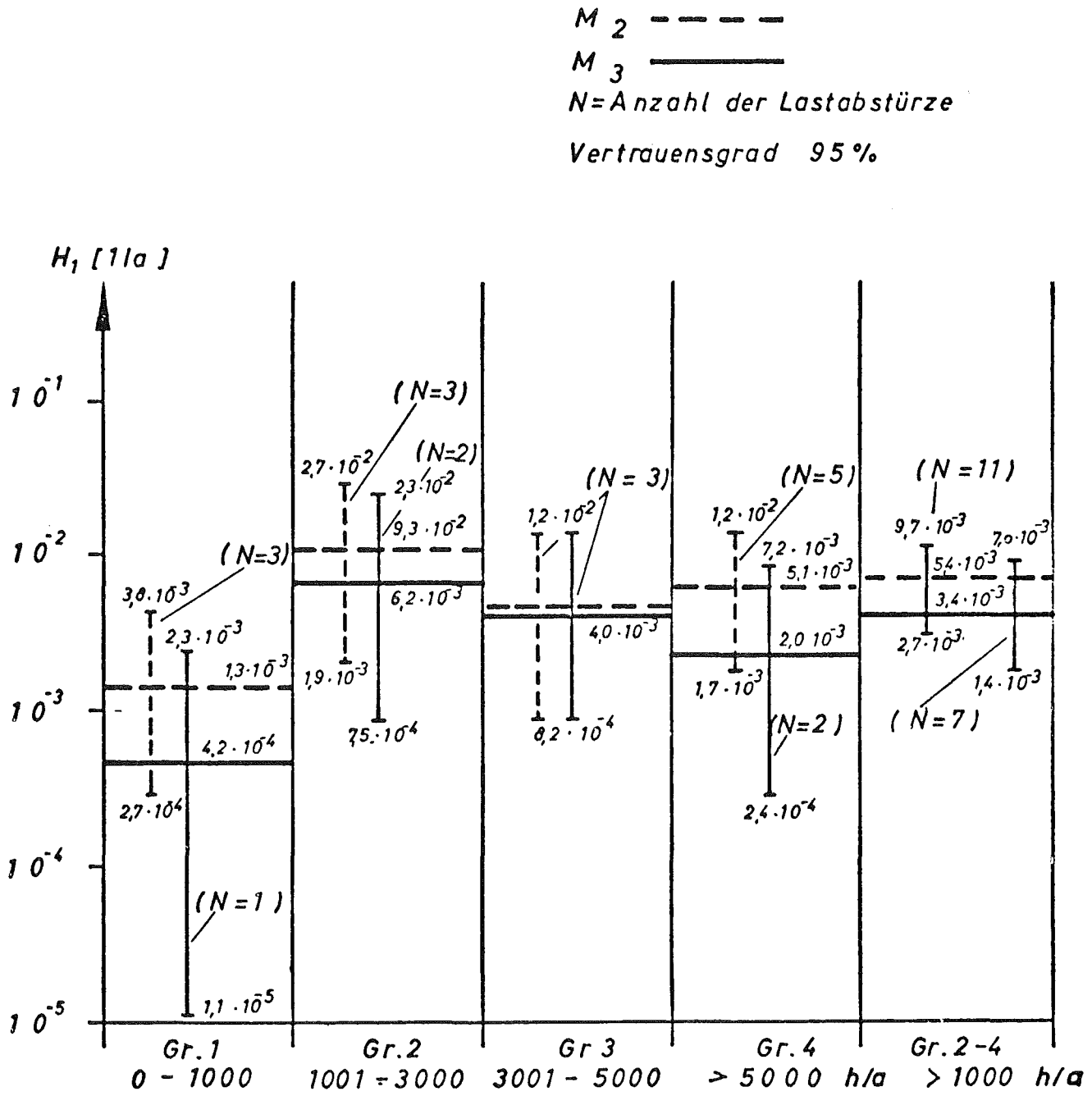


Bild 3

Rel. Absturzhäufigkeit für die Modellkrane M2 u. M3 pro Hubwerksjahr (Kalenderzeit) in Abhängigkeit der Betriebszeiten /25/

Diskussion

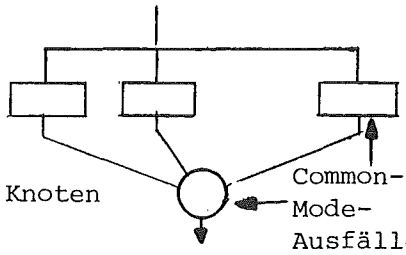
Frage: Wie berücksichtigen Sie bei Ihrer Risikoabschätzung Common Mode Fehler der unterschiedlichen Sicherheitssysteme, die durch ein Fehlverhalten des Operators verursacht werden?

Antwort: In der Fehlerbaumanalyse nehmen wir in der Regel unabhängige Komponentenausfälle an. Bewirkt der Ausfall einer einzelnen Komponente im System den Ausfall redundanter Komponenten, so wird das berücksichtigt.

Systematische Fehler, die zu einem gleichzeitigen Ausfall mehrerer Komponenten führen können, sind grundsäztlich nicht ausgeschlossen, ihre Quantifizierung ist dagegen sehr schwierig. Die Eintrittswahrscheinlichkeit ist einerseits geringer als die einzelner Komponenten und andererseits werden jeweils Änderungsmaßnahmen im System vorgenommen, sollte ein systematischer Fehler vorliegen.

In der laufenden Auswertung von Betriebserfahrungen werden diese Fälle ebenfalls erfaßt und soweit wie möglich quantifiziert. Diese Daten werden dann auch in der Fehlerbaumberechnung berücksichtigt.

Frage: Aufgrund der Anwendung von mehrfacher Redundanz besteht die Möglichkeit (vermehrt als bei nicht - oder wenig redundanten Systemen) die Redundanz durch Common-Mode-Ausfälle zu verlieren.



Wurde diese Frage beim Bsp. Druckentlastungssystem (6 v. 11) KKW Krümmel berücksichtigt? Resultat?

Antwort: Auf die Frage nach der Berücksichtigung gemeinsamer Ausfallursachen redundanter Komponenten bin ich bereits bei der Anfrage von Herrn Kopetz eingegangen.

Ich möchte an dieser Stelle noch ergänzen, daß bereits bei der Systemauslegung konkrete Maßnahmen gegen systematische Fehler getroffen werden, z.B. durch diversitäre Geräte in der Meßwerterfassung physikalischer Parameter, durch räumliche Trennung redundanter ver-

fahrenstechnischer Systeme, Überflutungsschutz, Reduzierung von Brandlasten.

Frage: Diesel sind Verschleißkomponenten. Durch periodische Starttests kann die Verfügbarkeit derselben erhöht werden. Das Modell durch Anwendung einer konstanten Startausfallrate fährt zum optimalen Resultat möglichst viele Starttests durchzuführen => λ_{start}=constant, ist eine irreführende Modellannahme. Wurde diese Tatsache bei den Untersuchungen berücksichtigt?

Antwort: Zu Ihrer Frage bezüglich der Häufigkeit von Prüfungen stimme ich Ihnen zu, daß die Verfügbarkeit einer stand by-Komponente aufgrund von Verschleiß nicht beliebig gesteigert werden kann. Die Prüfhäufigkeit einer Komponente wird daher in erster Linie nach qualitativ ingenieurmäßigen Gesichtspunkten bestimmt. Aus unseren Betriebserfahrungen ergibt sich andererseits jedoch eindeutig, daß bei Verkürzung längerer Prüffristen die Verfügbarkeit einer Stand-by-Komponente gesteigert werden kann. Ein Vergleich von wöchentlich und monatlich geprüften Notstromdieselaggregaten ergibt eine um den Faktor 4 günstigere Start-Ausfallwahrscheinlichkeit der wöchentlich getesteten Diesel.

Frage: Sie haben für den Störfall "Kleines Leck einer Hauptkühlmittelleitung" die Nichtverfügbarkeit der Sicherheitssysteme mit bis 10^{-2} angegeben. Dieser Wert ist für 4-strängige Systeme überrraschend hoch. Können Sie etwas zur Begründung dieses Ergebnisses sagen?

Antwort: Der verhältnismäßig hohe Unverfügbarkeitswert des Sicherheitssystems zur Beherrschung kleiner Lecks ergibt sich vorrangig aus dem Beitrag des Notspeisesystems, das zur schnellen Druckabsenkung der Primärseite in 2 von 4 Schaltung erforderlich ist. Andererseits haben die in diesem System vorhandenen Regelarmaturen zur Dampferzeugerhöhenstandsregelung ein hohes Gewicht. In meinem Vortragsmanuskript habe ich ferner ausgeführt, daß diese Ergebnisse für die DWR-Standardanlage vergleichbar sind, mit denen der Referenzanlage der deutschen Risikostudie. Durch die höhere Redundanz der Notstromversorgung in der Standardanlage (Notnetz 1 und 2, entsprechend 8 Dieseln), wobei

das Notnezt 1 zusätzlich die betrieblichen An- und Abfahrpumpen versorgen, erwarten wir für die genannten Störfälle auch günstigere Ergebnisse. Dieser Anteil wurde von uns jedoch nicht analysiert.

Frage: Eine weitere Frage betrifft die benutzten Daten. Die genannten Daten, z.B. $1{,}5 \cdot 10^{-5}$/h für eine Pumpe, gelten doch nur für eine bestimmte Betriebsweise. Benutzen Sie in Ihren Analysen für gleichartige Komponenten unterschiedliche Ausfallraten, z.B. für Dauerbetrieb andere als für sporadischen Betrieb und würden Ihre Berechnungen für sehr häufige Funktionstests in stand-by-Systemen ungünstigere Ergebnisse liefern, weil wegen der höheren Testbeanspruchung auch höhere Ausfallraten angesetzt werden?

Antwort: Ihre weitere Frage nach den Pumpendaten betrifft folgendes: Der angegebenen Wert gilt für Notkühlpumpen im stand-by-Betrieb. Pumpen im Dauerbetrieb liefern geringfügig höhere Ausfallraten (Faktor 2 bis 4). Diese Unterschiede werden dann auch in der Analyse berücksichtigt.

Auf die Frage nach der Verkürzung der Prüffristen war ich schon eingegangen. Wir würden jedoch einer verkürzten Prüffrist, die eindeutig zur Erhöhung des Verschleißes führt, nicht zustimmen. Die Modifizierung der Ausfallrate erübrigt sich daher.

Frage: Gibt es signifikante Unterschiede zwischen den Ergebnissen der vom TÜV durchgeführten Zuverlässigkeitsanalysen und denen der vom Hersteller eingereichten Analysen?

Antwort: Die Analysen wurden vom Hersteller als auch von uns ausgeführt. Es ergaben sich keine signifikanten Unterschiede.

Das bedeutet jedoch nicht, daß bei einer längerfristigen Bearbeitung Unterschiede auftauchen, die dann jeweils detailliert und sachbezogen ausdiskutiert werden.

Frage: Nach den Ausführungen der Herren Vetterkind und Balfanz habe ich den Eindruck, daß von Versagensarten bzw. -ursachen gesprochen wurde, die grundsätzlich vorauszusehen waren, - und daß sonst nichts

vorkommt. In der Luft- und Raumfahrt sieht es schlechter aus: Es passieren immer wieder Dinge, die grundsätzlich nicht in Rechnung gestellt wurden, weil man daran überhaupt nicht dachte.

Antwort: Das Sicherheitskonzept für ein Kernkraftwerk sieht vor, daß alle in einer Anlage denkbaren Störfälle Berücksichtigung finden. Dieses geschieht durch die Festlegung und Analyse repräsentativer Störfälle. Ebenfalls werden Ausfälle und deren Wirkungen der Komponenten des Sicherheitssystems untersucht und bewertet. Hierfür bedient man sich der Methoden der Zuverlässigkeitsanalysen. Die Frage der Vollständigkeit der möglichen Störfallereignisse und Abläufe wird darüber hinaus durch den vorliegenden Erfahrungsstand aus dem zurückliegenden Betrieb von Kernkraftwerken und durch eine Vielzahl von Versuchen (Experimenten) überprüft. Dennoch ist die Vollständigkeit einer Analyse nicht beweisbar. Die Grenze liegt in der Unmöglichkeit unbekannter Schadensmechanismen vorherzusagen.

An dieser Stelle möchte ich noch einmal auf die Zielsetzung der hier vorgestellten Zuverlässigkeitsanalysen hinweisen, wonach vorrangig die Bewertung vergleichender Art ist. Bei einer Risikoaussage stellt sich die Frage nach der Vollständigkeit sehr viel stärker.

Frage: Inwieweit ist die Bewertungsmöglichkeit der Störfallkette "Kleines Leck und Versagen der Notkühlung" als übertragbar auf andere Störfallketten zu betrachten?

Antwort: Die dargestellten Zuverlässigkeitsanalysen und Ergebnisse für die betrachteten Systeme liefern in Verbindung mit der Eintrittswahrscheinlichkeit der zu beherrschenden Störfälle auslegungsbedingte Wahrscheinlichkeiten für nicht beherrschte Störfälle. Da nun die genannten Sicherheitssysteme die Kühlfähigkeit des Reaktorkerns unter den verschiedenen Störfallbedingungen erhalten sollen, haben die ermittelten Wahrscheinlichkeitsgrößen die gleiche sicherheitstechnische Relevanz.

Frage: Ist die zugrundezulegende zulässige Wahrscheinlichkeit nicht von der Akzeptanz des Risikos (gebildet als Produkt von Wahrscheinlichkeit

und Auswirkung) abhängig und ist dies nicht heute eher eine politische als eine wissenschaftliche Frage?

Antwort: Eine richtungsweisende Wahrscheinlichkeitsgröße (Orientierungsgröße) für - auslegungsbedingt - nicht beherrschte Störfälle leiten wir aus dem heute anerkannten Auslegungsstand der Sicherheitsmaßnahmen selbst ab und orientieren uns hier an repräsentativen Störfallabläufen.

Bei der ursprünglichen Festlegung der Sicherheitsmaßnahmen zur Beherrschung äußerer Einwirkungen wurde ebenfalls eine vergleichende Wahrscheinlichkeitsbetrachtung angestellt.

Das erzielte Wahrscheinlichkeitsniveau für die verschiedenen Störfallabläufe und das damit verbundene Risiko ergibt sich letztlich aus den vorliegenden Sicherheitskriterien, in denen deterministische Forderungen an die Systemauslegung und die Redundanz festgeschrieben sind.

Die gedankliche Basis für die Forderung nach einer extrem geringen Wahrscheinlichkeit für ein nicht mehr zu betrachtendes Störfallereignis liegt andererseits darin, daß aufgrund der Unwahrscheinlichkeit dieses Ereignisses ein vorhandenes "Restrisiko" nicht mehr beeinflußt wird.

Verfügbarkeits- und Kapazitätsplanung für Prozeßsysteme mit Zwischenlagern

F. Fischer, W. Haußmann

Kernforschungszentrum Karlsruhe GmbH
Institut für Datenverarbeitung in der Technik
Postfach 3640, D-7500 Karlsruhe
Bundesrepublik Deutschland

Vortrag gehalten im Seminar:
"Methoden der Systemplanung bei gefordertem Langzeitbetriebsverhalten" am 26./27. Februar 1980 im I D T,
Kernforschungszentrum Karlsruhe GmbH, Karlsruhe

Gliederung

1. Einführung

Verfügbarkeits- und Kapazitätsplanung für Prozeßsysteme mit/ohne Zwischenlagern, ist ein Aufgabenbereich, den die Abteilung "Mathematische Modelle" des IDT zu bearbeiten hat.

Wir arbeiten projektbezogen innerhalb des Großprojekts "Wiederaufarbeitung und Abfallbehandlung" (PWA). Ein wichtiger Kooperationspartner dabei ist die Firma DWK (Deutsche Gesellschaft für Wiederaufarbeitung von Kernbrennstoffen). Sie hat die Planung für eine Wiederaufarbeitungsanlage durchzuführen.

Herr Haußmann und ich arbeiten seit einem Jahr an der o.a. Problematik. Wir haben in zahlreichen Diskussionen mit unserem Industriepartner ein gutes gemeinsames Problemverständnis erarbeitet. Es setzte uns in die Lage, gezielt Literaturrecherchen durchzuführen und Lösungsmöglichkeiten zu suchen.

Der Vortrag soll eine Einführung in die Problematik sein und Verständnis für die Schwierigkeiten der Problemlösung wecken.

Wir betrachten Produktionssysteme, die aus einer Anzahl miteinander zusammenhängender Prozeßteile (Verfahrenseinheiten, Maschinen) bestehen. Das zu produzierende Material durchläuft (durchfließt) nacheinander sämtliche Prozeßteile in der gleichen Abfolge. (Bild 1)

Gewöhnlich arbeitet ein Prozeßteil mit einer gewissen Produktionsrate (Durchsatz), d.h. er produziert eine bestimmte Anzahl Mengeneinheiten pro Zeiteinheit. Dann fällt der Prozeßteil aus und die Produktion der Station ist unterbrochen, bis die Reparatur erfolgreich durchgeführt ist.

Die feste Verkettung durch serielle Anordnung von Prozeßteilen hat zur Folge, daß das gesamte Produktionssystem stillsteht, sobald auch nur eine Maschine ausfällt.

Damit trotzdem das Produktionsziel erreicht wird, sind u.a. folgende Maßnahmen denkbar:

- Erhöhung der Zuverlässigkeit der Maschinen
- Redundante Auslegung von Maschinenteilen
- Errichtung von Pufferlagern.

Bei Linien-Produktionssystemen mit sehr großen Prozeßteilen sind einer redundanten technischen Auslegung sehr schnell ökonomische Grenzen gesetzt. Erhöhung der technischen Zuverlässigkeit der Maschinen und insbesondere die Einplanung von Zwischenlagern erscheinen dann vorteilhaft. (Bild 2)

Ein geeignetes Maß, um die Effektivität solcher Produktionssysteme zu charakterisieren, stellt die Verfügbarkeit des Systems dar.

Für Linien-Prozeßsysteme mit Zwischenlagern endlicher Lagerkapazität können Methoden der stochastischen Prozesse zur Untersuchung herangezogen werden.

Markov-Ansätze, die das Verhalten eines Zwei-Maschinen-Liniensystems analytisch behandeln und die Systemverfügbarkeit in Abhängigkeit von Maschinenparametern und der Lagergröße errechnen, existieren.

Die Darstellung eines solchen Modells bildet den Hauptgegenstand dieses Vortrages.

Größere Liniensysteme und Systeme mit verzweigten Strukturen sind mit der Markov-Methodik zwar lösbar, jedoch nicht mehr praktikabel. Der zu betrachtende Zustandsraum wird zu groß, der Formalismus unhandlich, schließlich bringt die Umsetzung der Gleichungssysteme in Computer-Algorithmen eine Anzahl numerischer Probleme.

Für größere Systeme mit Zwischenlagern sind dann analytische approximative Methoden zu suchen oder aber Simulationsmodelle aufzustellen.

2. Systemverfügbarkeit eines Liniensystems ohne Zwischenlager

Annahmen:

- Die Reparaturdauer- bzw. Lebensdauerverteilungen haben endliche Erwartungswerte.
- Die Reparaturdauer ist unabhängig von der Betriebsdauer der Einheit.
- Zwei oder mehr Komponenten können nicht zugleich ausfallen.
  - ist eine Maschine ausgefallen, so kann keine weitere ausfallen, d.h. Maschinen im Wartezustand fallen nicht aus.

Dann gilt nach Barlow/Proschan:

$$V_{system} = \frac{1}{1+\sum_{i=1}^{n} \frac{1-V_i}{V_i}} = \frac{1}{(1-n+\sum \frac{1}{V_i})}$$

$$= \left[1+\sum_{i=1}^{n} \frac{MDT_i}{MUT_i}\right]^{-1} = \left[1+\sum_{i=1}^{n} \frac{\lambda_i}{\mu_i}\right]^{-1} ,$$

oder symmetrisch geschrieben lautet die Beziehung:

$$\frac{1}{V_{sys}} - 1 = \sum_{i=1}^{n} \left(\frac{1}{V_i} - 1\right) .$$

Bemerkung:

i.A. $$V_{sys} \neq \prod_{i=1}^{n} V_i \quad .$$

Das Produkt der V_i macht eine Aussage über die Wahrscheinlichkeit, daß im n-Reihensystem n Einheiten gleichzeitig intakt sind. Es wird angenommen, die einzelnen Maschinen arbeiten total unabhängig voneinander, d.h. funktionstüchtige Komponenten arbeiten weiter während der Reparatur einer ausgefallenen Einheit.

Man kann zeigen

$$V_{sys} = \frac{1}{(1-n+\sum_{i=1}^{n} \frac{1}{V_i})} \geq \prod_{i=1}^{n} V_i$$

Gleichheit gilt für $n=1$ oder $V_i=1$ für alle i .

Beispiel:

$$n=3 \qquad \text{für} \quad i=1,2,3 \qquad V_i=0.5$$

$$V_{sys} = 0.25$$

$$\text{aber} \quad \prod_{i=1}^{3} V_i = 0.125 \quad .$$

D.h.: Die multiplikative Verknüpfung von Verfügbarkeiten eines Reihensystems unterschätzt die Systemverfügbarkeit!

3. Linien-Prozeßsysteme mit Zwischenlagern

Vorgehensschritte zur Erarbeitung eines Modells für Linien-Prozeßsysteme mit Zwischenlagern

Annahmen

- Systemverhalten
- Zustandsraum
- Verteilungen von Systemparametern

Ziel:

Angabe der Wahrscheinlichkeit, daß das System im stationären Zustand produktionsfähig ist.

Weg:

Erarbeitung eines stochastischen mathematischen Modells, das die o.a. stationäre Wahrscheinlichkeit liefert.

3.1 Modellbeschreibung für Linien-Prozeßsysteme mit mehreren Zwischenlagern

- Alle Maschinen sind synchronisiert, d.h. alle arbeitsbereiten Maschinen starten zum gleichen Zeitpunkt.

- Alle Maschinen haben den gleichen konstanten Durchsatz, D, (Mengeneinheit/Zeiteinheit).
  Die Zeitskala wird so normiert, daß D=1.

- Der Transport der Werkstoffe nimmt keine Zeit in Anspruch.

- Maschinen fallen zufällig aus.
  Ausfallzeit- und Störabstandsdauern sind zufällige Größen.

- Fällt eine Maschine aus, so wächst der Bestand des vorgelagerten Puffers.

  Bei hinreichend langer Ausfalldauer ist der Puffer voll. Die vorgelagerte Maschine muß gestoppt werden.

  Entsprechend fällt der Lagerbestand des nachgelagerten Puffers. Läuft bei langer Ausfalldauer der Maschine das Lager leer, so muß die nachgelagerte Maschine gestoppt werden. usw.

- Zwischenlager tragen dazu bei, die Auswirkungen von Maschinenausfällen auf die Produktion zu verringern (Entkopplungseffekt).

Bemerkung:

Die Annahme zeitkonstanter Produktionsdurchsätze ist dann gerechtfertigt, wenn die gemessenen regulären Produktionszeiten nur wenig um einen Mittelwert schwanken, d.h. die Varianzen der Produktionszeiten sind klein.

(Es läßt sich zeigen, daß im Gleichgewichtszustand häufig die Lager nahe an der unteren bzw. oberen Kapazitätsgrenze sind. Größere Schwankungen der Produktionszeiten würden schnell zu Lagerleer- bzw. -überlaufen führen.)

Wie lassen sich die Zustände des Prozeßsystems beschreiben?

Wichtige Bestimmungsgrößen sind

- die Maschinenzustände
- die Lagerzustände.

Für ein m-Maschinen-Linien-Prozeßsystem definieren wir den

Zustandsraum des Prozeßsystems.

Er ist die Menge aller (2m-1)-tupel s:

$$S := \{s/s = (n_1,\ldots,n_{m-1};\ \alpha_1,\ldots\alpha_m)\}$$

Lagerfüllung des Puffers ZL_i:

$$0 \leq n_i \leq N_i$$

Zustand der Maschine M_i:

$\alpha_i = 1$, wenn M_i technisch intakt

$\alpha_i = 0$, wenn M_i technisch defekt

Es kann α_i=1 sein und trotzdem arbeitet die Maschine M_i nicht (wegen Lagerleer- bzw. überlauf des vor- bzw. nachgelagerten Puffers)!

Nehmen wir einen diskreten Fertigungsfluß an (z.B. Maschinenteile, Automobile o.ä.), d.h. die n_i sind natürliche Zahlen, so ist die

Anzahl der Zustände $s \in S$ des Systems

$$2^m \prod_{i=1}^{m-1} (N_i+1)$$

Beispiel:

3 Maschinen, 2 Lager mit der Kapazität von je 10 Mengeneinheiten.

Anzahl Systemzustände = $2^3 11^2 = 968$.

Es ist ersichtlich, daß mit größer werdenden Prozeßsystemen die Anzahl der Systemzustände sehr schnell wächst.

Unser Ziel ist es nun, die Wahrscheinlichkeiten für die Übergänge der Zustände $s \in S$ zu finden, um daraus dann Schlüsse auf die Verfügbarkeit, d.h. die Wahrscheinlichkeit der Produktionsbereitschaft, des Systems zu ziehen.

3.2 Ein-Lager-Modell

Um die Lösungsproblematik einzuführen, beschränken wir uns auf die Beschreibung der analytischen Lösung des Ein-Lager-Modells (nach J.A. Buzacott).

Modellannahmen

- Es wird diskret gefertigt.

- Das System wird zu diskreten Zeitpunkten betrachtet.

  Beobachtungszeitpunkt ist der Endpunkt des Produktionszyklus um ein Werkstück zu fertigen.

  Ist α_2=1 (bzw. 0) zum Beobachtungszeitpunkt t, so produziert mit Wahrscheinlichkeit 1 das System bis zum Zeitpunkt t+1 eine (bzw. keine) Mengeneinheit.

- Es sind unbegrenzte Eingangs- bzw. Endlager vorhanden, d.h. die erste bzw. letzte Maschine wird niemals gestoppt, obwohl sie intakt ist.

- Die Maschinen sind synchronisiert und haben den Durchsatz D=1 Mengeneinheit/Zeiteinheit.

- Die Maschinen haben geometrisch verteilte Störabstandsdauern mit Parameter p_i (i=1,2), d.h. die Wahrscheinlichkeit des Aus-

falls der Maschine M_i (i=1,2) ist konstant gleich p_i.

Es gilt $MTBF_i = 1/p_i$ (i=1,2).

- Die Maschinen haben geometrisch verteilte Reparaturdauern mit Parameter r_i (i=1,2), d.h. die Wahrscheinlichkeit der Reparatur der Maschine (i=1,2) ist konstant gleich r_i (i=1,2).

  Es gilt: $MTTR = 1/r_i$ (i=1,2).

Maschinen-Übergangswahrscheinlichkeiten

$\alpha_i(t)$	$\alpha_i(t+1)$	$P(\alpha_i(t+1) \mid \alpha_i(t))$
1	1	$1 - p_i$
1	0	p_i
0	1	r_i
0	0	$1 - r_i$

- Maschinen können nur ausfallen, wenn sie gerade Werkstücke bearbeiten. Blockierte Maschinen können nicht ausfallen (z.B. bei n=0 bzw. n=N).

- Teilweise fertiggestellte Werkstücke werden nicht in den Prozeß weitergegeben, sondern in den vorgelagerten Puffer zurückgegeben.

  (m.a.W. der Lagerbestand ändert sich nicht!)

und schließlich

- das stochastische Modell des Systems wird im stationären Zustand untersucht.

  Alle Einschwingvorgänge sind abgeschlossen, d.h. das System kann durch eine stationäre Wahrscheinlichkeitsverteilung charakterisiert werden.

Bemerkungen:

- Die Annahme geometrisch verteilter Störabstands- und Reparaturdauern ist durch die Praxis gerechtfertigt (vgl. Dissertation von E. Groß-Hardt, TH Aachen (1966)).

  Für hinreichend kleine p, r kann man diese Verteilungen durch die stetige Exponentialverteilung mit Mittelwert 1/p bzw. 1/r approximieren.

- Die Annahme diskreter Verteilungen und diskreter Lagerzustände bedeutet keine wesentliche Einschränkungen.

  Gershwin hat gezeigt, daß die Schwankungsbreite der Ergebnisse diskreter/stetiger Modellannahmen bei rund $\pm$ 2% liegt.

Lösungsweg mit Markov-Ansatz

Aufgrund der getroffenen Annahmen können wir nun schrittweise die Lösung erarbeiten.

Unser Ziel ist dabei, die Verfügbarkeit des Systems, d.h. die Summe der Wahrscheinlichkeiten der Produktionszustände des Prozeßsystems zu finden.

1. Schritt: (Bild 3)

Erstellen eines Markov-Graphen, der die Übergänge der Systemzustände darstellt und die zugehörigen Übergangswahrscheinlichkeiten angibt (N=4). Mit N=4 haben wir dann $2^2(4+1) = 20$ Zustände.

2. Schritt: (z.B. N=4) (Bild 4) (bzw. Bild 5)

Indizierung der Systemzustände s

$s \equiv (n;1,1) \triangleq$ Zeile 1 bis 5

$s \equiv (n;0,1) \triangleq$ Zeile 6 bis 10

$s \equiv (n;1,0) \triangleq$ Zeile 11 bis 15

$s \equiv (n;0,0) \triangleq$ Zeile 16 bis 20

entsprechend $n=0,1,\ldots,4$

Anfertigen einer (20,20)-Matrix A der Übergangswahrscheinlichkeiten p_{ij} von i nach j (i,j=1,...,20).

3. Schritt: (Bild 6)

Aufstellen der Gleichgewichtsgleichungen ("Summe der abgehenden Ströme = Summe der ankommenden Ströme") für jeden Zustand $s \in S$

oder äquivalent dazu: (Bild 7)

Aufstellen des linearen Gleichungssystems zur Lösung der stationären Wahrscheinlichkeiten $P_i \equiv P(s=i)$

$$P' := (P_1,\ldots,P_{20})$$

$$P' = P'\cdot A$$

$$\sum_{i=1}^{20} P_i = 1 \quad .$$

4. Schritt:

Lösung des o.a. Gleichungssystems.

Es ergibt sich als Lösung unserer Aufgabe die Systemverfügbarkeit, V_{sys}^N, für das Seriensystem mit einem Zwischenlager:

$$V_{sys}^N = \sum_{n=0}^{N} P(n;1,1) + \sum_{n=1}^{N} P(n;0,1) \quad .$$

Mit

$$s := \frac{p_2}{r_2}\cdot\frac{r_1}{p_1} = \frac{1-V_2}{V_2}\cdot\frac{V_1}{1-V_1} = \frac{s_2}{s_1}$$

$$s_1 := \frac{p_1}{r_1} \qquad s_2 := \frac{p_2}{r_2} \qquad r := \frac{r_2}{r_1}$$

$$C = \frac{(p_1+p_2)(r_1+r_2) - p_1r_2(p_1+p_2+r_1+r_2)}{(p_1+p_2)(r_1+r_2) - p_2r_1(p_1+p_2+r_1+r_2)}$$

gilt für $s \neq 1$:

$$V_{sys}^{N} = \frac{1 - sC^{N}}{(1+s_1) - (1+s_2)sC^{N}}$$

und für $s=1$

$$s_1 = s_2 = s \quad , \qquad r = \frac{p_2}{p_1} = \frac{r_2}{r_1} \qquad \text{und}$$

$$V_{sys}^{N} = \frac{1 + r - r_2(1+s) + N \cdot r_2(1+s)}{(1+2s)(1 + r - r_2(1+s)) + N \cdot r_2(1+s)^2} \quad .$$

Gilt $r=1$, (d.h. $V_1 = V_2$ mit identischen Parametern) so folgt:

$$V_{sys}^{N} = V^{O} \cdot \frac{2 - r_2/V_2 + Nr_2/V_2}{2 - r_2/V_2 + (Nr_2/V_2^2) \cdot V^{O}} \quad .$$

Folgerungen:

1a) Existiert kein Zwischenlager, d.h. $N=0$, so ist

$$V_{sys}^{O} = \left[1 + \frac{p_1}{r_1} + \frac{p_2}{r_2}\right]^{-1}$$

$$= \left[\sum_{i=1}^{2} \frac{1}{V_i} - 1\right]^{-1} \quad .$$

1b) Ist der Puffer unendlich groß, d.h. N=∞, so gilt für

- $V_1 < V_2$ (d.h. C < 1, wegen $p_2/r_2 < p_1/r_1$)

$$V_{sys}^{\infty} = \left[1 + \frac{p_1}{r_1}\right]^{-1} = V_1$$

- $V_2 < V_1$ (d.h. C > 1, wegen $p_2/r_2 > p_1/r_1$)

$$V_{sys}^{\infty} = \left[1 + \frac{p_2}{r_2}\right]^{-1} = V_2 \quad .$$

D.h. bei unendlich großem Zwischenlager ist die Systemverfügbarkeit gleich der Verfügbarkeit der schwächsten Maschine.

2) Lagerkapazitätsänderungen oder Verbesserung der Maschinenverfügbarkeiten sind zwei Wege um die gewünschte Systemverfügbarkeit zu erhalten.

Beispiel: (Bild 8, Bild 8a) (Bild 9)

$V_{sys} = 0.4$ und $V_1 = 0.5$ vorgegeben.

Die Systemverfügbarkeit erreichen wir durch:

$V_2 = 0.67$ bei $N = 0$

$V_2 = 0.60$ bei $N = 4$

$V_2 = 0.5$ bei $N = 10$.

Wird $V_{sys} = 0.4$ und $V_1 = V_2$ vorgegeben:

$V_2 = 0.57$ bei $N = 0$

$V_2 = 0.425$ bei $N = 4$

$V_2 = 0.41$ bei $N = 10$

(Bild 10)

D.h. 'homogene, ausbalancierte' Systeme ($V_1=V_2$) brauchen bei vorgegebenen Lagerkapazitäten die niedrigsten Einzelverfügbarkeiten.

Anders ausgedrückt:

Die Lagerkapazitätserhöhung ist am wirksamsten bei ausbalancierten Systemen.

Ausbalancierte Systeme liefern bei fester Lagerkapazität die höchste Systemverfügbarkeit. (Bild 11)

Im Allgemeinen wird es leichter sein eine Kapazitätserweiterung vorzunehmen als die technische Verfügbarkeit von einzelnen Maschinen zu erhöhen.

3) Bei ausbalancierten Systemen ($V_1=V_2$) gibt es eine lineare Abhängigkeit zwischen Lagerkapazität und mittlerer Reparaturzeit, wenn V^N_{sys} vorgegeben ist.

Im N=f(V,MTTR)-Schaubild läßt sich dann ablesen, wie die Auswirkung der Reparaturzeitveränderungen auf die Zwischenlagerkapazität sind. (Bild 12)

4) Die Differenz $V^{\infty}_{sys} - V^{O}_{sys}$ gibt den maximal möglichen Zuwachs wieder, der durch die Einführung von einem Zwischenlager möglich ist.

Der relative Gewinn

$$G = \frac{V^{N}_{sys} - V^{O}_{sys}}{V^{\infty}_{sys} - V^{O}_{sys}}$$

(Bild 13) (Bild 14)

gibt an, welcher Bruchteil dieses Zuwachses an Systemverfügbarkeit bei vorgegebener Lagerkapazität erreicht wurde.

4. Simulation (Programm APSIS)

Es ist möglich verzweigte Strukturen (ohne Rückführungen) mit Zwischenlagern zu simulieren.

Flexibilität in Bezug auf:

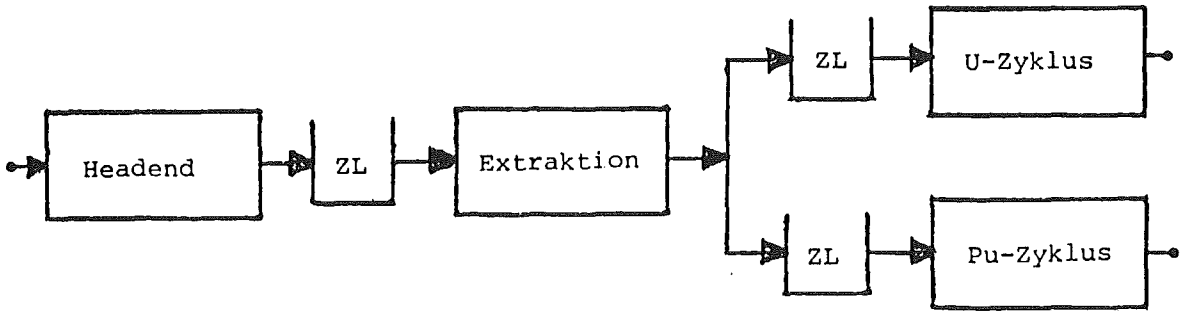
- Prozeßstruktur
- Lageranordnung und -größe
- Durchsatz (auch unbalancierte Systeme möglich)
- Störabstandsverteilungen
- Reparaturverteilungen.

Bei Angabe der Maschinenparameter (Ausfallrate, Reparaturrate), Lagergröße und Durchsatz lassen sich durch Simulation die Größen bestimmen:

- stationäre Systemverfügbarkeit
- Durchsatz des Systems
- mittlere Lagerbestände
- Anzahl der Lagerleer- und -überläufe
- Zeit bis zum ersten Lagerleer- und -überlauf.

Interaktives Eingreifen in dem Simulationsprozeß mit Hilfe eines speziellen Graphiksystems ist in Kürze möglich.

Es ermöglicht eine schnelle Veränderung der Systemparameter und ein Beobachten des Lagerverhaltens.



Simulationsbeispiel

Alle Verfahrenseinheiten der abgebildeten Prozeßstruktur haben die gleiche Verfügbarkeit V_{ein} und den gleichen Durchsatz D, die Lagerkapazität sei gleich dem n-fachen des Produktes aus mittlerer Reparaturzeit MTTR und Durchsatz, die Betriebs- und Reparaturdauern seien jeweils exponentialverteilt. Es zeigt sich, daß bei diesen Annahmen V_{sys} unabhängig vom Produkt MTTR·D ist. Für $n=\infty$ gilt $V_{sys}=V_{ein}$. Für n=O entspricht die vorgegebene Prozeßstruktur einem Seriensystem mit 4 Komponenten, dessen Systemverfügbarkeit analytisch bestimmt werden kann. Die Simulationsergebnisse für $2<n<\infty$ sind im folgenden Bild dargestellt.

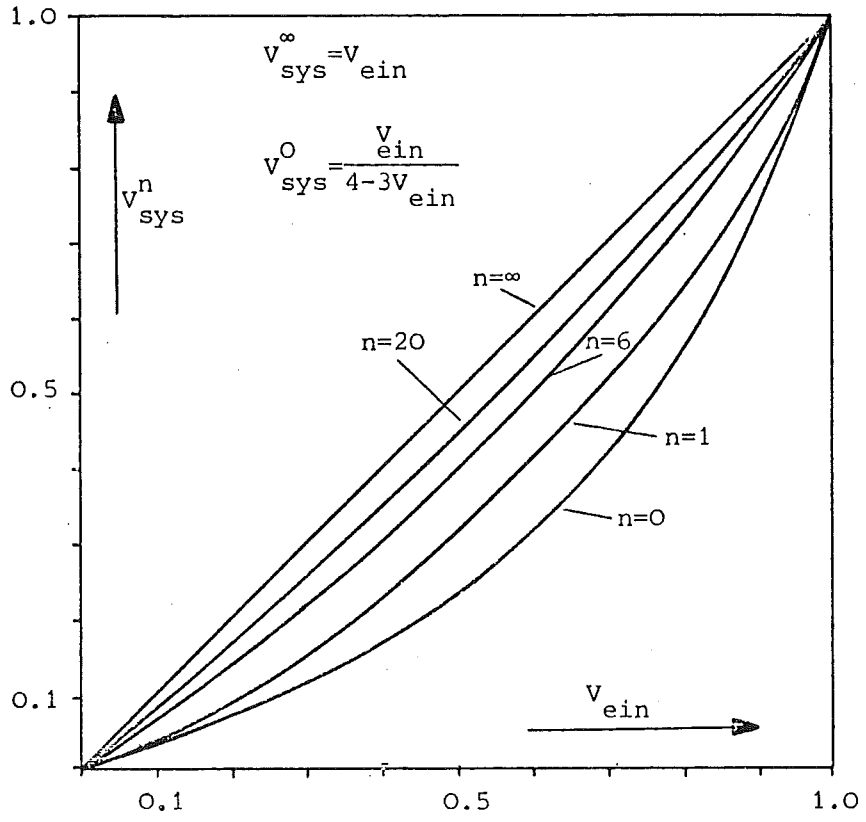


Abb.: Gesamtverfügbarkeit V^{n}_{sys} einer Prozeßstruktur mit Zwischenlagern als Funktion der Einzelverfügbarkeiten V_{ein} und der Lagerkapazität

A N H A N G

Definitionen, Sätze

T := Zeitdauer — Zufällige Größe
(z.B. Lebensdauer, Reparaturzeit)

$F(t) := P(T \leq t)$ — Wahrscheinlichkeitsverteilung der zufälligen Größe T .

Sie beschreibt die Wahrscheinlichkeit P, daß die Größe T kleiner oder gleich einem vorgegebenen Wert t ist.

Existiert die Ableitung dF(t)/dt so heißt

$$f(t) := \frac{dF(t)}{dt}$$ — Verteilungsdichte

$R(t) := 1 - F(t) = P(T>t)$ — Zuverlässigkeitsfunktion

Parameter bei reparierbaren Einheiten:

MUT ≡ MTBF (mean up time, mean time between failures)

Störabstand = mittlere Zeit zwischen zwei Ausfällen

Die MUT ist also der Erwartungswert derjenigen Zeitspanne, die mit dem Wiedereinsatz nach einer Reparatur beginnt und mit dem nächsten Ausfall endet.

MDT ≡ MTTR (mean down time; mean time to repair)

mittlere Reparaturdauer

Die MDT ist der Erwartungswert der Zeitspanne, die mit dem Ausfall beginnt und dem nächsten Wiedereinsatz nach der Reparatur endet.

Bemerkung:

Ist T eine zufällige Lebensdauer, so gilt im allgemeinen MUT ≠ mittlere Lebensdauer.

Für exponentialverteiltes T gilt jedoch MUT = E(T).

Ausfallrate bzw. Reparaturrate

$$\lambda := \frac{1}{MUT} \qquad \text{Ausfallrate}$$

$$\mu := \frac{1}{MDT} \qquad \text{Reparaturrate}$$

Charakterisierung bei stetigen Verteilungen durch f(t), F(t)

$$\lambda(t)dt = P(t \leq T \leq t+dt \mid T > t)$$

$$= \frac{f(t)}{1 - F(t)}$$

Verfügbarkeit einer reparierten Einheit E

$$V_E := \frac{MUT}{MUT+MDT} = \frac{\mu}{\lambda+\mu}$$

(Dabei wird angenommen, daß sich die Maschine im eingeschwungenen (stationären) Zustand befindet und die Ausfall- bzw. Reparaturraten konstant sind.)

Im Falle exponentiell verteilter Lebens- bzw. Reparaturdauern erhalten wir für die zeitabhängige Verfügbarkeit

$$V_E(t) = \frac{\mu}{\lambda+\mu} + (\alpha - \frac{\mu}{\lambda+\mu}) e^{-(\lambda+\mu)t}$$

α = Wahrscheinlichkeit des Ausfalls zur Zeit t=O

Ergebnisse über Markov-Ketten

Es sei die Zeit t diskret (=0,1,2,...).

Es sei die Zustandsmenge S diskret und endlich (z.B. s=1,2,...,M).

Die Zustände s(t) sind zufällig mit der Eigenschaft:

$$W(s(t+1)=j \mid s(t)=i,\ s(t-1)=i_1,\ldots,s(0)=i_t)$$

$$= W(s(t+1)=j \mid s(t)=i)$$

$$=: w_{ij}(t,t+1)$$

$w_{ij}(t,t+1)$ nennt man <u>Übergangswahrscheinlichkeit</u> vom Zustand i nach j in der Zeit von t bis t+1.

Eine Markov-Kette s(t) (t=0,1,2,...) heißt <u>homogen</u>, wenn die Übergangswahrscheinlichkeiten nicht von t abhängen, d.h.

$$w_{ij}(t,t+1) = w_{ij} \ .$$

Es gilt sicher

$$\sum_{j=1}^{M} w_{ij} = 1 \qquad \text{für alle} \quad i=1,\ldots,M \ .$$

Von einem Zustand i geht das System sicher während (t,t+1) in einen der Zustände j über.

Nach dem Satz von der totalen Wahrscheinlichkeit gilt dann

$$W(s(t+1)=j) = \sum_i W(s(t)=i)\ W(s(t+1)=j \mid s(t)=i)$$

$$= \sum_i W(s(t)=i) w_{ij}$$

oder kurz mit $W_i(t) := P(s(t)=i)$ $B=(w_{ij})$

$$W_j(t+1) = \sum_i W_i(t) w_{ij} \qquad i,j = 1,\ldots,M$$

$$W'(t+1) = \underline{W}'(t)B \qquad \underline{W}' = (W_1,\ldots,W_M)$$

Rekursive Anwendung dieser letzten Beziehung liefert

$$W'(t) = \underline{W}'(O)B^t$$

Eine Markov-Kette heißt <u>ergodisch</u>, wenn gilt:

(a) $\lim_{t\to\infty} B^t = A \equiv (p_{ij})$

A (M,M)-Matrix

und

(b) $\underline{P}' := \underline{P}'(O)A$

der <u>stationäre Zustandsvektor des Systems</u> unabhängig ist von $\underline{P}'(O)$.

Aus

$$\underline{W}'(t+1) = \underline{W}'(t)B$$

wird bei $t\to\infty$ für eine ergodische Markov-Kette:

$$\underline{P}' = \underline{P}'\cdot A$$

oder $$P_j = \sum_i P_i\, p_{ij} \qquad \text{für alle } i,j=1,\ldots,M\ .$$

Satz:

Ist A die Übergangsmatrix einer unzerlegbaren endlichen Markov-Kette und ist die Kette aperiodisch, so ist der stationäre Zustandsvektor $\underline{P}$ eindeutig bestimmt durch das Gleichungssystem

$$\sum_j P_j = 1$$

$$\underline{P}' = \underline{P}'\cdot A\ .$$

Die Voraussetzungen des Satzes sind für unser Modell erfüllt:

- Jeder Zustand ist direkt oder indirekt von jedem anderen zu erreichen.
- Es gibt Diagonalelemente in A, d.h. p_{ii}, mit $p_{ii}>0$ $i\in\{1,\ldots,M\}$ (z.B. die Übergänge in sich selbst. Das ist hinreichend für Aperiodizität).

Literatur

Barlow, R.E.; Proschan, F.: Statistische Theorie der Zuverlässigkeit. Verlag Harry Deutsch, Frankfurt, 1978.

Buzacott, J.A.: Automatic transfer lines with buffer stocks. J. Prod. Res. 5 (1967) 183-200.

Berliner, A.: Programmbeschreibung APSIS. Institut für Datenverarbeitung in der Technik, Kernforschungszentrum Karlsruhe, September 1979.

Fischer, F.; Haußmann, W.: Unveröffentlichte Ergebnisse

Gershwin, S.B.; Schick, I.G.: Analytic methods for calculating performance measures of production lines with buffer storages. Proceed. 1978 IEEE Conference on Decision and Control, San Diego 10-12 Jan. 1979, pp. 618-24.

Groß-Hardt, E.: Über den Einfluß von Werkstückpuffern auf die Kapazitätsausnutzung von Maschinenfließreihen. Dissertation TH Aachen, 1966.

Bilder:

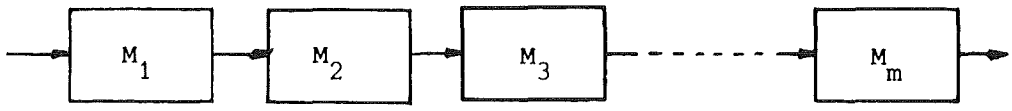
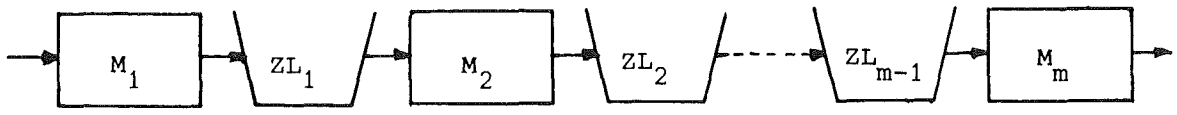


Bild 1: Linien-Prozeßsystem aus m Maschinen.



M_i : Maschine i i=1,...,m

ZL_j: Zwischenlager j j=1,...,m-1

Bild 2: Linien-Prozeßsystem aus m Maschinen und (m-1) Zwischenlagern.

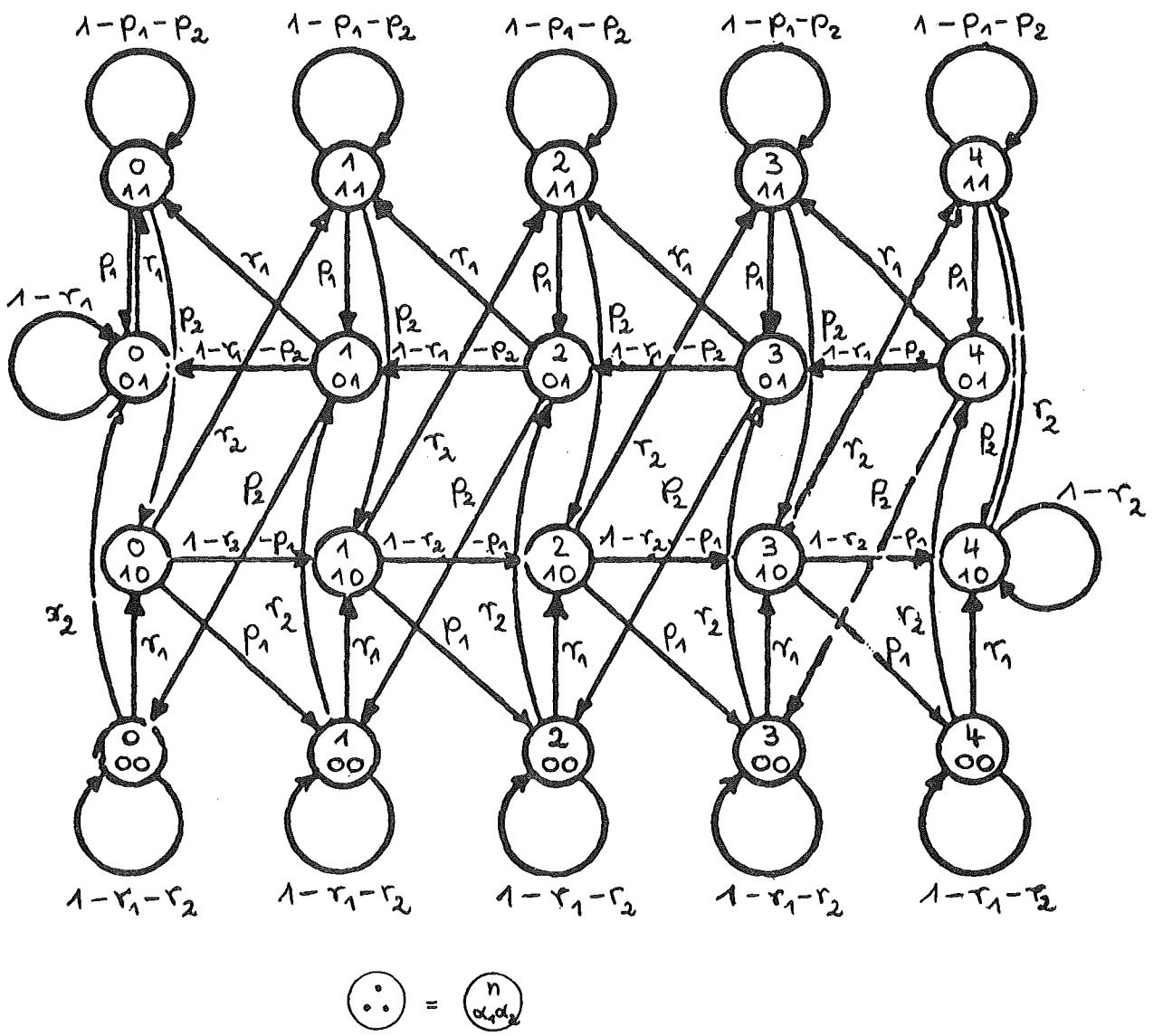


Bild 3: Markov-Graph der Übergangswahrscheinlichkeiten für das Ein-Lager-Modell (Buzacott) N=4

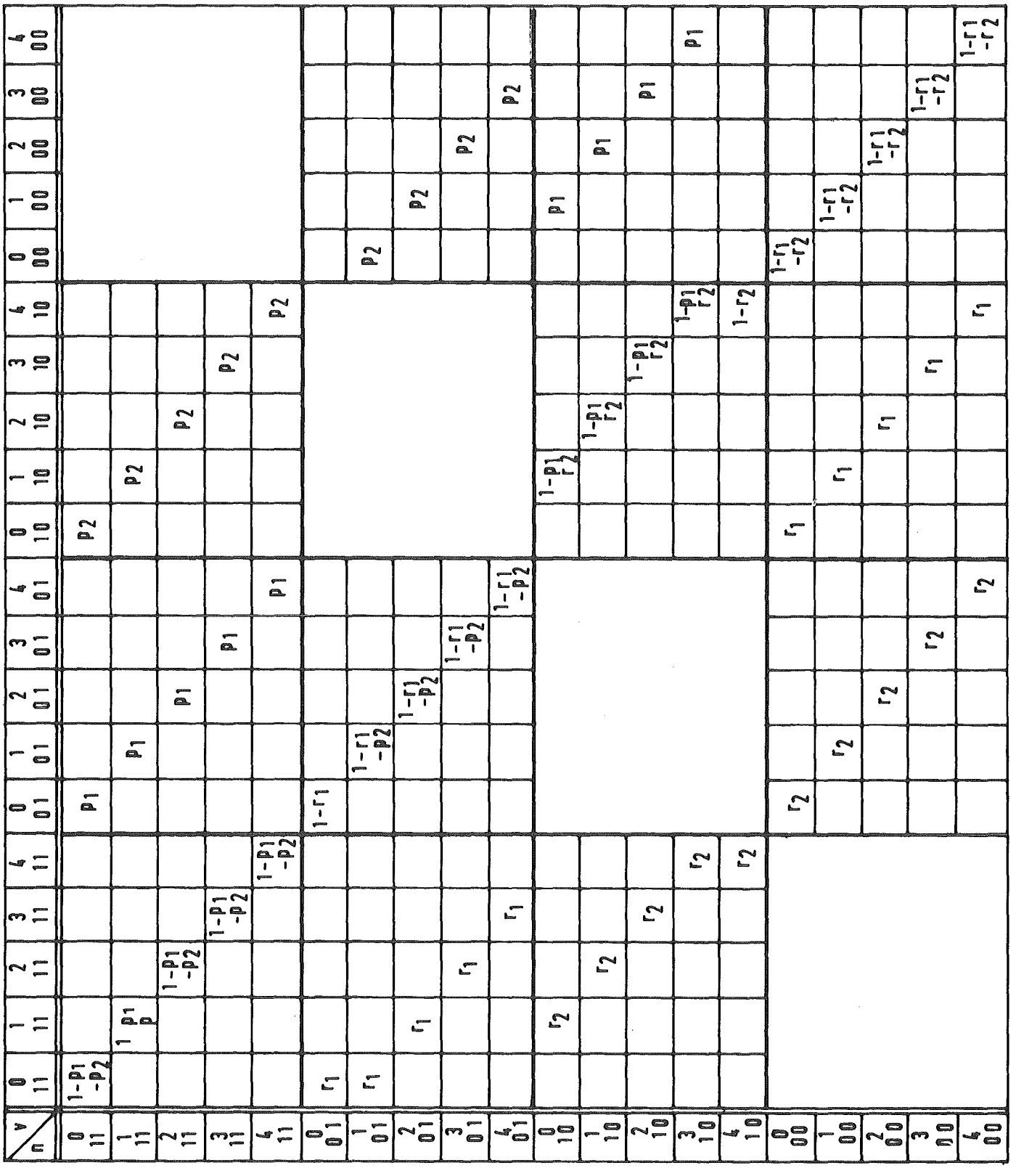


Bild 4: Matrix A der Übergangswahrscheinlichkeiten

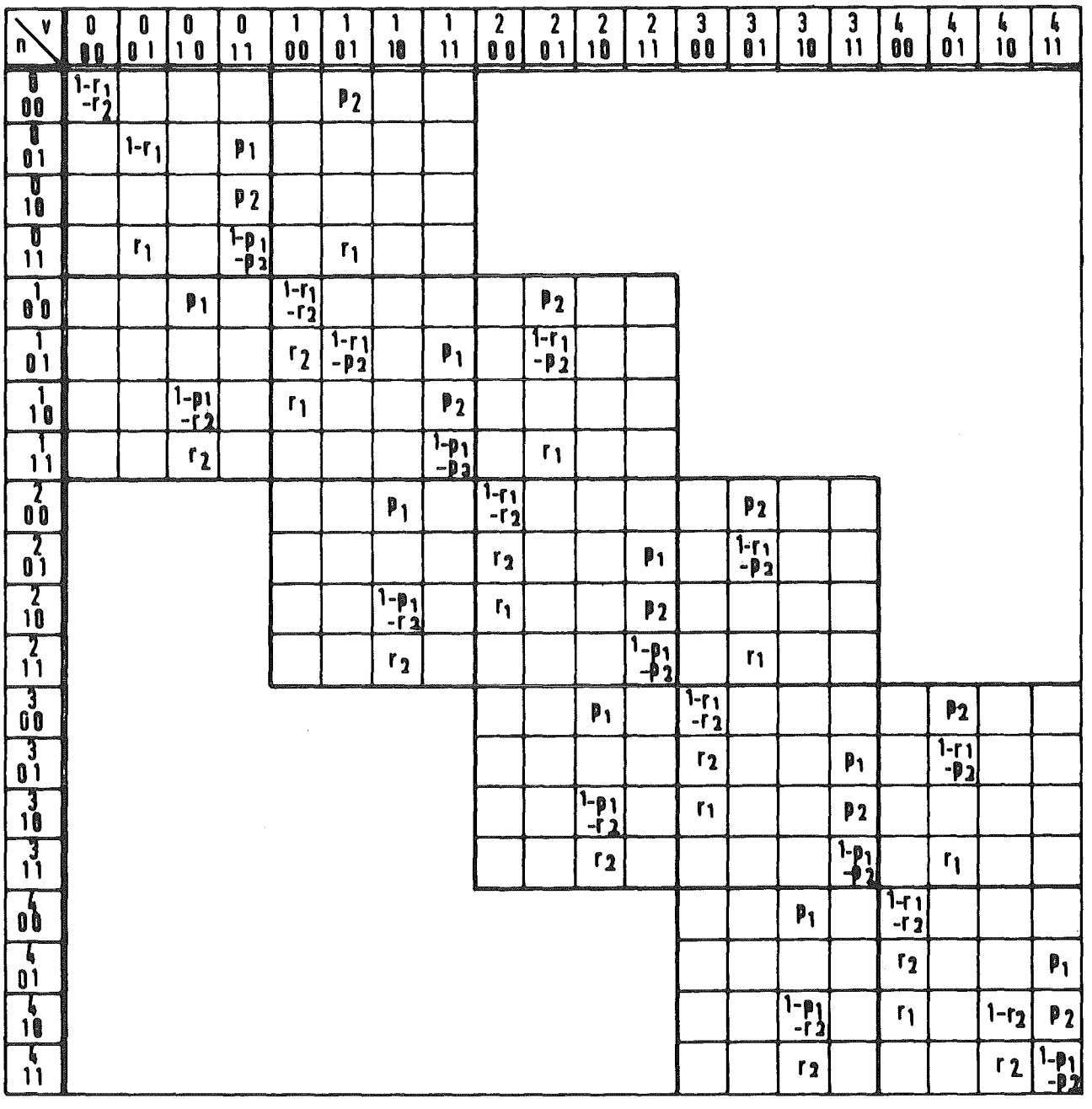


Bild 5: Block-triangulare Form der Übergangsmatrix des Markov-Graphen

$\alpha_1 = \alpha_2 = 1$:

$n=0$: $(p_1+p_2)\ P(0;1,1) = r_1\ P(0;0,1) + r_1\ P(1;0,1)$

$0<n<N$: $(p_1+p_2)\ P(n;1,1) = r_1\ P(n+1;0,1) + r_2\ P(n-1;1,0)$

$n=N$: $(p_1+p_2)\ P(N;1,1) = r_2\ P(N-1;1,0) + r_2\ P(N;1,0)$

$\alpha_1 = 0,\ \alpha_2 = 1$:

$n=0$: $r_1\ P(0;0,1) = p_1\ P(0;1,1) + (1-r_1-p_2)\ P(1;0,1) + r_2\ P(0;0,0)$

$0<n<N$: $P(n;0,1) = p_1\ P(n;1,1) + (1-r_1-p_2)\ P(n+1;0,1) + r_2\ P(n;0,0)$

$n=N$: $P(N;0,1) = p_1\ P(N;1,1) + r_2\ P(N;0,0)$

$\alpha_1 = 1,\ \alpha_2 = 0$:

$n=0$: $P(0;1,0) = p_2\ P(0;1,1) + r_1\ P(0;0,0)$

$0<n<N$: $P(n;1,0) = p_2\ P(n;1,1) + (1-p_1-r_2)\ P(n-1;1,0) + r_1\ P(n;0,0)$

$n=N$: $r_2\ P(N;1,0) = p_2\ P(N;1,1) + (1-p_1-r_2)\ P(N-1;1,0)$
$+ (1-r_2)\ P(N;1,0)$
$+ r_1\ P(N;0,0)$

$\alpha_1 = \alpha_2 = 0$:

$n=0$: $(r_1+r_2)\ P(0;0,0) = p_2\ P(1;0,1)$

$0<n<N$: $(r_1+r_2)\ P(n;0,0) = p_2\ P(n+1;0,1) + p_1\ P(n-1;1,0)$

$n=N$: $(r_1+r_2)\ P(N;0,0) = p_1\ P(n-1;1,0)$

Bild 6: Gleichgewichtsbeziehungen im stationären Zustand

	$P(0;1,1) = (1-p_1-p_2)\ P(0;1,1) + r_1\ P(0;0,1)$							
	$+ r_1\ P(1;0,1)$							
$0<n<N$	$P(n;1,1) = (1-p_1-p_2)\ P(n;1,1) + r_1\ P(n+1;0,1)$			$+ r_2\ P(n-1;1,0)$				
	$P(N;1,1) = (1-p_1-p_2)\ P(N;1,1)$			$+ r_2\ P(N-1;1,0)$				
				$+ r_2\ P(N;\ 1,0)$				
	$P(0;0,1) =$	$p_1\ P(0;1,1)$	$+ (1-r_1)\ P(0;\ 0,1)$				$+$	$r_2\ P(0;0,0)$
			$+ (1-r_1-p_2)\ P(1;\ 0,1)$					
$0<n<N$	$P(n;0,1) =$	$p_1\ P(n;1,1)$	$+ (1-r_1-p_2)\ P(n+1;0,1)$				$+$	$r_2\ P(n;0,0)$
	$P(N;0,1) =$	$p_1\ P(N;1,1)$					$+$	$r_2\ P(N;0,0)$
	$P(0;1,0) =$	$p_2\ P(0;1,1)$					$+$	$r_1\ P(0;0,0)$
$0<n<N$	$P(n;1,0) =$	$p_2\ P(n;1,1)$		$+ (1-p_1-r_2)\ P(n-1;1,0)$			$+$	$r_1\ P(n;0,0)$
	$P(N;1,0) =$	$p_2\ P(N;1,1)$		$+ (1-p_1-r_2)\ P(N-1;1,0)$			$+$	$r_1\ P(N;0,0)$
				$+ (1-r_2)\ P(N;\ 1,0)$				
	$P(0;0,0) =$		$p_2\ P(1;\ 0,1)$				$+ (1-r_1-r_2)$	$P(0;0,0)$
$0<n<N$	$P(n;0,0) =$		$p_2\ P(n+1;0,1)$	$+$	$p_1\ P(n-1;1,0)$	$+ (1-r_1-r_2)$		$P(n;0,0)$
	$P(N;0,0) =$				$p_1\ P(N-1;1,0)$	$+ (1-r_1-r_2)$		$P(N;0,0)$
	$1 = \sum_{(\alpha_1,\alpha_2)} \sum_{n=0}^{N} P(n;\alpha_1,\alpha_2)$							

Bild 7: Lineares Gleichungssystem $P^T=P^T\cdot A$ zur Bestimmung der Wahrscheinlichkeiten $P(n;\alpha_1,\alpha_2)$

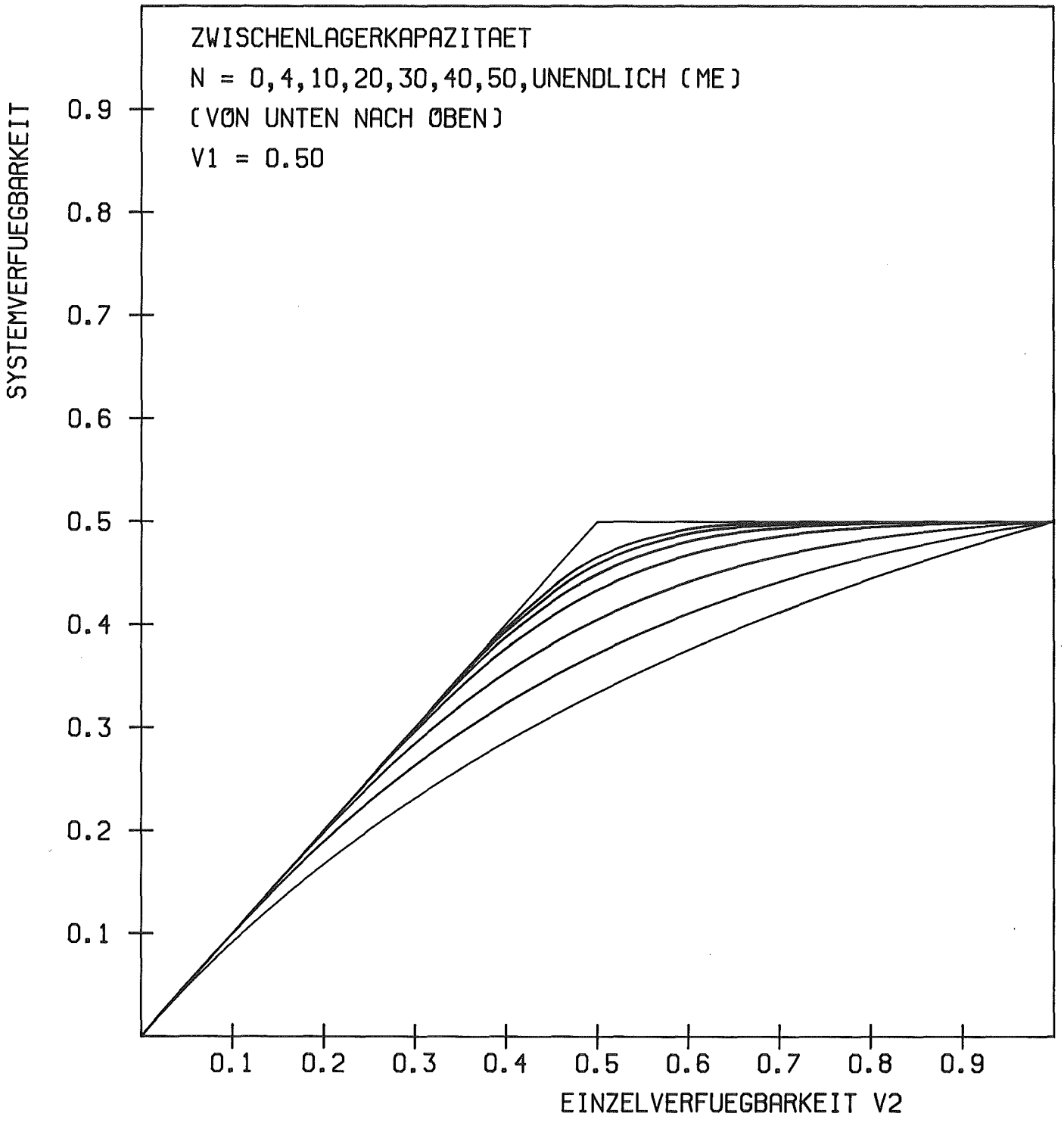


Bild 8: Die Stationäre Systemverfügbarkeit in Abhängigkeit von der Einzelverfügbarkeit.

Für Fall 1-5:	p_1=0.1	r_1=0.1	V_1=0.5
1	p_2=0.567	r_2=0.1	V_2=0.149
2	p_2=0.2	r_2=0.1	V_2=0.333
3	p_2=0.1	r_2=0.1	V_2=0.5
4	p_2=0.05	r_2=0.1	V_2=0.666
5	p_2=0.018	r_2=0.1	V_2=0.847

Bild 8a: System-Parameter für ein Ein-Lager-Modell

B e i s p i e l: (zu Bild 8!)

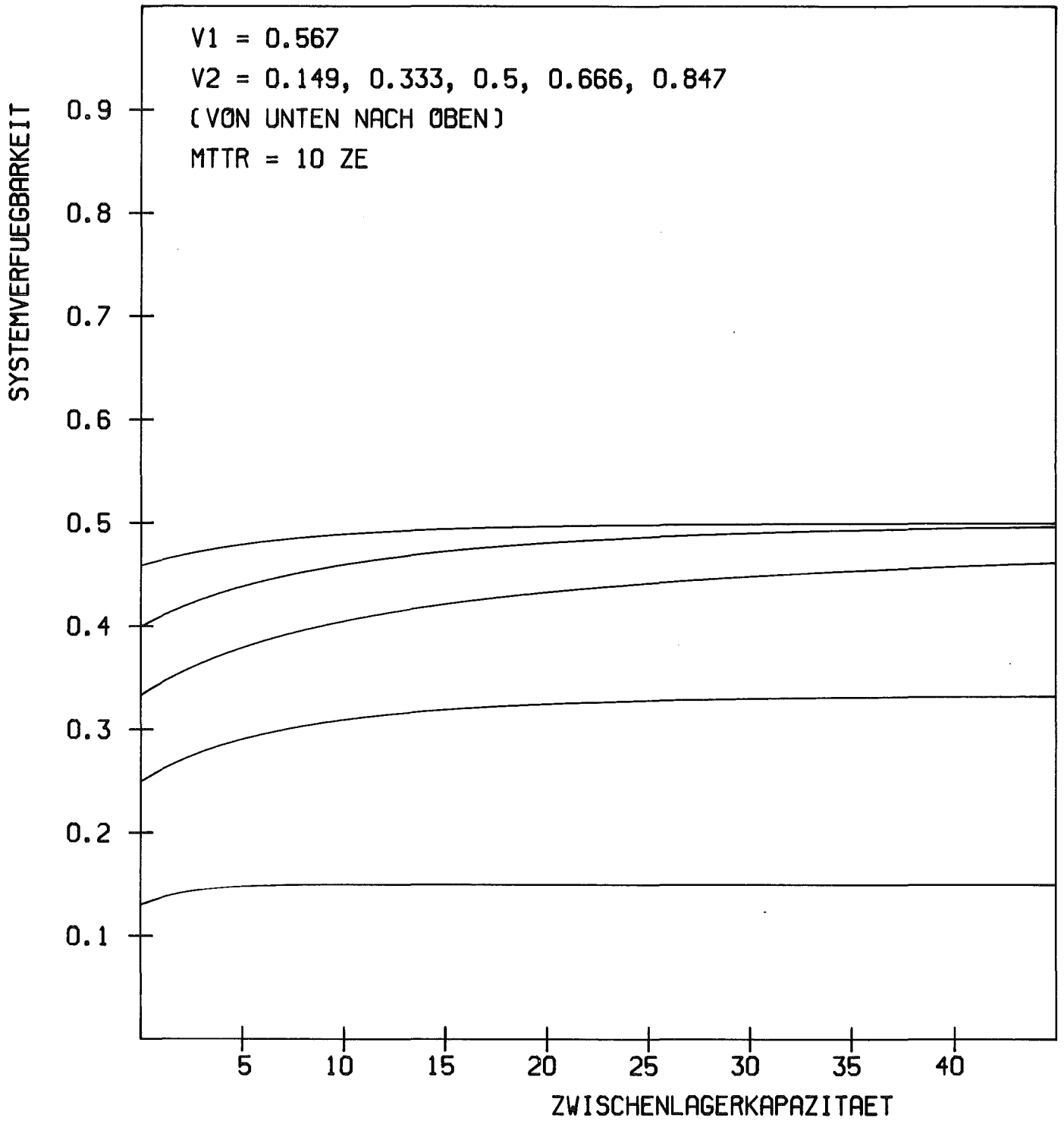


Bild 9: Stationäre Systemverfügbarkeit für das Ein-Lager-Modell mit V_1 fest, V_2 variabel.

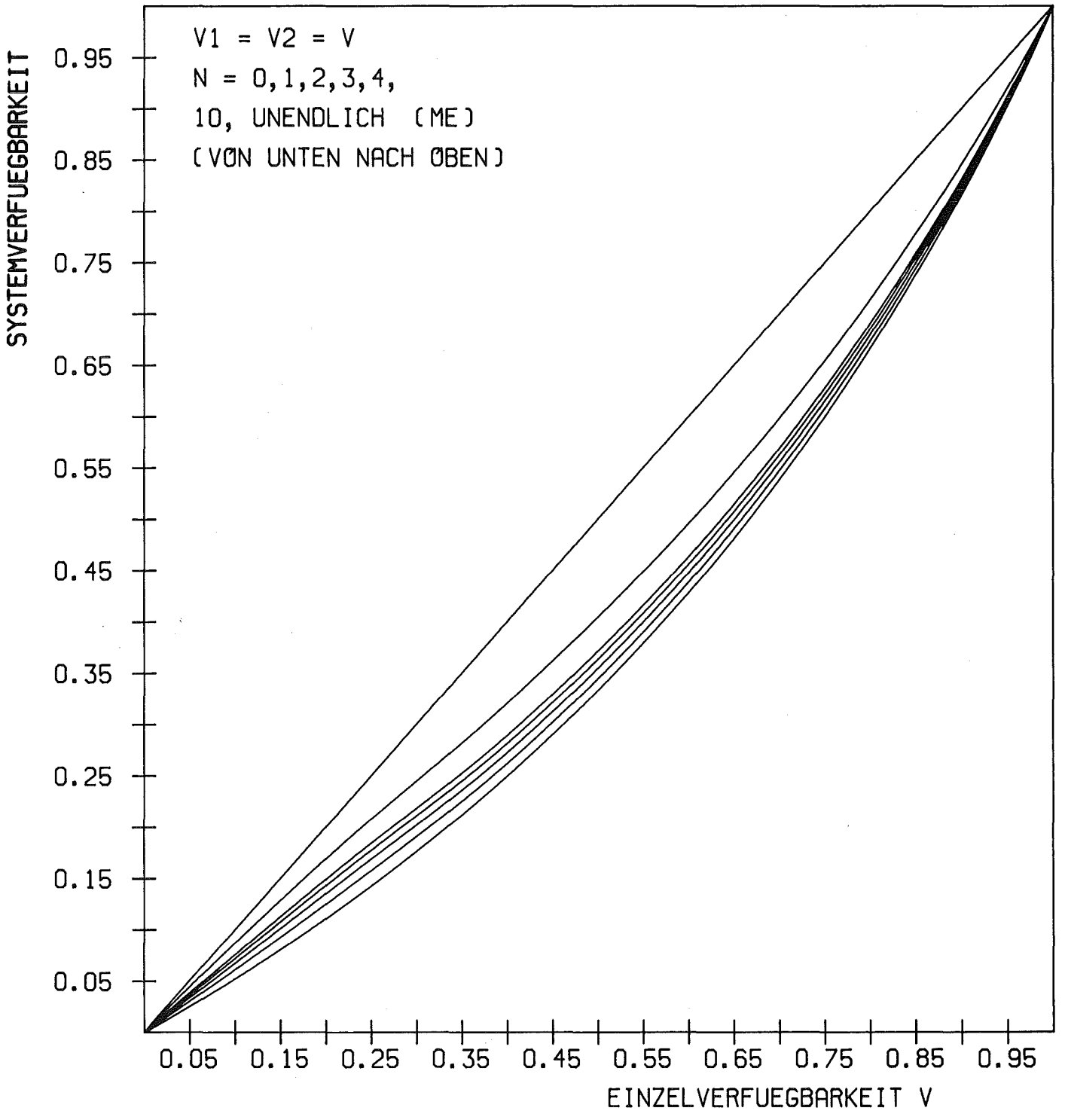


Bild 10: Systemverfügbarkeit mit und ohne Zwischenlager.

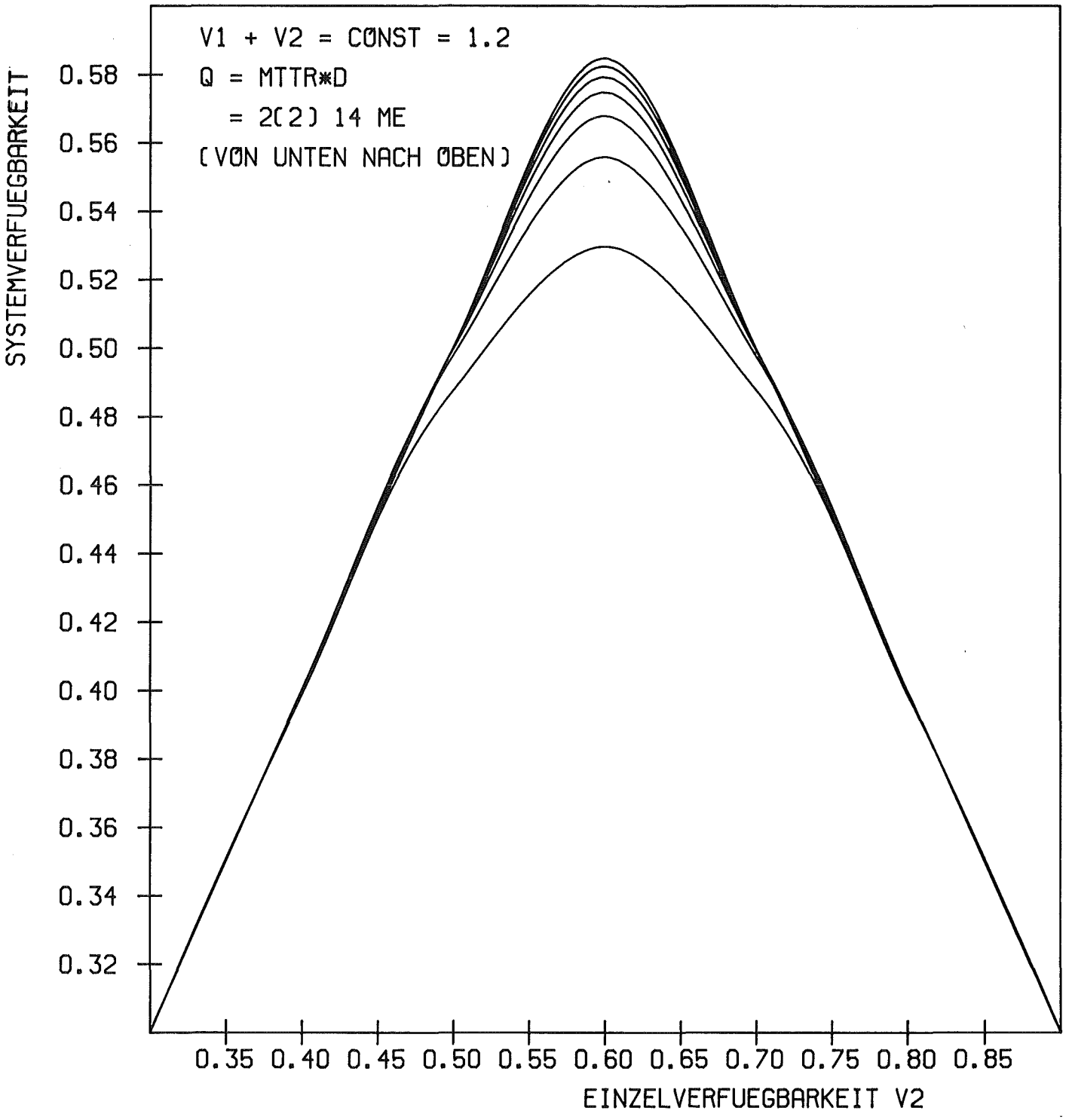


Bild 11: Stationäre Systemverfügbarkeit in Abhängigkeit von V_2 (V_1+V_2=const=1.2).

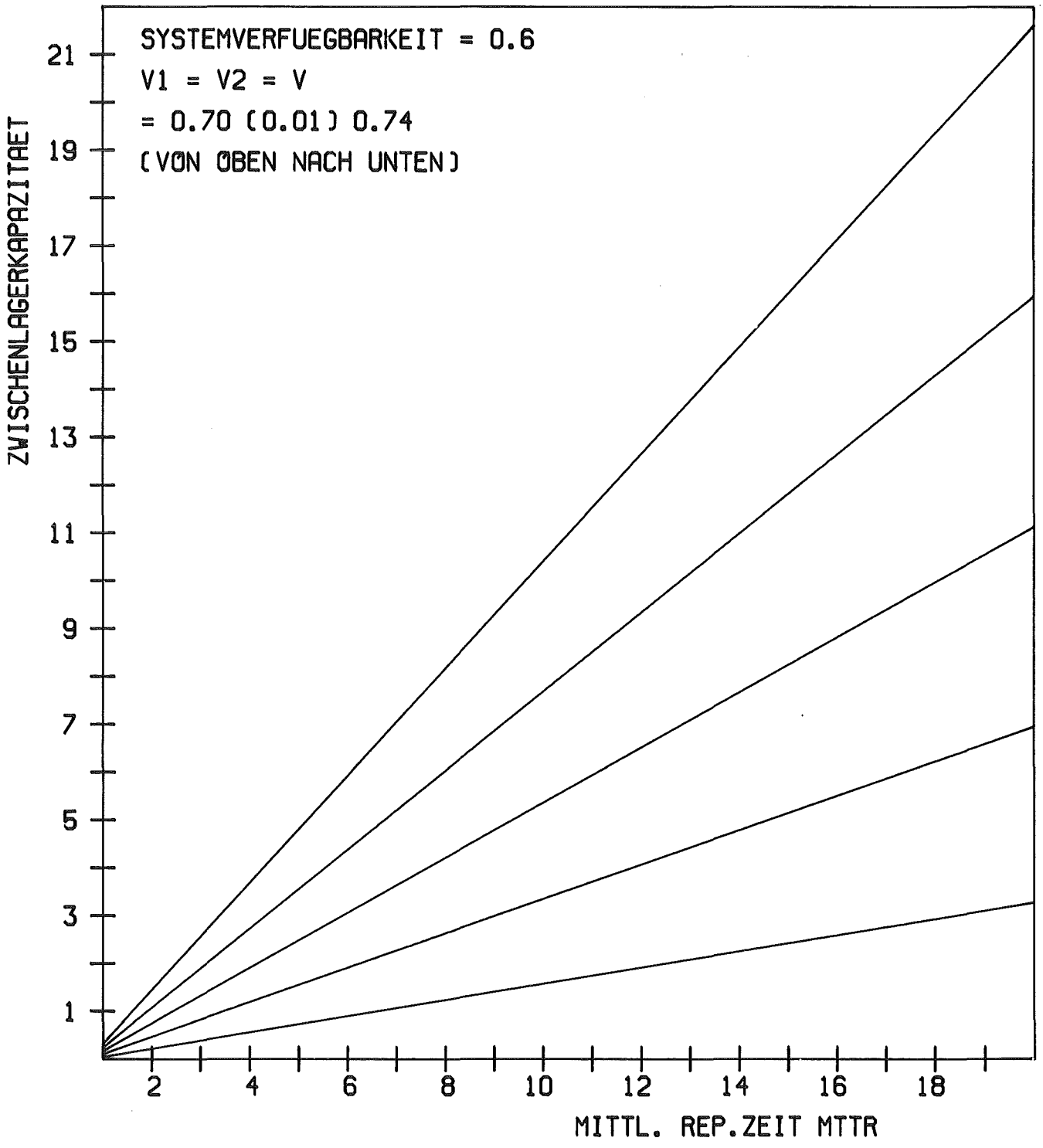


Bild 12: Abhängigkeit der Zwischenlagerkapazität von der mittleren Reparaturzeit.

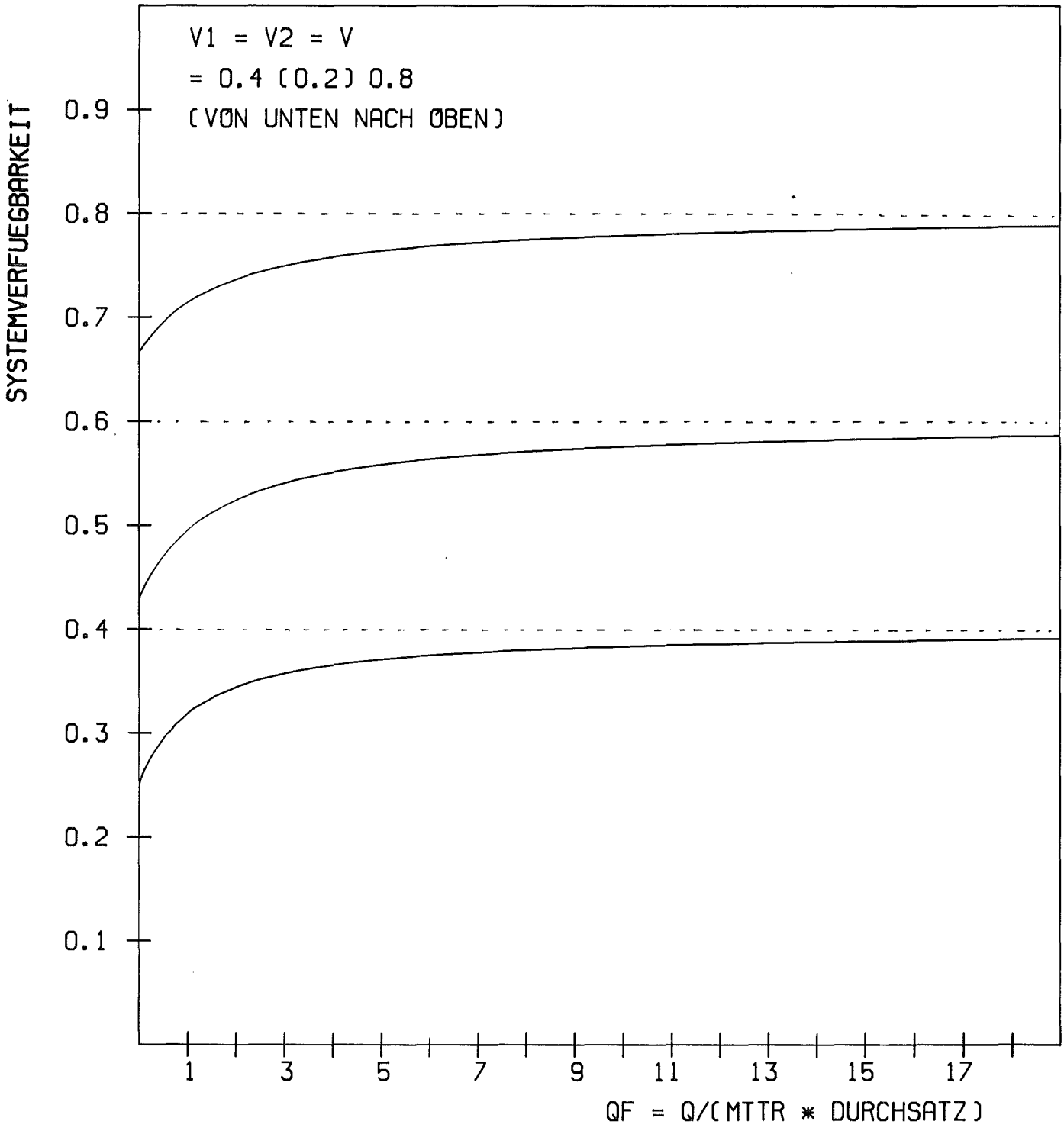


Bild 13: Darstellung der Abhängigkeit der Systemverfügbarkeit, V_{sys}, vom Verhältnis: Lagergröße/(mittl. Reparaturdauer · Durchsatz).

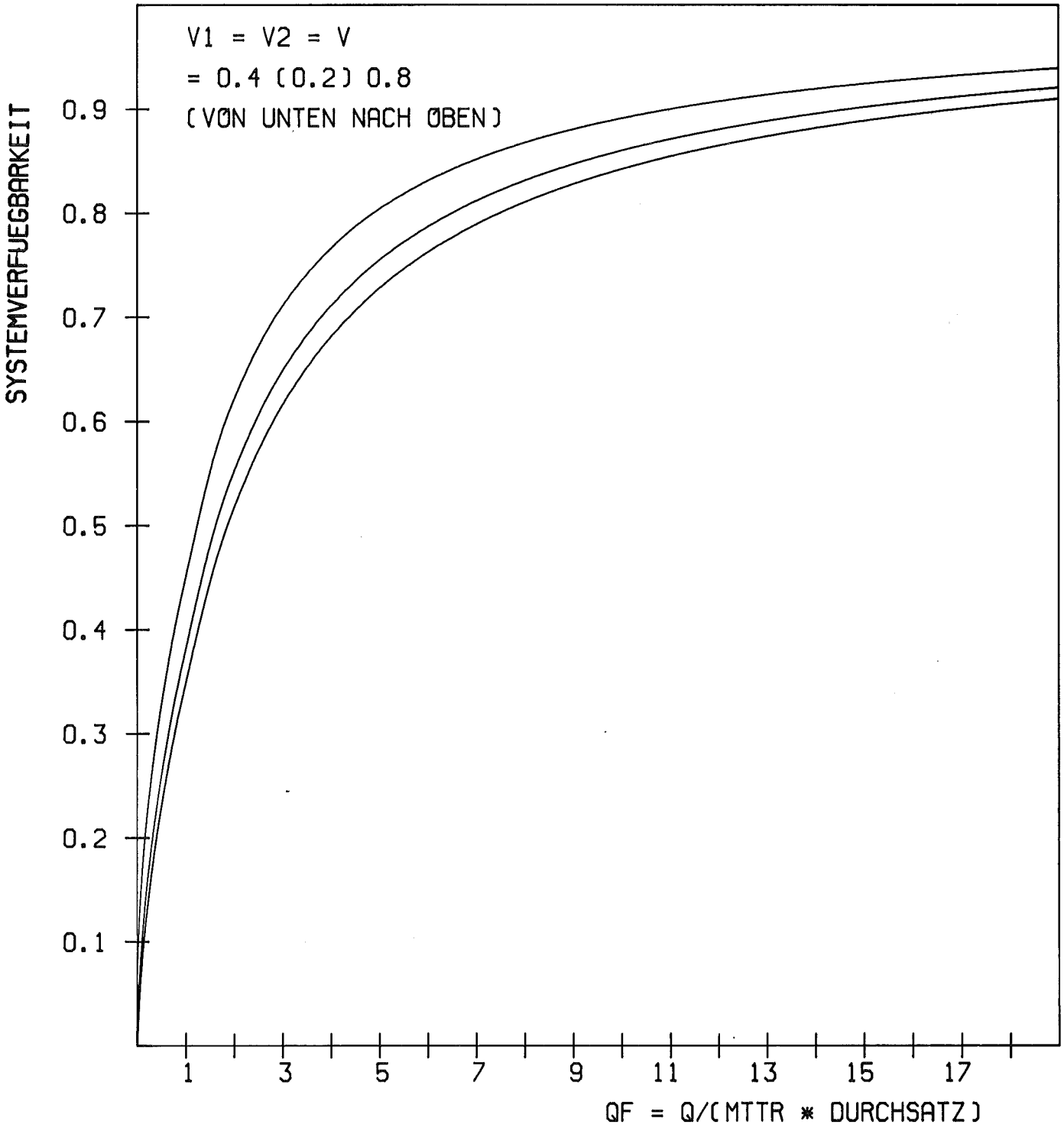


Bild 14: Darstellung der Abhängigkeit des relativen Gewinns, G, an Systemverfügbarkeit vom Verhältnis: Lagergröße/(mittl. Reparaturdauer · Durchsatz).

Diskussion

Frage: Wenn Sie in ihrem Modell die Wahrscheinlichkeiten p für Ausfall zeitunabhängig ansetzen, also nur stationäre Zustände betrachten, können Sie doch nur wiederum Gleichgewichtszustände, also ebenfalls zeitunabhängige Zustände bekommen. Werden die Ergebnisse damit nicht von vornherein relativ trivial?
Z.B. Abhängigkeit vom schwächsten Glied, stets volle Pufferspeicher, etc.

Antwort: Die Annahme zeitunabhängiger Reparatur- und Ausfallwahrscheinlichkeiten ist nicht hinreichend für die Stationärität des stochastischen Systems. Erst bei über alle Grenzen wachsendem Zeitparameter des stochastischen Systems wird Stationärität erreicht.

Die Abhängigkeit der Systemverfügbarkeit von den Systemparametern: Zwischenlagerkapazität, Ausfall- und Reparaturraten der Maschinen ist nicht trivial, wie die Ergebnisse von Buzacott zeigen. Die Fälle: kein Zwischenlager, unendlich großes Zwischenlager ("System so stark wie das schwächste Glied der Kette") sind im allgemeinen theoretischen Ergebnis enthalten.

Frage: Wie komplex wird das mathematische Modell, wenn man nicht mehr mit konstantem Durchsatz arbeitet?
Ist dieses Problem schon bearbeitet worden und von wem?

Antwort: Unseres Wissens nach ist es noch nicht gelungen in ein Modell mit diskretem Zustandsraum und diskreter Zeit unterschiedliche konstante Durchsätze in das Modell einzuarbeiten. Für den kontinuierlichen Fall hat der russische Autor Levin unterschiedliche konstante Durchsätze berücksichtigt.

(Levin, A.A., Pasko, N.I., Calculating the Output of Transfer Lines, Machines and Tooling (1969), Vol. 40, No. 8, S. 12-16).

Frage: Wie findet die "Regelung" des Systems statt?

Antwort: Bei dem Modell wird keine Betriebsstrategie unterstellt. Eine Regelung des Systems findet insofern statt, daß blockierte Maschinen nicht produzieren können.

Frage: Läßt sich dasselbe Modell auch mit Semi-Markov Prozessen bearbeiten?

Antwort: Der hier betrachtete Markov-Prozeß ist der Spezialfall eines Semi-Markov-Prozesses.

Bemerkung: Der Markov-Prozeß läßt sich eventuell durch Anwendung von Absorption und Merging vereinfachen.

Frage: Welche (Regelungs-)Eingriffe im simulierten Prozeß gewährleisten die Stationärität, also die Existenz eines stabilen Gleichgewichtszustands für die Belegung der Zwischenlager? In anderen vergleichbaren Warteschlangen-Problemen mit Warteräumen sorgen hierfür die Eigenschaften der Eingangsprozesse und die Verteilungen der Bedienungszeiten.

Antwort: Der Begriff der Stationärität ist bei stochastischen Prozessen die Betrachtung des Systems für $t \to \infty$. Die Stationärität eines Prozesses macht zunächst keine Aussage, z.B. über die "Stationärität" des Lagerbestandes, d.h. in diesem Fall, ob der Lagerbestand eine Asymptote hat. Hierfür sind, wie bei anderen Warteschlangenproblemen, die Systemparameter ausschlaggebend.

Frage: Eine methodologische Frage: Für die Bestimmung der stationären Wahrscheinlichkeiten muß man die Übergangswahrscheinlichkeiten generieren, und die Markov-Matrix aufstellen, und das Gleichungssystem lösen. Welches sind die Methoden, die großen Gleichungssysteme zu behandeln?

Bemerkung: Das Zeitverhalten bei einer M.-Matrix kann man mit der Potenzierungsmethode, die bei größeren Matrizen unübersichtlich wird,

lösen, oder den zweitgrößten Eigenwert bestimmen. Dann konvergiert das System grob gesagt, wie eine geometrische Reihe mit diesem Eigenwert.

Antwort: Die Matrizen sind u.a. schwach besetzt. Durch geeignete Umnumerierung der Zustände erreicht man Block-triangulare Matrizen. Dann wird man vermutlich die Ergebnisse über schwach besetzte Matrizen nutzen können (z.B. Buch: Tewarson: Sparse Matrices). Von uns sind noch keine numerischen Probleme in diesem Zusammenhang untersucht worden.

Frage: Das Ergebnis maximaler Systemverfügbarkeit bei genau gleicher Verfügbarkeit der einzelnen Verfahrenseinheiten ist doch sicher eine Konsequenz der Annahme gleicher Zwischenlagerkapazitäten? Ungleiche Zwischenlagerkapazitäten würden wahrscheinlich ungleiche Verfügbarkeiten der Verfahrenseinheiten als optimal nach sich ziehen.

Antwort: Ja! Das ist plausibel, aber noch nicht bewiesen, da für Mehr-Lager-Modelle noch keine geschlossenen Lösungen erzielt wurden.

Frage: Wie verhält sich der Erwartungswert der Lagerbelegung, insbesondere beim Optimum der Systemverfügbarkeit?

Antwort: Die größte Systemverfügbarkeit bei gegebener Lagerkapazität spielt sich bei gleichen Einzelverfügbarkeiten ein. Der erwartete Lagerbestand ist dann die halbe Lagerkapazität.

Frage: Wenn man den Prozeß, für den hier nur der stationäre Zustand betrachtet wurde in seinem Zeitverhalten untersuchen möchte, dann muß man anstelle des linearen Gleichungssystems das vollständige System von Differentialgleichungen berechnen. Wurden Rechnungen dieser Art durchgeführt, denn Rechenprogramme zur numerischen Bearbeitung solcher Probleme stehen ja zur Verfügung?

Antwort: Für Planungshilfen ist nur das Langzeitverhalten eines Systems geeignet, da Einschwingvorgänge nicht überbewertet werden sollen.

Um das zeitabhängige Verhalten diskreter Modelle zu untersuchen, müssen Folgen von linearen Gleichungssystemen gelöst werden.

Frage: In diesem Modell wurde angenommen, daß alle Zwischenlager gleich groß sind. Dies führt dazu, daß im optimalen Fall alle einzelnen Prozesse die gleiche Verfügbarkeit haben. Hat man Erfahrungen, z.B. von Le Havre, ob es als Entwicklungsziel vernünftig ist, zu gleichen Verfügbarkeiten zu streben? Die inhärente Verfügbarkeit verschiedener Prozesse kann ja sehr verschieden sein und es kann sehr teuer werden, nach gleicher Verfügbarkeit zu steuern. Eine andere Möglichkeit wäre die variierenden Verfügbarkeiten zu akzeptieren und die Größe der Zwischenlager kostengünstig zu wählen; z.B. wenn der Pu-Zyklus sehr unzuverlässig ist, sollte dieser Prozeß einen großen Soll-Durchfluß und große Zwischenlager vor und nach dem Prozeß haben. Andere Lager könnten kleiner sein.

Antwort: Optimierung der Systemverfügbarkeit bzgl. der Zwischenlagerkosten sind bislang von uns noch nicht durchgeführt worden. Es existieren jedoch Untersuchungen (Hahn, R., Produktionsplanung bei Linienfertigung, W. de Gruyter, Berlin (1972); von Stetten, R., Auslegung von Störungspuffern in kapitalintensiven Fertigungslinien, Krausskopf-Verlag, Mainz, 1977).

Bemerkung: 1.) In der Automobilindustrie wird bei der Produktion stets angestrebt, möglichst alle Pufferplätze (Zustand voll) durch entsprechende Maschinenkonstruktion etc. zu besetzen. Dadurch liegt die mittlere Besetzung stets in der Nähe der maximalen Pufferplätze.

2.) Stationärität wird durch zwangsweises Abschalten der vorausgehenden Maschine erreicht. Dies ist sicher im vorgestellten Simulationsprogramm enthalten.

Bemerkung: In der Entwicklung der analytischen Modelle gehen wir im IDT schrittweise vor. Im ersten Ansatz werden gleiche Verfügbarkeiten und Durchsätze angenommen, die zu handhabbaren analytischen Formeln

führen, aus denen man Einsichten und Abschätzungen gewinnen kann. Die Modelle werden dann in ihrer Weiterentwicklung sukzessive verfeinert werden. Da dabei die analytischen Ausdrücke sehr kompliziert und undurchsichtig werden, wird man zu Näherungen oder Simulationen übergehen müssen, wobei man möglicherweise die Ergebnisse und Einsichten der einfacheren Ansätze mit berücksichtigen kann.

Bemerkungen: 1. Reparaturverteilung: Falls Verhältnis

$$\text{MTTR/MTBF} \approx \frac{\lambda_{\text{Austausch}}}{\lambda_{\text{Reparatur}}} >> 1$$

kann exponentielle Rep.-Verteilung anstatt zeitabhängige Verteilungen (Log. Norm.) in weiten Grenzen numerisch verwendet werden ohne großen Genauigkeitssverlust (Mittelwerte der Verteilungen ähnlich groß).

2. Die numerischen Lösungen der homogenen Markov-Modelle (Differentialgleichungssysteme 1. Ordnung) sind bei 50-70 Zuständen mit der Trapezregel oder "Rückwärts-Euler" (stabil) kein Problem. Diese numerischen Methoden sind auch für steife Differentialgleichungssysteme anwendbar.

3. Markov-Modelle eignen sich auch für größere Systeme,

   a) wenn geeignete Strukturapproximationen durchgeführt werden können, d.h. Zustände mit 'kleiner' Eintretungswahrscheinlichkeit und weniger wichtiger Aussage weggelassen werden;

   b) wenn der Prozeß sich betriebsbedingt in verschiedene geeignete Zeitabschnitte untergliedern läßt (z.B. ganzes System intakt, Teil in Wartung, System überlastet). Die Modelle werden für die verschiedenen Zeitabschnitte separat berechnet und in einem Linearansatz wieder kombiniert.

$$P(t) = \sum_i a_i P_i(t); \quad \sum a_i = 1, \quad a_i = \text{Gewichtungsfaktoren},$$

P_i = Wahrscheinlichkeit des Systemzustandes i).

Analytische Modelle für Zuverlässigkeitsuntersuchungen von Kraftwerksystemen.

P. Zinterhof

Mathematisches Institut der Universität Salzburg

Das Studium komplexer Systeme, wie es etwa Energieversorgungssysteme sind, geschieht seit geraumer Zeit häufig mit Simulationssprachen. Es ist ohne Zweifel ein bedeutender Vorteil dieser Techniken, daß es vielfach nicht notwendig ist, tiefere und zeitaufwendigere Methoden heranzuziehen oder die formale Struktur des untersuchten Systems sehr weit zu analysieren. Ein entscheidender Nachteil dieser Techniken ist es aber, daß einerseits häufig unerträglich lange Berechnungen notwendig sind (wegen der i.A. sehr langsamen stochastischen Konvergenzen) und andererseits auf die Möglichkeit tieferer Einsichten in die Struktur des Systems oft von vornherein verzichtet wird.

Wir stellen uns daher die Aufgabe, explizite mathematische Modelle für die Untersuchung von Zuverlässigkeitsproblemen von Elektrizitätsversorgungssystemen so aufzustellen, daß einerseits die praktisch relevanten Größen wie Versorgungssicherheit, Verfügbarkeit, Leistungserwartung des Systems etc. möglichst rasch und genau berechnet werden können und andererseits die verwendeten formalen Strukturen möglichst genau der komplexen Wirklichkeit entsprechen und die in das Modell einfließenden Voraussetzungen möglichst klar überblickt werden können. Solche Modelle können zugeschnitten werden auf die Reserveprobleme verschieden großer Verbundsysteme, die Versorgungssicherheitsprobleme im Kurz-, Mittel- und Langzeitbereich, auf das Energieproblem gemischt hydraulischer und thermischer Systeme, die optimale Einsatzplanung mit verschiedenen Zielfunktionen wie es die "Versorgungssicherheit" oder die "Kosten" sind.

Bei der Analyse der Versorgungszuverlässigkeit von Kraftwerksystemen ist es auf jeden Fall nötig das Betriebsverhalten von Blöcken zu modellieren. Da sich dieses Betriebsverhalten über lange Zeiträume bekanntlich nicht sicher vorhersagen läßt, ist es angebracht, die Hilfsmittel und Methoden der Stochastik anzuwenden und hier besonders die Theorie der stochastischen Prozesse. Das Ziel ist die explizite Berechnung der Wahrscheinlichkeit $k(t,\tau)$, daß der vorliegende Block im Zeitintervall vom Zeitpunkt t bis zum Zeitpunkt $t+\tau$ störungsfrei im Betrieb ist, wobei im Zeitintervall von 0 bis t beliebig endlich viele Ausfalls- bzw. Inbetriebnahmeereignisse stattfinden dürfen und auch können. Sehr wichtig ist es dabei, die für den Ingenieur klare Tatsache, daß die Betriebswahrscheinlichkeit in der Zukunft stark vom Betriebszustand des Blockes zum Zeitpunkt $t=0$ und der bereits feststehenden Dauer dieses Zustandes bei $t=0$ abhängen werden: Die Wahrscheinlichkeit, daß ein Block z.B. in 500 Stunden für 100 Stunden störungsfrei arbeitet wird davon abhängen, ob er bei $t=0$ in Betrieb ist oder ausgefallen ist und wie lange bei $t=0$ dieser (Betriebs- oder Ausfalls-)Zustand bereits andauert. Das bedeutet mathematisch gesprochen, daß die Stochastik eines Blockes i.A. keine markoff'sche ist. Ältere Untersuchungen machten auch die überaus einschränkende Annahme, daß exakt bei $t=0$ eine Betriebsdauer beginnt und berechneten bloß die Wahrscheinlichkeit $k(t)$, daß zum Zeitpunkt t der Block in Betrieb ist.

In /1/ wurde eine exakte Formel für die beiden Bereitschaftskoeffizienten $k_A(t,\tau|t_A)$ und $k_B(t,\tau|t_B)$ gegeben. Es ist $k_A(t,\tau|t_A)$ die Wahrscheinlichkeit, daß ein Block im Zeitintervall von t bis $t+\tau$ störungsfrei in Betrieb ist unter der Bedingung, daß er bei $t=0$ bereits die Zeitdauer t_A ausgefallen ist. Analog dazu ist $k_B(t,\tau|t_B)$ die Wahrscheinlichkeit dafür, daß der Block im Zeitintervall von t bis $t+\tau$ in Betrieb ist unter der Bedingung, daß er bei t=0

bereits eine Zeitdauer t_B in Betrieb ist. Die Berechnung dieser Bereitschafts-koeffizienten bereitet nicht unbedeutende Schwierigkeiten, über die noch zu berichten ist.

In *BILD 1* und *2* ist der typische Verlauf von $k_B(t,\tau|t_B)$ und von $k_A(t,\tau|t_A)$ dargestellt.

BILD 1 : Wahrscheinlichkeit der Betriebsbereitschaft nach t Stunden über ein Zeitintervall τ = 0, 10, 50, 100, 500 Stunden des Kraftwerkes im Erneuerungsprozeß, wenn es zum Zeitpunkt t = 0 in Betrieb ging.

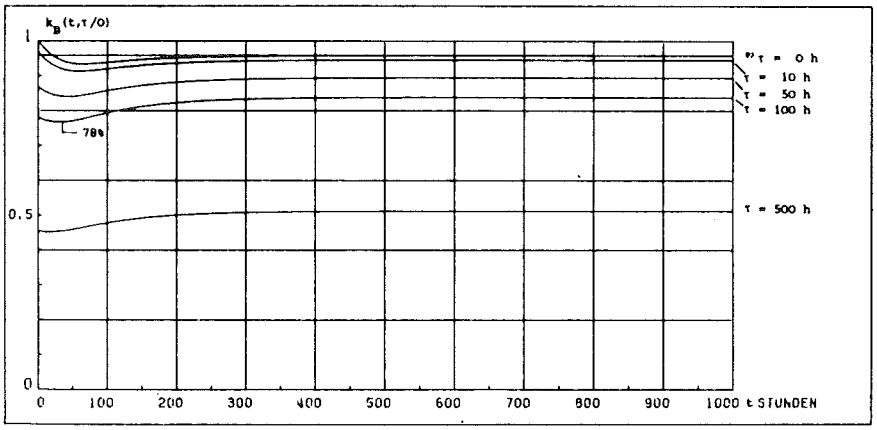
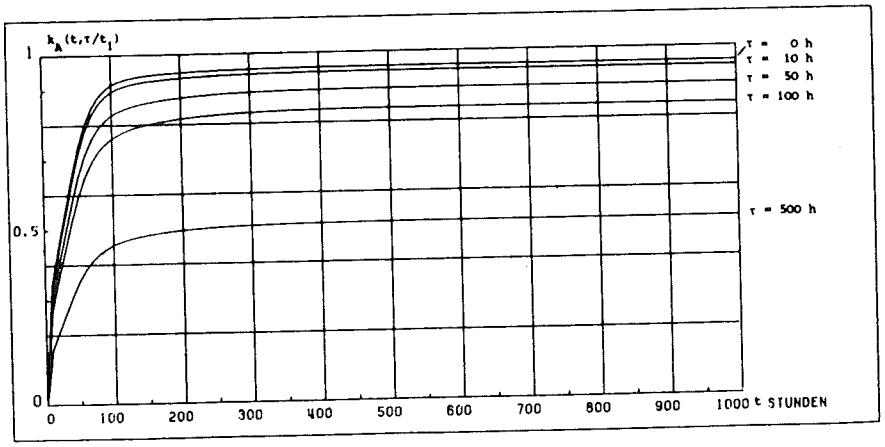


BILD 2 : Wahrscheinlichkeit der Betriebsbereitschaft über ein Zeitintervall τ = 0, 10, 50, 100, 500 Stunden des Kraftwerkes im Erneuerungsprozeß, wenn es zum Zeitpunkt t_1 = 0 ausgefallen ist.



Die Berechnung dieser bedingten Intervallbereitschaftskoeffizienten zeigt, daß diese durch unendliche Reihen von Faltungspotenzen der Dichten der Betriebsdauern und der Ausfallsdauern dargestellt werden.

Sei etwa zunächst $k_B(t,\tau|t_B)$ die Wahrscheinlichkeit ausfallsfreier Arbeit des Blockes im Zeitintervall $(t,t+\tau)$ unter der Bedingung, daß bei $-t_B$ eine Betriebsperiode begann und bekanntermaßen bis $t=0$ andauerte. Um $k_B(t,\tau|t_B)$ zu berechnen, bezeichnen wir mit A_n das Ereignis, daß der Block zwischen t und $t+\tau$ ausfallsfrei ist und bis t genau n Erneuerungen durchmachte, alles unter der Bedingung einer open-end-Betriebsperiode von $-t_B$ bis $t=0$. Dann gilt

$$Prob(A_0(t,\tau|t_B)) = \frac{1 - F(t_B+t+\tau)}{1 - F(t_B)}$$

wobei F(t) die Wahrscheinlichkeit ist, daß die Betriebsdauer kleiner oder gleich t ist.

Für $n \geq 1$ gilt

$$Prob\ (A_n(t,\tau|t_B)) = Prob\ (\tau_1'+\tau_1''+ \ldots +\tau_n'+\tau_n''<t+t_B<\tau_1'+\tau_1''+ \ldots +$$

$$+\tau_n''+\tau_{n+1}'-\tau|\tau_1'>t_B) =$$

$$\int_0^{t+t_B} Prob\ (x<\tau_1'+\tau_1''+ \ldots +\tau_n'+\tau_n''<x+dx|\tau_1'>t_B).$$

$$Prob\ (\tau_{n+1}' > t_B + t + \tau - x) =$$

$$\int_0^{t+t_B} [\ 1 - F(t + t_B + \tau - x)\ ] \cdot \varphi_n\ (x|\ t_B)\ dx\ ,$$

wobei mit $\frac{d}{dt}F(t)=f(t)$ gilt

$$\varphi_n\ (x|\ t_B) = f\ (x|\ \tau_1' > t_B) * f\ (x)^{*(n-1)} * g\ (x)^{*n}$$

und wobei das Symbol '*' die Faltung zweier Funktionen, d.h. $f(x)^{*(n-1)}$ die n-1-fache Faltung der Funktion f(x) mit sich selbst bedeutet.

Daraus ergibt sich wegen der Unvereinbarkeit der A_n

$$k_B\,(t,\tau \mid t_B) = Prob\,(\sum_{n=0}^{\infty} A_n\,(t,\tau \mid t_B) =$$

$$Prob\,(A_0) + \sum_{n=1}^{\infty} Prob\,(A_n) =$$

$$\frac{1 - F(t_B + t + \tau)}{1 - F(t_B)} + \sum_{n=1}^{\infty} \int_0^{t+t_B} [1 - F(t_B+t+\tau-x)\,]\,\varphi_n(x \mid t_B)\,dx$$

und weiter

$$k_B(t,\tau \mid t_B) = \frac{1 - F(t_B+t+\tau)}{1 - F(t_B)} + \int_0^{t+t_B} [\,1 - F(t+t_B+\tau-x)\,]\cdot h_{2B}(x \mid t_B)\,dx$$

Hier ist $f(t)$ die Dichte der Verteilung $F(t)$ der Betriebsdauern und $g(t)$ die Dichte der Verteilung $G(t)$ der Reparaturdauern des Blockes und $h_{2B}(x \mid t_B)$ die sogenannte bedingte Erneuerungsdichte

$$h_{2B}(x \mid t_B) = \sum_{n=1}^{\infty} f(x \mid t_B) * g(x) * (f*g)^{*(n-1)}$$

Da die explizite Summation dieser unendlichen Reihen nicht so ohne weiteres möglich ist, wird das gesamte Problem Laplace-transformiert unter der approximationstheoretisch legitimen Annahme, daß die zugrunde gelegten Dichten $f(t)$ der Betriebsdauer und $g(t)$ der Ausfallsdauern durch Mischungen (Linearkombinationen) von Gamma-Verteilungsdichten dargestellt werden. Dann läßt sich die Laplace-transformierte Reihe zu einer im wesentlichen rationalen Funktion summieren, deren Pole alle in der linken Halbebene liegen. Die rationalen Anteile sind dann in Partialbrüche zu zerlegen und es gelingt die Rücktransformation in den Originalbereich sofort und explizit, sodaß letzlich alle Bereitschaftskoeffizienten durch endliche Summen von Exponential- und unvollständigen Gamma-Funktionen dargestellt werden. Diese explizite Darstellung macht es möglich, die Berechnung von Bereitschaftskoeffizienten auf den zur Zeit erhältlichen Minirechnern im Real-Time-Betrieb vorzunehmen und Kraftwerke mit beliebigem Ausfalls- und Reparaturverhalten zu simulieren.

Da es nun möglich ist, das stochastische Ausfallsverhalten von Blöcken zu berechnen, ist es auch möglich, explizite analytische Modelle für das Verhalten von komplexen Energieversorgungssystemen in Hinblick auf die Versorgungssicherheit anzugeben und auch für den on-line- bzw. Real-Time-Betrieb so zu implementieren, daß in Abhängigkeit vom letzten Ausfalls- oder Inbetriebnahmeereignis im System die Leistungserwartung für jeden Zeitpunkt in der Zukunft rasch berechnet werden kann und auch die Sicherheit der Aufbringung berechnet werden kann. Da nun ein explizites analytisches Modell für die Beschreibung von komplexen Systemen vorliegt, kann man auch den Einfluß der Änderung der wesentlichen Parameter des Systems auf die Zielfunktionen des Systems wie Leistungserwartung bzw. Versorgungssicherheit, studieren. Solche Parameter sind etwa die Anzahlen der Blöcke, Nennleistungen, Verfügbarkeiten, Status des Systems bzw. Ausfallssituation, Ausbaupläne, Lasten, Lieferver-

träge, Verbundsituation etc. Der Modellansatz ist dabei recht allgemein, sodaß Probleme und Situationen, die für die verschiedenen Bereiche interessant sind, studiert werden können. Ein Reserve- bzw. Versorgungsproblem stellt sich natürlich für eine Landesgesellschaft mit hohem hydraulischen Anteil ganz anders als für einen internationalen Verbund mit hohem thermischen Anteil. Da jedenfalls analytische Modelle vorliegen, können grundsätzlich die Modelle bzw. die Systeme, die damit modelliert werden, auch optimiert werden. Als Zielfunktion mag etwa die Güte der Versorgungssicherheit dienen unter der Nebenbedingung, daß eine Leistungserwartung nicht unterschritten werden darf. Optimiert kann etwa werden über eine Menge von Einsatzplänen. In diese Modelle fließt eine Reihe von Voraussetzungen ein, wie eine sorgsame Lektüre der bisherigen Literatur zeigt. Es ist sicher fruchtbar, einige dieser Voraussetzungen kritisch zu beleuchten und zu überlegen wie und ob man sich davon freimachen kann.

In den bisherigen Arbeiten wurde stets angenommen, daß die aufeinanderfolgenden Ausfalls- bzw. Betriebsdauern voneinander stochastisch unabhängig sind, daß also die Verteilung der Summen der entsprechenden Zufallsvariablen durch Faltungen erhalten wird. Diese Annahme führt ohne Zweifel zu einer ersten und brauchbaren Näherung. Diese Unabhängigkeitsvoraussetzung ist sicher nicht ganz falsch, sie ist aber i.A. leider auch nicht ganz richtig: Die Erwartungswerte, also die ersten Momente der Verteilungen werden dadurch nicht beeinflußt, jedoch die zweiten und höheren Momente, also letztlich die Gestalt der Verteilung. Ursache ist u.a. daß die Reparaturdauer von der Ausfallsursache des komplexen Systems "Kraftwerk" und damit wohl von der Dauer der unmittelbar vorhergegangenen Betriebszeit abhängt. Zur empirischen Untersuchung der Richtigkeit dieser Unabhängigkeitshypothesen ist sehr umfangreiches

Datenmaterial nötig. Es wurde ein Modell konstruiert, das von diesen Problemen sui generis frei ist, da die beschriebene Schwierigkeit durch den Kunstgriff der Konstruktion eines zum vorliegenden zweistufigen äquivalenten im wesentlichen einstufigen Erneuerungsprozess umgangen wurde; die zur rechnerischen Realisierung dieser Modifikation nötigen statistischen Betrachtungen bedürfen des gleichen Datenumfanges wie die Implementierung des klassischen zweistufigen Prozesses mit der Unabhängigkeitshypothese. Ein weiterer Aspekt scheint rein mathematisch-theoretisch zu sein: Es wurde bisher immer angenommen, daß die vorliegenden Verteilungen $F(t)$ und $G(t)$ der Betriebs- bzw. Ausfallsdauern Dichten $f(t)$ und $g(t)$ besitzen, also absolut stetig sind. Diese Annahme wird in der klassischen Erneuerungstheorie gemacht und vor allem deshalb als legitim angesehen, weil diese Annahme zu einer "schönen Theorie" mit leichteren Beweisen führt. Diese Annahme erfreut sich einer hohen Überzeugungskraft und auch Wertschätzung, wahrscheinlich weil sie in den bekannten Werken über Zuverlässigkeitstheorie immer wieder als plausibel und gerechtfertigt bezeichnet wird. Tatsache ist jedoch, daß man sich durch diese ohne Zweifel beweistechnisch nützlichen Voraussetzung den Weg zu vielen realistischen Modellen versperrt: Man kann etwa unter der Voraussetzung der Absolutstetigkeit der auftretenden Verteilungen das Phänomen von time-lags beim Hochfahren von Blöcken und Anfahrversagen nur schwer beschreiben, die Modellierung von Erneuerungsprozessen mit fixen bzw. teilweise deterministischen Reparaturdauern bzw. Revisionsdauern ist praktisch nicht möglich, da in diesen Fällen Dichten eben überhaupt nicht oder lokal nicht existieren. Diese Schwierigkeiten wurden durch Konstruktion eines allgemeineren Modells und der Entwicklung einer adäquaten Zuverlässigkeitstheorie, die auf der Theorie der Faltungspotenzen allgemeinen Wahrscheinlichkeitsmaße unter konsequenter Verwendung von Stieltjes-Integralen letztlich durchaus im Rahmen der klassischen reellen Analysis gelöst. Auf der numerischen Seite treten dann naturge-

mäß statt der Laplace-Transformation der Dichten die Laplace-Stieltjes-Transformationen von Wahrscheinlichkeitsverteilungen auf. Die explizite Rücktransformation macht natürlich größere Schwierigkeiten, da ja schon im absolut stetigen Fall Kummer'sche Transzendente, also sogenannte einfache transzendente Funktionen auftreten können. Mit den heutigen Rechenanlagen ist aber eine rasche und befriedigende Approximation möglich.

Ein weiterer Diskussionspunkt ist ohne Zweifel die Modellierung von Systemen von Kraftwerken. Auch hier wurde sehr häufig stillschweigend und auch von uns die Hypothese der Unabhängigkeit der Blöcke angenommen. Diese Annahme schadet nicht bei der Berechnung der erwarteten Systemleistung. Bei der Beurteilung der Versorgungssicherheit durch ein System von Blöcken ist aber jedenfalls ein Modell angebracht, das die tatsächlichen Abhängigkeiten der Blöcke berücksichtigt. Ein solches Modell liegt ebenfalls vor. Die dazugehörige Optimierungsrechnung ist formal ähnlich der Faktorenanalyse in der multivariaten Statistik und führt auf quadratische Programme mit linearen Nebenbedingungen, also Dinge, die man heute bei den Systemen der uns interessierenden Größe rechnerisch wohl beherrscht.

Abschließend soll noch erwähnt werden, daß ein Modell zur Beschreibung eines Speichersystems, also eines Systems mit endlichem zeitabhängigem Energievorrat, das stochastisch beliefert (aufgefüllt) wird und auch stochastisch gemäß einer durch die Nachfrage und die Einsatzstrategie vorgegebenen Wahrscheinlichkeitsverteilung abgebildet wird, vorliegt. Das Modell beruht auf einer stochastischen Differentialgleichung für die Lösungsmethoden entwickelt werden, sodaß das Problem des begrenzten Energievorrates von Speichersystemen im Zusammenhang mit einem thermischen System gerechnet und auch für verschiedene Situationen simuliert werden kann.

L I T E R A T U R:

/1/ W. Koenne, P. Zinterhof, Zuverlässigkeitstheoretische Analyse von Elektrizitätsversorgungssystemen. Schriftenreihe der Technischen Universität Wien, Springer-Verlag Wien New York 1978.

Diskussion

Frage: In der Physik werden Laplace-Transformationen zur Behandlung partieller Differentialgleichungen dergestalt verwendet, daß wesentliche physikalische Aussagen aus der Laplace-Transformierten gewonnen werden können. Dadurch kann die in den meisten Fällen mühselige Rücktransformation oft vermieden werden. Gilt dies auch für einige der die stationären Lösungen Ihrer Problemstellung beschreibenden Größen?

Antwort: Ja! Aus den bekannten Beziehungen zwischen der Originalfunktion f und der Laplace-Transformierten $\tilde{f}$ lassen sich die asymptotischen Werte der Originalfunktion (Verfügbarkeiten, Wert bei t=0!) im Laplacebereich ohne Rücktransformation berechnen. Da sich Verfügbarkeiten leicht aus den Rohdaten ermitteln lassen, dient dies auch als Rechenprobe.

Frage: Existiert eine Erneuerungsgleichung für die Bereitschaftskoeffizienten $k_A(t,\tau|t_A)$, $k_B(t,\tau|t_B)$?

Antwort: Für die Bereitschaftskoeffizienten gelten Integralgleichungen vom Volterra'schen Typ (Faltungstyp), die einer numerischen Behandlung zugänglich sind. Diese benötigen wir nicht, da wir das Gesamtproblem auf die Berechnung von Nullstellen von Polynomen reduzieren könnten, die im Allgemeinen wesentlich unproblematischer ist.

Frage: Zur Auffindung möglichst echt zufallsverteilter Parameterkombination wird eine Methode aus der analytischen Zahlentheorie erwähnt. Als einfaches Beispiel für einen solchen Phasenraum wurde ein Rechteck genannt. Es wäre interessant doch einige Stichworte über die Methode, die der Monte-Carlo-Simulation offenbar weit überlegen ist, zu erfahren?

Antwort: Sei F(x) die Gleichverteilung auf E^s (s-dimensionaler Einheitswürfel) und $F_N(x)$ die empirische Verteilungsfunktion der Punkte $x_1,\ldots,x_N \in E^s$, so ist

$$D_N = \sup_{x \in E^s} |F_N(x) - F(x)| \leq \frac{c}{\sqrt{N}} \sqrt{\text{loglog } N}$$

für zufällige Punkte (stochastisch und größenordnungsmäßig). Für zahlentheoretische Gitter (sogenannte good lattice points) gilt:

$$D_N \leq c \cdot \frac{\log^{s-1} N}{N} \quad .$$

Die guten Gitterpunkte sind also wesentlich besser gleichverteilt als zufällige Stützknoten nach Monte-Carlo. Solche Punkte wurden für die Auswahl guter Startwerte gewählt.

Analytische und simulative Verfahren zur Berechnung der Zuverlässigkeitsmerkmale komplexer Systeme

L. Camarinopoulos

Vortragsmanuskript zum Seminar "Methoden der Systemplanung bei gefordetem Langzeitbetriebsverhalten" am 26./27. Februar 1980 im Kernforschungszentrum Karlsruhe

1. Allgemeines

Der Ablauf der Zuverlässigkeitsanalyse eines komplexen Systems ist in der Abb. 1 schematisch dargestellt.
Gegestand des Vortrages sind Verfahren zur probabilistischen Auswertung (Punkt 6) des dabei entstehenden Fehlerbaums bzw. Blockschaltbildes.
Die Auswertung von Fehlerbäumen komplexer Systeme ist von Hand kaum durchführbar. Große Fehlerbäume lassen sich nur unter Anwendung rechnengestützer Methoden sinnvoll behandeln. Wegen der hierfür notwendigen langen Rechenzeiten und großen Speicherkapazitäten soll die Auswahl der Methoden sehr sorgfältig vorgenommen werden.
Die erarbeiteten Methoden haben analytischen oder simulativen (Monte-Carlo) Charakter. Beide Formen ergänzen sich (Abb. 2) z.B. derart, daß bei sehr kleinen Eintrittswahrscheinlichkeiten die analytischen Verfahren vorteilhafter sind, da sie frei sind von statistischen Unsicherheiten des Monte-Carlo-Verfahrens. Dagegen sind die simulatorischen Verfahren dann günstiger, wenn die Systeme groß sind und komplizierte Randbedingungen berücksichtigt werden müssen (Abhängigkeiten zwischen den Komponenten, beschränkte Wartungs- und Reparaturkapazitäten, Berücksichtigung komplexer Instandsetzungsstrategien usw.).
Im folgenden soll ein kurzer Überblick über beide Methoden gegeben werden.

2. Analytische Verfahren

2.1 Einleitung

Von den analytischen Berechnungsmethoden zur Ermittlung der Zuverlässigkeitsmerkmale großer vermaschter Systeme erscheint die Vorgehensweise über die Minimalschnitte am aussichtreichsten. Diese Methode gliedert sich in zwei Schritte

- das Auffinden der Minimalschnitte einer gegebenen Struktur (die meistens in Form eines Fehlerbaums vorliegt)
- die anschließende Berechnung der Zuverlässigkeitsmerkmale der gefundenen Minimalschnitte und, daraus resultierend, der des Systems

In der Literatur findet man eine beträchtliche Anzahl von Veröffentlichungen, die sich mit der Ermittlung von Minimalschnitten mittels deterministischer Methoden befassen. Sie lassen sich global in die folgenden zwei Kategorien einteilen:

1. Verfahren, die aus trivialen kombinatorischen Überlegungen heraus (Truth-Table) alle bzw. den größten Teil der 2^n Kombinationen (bei n Systemkomponenten) auf ihre Zugehörigkeit zu den Minimalschnitten hin untersuchen
2. Verfahren, die durch Berücksichtigung der jeweiligen Systemstruktur die Anzahl der zu untersuchenden Kombinationen erheblich einschränken

Der Aufwand der Verfahren aus der erster Kategorie wächst ungefähr proportional mit $(1/k)\cdot(n/k)^k$, wenn k der höchste zu berücksichtigende Redundanzgrad ist. Damit sind solche Verfahren für große komplexe Systeme nicht anwendbar.
Der im Abschnitt 2.2 vorgestellte Algorithmus stammt deswegen aus der zweiten Kategorie und scheint der effizienteste aus einer Reihe bis jetzt vorgeschlagenen Algorithmen /1,2,3,4/ zu sein. Er wurde erstmalig in /5/ vorgestellt und bildet seitdem die Grundlage der meisten modernen analytischen Programmen /6,7,8/.
In Abschnitt 2.3 werden dann Berechnungsvorschriften für Zuver-

lässigkeitsmerkmale von Minimalschnitten unter Berücksichtigung der gebräuchlichsten Komponenteninstandsetzungsmodelle (Selbstmeldung, Inspektion) abgeleitet.
Durch die Anwendung des Exklusions-Inklusions-Prinzips können daraus ausgezeichnete Näherungen für die Kennwerte des Gesamtsystems gewonnen werden.
Auch effiziente Verfahren zur Identifikation von Minimalschnitten können allerdings nicht über die Tatsache hinweggehen, daß ein technisches komplexes System mehrere Millionen von Minimalschnitten, von denen in der Regel nur eine geringe Anzahl das Ergebnis bestimmt, aufweisen kann. Im Abschnitt 2.4 werden Abschneideprozeduren zum Aussortieren nicht relevanten Minimalschnitte aufgeführt, die zum erheblichen Rechenzeit- und Speicherplatzreduktion führen und somit die erfolgreiche Behandlung von Systemen mit quasi unbeschränkter Anzahl von Komponenten erlauben (1000 Komponenten und mehr).
Die Leistungsfähigkeit analytischer Verfahren wird schließlich im Abschnitt 2.5 am Beispiel eines möglichen Konzeptes zur Energieversorgung des Nuklearen Entsorgungszentrums aufgezeigt.

2.2 Ein Algorithmus zur Auffindung der Minimalschnitte eines Fehlerbaums

Im folgenden wird davon ausgegangen, daß die Systemstruktur in Form eines Fehlerbaums vorliegt. Ziel des Algorithmus ist somit die Ermittlung aller Minimalschnitte des Fehlerbaums.
Ausgehend vom TOP-Gatter werden im Ablauf des Algorithmus alle logischen Gatter des Fehlerbaums durch ihre Eingänge sukzessiv ersetzt.

Anmerkung: Mit TOP-Gatter wird in der Fehlerbaumterminologie das Gatter benannt, das das unerwünschte Ereignis darstellt. Es wird gewöhnlich ganz oben im Fehlerbaum abgebildet.

D.h. im Rahmen des Algorithmus erfolgt ein logisches Ausmultiplizieren der zum Fehlerbaum korrespondierenden Bool'schen Funktion. Die einfachste und gleichzeitig verständlichste Mög-

lichkeit den Algorithmus zu veranschaulichen ist seine Funktionsweise anhand eines praktischen Beispiels zu demonstrieren. Für eine mehr formale Vorstellung sei auf /5,6/ verwiesen.
Im Bild 3 ist eine stark vereinfachte Schaltung der Eigenbedarfversorgung eines Kraftwerkes abgebildet.
Der korrespondierende Fehlerbaum ist im Bild 4 dargestellt.
Der Algorithmus beginnt nun mit der Entwicklung des TOP-Gatters. Falls das TOP-Gatter ein ODER-Gatter ist, werden seine Eingänge in separaten Zeilen einer Matrix eingetragen. Handelt es sich um ein UND-Gatter werden dagegen seine Eingänge als separate Spaltenelemente der ersten Matrixzeile behandelt. In dem vorliegenden Fall, da es um ein Oder-Gatter handelt, bekommen wir folgende drei Matrixzeilen

G1
EBT
EBS

Die Idee des Algorithmus ist jedes Gatter durch seine Eingänge, d.h. weitere Gatter bzw. Komponenten nach der oben beschriebenen Art zu ersetzen bis die entstehende Matrix aus lauter Komponenten besteht. Die Zeilen dieser Matrix korrespondieren zu den gesuchten Schnitten. Ein UND-Gatter erhöht dabei den Redundanzgrad, während ein ODER-Gatter die Zeilenanzahl und somit die Anzahl der Schnitte erhöht.
In diesem Sinne wird als nächster Algorithmusschritt das UND-Gatter G1 durch seine Eingänge G2 und G3 ersetzt, die wie folgt eingehen

G2, G3
EBT
EBS

Eine Wiederholung dieser Prozedur bis auf Komponentenebene unter Berücksichtigung der Beziehungen

$A \cap A = A$ (Idempotenzeigenschaft) (1)

$A \cup A \cap B = A$ (Absorbtionseigenschaft) (2)

führt schließlich auf folgende 9 Minimalschnitte (Die Elemente je einer Matrixzeile stellen die Komponenten eines Minimalschnittes dar):

EBS
EBT
MT, MS
MT, AG
NE, MS
NE, AG
G, GS
G, MT
G, NE

Die Beziehung (1) kommt dann zur Anwendung, wenn innerhalb eines Minimalschnittes im Ablauf des Algorithmus die gleiche Komponente oder Gatter öfters auftritt. Die Beziehung (2) kann dagegen zum Aussortieren nicht minimaler oder mehrmals gefundener Schnitte benutzt werden, d.h. z.B. von drei Zeilen

x_1, x_2
x_1, x_2, x_3
x_1, x_2

bleibt bei Anwendung der Beziehung (2) lediglich die Zeile x_1, x_2 übrig.

Anmerkung: Falls der untersuchte Fehlerbaum keine Wiederholungen bezüglich Gatter bzw. Komponenten aufweist, d.h. die Fehlerbaumkomponenten und -Gatter treten nur an einer Stelle im Fehlerbaum vor, so brauchen die eben aufgeführten Reduktionsbeziehungen nicht angewandt werden. In diesem Fall liefert nämlich der Algorithmus direkt die Minimalschnitte des untersuchten Fehlerbaums.

Zu erwähnen sei abschließend, daß der hier vorgestellte Algorithmus auch zur Auffindung der Minimalphade eines Fehlerbaums erfolgreich angewandt werden kann. Hierzu braucht lediglich der duale Fehlerbaum behandelt werden.

2.3 Berechnung der Zuverlässigkeitsmerkmale von Minimalschnitten unter Berücksichtigung der meistgebräuchlichen Komponenteninstandsetzungsmodelle

2.3.1 Allgemeine Zusammenhänge zwischen den Kennwerten eines Systems und seiner Minimalschnitte

Sind die Minimalschnitte einer Struktur (Fehlerbaum) identifiziert, so laßen sich über das Inklusions-Exklusionsprinzip die wichtigsten Systemwerte in Abhängigkeit der Kennwerte der Minimalschnitte ausdrücken.
Bezeichnet man mit $\overline{R}(t)$ die Systemausfallwahrscheinlichkeit und mit $\overline{A}(t)$ die Systemunverfügbarkeit zum Zeitpunkt t, so gilt

$$\overline{R}(t) \leq \sum_{i=1}^{M} \overline{R}_i(t) \qquad (3)$$

$$\overline{A}(t) \leq \sum_{i=1}^{M} \overline{A}_i(t) \qquad (4)$$

wobei $\overline{R}_i(t)$ die Ausfallwahrscheinlichkeit, $\overline{A}_i(t)$ die Unverfügbarkeit des Minimalschnittes i zum Zeitpunkt t und M die Anzahl der vorhandenen Minimalschnitte bedeutet.
Bei technischen Systeme ist in der Regel die Wahrscheinlichkeit, daß Systemausfälle durch gleichzeitigen Ausfall mehrerer Minimalschnitte verursacht werden, vernachlässigbar, so daß die oben angegebenen Beziehungen ausgezeichnete Näherungen darstellen. Prinzipiell können selbstverständlich auch höhere Terme der Inklusions-Exklusionsbeziehung herangezogen werden, womit schärfere Schranken zu gewinnen wären.
Bei einem System mit M Minimalschnitten müßten allerdings $\binom{M}{2}$ zusätzliche Terme berechnet werden, allein um die zweite Doppelsumme bilden zu können. Bei M=1000 würde dies ca. eine halbe Million Terme bedeuten. Aus diesem Grunde in Verbindung mit der

Tatsache, daß in den meisten Fällen die Beziehungen (3) und (4) für die praktischen Belange ausreichend genau sind, beschränken sich analytische Programme meistens auf die Auswertung der Einfachsumme der Inklusions-Exklusions-Beziehung.

2.3.2 Berechnung der Kennwerte eines Minimalschnittes

Die Beziehungen (3) und (4) erlauben eine Verlagerung der Problematik der Berechnung von Zuverlässigkeitsmerkmalen von der Systemebene in die Ebene der Minimalschnitte, was eine wesentliche Vereinfachung darstellt.
Im vorliegenden Abschnitt werden Berechnungsvorschriften für relevante Zuverlässigkeitsmerkmale von Minimalschnitten als algebraische Ausdrücke der Nichtverfügbarkeit und der Ausfallhäufigkeitsdichtefunktion der Systemelemente aufgeführt. Da diese zwei Größen für eine Vielzahl von Instandsetzungsmodelle leicht angebbar sind (siehe auch Abschnitt 2.3.3), zeichnen sich die hergeleiteten Berechnungsvorschriften neben einer guten Genauigkeit auch durch eine große Flexibilität aus.
Bei den folgenden Ausführungen wird bezüglich des Ausfall- und Reparaturverhaltens der Systemkomponenten Unabhängigkeit vorausgesetzt.

2.3.2.1 Unverfügbarkeit eines Minimalschnittes

Die Unverfügbarkeit $\bar{A}_i(t)$ eines Minimalschnittes c_i bestehend aus k Komponenten berechnet sich bei vorausgesetzter Unabhängigkeit zu

$$\bar{A}_i(t) = \prod_{j=1}^{k} \bar{A}_{ij}(t) \qquad (5)$$

wobei $\bar{A}_{ij}(t)$ die Unverfügbarkeit der Komponente j bedeutet.
Mit der Beziehung (5) ist also auch der Minimal- bzw. der Maximalwert (der z.B. zur Beurteilung der Güte von Bereitschaftssystemen herangezogen wird) berechenbar.
Ebenfalls kann der stationäre Wert $\bar{A}_i(t \to \infty)$ berechnet werden, wenn man für $\bar{A}_{ij}(t)$ die stationären Unverfügbarkeitswerte der

Komponenten $\overline{A}_{ij}(t\to\infty)$, $j=1,2,\ldots,k$ einsetzt.
Schließlich erhält man durch Integration die für Risikofragestellungen interessierende mittlere Unverfügbarkeit $\overline{A}_i(T)$ innerhalb des Beobachtungsintervalls $(0,T)$ zu

$$\overline{A}_i(T) = \frac{1}{T}\int_0^T \overline{A}_i(t)\,dt = \frac{1}{T}\int_0^T \prod_{j=1}^{k} \overline{A}_{ij}(t)\,dt \qquad (6)$$

2.3.2.2 Ausfallwahrscheinlichkeit eines Minimalschnittes

Auch für die verhältnismäßig einfache Struktur eines Parallelsystems (bzw. eines Minimalschnittes) ist die Berechnung der Ausfallwahrscheinlichkeit im allgemeinen nicht exakt durchführbar.
Die Alternative ist nur in Näherungsverfahren zu suchen, deren Genauigkeit jedoch sehr unterschiedlich ist und z.B. stark vom jeweiligen Datensatz (Ausfallraten, Reparaturraten) der Komponenten abhängt.
Den effektivsten und flexiblesten Weg, speziell im Hinblick auf EDV-Anwendung, bietet die Approximation der Ausfallwahrscheinlichkeit $\overline{R}_i(t)$ über die Ausfallhäufigkeit $M_i(t)$.
Generell gilt die Ungleichung

$$\overline{R}_i(t) \leq \text{Min}\left\{1,\ M_i(t)\right\} \qquad (7)$$

Da bei technischen Systemen die Wahrscheinlichkeit von mehrmaligen Ausfällen eines Minimalschnittes innerhalb des Betrachtungszeitraumes in der Regel vernachlässigbar ist, gilt mit für praktische Belange ausreichender Genauigkeit

$$\overline{R}_i(t) \approx M_i(t)$$

Eine Beziehung, die die Berechnung der Größe $M_i(t)$ eines Minimalschnittes ermöglicht wurde erstmalig in /9/ formuliert.
Sie lautet

$$M_i(t) = \int_0^t m_i(x)dx = \int_0^t \sum_{j=1}^{k} m_{ij}(x) \prod_{\substack{l=1 \\ l\neq j}}^{k} \bar{A}_{il}(x)dx \qquad (8)$$

wobei

$m_i(x) = \sum_{j=1}^{k} m_{ij}(x) \prod_{\substack{l=1 \\ l\neq j}}^{k} \bar{A}_{il}(x)$: die Ausfallhäufigkeitsdichte des Minimalschnittes i

k : Anzahl der Komponenten des betrachteten Minimalschnittes

$\bar{A}_{ij}(x)$: Unverfügbarkeit der Komponente j

$m_{ij}(x)$: Ausfallhäufigkeit der Komponente j

bedeuten.

Die grundlegende Beziehung (8) leitet sich aus der wahrscheinlichkeitstheoretischen Überlegung ab, daß ein Ausfall eines Minimalschnittes innerhalb (t, t+dt) dann eintritt, wenn eine seiner Komponenten, z.B. j, in (t,t+dt) ausfällt (die Wahrscheinlichkeit dafür ist $m_{ij}(t)dt$) und alle anderen Komponenten bereits vor t ausgefallen waren $\left(\prod_{\substack{l=1 \\ l\neq j}}^{k} \bar{A}_{il}(x)\right)$, summiert über alle Möglichkeiten.

Ihre große praktische Bedeutung liegt darin, daß sie die Ausfallhäufigkeitsdichte eines Minimalschnittes in Abhängigkeit der Unverfügbarkeit und der Ausfallhäufigkeitsdichte seiner Komponenten ausdrückt, womit die Problematik von der Ebene der Minimalschnitte in die Komponentenebene verlagert wird.

Im Abschnitt 2.3.3 werden die Größen $m_{ij}(t)$ und $\bar{A}_{ij}(t)$ für die gebräuchlisten Komponenteninstandsetzungsmodelle angeben. Dies erlaubt über (8) die Bestimmung der Größe $m_i(t)$. Die Häufigkeitsfunktion $M_i(t)$ bzw. die Ausfallwahrscheinlichkeit $\bar{R}_i(t)$ errechnet man am zweckmäßigsten durch nummerische Integration der $m_i(t)$-Funktion.

2.3.3 Zuverlässigkeitskenngrößen bei verschiedenen Instandsetzungsmodellen

Im Abschnitt 2.3.2 sind Beziehungen abgeleitet worden, die die wichtigsten Kennwerte eines Minimalschnittes in Abhängigkeit folgender zwei Größen

- Ausfallhäufigkeitsdichte $m_{ij}(t)$
- Unverfügbarkeit $\overline{A}_{ij}(t)$

seiner Komponenten ausdrücken.
Im vorliegenden Abschnitt werden diese Größen für die gebräuchlichen Instandsetzungsmodelle ermittelt. Prinzipiell gelten die angegebenen Formeln für beliebig verteilte Lebens- bzw. Reparaturzeiten. Wegen ihrer großer praktischen Bedeutung wird der Fall einer Exponentialverteilung explizit behandelt.

2.3.3.1 Nicht reparierbare Komponenten

In diesem Fall wird das Komponentenverhalten durch die Verteilungsfunktion der Lebensdauer $F_{ij}(t)$ vollständig beschrieben.
Es gilt

$$\overline{A}_{ij}(t) = \overline{R}_{ij}(t) = F_{ij}(t) \qquad (9)$$

und

$$m_{ij}(t) = f_{ij}(t) = \frac{d}{dt}\left\{F_{ij}(t)\right\} \qquad (10)$$

Bei Verwendung von Exponentialverteilungen erhällt man trivialerweise

$$\overline{A}_{ij}(t) = 1-e^{-\lambda_{ij}t}$$

und

$$m_{ij}(t) = \lambda_{ij} \cdot e^{-\lambda_{ij}t}$$

wobei λ_{ij} die konstante Ausfallrate der Komponente j bedeutet.

2.3.3.2 Reparierbare, selbstmeldende Komponenten

Das Komponentenverhalten wird hier durch die Verteilungsfunktionen der Lebensdauer $f_{ij}(t)$ und der Reparaturdauer $g_{ij}(t)$ bestimmt. Man nennt den zugrundeliegenden Prozeß der sich abwechselnden Ausfälle und Erneuerungen der Komponenten einen alternierenden Erneuerungsprozeß.
Die Unverfügbarkeit $\bar{A}_{ij}(t)$ und die Ausfallhäufigkeitsdichte $m_{ij}(t)$ lassen sich nach mehreren Methoden bestimmen. (Erneuerungstheorie, Markoff-Behandlung).

Erneuerungstheoretische Überlegungen führen zu folgenden Integralgleichungen für die zwei hier interessierenden Größen

$$\bar{A}_{ij}(t) = \int_0^t m_{ij}(u)\left[1-G_{ij}(t-u)\right]du \qquad (11)$$

und

$$m_{ij}(t) = f_{ij}(t) + \int_0^t \int_0^{t-x} m_{ij}(t-x-u).f_{ij}(x).g_{ij}(u)\,dx\,du \qquad (12)$$

Beide Integralgleichungen sind vom Faltungstyp und lassen sich in den meisten Fällen mühelos durch Anwendung der Laplace-Transformation lösen.
Liegen exponentialverteilte Lebens- und Reparaturzeiten vor, so ergibt sich

$$\bar{A}_{ij}(t) = \frac{\lambda_{ij}}{\lambda_{ij}+\mu_{ij}}\left\{1-e^{-(\lambda_{ij}+\mu_{ij})t}\right\}$$

und

$$m_{ij}(t) = \frac{\lambda_{ij}\cdot\mu_{ij}}{\lambda_{ij}+\mu_{ij}}\left\{1+\frac{\lambda_{ij}}{\mu_{ij}}\,e^{-(\lambda_{ij}+\mu_{ij})t}\right\}$$

wobei λ_{ij} die konstante Ausfallrate und μ_{ij} die konstante Reparaturrate der Komponente j bedeuten.

2.3.3.3 In regelmäßigen Zeitabständen Tw inspizierte Komponenten

Dieses in der Praxis bezüglich Bereitschaftskomponenten sehr verbreitetes Modell geht davon aus, daß eine Komponente j in regelmäßigen Zeitabständen Tw_{ij} inspiziert (funktionsgetestet) wird und daß unmittelbar nach einer erfolgreichen Inspektion die Komponente wie neu zu behandeln ist.
Geht man weiterhin davon aus, daß

- während der Inspektionsdauer die Verfügbarkeit der Komponente nicht beeinträchtigt wird (eine Annahme, die bei Inspektionsdurchführung speziell von in Bereitschaft stehenden Sicherheitssystemen weitgehend realisiert wird)

- die mittlere Reparaturdauer $MTTR_{ij}$ klein gegenüber dem Inspektionsintervall ist ($MTTR_{ij} \ll Tw_{ij}$)

so ergibt sich für die gesuchten Größen

$$\bar{A}_{ij}(t) = F_{ij}(t-nTw_{ij})$$

$$m_{ij}(t) = f_{ij}(t-nTw_{ij})$$

für $nTw_{ij} \leq t \leq (n+1)Tw_{ij}$

bzw. für exponentialverteilte Lebensdauern trivialerweise

$$\bar{A}_{ij}(t) = 1-e^{-(t-nTw_{ij})\cdot\lambda_{ij}}$$

$$m_{ij}(t) = \lambda_{ij} e^{-(t-nTw_{ij})\cdot\lambda_{ij}}$$

für $nTw_{ij} \leq t < (n+1)Tw_{ij}$

In der Abbildung 5 sind die beiden Größen schematisch dargestellt.
Der periodische Charakter ist eindeutig zu erkennen

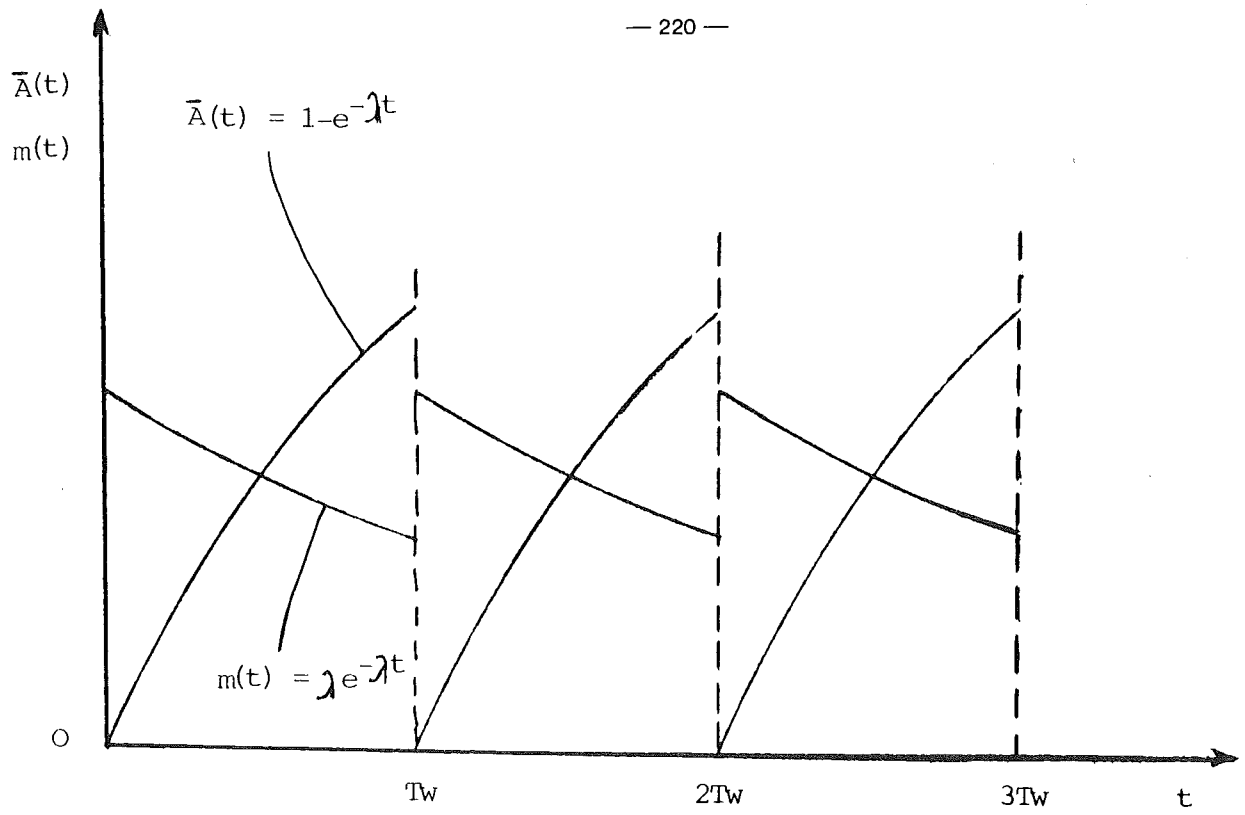


Bild 5: Verlauf der Unverfügbarkeit A(t) und der Häufigkeitsdichtefunktion m(t) einer gewarteten Komponente

In Ausnahmefällen, wo die eingangs gemachten Voraussetzungen nicht zutreffen, nehmen die Beziehungen (13) und (14) eine komplexere Gestalt an. Eine Ableitung für den Fall, daß

- eine Reparatur eine Zeit τ_{ij} dauert
- bei der Inspektion die betreffende Komponente während der Zeit Θ_{ij} unverfügbar bleibt

is t in /10/ durchgeführt.
Ohne Probleme läßt sich im Rahmen der hier vorgestellten Vorgehensweise auch eine konsekutive Durchführung der Inspektion redundanter Komponenten rechnerisch erfassen.
In der Praxis werden redundante, gleichartige Komponenten (z.B. 4x50% Diesel, 3x100% Pumpen etc.) nicht simultan, sondern konsekutiv inspiziert. Man erreicht damit eine merkliche Verbesserung der Verfügbarkeit von Bereitschaftssystemen.
Bei k redundanten Komponenten mit einheitlichem Inspektionsintervall Tw wird somit in Abständen von Tw/k konsekutiv jeweils eine Komponente inspiziert. Dies ergibt für die interessierenden Kennwerten der innerhalb Tw als j-te (j=1,2,..,k) inspi-

zierten Komponente.

$$\overline{A}_{ij}(t) = \begin{cases} F_{ij}(t) & \text{für } 0 \leq t < (j-1)Tw/k \\ & \\ F_{ij}\left(t - \frac{(j-1)Tw}{k} - nTw\right) & \text{für } (j-1)\frac{Tw}{k} + nTw \leq t < (j-1)\frac{Tw}{k} + (n+1)Tw \end{cases} \quad (15)$$

und

$$m_{ij}(t) = \begin{cases} f_{ij}(t) & \text{für } 0 \leq t < (j-1)Tw/k \\ & \\ f_{ij}\left(t - \frac{(j-1)Tw}{k} - nTw\right) & \text{für } (j-1)\frac{Tw}{k} + nTw \leq t < (j-1)\frac{Tw}{k} + (n+1)Tw \end{cases} \quad (16)$$

2.4 Abschneideverfahren

Wie bereits erwähnt, ist zur effizienten Berechnung von Systemen mit mehr als einigen tausend Minimalschnitten ein wirksames Abschneide verfahren notwendig, welches nicht signifikante Schnitte noch <u>während ihrer Entwicklung</u> erkennt und eliminiert.
Bei einigen bekannten Verfahren wird dazu der Redundanzgrad eines Minimalschnittes zugrundegelegt. Dabei werden alle Schnitte, deren Komponentenzahl einen vor der Rechnung festgelegten Wert k überschreitet, nicht betrachtet. Da im allgemeinen nicht gewährleistet ist, daß z.B. ein Minimalschnitt mit l Komponenten weniger signifikant als einer mit s Komponenten (s<l) ist, kann diese Vorgehensweise speziell bei Systemen, deren Komponenten stark unterschiedliche Zuverlässigkeitsmerkmale aufweisen, zu erheblichen Fehlern führen.
Der hier vorgestellte Algorithmus ermöglicht die Anwendung eines weitgehend adäquaten Verfahrens. Dabei wird die Signifikanz eines Schnittes anhand relevanter quantitativer Merkmale beurteilt, die während des Algorithmenablaufs auch für unfertige Schnitte laufend berechnet werden.
Bezeichnet man mit c_i^j einen solchen unfertigen Schnitt, der bereits aus j Komponenten besteht, so folgt bei der Hinzunahme im Ablauf der Algorithmus einer weiteren Komponente j+1 für den momentanen Stand der Häufigkeitsdichtefunktion $m_i^{j+1}(t)$ dieses Schnittes (siehe Beziehung (8))

$$m_i^{j+1}(t) = m_i^j(t) \cdot \overline{A}_{j+1}(t) + m_{j+1}(t) \cdot \overline{A}_i^j$$

bzw. für die Unverfügbarkeit

$$\overline{A}_i^{j+1}(t) = \overline{A}_i^j(t) \cdot \overline{A}_{j+1}(t)$$

wobei $m_{j+1}(t)$ und $A_{j+1}(t)$ die Merkmale der (j+1)-Komponente bedeuten.

Anmerkung: Die Ausfallhäufigkeitdichte kann nach den Ausführungen im Abschnitt 2.3.2.2 als relevantes Merkmal im Rahmen einer Ausfallwahrscheinlichkeitsrechnung zugrundegelegt werden.

Bezeichnet man weiterhin mit $W_m(c_i^{j+1},t)$ bzw. $W_{\overline{A}}(c_i^{j+1},t)$ die Ausfallhäufigkeitsdichte bzw. Unverfügbarkeit des Teilsystems (Teilfehlerbaums), das nach Durchführung des Einsetzens und logischen Ausmultiplizierens der unfertigen Teile (logischen Gatter) des betrachteten Schnittes ensteht, so gilt allgemein

$$m_i^{j+1}(t) \gtrdot W_m(c_i^{j+1},t) \qquad (17)$$

und

$$\overline{A}_i^{j+1}(t) \gtrdot W_{\overline{A}}(c_i^{j+1},t) \qquad (18)$$

Aus den Beziehungen (17) und (18) folgt, daß die Größen $m_i^{j+1}(t)$ und $\overline{A}_i^{j+1}(t)$ eine obere Schranke für die quantitative Signifikanz (abhängig von der zu berechnenden Größe) einer unfertigen Menge c_i^{j+1} darstellen.
Bei Vorgabe einer Zahl ξ können somit alle Schnitte eliminiert werden, deren so ermittelte Größen $m_i^1(t)$ bzw. $\overline{A}_i^1(t)$ kleiner als $\sum_{j=1}^{r} m_j(t) \cdot \xi_m$ bzw. $\sum_{j=1}^{r} \overline{A}_j(t) \xi_{\overline{A}}$ sind, wobei r die Anzahl der jeweils momentan vorliegenden Minimalschnitte, $m_j(t)$ bzw. $\overline{A}_j(t)$ die Merkmale eines bereits vorliegenden Minimalschnittes j bedeuten

und ε_m und $\varepsilon_{\bar{A}}$ frei wählbar sind.
Durch Addition der Kenngrößen m bzw. $\bar{A}$ der abgeschnittenen Mengen erhält man darüberhinaus eine obere Grenze für die quantitative Relevanz der abgeschnittenen Fehlerbaumteile. Sollte der abgeschnittene Teil in der Größenordnung des berechneten Teils sein, so kann die Auswertung mit kleineren Werten ε_m bzw. $\varepsilon_{\bar{A}}$ wiederholt werden. (Bei der Behandlung von Fehlerbäumen technischer Systeme sind Werte von $\varepsilon = 10^{-2} \div 10^{-4}$ ausreichend).
Der große Vorteil einer so gestalteten Abschneideprozedur liegt darin, daß durch die Möglichkeit auch unfertige Schnitte (Schnitte also die sowohl Komponenten als auch Gatter enthalten und somit deren vollständige logische Entwicklung auf eine beträchtliche Anzahl von Minimalschnitten führen würde) kontrolliert aussortieren zu können, die Anzahl der letztendlich zu berücksichtigenden Minimalschnitte und somit die benötigte Rechenzeit und Speicherplatzbedarf drastisch reduziert werden.
Die Effektivität des Verfahrens wird in Abschnitt 2.5 anhand eines praktischen Beispiels vorgeführt.

2.5 Zuverlässigkeitsanalyse eines realistischen Notstromversorgungskonzeptes

Die Leistungsfähigkeit analytischer Verfahren bei der Behandlung komplexer Systeme soll am Beispiel eines möglichen Konzeptes zur Energieversorgung des Nuklearen Entsorgungszentrums (NEZ) aufgezeigt werden /11/.

Systemaufbau und Betriebsweise
Das hier untersuchte Schaltungskonzept ist in Abbildung (6) dargestellt. Die elektrischen Verbraucher des NEZ sind in zwei Bereiche unterteilt, die jeweils durch eine Energiezentrale versorgt werden. Die Energiezentralen sind in sich dreistängig aufgebaut.
Jeder Strang besteht aus einer 10 KV-Normalschiene, einer 10 KV-Notstromschiene, einem Notstromdieselaggregat, einem Dreiwicklertransformator und der zugehörigen Verkabelung.
Die Netzversorgung erfolgt über eine -jeder Energiezentrale zugeordnete- Doppelsammelschiene, die jeweils eine als unabhängig

angesehene Netzeinspeisung hat. Diese wird aus Gründen der Leistungsaufteilung über zwei Schalter geführt. Bei Bedarf kann die Netzversorgung einer Energiezentrale auch über die Kreuzverbindungen durch die andere Doppelsammelschiene erfolgen.
Die Notstromschienen stehen stets alle unter Spannung, von den Normalschienen jeweils nur zwei.

TOP-Ereignis

Unerwünschte Ereignisse sind Ausfälle von sicherheitstechnisch relevanten Funktionen im NEZ. Da die entsprechenden Komponenten alle an die Notstromschienen angeschlossen sind, bedeutet dies für die Ausfallursache Spannungsausfall in erster Linie: Spannungslosigkeit der Notstromschienen. Ausfälle von Komponenten zwischen Notstromschiene und Verbraucher sind demgegenüber von untergeordneter Bedeutung.
Da beide Energiezentralen verschiedene Bereiche versorgen, läßt sich das TOP-Ereignis folgendermaßen definieren:

> Spannunglosigkeit an allen drei Notstromschienen einer der beiden Energiezentralen.

Durchführung der Rechnung

Die Auswertung der Fehlerbäume wurden mit dem analytischen Programm des Instituts für Kerntechnik der TU-Berlin durchgeführt. Errechnet wurde die Eintrittswahrscheinlichkeit des weiter oben angegebenen TOP-Ereignisses, d.h. die Ausfallwahrscheinlichkeit $\bar{R}(t)$.
Als Beobachtungszeitraum wurde 1 Jahr (8760 h) gewählt.
Da in dieser Analyse auf die Ermittlung absoluter Zahlenwerte nicht ankommt, sondern lediglich auf den Nachweis der Leistungsfähigkeit analytischer Methoden auf praktische Fragestellungen, sind Common-Mode-Ausfälle, speziell im Bereich der Dieselaggregate, nicht berücksichtigt. Dadurch sind z.T. auch die sehr kleinen Eintrittswahrscheinlichkeiten zu erklären.
Um den Einfluß der reinen schaltungsspezifischen Komponenten am Gesamtergebnis zu erfassen wurden zwei Varianten durchgerechnet:

Variante 1: Ausfallmöglichkeiten der Energiequellen (Netze, Dieselaggregate) wurden berücksichtigt.

Variante 2: Annahme, daß die Energiequellen während des Untersuchungszeitraums ausfallfrei arbeiten.

Der Vergleich beider Ergebnisse ermöglicht die Beantwortung der Frage, ob eine Verbesserung des Schaltungskonzeptes bei vorgegebener Zuverlässigkeit der Energiequellen noch sinnvoll ist.
Die Ergebnisse der Rechnungen sind in der Tabelle 1 aufgestellt. Man entnimmt daraus, daß das Ergebnis durch das Ausfallverhalten der Quellen dominiert wird, sodaß reine Schaltungsverbesserungen aus Zuverlässigkeitsgesichtspunkten heraus nicht sinnvoll sind. Mitangegeben sind in der Tabelle 1 die Gesamtzahl der Systemschnitte, sowie die benötigte Rechenzeit. Bei der enorm großen Anzahl der vorhandenen Systemschnitte, die im Millionenbereich liegt, sind die günstigen Rechenzeitverhältnisse hauptsächlich auf die Effektivität der in Abschnitt 2.5 angesprochenen Abschneideprozedur zurückzuführen, ohne deren Einsatz eine Berechnung in vertretbaren Rechenzeiten kaum durchzuführen wäre.

3. Simulative Verfahren

3.1 Direkte Simulationsverfahren

Simmulationsverfahren zur Berechnung der Zuverlässigkeitsmerkmale technischer Systeme bestehen im wesentlichen darin, Störabläufe für das betrachtete System zu simulieren, wobei jedesmal aus den statistisch bekannten Verteilungfunktionen der einzelnen Systemelemente mittels eines Zufallsgenerators Ausfallzeiten T_{ij} und Reparaturzeiten R_{ij} sequentiell generiert werden. Bezeichnet man mit $T_{i(j)}$ den Zeitpunkt des j-ten Ausfalls und mit $R_{i(j)}$ den Zeitpunkt der Beendigung der j-ten Reparatur des i-ten Elementes, so gilt

$$T_i(j) = \sum_{k=1}^{j-1} (T_{ik}+R_{ik}) + T_{ij}$$

und

$$R_i(j) = \sum_{k=1}^{j} (T_{ik}+R_{ik})$$

$T_{i(j)}$ und $R_{i(j)}$ legen somit fiktive Zeitpunkte fest, an denen ein einzelnes Element ausfällt bzw. wieder einsatzbereit ist.
In diesem Zusammenhang sei erwähnt, daß bei der Bildung der Ausfall- und Reparaturzeiten eines Elementes die realistischen elementspezifischen Instandsetzungsstrategien sowie sonstige Nebenbedingungen zu berücksichtigen sind. Während z.B. bei selbstmeldenden Elementen R_{ik} der Reparaturzeit im engeren Sinne gleichzusetzen ist, muß bei Komponenten, deren Ausfall lediglich bei einer Inspektion festzustellen ist, das Inpektionsmuster bei der Bildung von R_{ik} berücksichtigt werden. Fällt also eine nicht selbstmeldende Komponente zum ersten Mal im Zeitpunkt t aus und ist die nächste Inspektion zum Zeitpunkt t' fällig, so erhält man für R_{ik}

$$R_{ik} = (t'-t)+R'_{ik}$$

wobei R'_{ik} die eigentliche Reparaturzeit bedeutet.

Beschränkte Reparaturkapazitäten, Wartungsverbote sowie sonstige Abhängigkeiten zwischen den Systemelementen /12/ lassen sich ebenfalls durch eine entsprechende Generierung der Ausfall- und Reparaturzeiten behandeln. Die Erfahrung hat allerdings gezeigt, daß es im Hinblick auf Rechenzeit- und Kapazitätsbedarf nicht ratsam ist, alle denkbaren Nebenbedingungen in einem Programmalgorithmus fest einzubauen. Es empfielt sich deswegen, bei fest zu programmierenden Basisalgorithmus die benötigten Zeiten unter Zugrundelegung der für die meisten Systeme zutreffenden Voraussetzung unabhängiger Komponenten zu generieren. Eine Berücksichtigung spezieller systemspezifischer Nebenbedingungen kann dann meistens durch geringe Modifikationen des Basisalgorithmus erfolgen.
Für die obige Vorgehensweise spricht auch die Tatsache, daß es besonders schwierig ist, die Eigenheiten komplexer Systeme a priori vollständig zu erfassen, so daß in vielen Fällen auch ein sehr verfeinerter Algorithmus zur Untersuchung eines speziellen Systems doch modifiziert werden müßte. Die Möglichkeit, letzteres mit verhältnismäßig geringem Aufwand zu erreichen, stellt den großen Vorteil von Simulationsmethoden dar und eben dies ginge bei der Benutzung eines noch so feinen, aber festen Algorithmus zum Teil verloren.
In der Abb. 7 ist der Ablauf eines Simulationsalgorithmus zur Berechnung der Ausfallwahrscheinlichkeit $\overline{R}(T)$ eines Systems dargestellt. Seine detaillierte Erläuterung findet man in /13/.
Als konsistente Schätzung für die Ausfallwahrscheinlichkeit $\overline{R}(T)$ bekommt man

$$\hat{\overline{R}}(T) = \frac{r}{N}$$

wobei N die Gesamtzahl der Durchläufe (Simulationsspiele) und r die Anzahl der Durchläufe, die zu einem Systemausfall geführt haben, bedeuten.
Durch geringe Modifikationen läßt sich der Algorithmus auch zur Berechnung anderer Zuverlässigkeitsmerkmale verwenden /13/.

3.1.1 Statistische Sicherung und Grenzen des direkten Simulationsverfahrens

Aus dem zentralen Grenzwertsatz errechnet sich das minimal erforderliche N von Simulationsdurchläufen um einen relativen Fehler ε nach

$$\varepsilon = \left| \frac{\hat{\bar{R}} - \bar{R}}{\bar{R}} \right|$$

mit einer Wahrscheinlichkeit von ca. 68% nicht zu übersteigen zu

$$N = \frac{1}{\varepsilon^2} \frac{\sigma^2}{\bar{R}^2}$$

Dabei bedeutet σ^2 die Varianz eines einzelnen Durchlaufs und läßt sich angeben zu (Bernoulli-Spiel)

$$\sigma^2 = \bar{R}(1-\bar{R})$$

woraus für N die Beziehung folgt

$$N = \frac{1}{\varepsilon^2} \cdot \frac{1-\bar{R}}{\bar{R}} \approx \frac{1}{\varepsilon^2} \cdot \frac{1}{\bar{R}} \qquad (19)$$

Zur Untersuchung eines Systems mit einer Ausfallwahrscheinlichkeit von 10^{-6} wären also gemäß dieser Beziehung 10^8 Spiele notwendig, um mit einer Wahrscheinlichkeit von68% eine Angabe mit einem relativen Fehler von höchstens $\pm$ 10% zu gewährleisten. Obwohl die Dauer eines Simulationsdurchlaufs auf einer elektronischen Rechenanlage vom jeweiligen System, insbesondere vom Umfang und Form seiner Strukturfunktion sowie der speziellen statistischen Daten abhängig ist, wäre ein Durchschnittswert von 50 μsec pro Spiel und Komponente, auch auf einer schnellen Rechenmaschine (z.B. CD-6400) eher als optimistisch zu bezeichnen. Unter Zugrundelegung dieses optimistischen Wertes wären zur Untersuchung eines Systems, bestehend aus 100 Elementen, unter den oben erwähnten Annahmen ca. 150 Stunden erforderlich.
Daraus wird ersichtlich, daß die Methode der direkten Simulation bei hohen Genauigkeitsforderungen bzw. bei kleinen Ausfallwahr-

scheinlichkeiten (10^{-4}-10^{-5}) trotz ihrer sonstigen großen Vorteile nicht ohne Modifikation anwendbar ist
Bei vielen technischen Systemen, speziell aber bei solchen, wo ein Versagen Menschenleben in Gefahr bringt (Kernkraftwerke, Luft- und Raumfahrt), werden aber Ausfallwahrscheinlichkeiten in der Größenordnung 10^{-6}-10^{-9} gefordert. Insofern erscheint es notwendig, ein Verfahren zu entwickeln, das auch solche Systeme in vertretbaren Rechenzeiten analysieren kann, zumal solche Verfahren nicht nur zum Nachweis einer erzielten Sicherheit, sondern zunehmend als Konstruktionshilfe in der Projektierungsphase Bedeutung haben.
Aus Beziehung (19) läßt sich unmittelbar folgern, daß nur zwei Möglichkeiten zur Verfügung stehen, um dies zu erreichen:

1. Herabsetzung der Dauer einer Realisierung
2. Herabsetzung der erforderlichen Realisierungen N bei gegebener Genauigkeitsforderung ε, über eine Reduktion der Varianz des Verfahrens.

Zu 1 : Mit dem ersten Punkt beschäftigt sich der Abschnitt 3.1.2

Zu 2 : Mit der für jede Realisierung notwendigen Generierung einer großen Anzahl von Ausfall- und Reparaturzeiten, sowie der mehrfach notwendigen Auswertung der Strukturfunktion sind allerdings der Dauer eines Spiels gewisse Grenzen gesetzt, die auch bei noch so geschickten Algorithmen nicht entscheidend unterschritten werden können. Als Alternative bleibt somit die Varianzreduktion, welche im Abschnitt 3.2 näher untersucht wird.

3.1.2 Maßnahmen zur Herabsetzung der Dauer einer Realisierung

Die zur Abwicklung einer Simulationsrechnung notwendige Zeit wird fast ausschließlich zur Durchführung folgender Prozeduren benötigt:

1. Generierung gleichverteilter Pseudozufallszahlen im Intervall (0,1)
2. Transformation der Zufallszahlen zur Erzeugung der gewünschten Verteilung
3. Sortieren der Zeiten bzw. Aufsuchen der jeweils minimalen

Ausfallzeit

4. Auflösen der logischen Gleichungen (Fehlerbaum)

Eine Rechenzeitersparnis läßt sich hauptsächlich durch Modifikation von Block 2 erzielen, da die Blöcke 1, 3, 4 in ihrem Aufbau entweder trivial sind oder aber fest vorliegen und wenig Spielraum zur Veränderung bieten.
Eine optimale Vorgehensweise zur Erzeugung der Ausfallzeiten für technisch interessante Problemstellungen soll am Beispiel der Exponentialfunktion aufgezeigt werden. Bekanntlich lassen sich exponentiell verteilte Größen T_i mit der Verteilungsfunktion

$$F_i(t) = 1-e^{-t/MTTF_i} \tag{20}$$

durch Auflösen der Beziehung (20) generieren gemäß

$$T_i = -MTTF_i \ln Z_i \tag{21}$$

wobei Z_i eine im Intervall (0,1) gleichverteilte Zufallszahl ist (Ausgabegröße von Block 1).
Da die Berechnung von Logarithmen auf universellen elektronischen Dateverarbeitungsanlagen rechenintensiv ist, ist diese übliche Vorgehensweise nicht optimal. Bei technischen Systemen ist die Zuverlässigkeit der Systemelemente in der Regel so hoch daß sie selten innerhalb (0,T) ausfallen. Erfolgt aber ein Ausfall einer Komponente außerhalb (0,T), so ist auch die absolute Größe ihrer Lebensdauer nicht von Interesse, womit in solchen Fällen das Auflösen von (21) unnötig ist. Es emfielt sich deswegen zur Erzeugung von Ausfallzeiten folgende Prozedur zugrunde zu legen

$$T_i = \begin{cases} -MTTF_i \ln Z_i & \text{für } Z_i < \overline{R}_i(T) \\ > T & \text{sonst} \end{cases} \tag{22}$$

wobei $\overline{R}_i(T) = 1-e^{-T/MTTF_i}$ die Ausfallwahrscheinlichkeit der jeweiligen Komponente im betrachteten Intervall (0,T) ist.
Die oben angegebene Prozedur erlaubt also, das rechenintensive Auflösen der Beziehung (21) nur auf die Fälle zu beschränken, bei denen Systemelemente im betrachteten Intervall ausfallen

also nur, wenn die absolute Größe T_i von Interesse ist, und ist ohne weiteres auf beliebige Verteilungsfunktionen anwendbar. Zusätzlich wird dadurch die Anzahl der Eingänge der Minimier- bzw. Sortieralgorithmen drastisch verkleinert (Ausfallzeiten, die größer sind als T brauchen in dem betreffenden Spiel nicht weiter betrachtet zu werden), was einen weiteren großen Gewinn mit sich bringt.
Ein weiterer, speziell bei Systemen mit reparierbaren Komponenten zusätzlicher Gewinn läßt sich durch frühzeitiges Abbrechen von Simulationsdurchläufen, die nicht zum Eintreffen des untersuchten Ereignis führen können, erzielen. Bedenkt man, daß bei technischen Systemen lediglich ein minimaler Bruchteil der insgesamt durchgeführten Spiele zum Systemausfall führt, so wird der potentielle Gewinn bei einem frühzeitigen Abbrechen unwesentlicher Spiele evident.
Es sei mit A das Ereignis von mindestens einem Systemausfall innerhalb (O,T) bezeichnet. Weiterhin bezeichnet man mit B das Ereignis von mindestens einem Systemausfall innerhalb (O,T) unter der Annahme, daß die Systemelemente nicht reparierbar sind. Da offensichtlicherweise A in B vollständig enthalten ist, gilt die Verknüpfung:

$$A \cap \overline{B} = \emptyset$$

Daraus läßt sich folgern, daß alle Spiele, bei denen das System trotz der Annahme nicht reparierbarer Elemente intakt bleibt, nicht weiter verfolgt zu werden brauchen, sondern gleich abgebrochen werden können.
Der zugrundezulegende Algorithmus zur Berücksichtigung der oben beschriebenen Gegebenheiten lautet:

1. Berechnung der Ausfallwahrscheinlichkeiten $\overline{R}_i(T)$, $i=1,\ldots,n$ der einzelnen Systemelemente
2. Erzeugung von n gleichverteilten Zufallszahlen Z_i, $i=1,\ldots,n$
3. Falls $Z_i < \overline{R}_i(T)$, $i=1,\ldots,n$ soll die Zustandsvariable x_i der Komponenten i "ausgefallen" gesetzt werden, andernfalls muß x_i intakt bleiben

4. Mit dem unter Punkt 3. gewonnenen Werten des Zustandsvektors $\underline{x}$ ist die Strukturfunktion $y=\varphi(\underline{x})$ (d.h. der Fehlerbaum) aufzulösen. Fällt dabei das System aus, müssen entsprechend der Ausführungen in diesem Abschnitt für die ausgefallenen Komponenten Ausfallzeiten generiert werden. Dabei können die gleichen Zufallszahlen benutzt werden. Erfolgt aber kein Systemausfall, kann das Spiel abgebrochen werden. Der hier beschriebene Algorithmus kann problemlos an dem Simulationsprogramm unmittelbar vor den Sortierprozeduren der Ausfallzeiten eingefügt werden. Der durch seine Anwendung erzielbare Rechenzeitgewinn beträgt abhängig vom spezifischen System einen Faktor 5 bis über 20.

3.2 Varianzreduzierende Simulationsmethoden

Die Idee einer Varianzreduktion im Zusammenhang mit Monte-Carlo Simulationsverfahren ist nicht neu. Detaillierte Zusammenstellungen der bekanntesten und effizientesten Verfahren, wie z.B. Importance Sampling, Benutzung von korrelierten Hilfsvariablen, Benutzung von antithetischen Variablen, geschichtete Stichproben usw. finden sich in /14,15,16,17/.
Leider lassen sich die meisten Verfahren nur auf eindimensionale Probleme ohne weiteres mit Erfolg anwenden und verlieren einen großen Teil der Wirksamkeit, falls sie auf mehrdimensionale Modelle, die ja gerade das Haupteinsatzfeld von Simulationsmethoden bilden, angewandt werden.
Generell läßt sich sagen, daß bis heute keine Methode existiert, deren Anwendung auf verschidenartig strukturierte mehrdimensionale Modelle, eine Varianzreduktion garantiert. Es läßt sich jedoch absehen, daß eine, dem speziellen Problem zugeschnittene Anwendung einiger Verfahren, einen entscheidenden Gewinn mit sich bringen wird.
Für das vorliegende Modell scheint das Verfahren der gewichteten Stichproben (Importance Sampling) am geeignetsten,
Seine Hauptvorteile sind eine bei geschickter Anwendung hohe Effizienz, sowie die prinzipiell uneingeschränkte Einsatzfähigkeit auf mehrdimensionale Probleme.
Die hauptsächlichen Schwierigkeiten liegen in der Wahl einer varianzreduzierenden Funktion.

3.2.1 Das Verfahren der gewichteten Stichproben (Importance Sampling)

Die prinzipielle Vorgehensweise soll am Beispiel der Ausfallwahrscheinlichkeit $\bar{R}(T)$ im folgenden erläuter werden.
Bezeichnet man mit $\beta(\underline{\omega})$ eine Indikatorvariable mit der Eigenschaft

$$\beta(\underline{\omega}) = \begin{cases} 1 & \text{System fällt innerhalb } (0,T) \text{ aus} \\ 0 & \text{sonst} \end{cases}$$

so läßt sich die Ausfallwahrscheinlichkeit als Erwartungswert von $\beta(\underline{\omega})$ darstellen laut

$$\bar{R}(T) = E\{\beta(\underline{\omega})\} = \int_{(\underline{\omega})} \beta(\underline{\omega}) \cdot f(\underline{\omega}) \cdot d\underline{\omega} \qquad (23)$$

wobei die Zufallsmatrix $\underline{\omega}$ die Lebens- und Reperaturzeiten aller m Systemelemente (Fehlerbaumelemente) beinhaltet und $f(\underline{\omega})$ die korrespondierende Verteilungsdichtefunktion bedeutet und von den Verteilungsdichtefunktionen der Lebens- und Reparaturzeiten der Systemkomponenten abhängt.
Eine mögliche Realisierung der Matrix $\underline{\omega}$ lautet sinngemäß

$$\underline{\omega} =: \begin{pmatrix} T_{11}, R_{11}, T_{12}, R_{12}, \ldots\ldots\ldots \\ T_{21}, R_{21}, T_{22}, R_{22}, \ldots\ldots\ldots \\ \cdot \\ \cdot \\ \cdot \\ T_{m1}, R_{m1}, T_{m2}, R_{m2}, \ldots\ldots\ldots \end{pmatrix}$$

mit T_{ij} die j-te Lebensdauer und R_{ij} die j-te Reparaturzeit der i-ten Komponente.
Der im Abschnitt 3.1 erläuterte Algorithmus läuft auf die Berechnung der Gleichung (23) hinaus. Die korrespondierende Varianz σ^2 des direkten Verfahrens errechnet sich wegen der Idempotenseigenschaft von $\beta(\underline{\omega})$ zu

$$\sigma^2 = E\left\{(\beta(\underline{\omega}) - \bar{R}(T))^2\right\} = E\left\{\beta(\underline{\omega})^2\right\} - \bar{R}(T)^2$$
$$= E\left\{\beta(\underline{\omega})\right\} - \bar{R}(T)^2 = \bar{R}(T)\,(1-\bar{R}(T))$$

Führt man eine neue Verteilungsdichtefunktion $f^*(\underline{\omega})$ ein und erweitert man die Beziehung (23) zu

$$R(T) = \int_{(\underline{\omega})} \beta(\underline{\omega}) \cdot f(\underline{\omega}) \cdot d\underline{\omega} = \int_{(\omega)} \underbrace{\beta(\underline{\omega}) \cdot \frac{f(\underline{\omega})}{f^*(\underline{\omega})}}_{=\beta^*(\underline{\omega})} \cdot f^*(\underline{\omega}) \cdot d\underline{\omega}$$

$$= \int_{(\omega)} \beta^*(\underline{\omega}) \cdot f^*(\underline{\omega}) \cdot d\underline{\omega} \qquad (24)$$

so liefert $\beta^*(\underline{\omega})$ ebenfalls eine ewartungstreue Schätzung für die Ausfallwahrscheinlichkeit $\bar{R}(T)$. D.h. generiert man die Ausfall- und Reperaturzeiten über $f^*(\underline{\omega})$ statt $f(\underline{\omega})$ und wichtet die auftretenden Systemausfälle mit $f(\underline{\omega})/f^*(\underline{\omega})$ statt mit 1 wie bisher im direkten Verfahren, so gilt

$$\lim_{N\to\infty} \hat{\bar{R}}^*(T) = \lim_{N\to\infty} \hat{\bar{R}}(T) = \bar{R}(T) \qquad (25)$$

Während hierbei die Erwartungswerte übereinstimmen, trifft dies für die Streuung der zwei Verfahren nicht zu, wie sich leicht sehen läßt: Da $\beta^*(\underline{\omega})$ nicht mehr idempotent ist, gilt für die Varianz des gewichteten Verfahrens

$$\sigma^{*2} = E^*\left\{\beta^{*2}\right\} - E^*\left\{\beta^*\right\}^2 = E^*\left\{\beta^{*2}\right\} - \bar{R}(T)^2 \qquad (26)$$

welche im allgemeinen verschieden von der Varianz $\sigma^2 = \bar{R}(T)\,(1-\bar{R}(T))$ des direkten Verfahrens ist. $E^*\{\cdot\}$ bedeutet dabei eine Erwartungswertsbildung unter Zugrundelegung der Dichtefunktion $f^*(\underline{\omega})$.

Die benötigten Durchläufe im direkten bzw. im gewichteten Fall läßen sich in Relation zu den korrespondierenden Varianzen laut

$$\frac{N}{N^*} = \frac{\sigma^2}{\sigma^{*2}}$$

Gelingt es nun, eine Funktion $f^*(\underline{\omega})$ zu finden, die auf $\sigma^{*2} < \sigma^2$ führt, so ist bei gegebener Genauigkeitsforderung die nötige Anzahl N^* von Durchläufen in gewichteten Verfahren um den Faktor $\frac{\sigma^2}{\sigma^{*2}} > 1$ kleiner.
Da im Endeffekt nicht eine Varianzreduktion allein, sondern primär eine Rechenzeitreduktion erstrebt wird, soll zusätzlich der im zweiten Verfahren wahrscheinlich auftretende Mehraufwand, den durch die Varianzreduktion erzielten Gewinn nicht übersteigen. Bezeichnet man mit a den Aufwand im direkten und mit a^* den Aufwand im gewichteten Verfahren, so liefert

$$E = \frac{a.\sigma^2}{a^*\sigma^{*2}} = \frac{a.N}{a^*.N^*}$$

ein solides, allerdings von der benutzten Rechenanlage abhängiges Maß zur Beurteilung der Effizienz der Verfahren. Im Sinne einer Rechenzeitreduktion soll $E > 1$ sein.

3.2.2 Zur Wahr der Dichtefunktion $f^*(\underline{\omega})$

Wie im Abschnitt 3.2 erwähnt wurde, gibt es noch keine allgemeine, praktisch anwendbare Theorie, die eine optimale Wahl der Funktion $f^*(\underline{\omega})$ für mehrdimensionale Modelle gestattet.
Zwar wäre es z.B. bei einer Ausfallwahrscheinlichkeitsberechnung durch eine Wahl von $f^*(\underline{\omega})$ zu

$$f^*(\underline{\omega}) = \left\{ \beta(\underline{\omega}) \frac{f(\underline{\omega})}{\overline{R}(T)} \right. \qquad (27)$$

möglich, die Varianz σ^{*2} des gewichteten Verfahrens in diesem Fall wegen

$$\sigma^{*2} = \overset{*}{E}\left\{\left(\beta^{*} - \overset{*}{E}(\beta^{*})\right)^{2}\right\} = \overset{*}{E}\left\{\left(\bar{R}(T) - \bar{R}(T)\right)^{2}\right\} = 0$$

zu eliminieren, womit das genaue Ergebnis in einem einzigen Spiel erhältlich wäre. Praktisch ist dies offensichtlich aber nicht durchführbar, da hierzu der gesuchte Mittelwert (in diesem Fall die Systemausfallwahrscheinlichkeit) bekannt sein müßte, womit sich eine Simulationsrechnung erübrigen würde.
Allerdings läßt sich aus der Struktur der Dichtefunktion nach (27) eine intuitiv verständliche Eigenschaft, welche realisierbare Dichtefunktionen besitzen müssen, um eine Varianzreduktion zu bewirken, erkennen; nämlich die Eigenschaft Zufallsmatrizen mit $\beta(\underline{\omega}) = 1$ eine größere Eintrittswahrscheinlichkeit zuzuordnen, als sie in Wirklichkeit besitzen und somit zwangsläufig Matrizen $\underline{\omega}$ mit $\beta(\underline{\omega}) = 0$ mit einer niedrigeren Wahrscheinlichkeit, im Optimalfall mit Wahrscheinlichkeit 0, zu belegen.
Ein Beweis, daß diese Eigenschaft sogar eine notwendige Bedingung für jede varianzreduzierende Dichtefunktion $f^{*}(\underline{\omega})$ ist, findet sich in/13/.
Leider ist diese Bedingung keinesfalls hinreichend, eine Tatsache die man anhand eines eindimensionalen Beispiels leicht verifizieren kann /13/.
Zur Problematik der Wahl von effektiven Dichtefunktionen $f^{*}(\underline{\omega})$ bei mehrdimensionalen Fragestellungen (wie sie bei der Auswertung von Fehlerbäumen auftreten) kann im Rahmen dieses Vortrages nicht eingegangen werden und wird auf die Literatur verwiesen /18, 13/.
Trotzdem sollte die Dichtefunktion

$$f_i^{*}(t) = \begin{cases} \bar{R}_i^{\,r-1}(T) \cdot f_i(t) & t \leq T \\ \dfrac{1-\bar{R}_i^{\,r}(T)}{1-\bar{R}_i(T)} \cdot f_i(t) & t > T \end{cases} \qquad (29)$$

mit

$f_i(t)$: Verteilungsdichtefunktion der Lebensdauer der i-ten Komponente

r : Wichtungsfaktor ; $0 \leqslant r \leqslant 1$

T : Beobachtungszeit

die zu sehr guten Ergebnissen in der Praxis führt, abschliessend erwähnt werden. Ihr Hauptvorteil liegt daran, daß sie Ereignisse, die im normalen (ungewichteten) Fall gleichwahrscheinlich sind, auch im gewichteten Fall weitgehend gleichwahrscheinlich beläßt. Dies läßt sich am ehesten klarmachen, wenn man zwei Minimalschnitte c_1 und c_2 mit der Komponenten

c_1 : 1,2

c_2 : 3,4,5,6

betrachtet.
Bei der Zugrundelegung der Dichtefunktion (29) ergibt sich die Ausfallwahrscheinlichkeit dieser Minimalschnitte bei vernachlässigung intakter Komponenten im gewichteten Verfahren zu

$$\overline{R}^{*}_{c_1} = \overline{R}^{\,r}_{c_1} = (\overline{R}_1 . \overline{R}_2)^r$$

und

$$\overline{R}^{*}_{c_2} = \overline{R}^{\,r}_{c_2} = (\overline{R}_3 . \overline{R}_4 . \overline{R}_5 . \overline{R}_6)^r$$

sodaß aus $\overline{R}_{c1} = \overline{R}_{c_2}$ auch $\overline{R}^{*}_{c_1} = \overline{R}^{*}_{c_2}$ folgt.

Eine lineare Wichtung der Ausfallwahrscheinlichkeiten der einzelnen Komponenten würde dagegen, speziell bei stark unterschiedlichen Redundanzgraden der einzelnen Minimalschnitte, zu großen Verzerrungen im gewichteten Fall führen.

Literatur

/1/ Kim, Y.H., Case, K. E., Ghare, P. M.:
A Method for Computing Complex System Reliability.
IEEE Transactions on Reliability Vol. R-21, No. 4, November

/2/ Jensen, P., Bellmore, M.:
An Algorithm to Determine Reliability of a Complex System.
IEEE Transactions on Reliability Vol. R-18, No. 4, November 1

/3/ Nelson, A., Batts,J., Beadles, R.:
A Computer Programm for Approximating System Reliability
IEEE Transactions on Reliability Vol. R-19, No. 2, May

/4/ Reinschke :
Zuverlässigkeit von Systemen.
Band 1, VEB-Verlag Technik, Berlin 1973

/5/ Fussel, J., Vesely, W.:
A New Methodology for Obtaining Cut Sets for Fault Trees Trans.
Am Nucl. Soc. 15, 262 (1972)

/6/ Kamarinopoulos, L., Richter, G.:
KARI- ein neues analytisches Programm zur Berechnung von Zuverlässigkeitsmerkmalen technischer Systeme.
Angewandte Informatik 12/75

/7/ Vesely, W. E., Narum, R. E.:
PREP and KITT: Computer Codes for the Automatic Evaluation of Fault Trees.
Idaho Nuclear Co. 1970

/8/ Fussel, G. G. et al:
MOCUS: A Computer Programm to Obtain Minimal Sets from Fault Trees.
Aerojet Nuclear Co. ANCR-1156, August 1974

/9/ Vesely, W. E.:
A Time-Dependent Methodology for Fault Tree Evaluation.
Nucl. Eng. Design 13 (1970) 337

/10/ Caldarola, L.:
Unavailability and Failure Intensity of Components.
Nuclear Engineering and Design 44 (1977)

/11/ Becker, A.:
Unveröffentlichte Ergebnisse,
Institut für Kerntechnik, TU-Berlin (1979).

/12/ Kamarinopoulos, L.:
Direkte und gewichtete Simulationsverfahren zur Berechnung der Zuverlässigkeit technischer Systeme.
Dissertation TU-Berlin (1972).

/13/ Kamarinopoulos, L.:
Anwendung von Monte-Carlo-Verfahren zur Ermittlung von Zuverlässigkeitsmerkmalen technischer Systeme.
Institut für Luft und Raumfahrt, ILR-Bericht 14
TU-Berlin (1976)

/14/ Hammersley, I.M., Handscomb, D.C.:
Monte Carlo Method.
London: Methuen a. Co LTD (1964)

/15/ Kahn, H.:
Use of Different MonteCarlo Sampling Techniques.
Symposium on MonteCarlo Methods es. H.A. Meyer, S. 146-190 (1956).

/16/ Spanier, J., Gelbard, M.E.:
Monte Carlo Principles and Neutron Transport Problems.
Addison-Wesley Publishing Company, (1969).

/17/ Köcher, D., e.a.:
Einführung in die Simulationstechnik.
Deutsche Geselschaft für Operations Research (1972).

/18/ Nagel, P.:
A Monte Carlo Method to Compute Fault Tree Probabilities.
System Safety Symposium (1965).

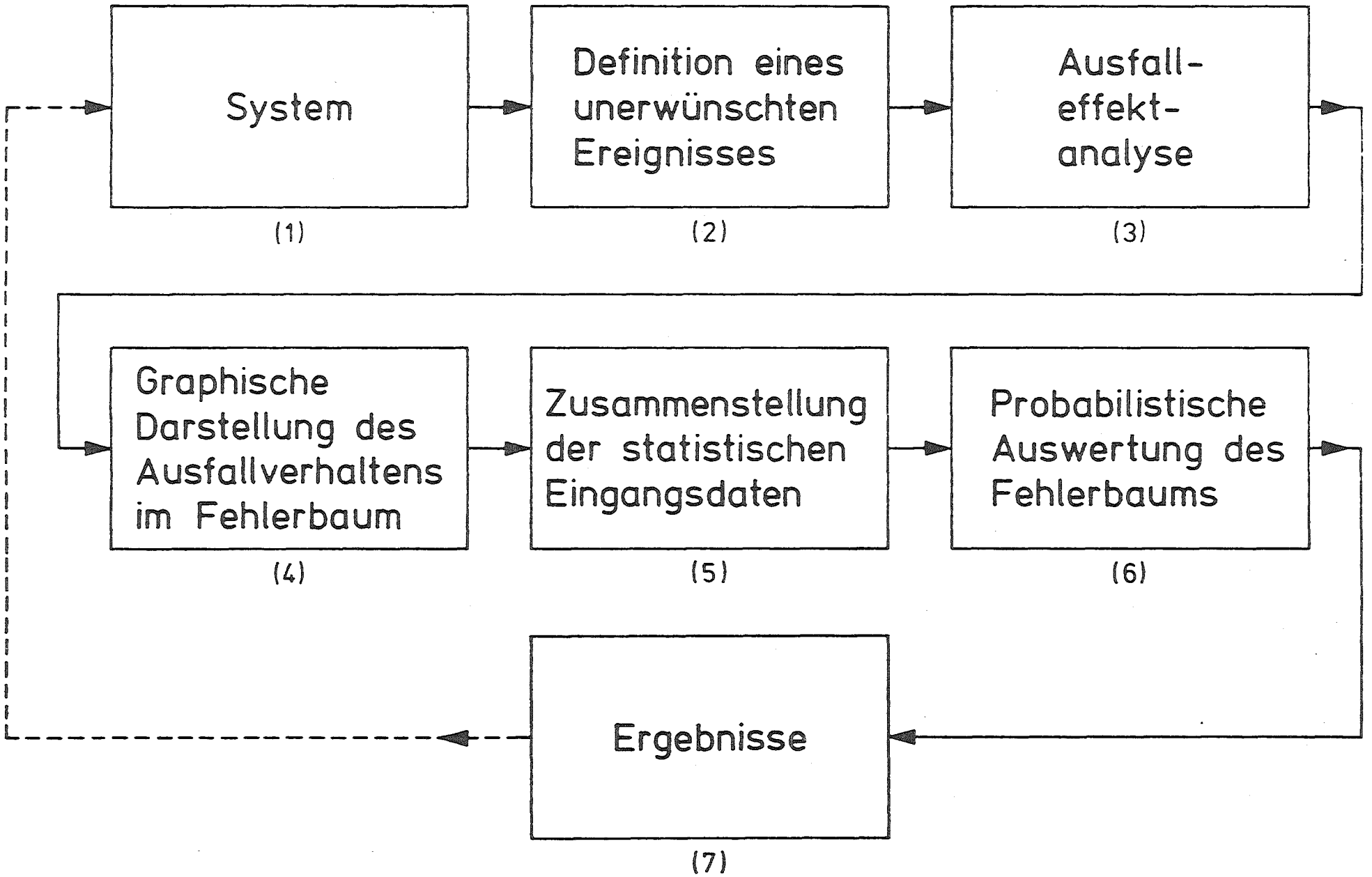


Bild 1 : Schematische Ablauf einer Zuverlässigkeitsanalyse

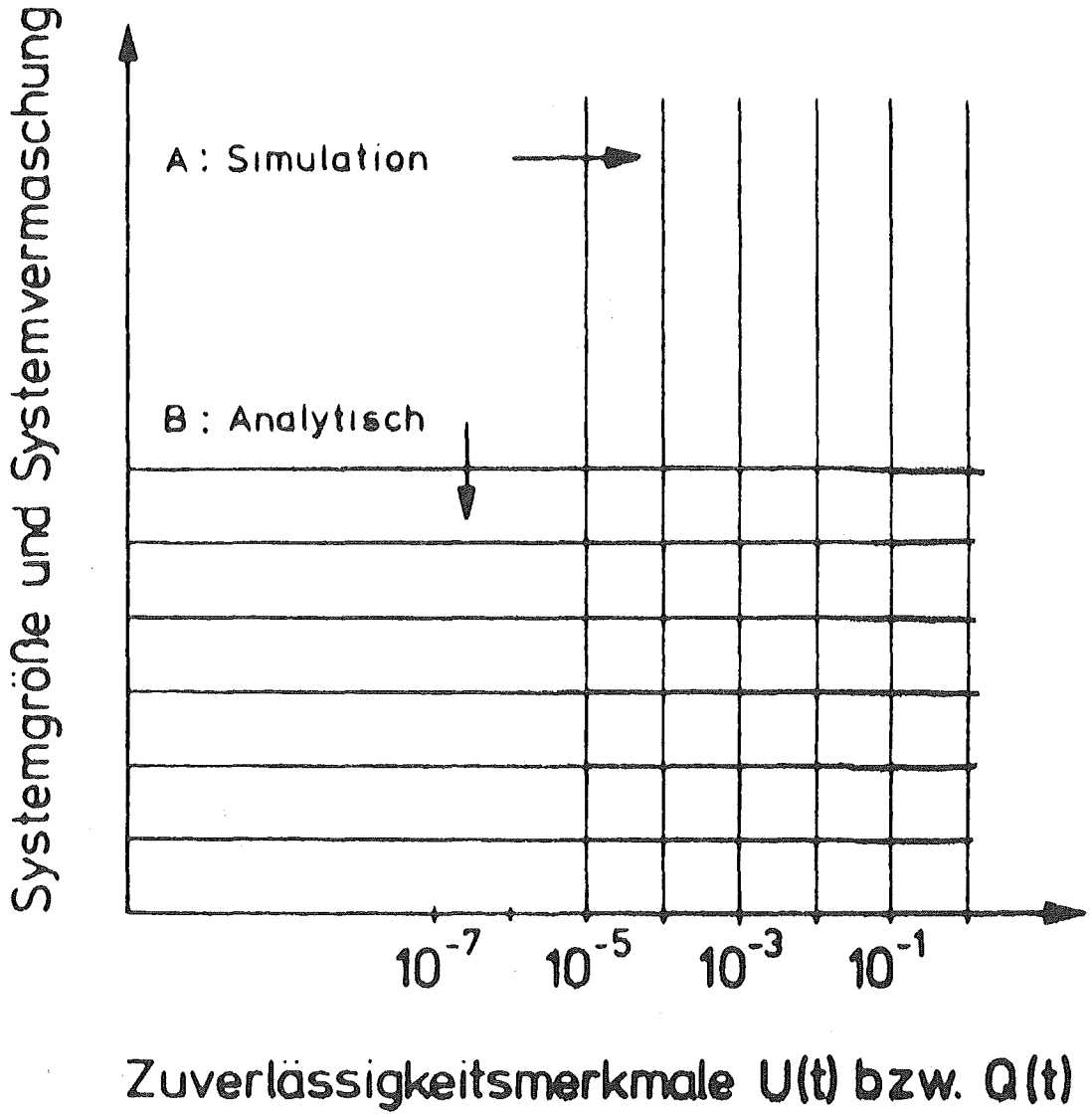


Bild 2 : Einsatzfelder analytischer und simulativer Verfahren

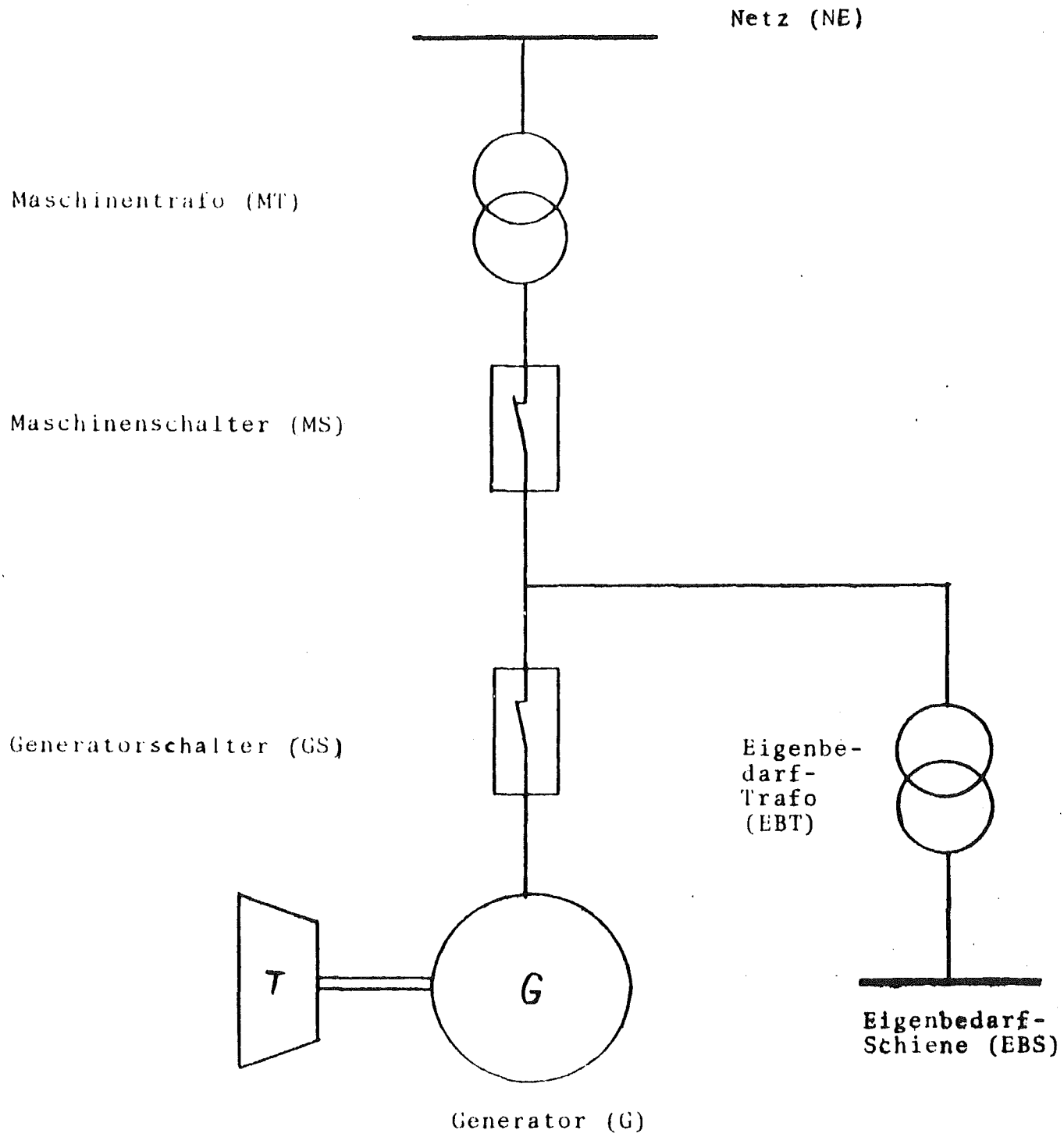


Bild 3 : Vereinfachte Eigenbedarfsschaltung
eines Kernkraftwerkes

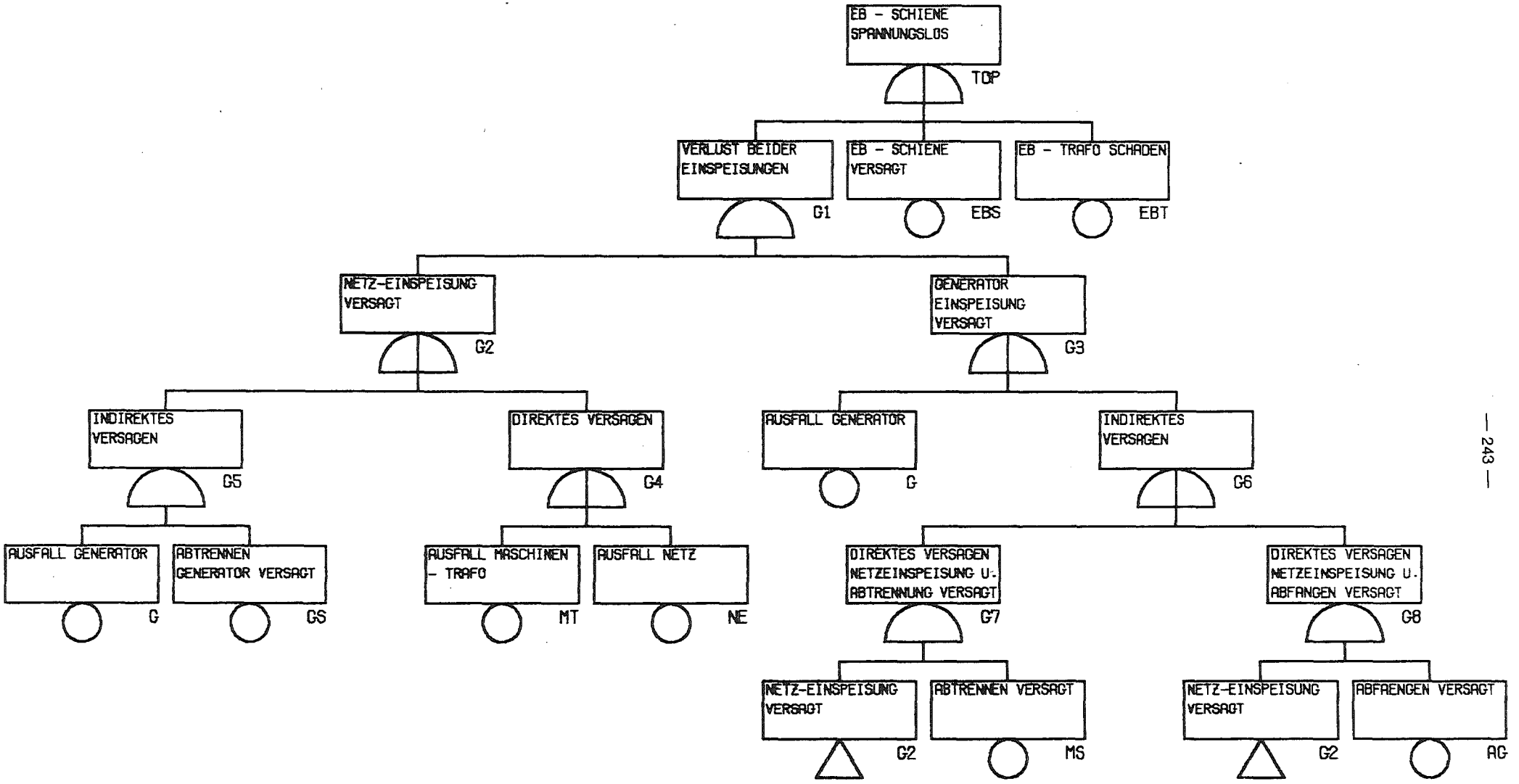
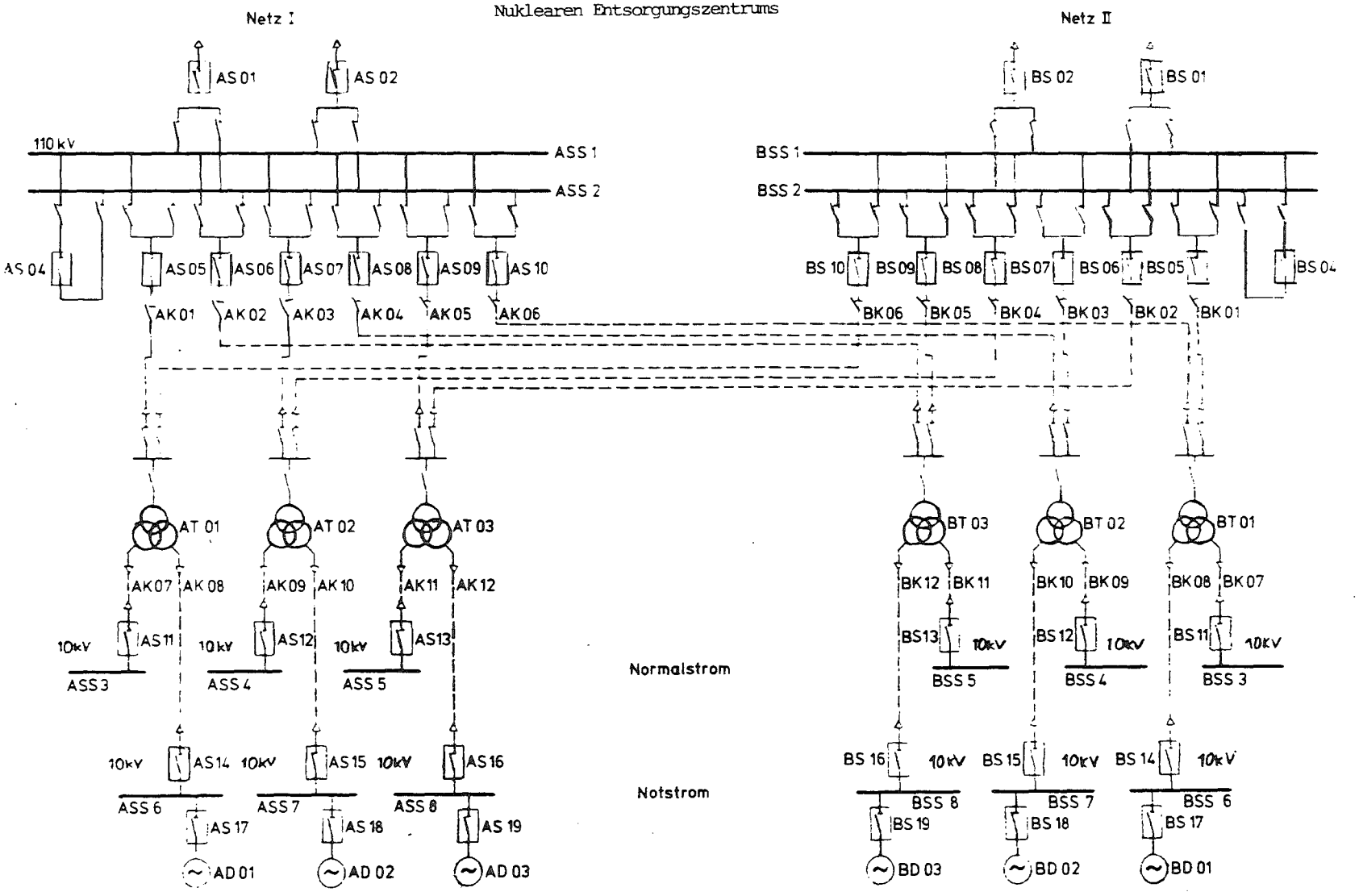


Bild 4 : Fehlerbaum zur Schaltung aus Bild 3

Bild 6: Schaltungskonzept zur Energieversorgung eines Nuklearen Entsorgungszentrums



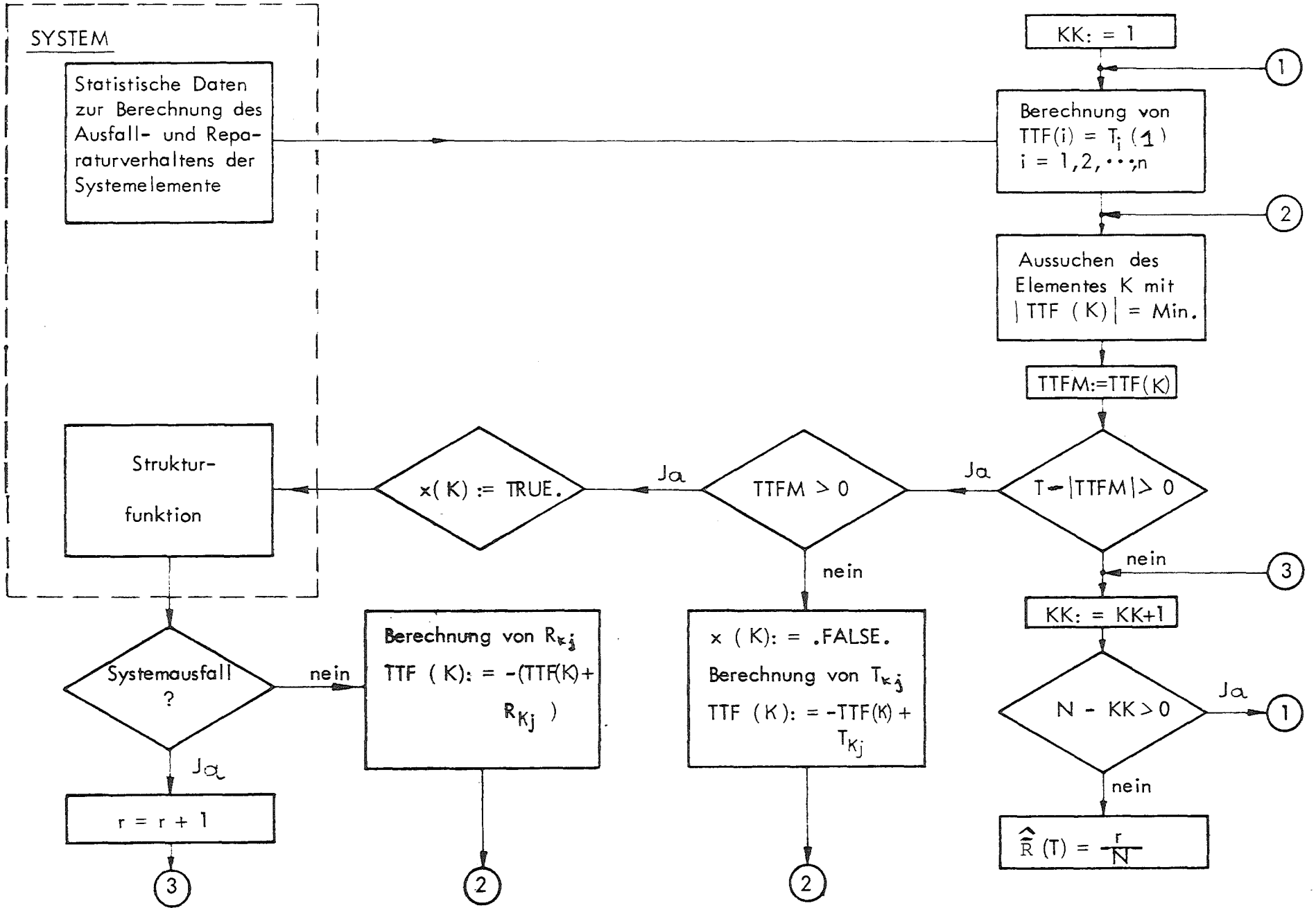


Bild 7 : Ablaufplan des Simulationsmodells zur Berechnung der Ausfallwahrscheinlichkeit $\bar{R}$ (T) eines Systems

Tabelle 1 : Ergebnisse der Fehlerbaumauswertung

	Gesamtzahl d. System-schnitte	Zahl d. dominant. Systemschn.	rel. Abschn. Kriterium	Ausfallwsk. d. Systems pro Jahr	Rechen-zeit (CYBER 175)
Variante 1 (mit Quellen)	ca. 85.000.000	ca. 50	10^{-3}	2.4 10^{-6}	ca. 200 sec.
Variante 2 (ohne Quellen)	ca. 6.000.000	ca. 60	10^{-5}	7.3 10^{-11}	ca. 50 sec.

Diskussion

Frage: Die Approximation des Fehlerbaumes wird aufgrund der Eintretenswahrscheinlichkeit der Cuts gemacht. Ist eine technische (auswirkungsbezogene) Gewichtung ebenfalls oder zusätzlich möglich, auch bei mehreren Millionen Cuts?

Antwort: Man kann Minimalschnitte bzw. Fehlerbaumteile auch anhand anderer Kriterien beurteilen. Im Zusammenhang mit Risikofragestellungen wäre z.B. die Risikogröße laut

$$R = H \cdot A$$

mit

R: Risiko

H: Häufigkeit

A: Auswirkungen (z.B. in Ci/Störfall).

Ein Verfahren das auf dieser Basis arbeitet ist im Institut für Kerntechnik der TU-Berlin bereits entwickelt worden und konnte erfolgreich im Rahmen der Sicherheitsstudie der Entsorgung (PSE) eingesetzt werden.

Frage: Welche Reparatur-Politiken können mit dem vorliegenden Programm angewendet werden, neben der Annahmen unabhängiger Reparatur (Anzahl der Reparaturen entspricht der Anzahl der Systemkomponenten)?

Antwort: Die gebräuchlichsten Instandsetzungsstrategien die mit analytischen Programmen erfaßbar sind, sind im Vortrag angesprochen worden. Kompliziertere Strategien, z.B. Reparaturbeschränkungen, Warteschlangeprobleme, etc. lassen sich mit analytischen Methoden, speziell bei großen Fehlerbäumen kaum behandeln. In solchen Fällen ist eine gestaffelte Vorgehensweise vorteilhaft

- Reduktion des Fehlerbaums auf die wichtigsten Ereignisse mittels analytischer Techniken,
- anschließende systemtreue Nachbildung des übriggebliebenen Teils durch simulative Verfahren.

Frage: Vor einigen Jahren haben wir Fehlerbäume von Systemen mit periodischer Inspektion untersucht und dabei das Importance Sampling Verfahren eingesetzt (Ch. Schneider, "Fehlerbaumanalyse von periodisch inspizierbaren Systemen mit Hilfe von Monte Carlo Methoden", Dissertation an der Universität Karlsruhe (1978)). Dabei haben wir die Exponentialdichten durch Exponentialdichten mit geändertem Parameter ersetzt und in der Tat eine - wenn auch nicht sehr große - Rechenzeitverkürzung erzielt. Hätten wir zu einer größeren Rechenzeitverkürzung kommen können, wenn wir eine nichtexponentielle Ersatzdichte zugelassen hätten?

Antwort: Ich möchte Ihre Frage uneingeschränkt mit Ja beantworten. Skalierungen der Ausfallrate λ_i zu $\alpha_i \cdot \lambda_i$ ($\alpha_i > 1$) unter Beibehaltung der Verteilungsform (exponentiell) sind im mehrdimensionalen Fall nicht effektiv. Eine Wahl $\alpha_i \geq 2$ führt sogar im allgemeineren zu unendlicher Varianz.

Ich meine, daß eineVerwendung der am Ende des Vortrages erwähnten Verteilungsdichtefunktion $f^*(t)$ auch in Ihrem Problem weit größere Rechenzeitgewinne gestatten wird.

Frage: Immerhin hat die Näherung der Vernachlässigung von Vereinigungen von Schnittmengen den Vorteil, daß man eine Abschätzung der Systemverfügbarkeit nach oben erhält.

In diesem Sinne ist die Vernachlässigung von Schnittmengen nach irgendwelchen Kriterien kritisch, da dadurch eine Abschätzung der System-Unverfügbarkeit nach unten entsteht. Oft ist es möglich, Schnittmengen statt sie wegzulassen in ihrer Unverfügbarkeit nach oben abzuschätzen.

Antwort: Die abgeschnittenen Fehlerbaumteile werden bezüglich ihres Beitrages zum jeweils berechneten Zuverlässigkeitsmerkmal konservativ abgeschätzt. Eine Angabe über die quantitative Signifikanz der abgeschnittenen Fehlerbaumteile wird nach Beendigung der Rechnung vom Programm mit ausgegeben. Somit ist die von Ihnen in Frage gestellte Konservativität garantiert.

Frage: Bemerkung: Ich möchte die Aussagen von Herrn Camarinopoulos unterstützen. In einer Analyse eines Abschaltsystems von KWU hat es gezeigt, daß die Cut-Set sehr effektiv sind, und daß eine relativ geringe Anzahl von Cut-Sets (etwa 70) die Verfügbarkeit bestimmen. Die längeren Cut-Sets von 5 und 6 Komponenten haben einen sehr geringen Einfluß gehabt.

Frage: Haben Sie Programme für die analytische Auswertung von Fehlerbäumen?

Antwort: Ja! Im Institut für Kerntechnik der TU-Berlin sind simulative und analytische Programme entwickelt worden, die auf die hier vorgestellten Verfahren basieren.

Frage: Bemerkung: Meine Frage betrifft das beim analytischen Verfahren angewandte Abschneiden von Fehlerbaumzweigen mit dem Wichtungsfaktor E. Wenn man ein Problem auf ca. 100 Ausdrücke reduziert und dabei etwa eine Million ähnlicher Ausdrücke abschneidet, dann stellt sich die Frage, ob eine solche Reduktion im allgemeinen Fall möglich ist, bzw. ob vollständige Kontrolle darüber gegeben ist, daß der abgeschnittene Rest vernachlässigbar ist. Ich möchte hinzufügen, daß mir die Anwendbarkeit analytischer Verfahren wichtig erscheint, weil ich nur bestätigen kann, daß bei Systemnichtverfügbarkeiten von $<10^{-6}$ Simulationsverfahren einen sehr hohen Rechenzeitaufwand erfordern.

Antwort: Die hier vorgestellte Abschneideprozedur gestattet es den abgeschnittenen Teil konservativ abzuschätzen. Nach Beendigung der Auswertung hat man also neben dem gesuchten Ergebnis auch eine konservative Angabe über den Beitrag der abgeschnittenen Fehlerbaumteile am berechneten Zuverlässigkeitsmerkmal. Insofern ist die von Ihnen angesprochene vollständige Kontrolle vorhanden.

Frage: Sie haben aus Ihrem analytischen Programm das Abschneideverfahren für Minimalschnitte und die damit verbundene Unsicherheitsangabe E dargestellt. Wieweit ist dieses Verfahren noch praktikabel, wenn man bei den Eingangsdaten auch deren Varianz mit berücksichtigen will?

Antwort: Vom Methodischen her ist das Abschneideverfahren auch im Rahmen von Unsicherheitsanalysen voll übertragbar. In diesem Fall sollten sich die Abschneideprozeduren an den Mittelwerten der Ausfalldaten orientieren.

Die Gefahr Minimalschnitte aufgrund von Mittelwertvergleichen abzuschneiden, die trotz kleiner Mittelwerte einen entscheidenden Einfluß auf die Varianz des Gesamtergebnisses haben, ist prinzipiell vorhanden. Hierzu müßte allerdings die Standardabweichung der Ausfalldaten den Mittelwert um Zehnerpotenzen dominieren, ein Sachverhalt der bei praktischen Berechnungen kaum vorkommt.

Sollten solche Effekte trotzdem berücksichtigt werden, so könnte die Standardabweichung - oder eine andere die jeweilige Unsicherheit charakterisierende Größe - als zusätzlichen Wichtungsparameter in der Abschneideprozedur aufgenommen werden.

Frage: Um Fehlerbäume analytisch auszuwerten, wurden sie i.a. in Minimalschnitte zerlegt. Gibt es andere Zerlegungen (z.B. disjunkte Zerlegungen, Module, etc.), die bei der numerischen Auswertung effektiver sind?

Wer verwendet solche anderen Zerlegungen?

Antwort: Selbstverständlich gibt es auch andere, alternative Möglichkeiten um große Fehlerbäume zu berechnen. Einige davon haben Sie bereits genannt. Ich bin der Meinung, daß die Modularisierung eine der vielversprechendsten Methoden darstellt. Zum Teil (simple Modularisation) wenden wir sie auch im IKT an.

Allerdings muß auch hier, speziell wenn der untersuchte, Fehlerbaum Dublikationen von Ereignissen beinhaltet, letztlich auf die Minimalschnitte partiell zurückgegriffen werden.

Einen gewissen Nachteil der Modularisierung sehe ich darin, daß die an sich zur Schwachstellenanalyse sehr anschauliche Darstellung in Minimalschnitten z.T. verloren geht.

Frage: Berechnung nach Cut-Sets. Bei dem gezeigten Beispiel waren nur 50 Cut-Sets aus der Menge der möglichen Sets relevant. Wie konservativ wird die Abschätzung des Gesamtergebnisses nach $A_B = \sum_{i=0}^{n} A_i$ ($-\Sigma A_i A_j$ soll vernachlässigbar sein!) bei der Berechnung von z.B. 10.000 Cut-Sets; da die Gesamtmengen von Cut-Sets in die Millionen gehen kann.

Antwort: Die Beziehungen

$$\bar{A}(t) \leq \sum_{i=1}^{m} \bar{A}_i(t)$$

bzw.

$$\bar{R}(t) \leq \sum_{i=1}^{m} \bar{R}_i(t)$$

leiten sich direkt aus dem Poincuré'schen Satz (Inklusions-Exklusion-Prinzip) und sind generell gültig. Ihre Gültigkeit wird von der Anzahl m (10.000 oder mehr) der Minimalschnitte kaum berührt.

Frage: Bei Interatom wurde bereits vor 8 Jahren ein analytisches Fehlerbaum-Rechenprogramm entwickelt, das nach einer zur Suche von Cut-Sets alternativen Methode arbeitet:

Der Fehlerbaum wird in eine Störfallablaufanalyse nach Komponentenzuständen transformiert. Durch Einführung einer Wahrscheinlichkeitsschranke erhält man als Endereignisse Fehlerwege, Intaktweg und vernachlässigte Wege. Der Fehlergehalt der Vernachlässigungswege wird simulativ ermittelt. Das Verfahren ist rechenzeitmäßig zur Suche von Cut-Sets konkurrenzfähig.

Antwort: Mit dem Ziel die Leistungsfähigkeit vorhandener Rechenprogramme (analytischer und simulativer) zur Zuverlässigkeitsanalyse zu vergleichen, veranstaltete 1975/1976 das BMFT ein "Wettrechnen". Teilgenommen haben z.B. KfK, IAGB, INTERATOM, IRS, ISPRA, LRA, MBB, TU-Berlin u.a. Die Ergebnisse sind im Abschlußbericht "Vergleich von Rechenprogrammen zur Zuverlässigkeitsanalyse von Kernkraftwerken" dokumentiert und allgemein zugänglich.

Softwarezuverlässigkeit

H. Kopetz

Technische Universität Berlin
Institut für Technische Informatik

Einleitung

Die Diskussion um die Zuverlässigkeit von Computersystemen ist in den letzten Jahren durch folgende Phänomene bestimmt worden:

- Die Zuverlässigkeit der Hardware hat mit der zunehmenden Integration (Wegfall von fehleranfälligen Verbindungen) zugenommen.
- Die Zuverlässigkeit der Software, hat mit dem Trend zu immer umfangreicheren und komplexeren Systemen abgenommen.

Bei vielen Anwendungen ist als Ergebnis dieser Entwicklung die Software zum bestimmenden Element für die Gesamtzuverlässigkeit eines Systems geworden.

In der vorliegenden Arbeit sollen zuerst begriffliche Festlegungen aus dem Bereich der Zuverlässigkeit von Software zur Diskussion gestellt und Ansätze zur Entwicklung fehlertoleranter Systeme dargestellt werden.

Begriffliche Festlegungen

Ausgehend vom Begriff der Systemzuverlässigkeit (Abb. 1) kann die Softwarezuverlässigkeit als Wahrscheinlichkeit definiert werden (Abb. 2). Das zufällige Ereignis ist jedoch nicht im alterungsbedingten Ausfall, sondern in der Aktivierung einer fehlerhaften Funktion zu sehen. Software Fehler sind Entwurfsfehler, ihre Ursache liegt in einem fehlerhaften Programm (einem Programmfehler). In welcher Phase der Programmentwicklung (Systemanalyse, Programmierung, Übersetzen) der Programmfehler entstanden ist, ist für die gegenwärtige Betrachtung ohne Bedeutung.

Während bei der Analyse der Zuverlässigkeit von Software der beabsichtigte (meist nur informell festgelegte) Einsatz eines Softwaresystems als Bezugspunkt genommen wird, behandelt der Begriff der Richtigkeit nur die Konsistenz zwischen der Programmspezifikation (möglichst formal) und den zu untersuchenden Programmen (Abb. 3).

Wenn man die Auswirkungen eines Entwurfs-(Software-)fehlers betrachtet, so ist hier eine Unterscheidung zwischen den "funktionellen" und "nichtfunktionellen" Systemen (Abb. 4) vorzunehmen. Bei funktionellen Systemen ist die Fehlerfunktion (Abb.5) durch das Programm bestimmt, bei "nicht funktionellen" Systemen wird sie abhängig vom inneren Zustand des Programms, d.i. von der vorangegangenen Verwendung des Programms.

Allein auf Grund der Fehlersymptome läßt sich nicht feststellen, ob der betrachtete Fehler auf einen Alterungs-(Hardware) oder Entwurfsfehler(Software) zurückzuführen ist, denn sowohl Hardware- wie auch Softwarefehler können zu einem "algorithmischen" Fehler führen (Abb. 6). Vor allem in nichtfunktionellen Systemen ist der Begriff des "Fehlerlatenzintervalls" wichtig (Abb. 8). Es kann ein langes Zeitintervall zwischen dem Auftreten eines fehlerhaften inneren Zustandes und dem beobachtbaren äußeren Fehler vergehen.

Der wesentliche Unterschied zwischen dem Alterungs-(Hardware) und Entwurfsfehler(meist Software) zeigt sich bei der Reparatur (Abb. 10) Alterungsfehler können durch den Austausch der fehlerhaften Komponente behoben werden, die Behebung von Entwurfsfehlern erfordern eine Änderung des Entwurfs (Umkonstruktion).

Komplexität im Entwurf

Eine der wesentlichen Ursachen für das Auftreten von Entwurfsfehlern ist in der "Komplexität" des Entwurfs zu suchen, d.i. Komplexität in Bezug auf die beschränkte Auffassungsgabe des menschlichen Geistes. Leider gibt es bis heute keine allgemein akzeptierte Metrik, nach der die Komplexität eines Softwareentwurfs gemessen werden kann.

Das Problem der "Entwurfskomplexität" ist ein allgemeines Problem, das nicht auf die Software beschränkt ist. Mittels Software können jedoch Funktionen von einer Komplexität realisiert werden, die in der klassischen Hardwaretechnik außerhalb des Bereichs des technisch möglichen liegen. Dies ist meiner Meinung nach der Hauptgrund, warum erst bei der Realisierung umfassender Computerprojekte das Problem der Entwurfs-(Software)Fehler so stark in den Vordergrund getreten ist.
Die Erkenntnis, "Software sei unzuverlässig" und sei daher für gewisse z.B. sicherheitsrelevante Bereiche, auszuschließen, ist gleichbedeutend mit einem (hoffentlichen bewußtem) Verzicht auf Funktionalität. Die Frage ob eine auf diese Weise mittels der konventionellen Steuerungstechnik realsierte Funktion zuverlässiger ist als eine vergleichbar einfache "Computerlösung" ist keineswegs selbstverständlich. Die Softwaretechnik bietet umfassendere Methoden zur Darstellung umfangreicher Systeme und damit zum "Management der Komplexität", als die konventionelle Steuerungstechnik, und im konventionellen Hardwareentwurf sind mehr fehleranfällige Verbindungen anzutreffen als bei der Verwendung eines hochintegrierten Mikrocomputer Bausteins.
Die hier angestellt Argumentation setzt allerdings voraus, daß die Komplexität einer "Computerlösung" auf die gegebene Problemstellung und nicht auf den gewählten Lösungsansatz - einschließlich der verfügbaren Hilfsmittel - zurückzuführen ist.

Fehlertoleranz versus Fehlerintoleranz

Es gibt zwei, sich einander ergänzende Vorgangsweisen um Systeme von hoher Zuverlässigkeit zu entwickeln:

- Fehlerintoleranz und
- Fehlertoleranz

Bei der Fehlerintoleranz wird versucht das Auftreten eines Fehlers durch geeignete Maßnahmen der Qualitätsprüfung ausreichend unwahrscheinlich werden zu lassen. Da Software nicht "altert" kann bei Anwendung einer geeigneten Methodologie (z.B. Analytische Verfikation von Programmen) das angestrebte Ziel prinzipiell erreicht

werden. Bis heute sind jedoch weder Methoden der analytischen Programmverfikation noch Testverfahren bekannt geworden, die es ermöglichen nachzuweisen, daß große Programmsysteme frei von Entwurfsfehlern sind. Es ist auch anzunehmen, daß in absehbarer Zukunft keine grundlegende Änderung dieser Situation eintreten wird.

Im Rahmen der Fehlerintoleranz wird nun die Möglichkeit des Auftretens von Fehlzuständen während des Einsatzes eines Softwareprodukts explizit berücksichtigt und es werden Maßnahmen vorgesehen, um aus dem fehlerhaften Zustand wieder in einen fehlerfreien Zustand zurückzufinden (Abb. 13). Fehlertoleranz setzt Redundanz voraus, d.h. im System sind zusätzlich zu dem für die Verarbeitung notwendigen Komponenten auch Teile enthalten, die einen Fehlzustand erkennen (Fehlererkennung) und ihn eventuell beheben können. Abb. 17 enthält die wichtigsten Methoden der Fehlererkennung. Im Rahmen der Fehlerbehebung unterscheidet man zwischen "forward" Fehlerbehandlung und "backward" Fehlerbehandlung. Bei der forward Fehlerbehandlung werden nur die Fehlersymptome, d.i. der fehlerhafte Zustand behoben. Diese Methode ist vor allem in zeitkritischen Realzeitsystemen von Bedeutung. Bei der "backward" Fehlerbehandlung wird auf einen früheren Systemzustand (checkpoint) zurückgegriffen . Bei permanenten Fehlern müssen auch die fehlerhaften Teile diagnostiziert und ausgetauscht werden (Rekonfiguration der Hardware und/oder der Software).

Vorhersage der Zuverlässigkeit von Software

Experimentelle Daten, die über das Auftreten von Fehlern während des Einsatzes von umfangreichen Softwaresystemen (z.B. große Betriebssysteme) beobachtet wurden, lassen erkennen, daß die Fehler mit einer gewissen Regelmäßigkeit auftreten. Diese Beobachtung wurde zum Anlaß genommen, probabilistische Modelle zur Vorhersage der Zuverlässigkeit von Softwaresystemen zu entwickeln. Typische Annahme in solchen Modellen sind

- die Eingabebelastung ist proportional der von einem System konsumierten CPU Zeit

- die Fehlerfunktion ändert sich quasi kontinuierlich bei der Durchführung von Programmänderungen

Unter diesen Annahmen läßt sich eine erwartete MTTF von Software errechnen. Ebenso ergibt sich die Möglichkeit die Änderung der MTTF als Folge des "Debugging" auszudrücken.

Die Ergebnisse dieser Modelle haben bei umfangreichen Systemen, deren Eingabeverteilung stark variiert, (z.B. Betfiebssysteme) überraschend gute Resultate erzielt.

Bei komplexen Systemen, die für den einmaligen Einsatz konzipiert werden (mission oriented systems) gibt es bislang jedoch kein allgemein akzeptiertes Verfahren, um die Zuverlässigkeit der Software vorherzusagen.

Literatur

Kopetz, H., Softwarezuverlässigkeit
Carl Hanser Verlag, München, 1976
überarbeitete Fassung: Software Reliability,
Mc Millan, London 1979

Rault, J.C., An approach towards reliable software,
Proc. 4th International Conference on Software
Engineering, Munich 1979, p. 220 - 230

In diesen beiden Arbeiten finden sich ausführliche Literaturangaben

Randell, B., Reliability Issues in Computing System
Design, ACM Computing Surveys, Vol. 10, No 2,
June 1978, p. 123 - 165

Muso, J.R., Software Reliability measures applied
to system engineering, Proc. of the National
Computer Conference, AFIPS Press, Montreal N.J.,
p. 941 - 946

Systemzuverlässigkeit

Systemzuverlässigkeit ist die Wahrscheinlichkeit, daß ein Computersystem die beabsichtigte Aufgabe während einer vorgegebenen Zeit unter festliegenden Umweltbedingungen erfüllt.

Abb. 1 Definition Zuverlässigkeit

Softwarezuverlässigkeit

Softwarezuverlässigkeit ist die Wahrscheinlichkeit, daß ein Softwaresystem die beabsichtigte Aufgabe für eine vorgegebene Anzahl von Eingabefällen unter festliegenden Eingabebedingungen erfüllt, vorausgesetzt Hardware und Eingabe sind fehlerfrei.

Abb. 2 Definition Softwarezuverlässigkeit

Richtigkeit

Ein Programm P ist dann richtig in Bezug auf die Vorbedingung $\varphi(x)$ und die Endbedingung $\psi(x, z)$, wenn für alle x aus D_X die Vorbedingung $\varphi(x)$ erfüllt, das Programm P(x) definiert und die Endbedingung $\psi[x, P(x)]$ wahr ist.

Abb. 3 Definition Richtigkeit

Funktionelles System

Ein System ist funktionell, wenn die Ein - Ausgabebeziehung einer Berechnung unabhängig ist von der vorangegangenen Berechnung (d. h. es wird kein innerer Zustand gespeichert). Andernfalls ist ein System nicht funktionell.

Abb. 4 Definition Funktionelles System

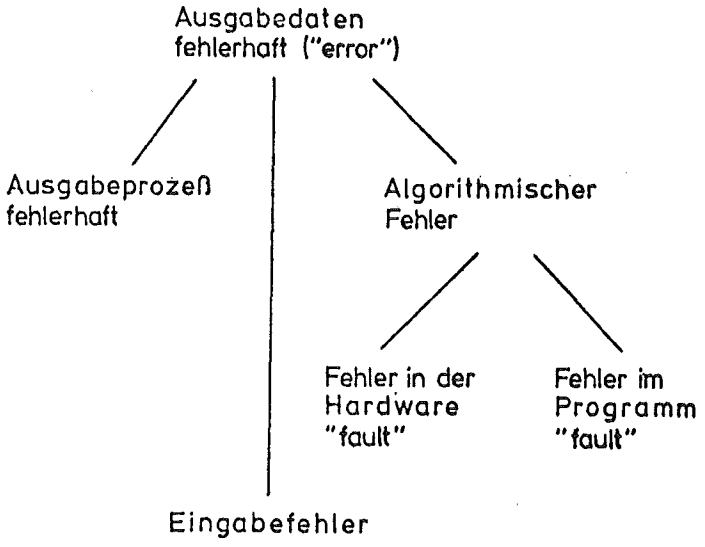
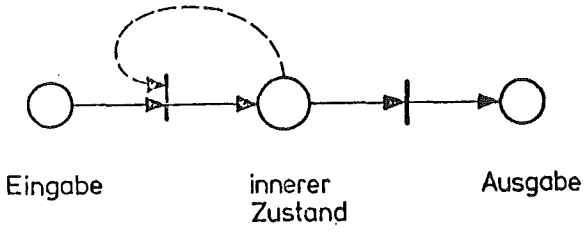


Abb. 5 Fehlerrate auf Grund von Softwarefehlern in einem funktionellen System

$$\lambda_n = \sum_i e(i)\, p(i)$$

λ_n Fehlerrate
$e(i)$ Fehlerfunktion
$p(i)$ Eingabewahrscheinlichkeit

Abb. 6 Analyse von Ausgabebefehlen in einem funktionellen System



Fehlerfunktion abhängig vom inneren Zustand

Abb. 7 Fehlverhalten eines nichtfunktionellen Systems

Fehlerlatenzintervall

Zeitintervall zwischen Auftreten eines Fehlers und seiner Auswirkung.

Abb. 8 Definition Fehlerlatenzintervall

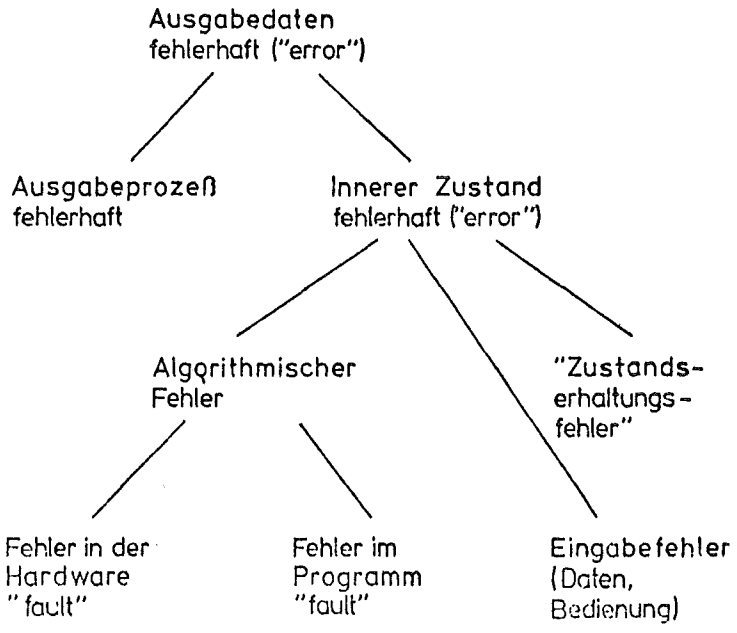


Abb. 9 Analyse von Ausgabefehlern in einem nichtfunktionellen System

Der wesentliche Unterschied zwischen Hardware (Alterungs-) und Software (Entwurfs-) Fehler zeigt sich bei der Reparatur:

Alterungsfehler ⇒ Austausch der fehlerhaften Komponente

Entwurfsfehler ⇒ Neukonstruktion

Abb. 10 Unterschied zwischen Alterungs- und Entwurfsfehlern

Selbst wenn es gelingen würde fehlerfreie Software zu erstellen, bliebe noch immer das Problem der Systemzuverlässigkeit offen!

Abb. 11 Softwarezuverlässigkeit versus Systemzuverlässigkeit

Erhöhung der Systemzuverlässigkeit

FEHLERINTOLERANZ

- Qualitätskomponenten in der Hardware
- Fehlerfreie Programme
- Fehlerfreie Eingabe

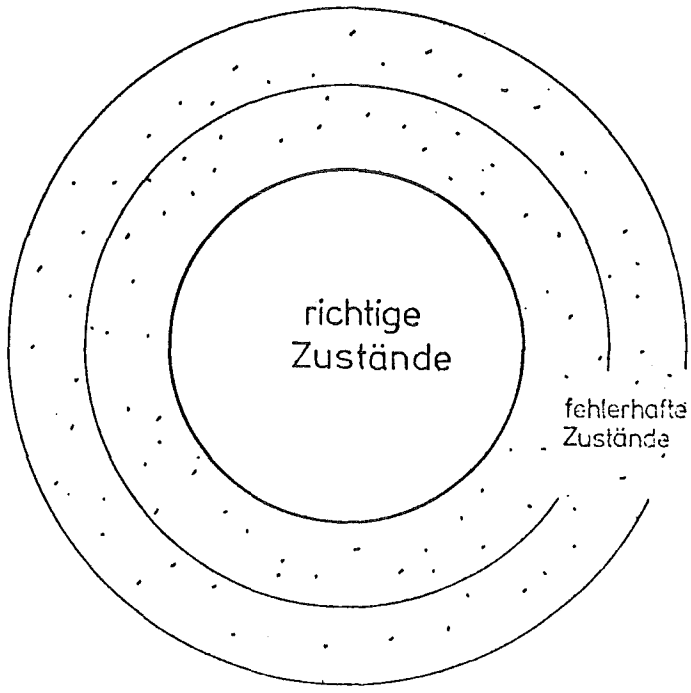
FEHLERTOLERANZ (Redundanz)

- Fehlererkennung
- Fehlerbehandlung
- Rekonfiguration fehlerhafter Komponenten (Hardware, Software)

Abb. 12 Erhöhung der Softwarezuverlässigkeit

Fehlertoleranz

Ein System ist fehlertolerant, wenn die Auswirkungen von Fehlern während des Rechenprozesses durch Redundanz kompensiert werden.



Fehlertoleranz versucht fehlerhafte Zustände zu erkennen und zu korrigieren

Abb. 13 Definition Fehlertoleranz

Abb. 14 Fehlertoleranz versus Fehlerintoleranz

Redundanz

Zusätzliche Subsysteme oder Programme, die mittels alternativer, unabhängiger Methoden gültige Ergebnisse erzielen.

Abb. 15 Redundanz

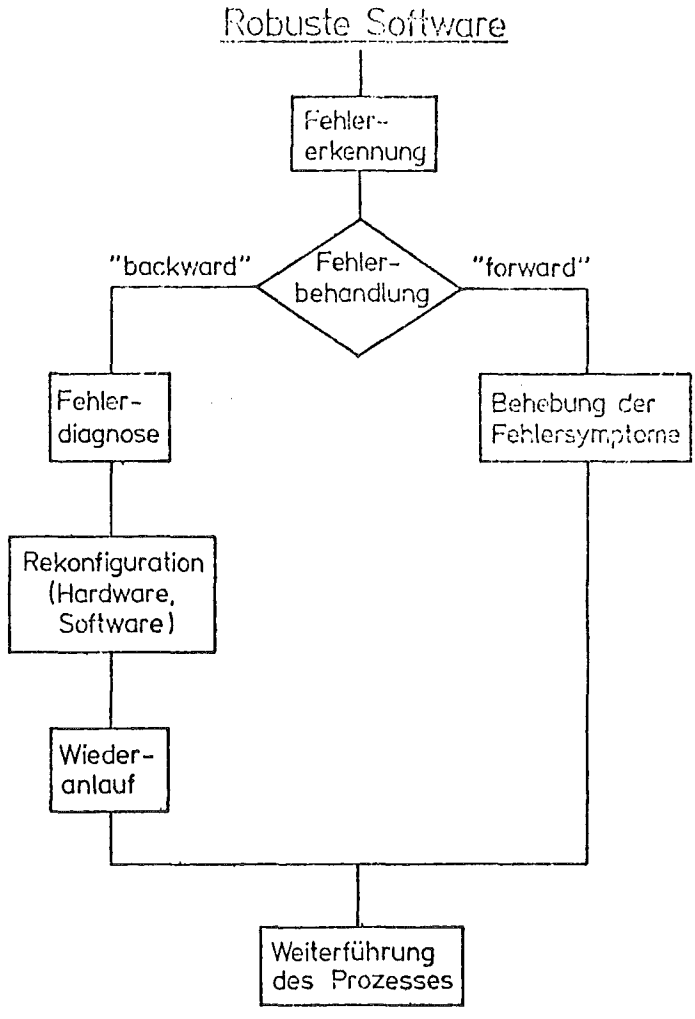


Abb. 16 Forward und Backward Error Recovery

Methoden der Fehlererkennung

FEHLERART	METHODE
Fehler im inneren Zustand	Plausibilitätsüberprüfung "run time assertion"
"Zustands-erhaltungsfehler"	Strukturelle Redundanz (z. B. Parity)
Algorithmischer Fehler	Zeitüberwachung "run time assertion" Strukturelle Redundanz
Eingabefehler	Überprüfung des Eingabe-bereichs Plausibilitätsüberprüfung

Abb. 17 Methoden der Fehlererkennung

Vorhersage der Zuverlässigkeit

Systeme im kontinuierlichen gleichmäßigen Einsatz (z. B. große Betriebssysteme)

- Modelle von Jelinski, Moranda, Musa, Shooman et. et.

Systeme für "einmaligen" Einsatz (mission oriented systems, z. B. Raketenstart)

- keine Modelle verfügbar

Abb. 18 Vorhersage der Zuverlässigkeit

Software Zuverlässigkeitsmodelle (z. B. Musa)

ANNAHMEN:

- CPU Zeit ist Maß für "Eingabebelastung"
- Eingabebelastung / CPU Einheit konstant
- Fehlerfunktion ändert sich nur bei Programmodifikationen

AUSSAGEN:

- MTBF zwischen Softwarefehler
- Veränderung der MTBF über die Zeit als Folge von Programmodifikationen

Abb. 19 Softwarezuverlässigkeitsmodelle

Diskussion

Frage: Was sind Ihrer Erfahrung nach heutzutage die effizientesten Methoden zur Erstellung korrekter Software?

Antwort: Am wichtigsten ist meiner Meinung nach die Projektabwicklung nach den Grundsätzen des Configuration-Management. Dabei ist der Erstellung einer vollständigen und widerspruchfreien funktionellen Spezifikation besondere Aufmerksamkeit zu widmen. Selbstverständlich nehme ich an, daß die gängigen Methoden des "Software engineering" angewandt werden.

Frage: Ist die Software-Zuverlässigkeit theoretisch vorhersagbar?

Antwort: Es gibt Modelle (z.B. Jelinski, Moranda od. Musa) mittels der die Zuverlässigkeit von Software (z.B. MTBF) vorhergesagt werden kann. Diese Modelle beruhen aber auf teilweise fraglichen Annahmen. Die Zuverlässigkeit von Software für "Mission oriented Systems" ist mit heutigen Methoden kaum vorhersagbar.

Frage: 1. Eine Anmerkung zu den statistischen Modellen von Shooman, Musa usw.

a) Wir diskutierten vor einiger Zeit im IDT diese stat. Modelle und kamen zu rel. negativen Aussagen.

b) In der Arbeitsgruppe "Statist. Methoden der Zuverlässigkeit" des VDI behandeln wir den Zusammenhang von Verteilungen mit Fehlermodellen (z.B. Weibull). Daher habe ich den Eindruck, daß bei Software keine mit Materialverhalten vergleichbaren Fehlermodelle existieren.

2. Im Bereich der Hardware haben wir eine Dualität.

Fehlerdiagnose (Fehlerintoleranz) und Redundanz (Fehlertoleranz).

Können Sie diese Dualität für Software bestätigen?

Antwort: Meiner Meinung nach ergänzen sich im Bereich der Software Fehlerintoleranz und Fehlertoleranz.

Frage: Können Sie etwas über praktische Erfahrung mit Software-Diversität (Redundanz in ihrer Nomenklatur) sagen?

Antwort: Es gibt einige Institutionen, die z.T. praktische Untersuchungen über die Software-Diversität durchführen (z.B. Prof. Avizienis, UCLA; Prof. Randell, Newcastle UK).

In gewisser Weise stellt auch das "Exception Handling" eine Software-Diversität dar. Bei der Implementierung umfangreicher Realzeitsysteme werden die Methoden des Exception Handling im großen Umfang praktisch und mit viel Erfolg eingesetzt.

Frage: Versteht man unter "forward error recovery" ein Verfahren, den Fehler unter Umgehung der Suche nach der fehlerverursachenden Komponente zu beheben?

Antwort: Ja!

Frage: Problem des Wiederanlaufes bei "forward error recovery": Wird der Fehler in "unendlich kurzer Zeit" behoben?

Antwort: Jedes Realzeitsystem basiert auf einem "kleinsten" Zeittakt (z.B. 10 msec). In vielen Fällen können die Folgen eines Fehlers, die Fehlersymptome, innerhalb eines solchen Zeitintervalls behoben werden. Es treten dann keine Auswirkungen auf das Echtzeitverhalten des Systems auf.

Teilnehmerliste

Name	Firma
Dipl.-Ing. C. Arnoldt	KWU AG, Erlangen
Ing. H.P. Balfanz	TÜV Norddeutschland e.V., Hamburg
Dipl.-Ing. H. Bäumel	Dornier System, Friedrichshafen
Ing.(grad.) G. Breiling	Babcock-Brown Boveri Reaktor GmbH, Mannheim
Dr. L. Camarinopoulos	Technische Universität Berlin
Dr. Chrobok	KEWA, Hannover
Dr. Demmelmeier	Technische Universität München
Dr. J. Doehler	Dornier System, Friedrichshafen
Dr. Heinz H. Frey	AG Brown Boveri & Cie, Baden, Schweiz
Dr. Giovanelli	Industrie-Anlagen-Betriebs-Ges., Ottobrunn
Dipl.-Ing. W. Güldner	GRS Garching
Dr. H.W. von Guérard	Berater bei IABG, Ottobrunn
Dipl.-Ing. K. Hanning	Brown Boveri & Cie, Abt. GK/TS1, Mannheim
Dr. J. Hinrichs	Hochtemperatur Reaktorbau GmbH, Mannheim
Dr. S. Jokela	Contraves AG, Glattbrugg, Schweiz
Dr. Keller	Industrie-Anlagen-Betriebs-Ges., Ottobrunn
Prof. DDr. W. Koenne	Österr. Verbundgesellschaft, Wien
Prof. Dr. H. Kopetz	Technische Universität Berlin
H. Kraus	Technische Universität München
Dr. H.H. Kretzen	Interatom GmbH, Bergisch Gladbach
Freiherr von Linden	GRS Garching
Prof. Dr. M. Mäiß	Technische Fachhochschule Berlin
Dr. W. Mergenthaler	Daimler Benz AG, Stuttgart
Dr. H. Sobottka	KWU, Erlangen
Dr. E. Schwarzer	Daimler Benz AG, Sindelfingen
Dr. O.N. Staubli	Dornier System, Friedrichshafen
Ing. Thiele	Krauss-Maffei AG, München
Dr.-Ing. D. Vetterkind	Rheinisch Westf. Elektrizitätswerk, Essen
Prof. Dr. P. Zinterhof	Universität Salzburg
Ing. P. Fritz	GWK, Karlsruhe
Dr. H. Hübner	GWK, Karlsruhe

Dr. J. Lausch	GWK, Karlsruhe
Dipl.-Ing. K. Jaschke	GWK, Karlsruhe
F. Stopfkuchen	GWK, Karlsruhe

Teilnehmer aus dem Kernforschungszentrum Karlsruhe

Dr. R. Avenhaus	IDT
Dr. H. Borgwaldt	INR
Dr. L. Caldarola	IRE
Dr. F. Fischer	IDT
Dr. S. Flach	PWA/PL
Dipl.-Inf. L. Gmeiner	IDT
Dipl.Wi.-Ing. W. Haußmann	IDT
Dr. F. Horsch	PNS/PL
Dr. K. Nagel	IDT
Ing. W. Seither	IT-M
Prof. Dr. H. Trauboth	IDT
Dipl.-Math. U. Voges	IDT
Dr. G. Weber	IDT
Dr. H. Wenzelburger	IDT/IRE