KERNFORSCHUNGSZENTRUM

KARLSRUHE

Januar 1974 KFK 1811

Institut für Angewandte Systemtechnik und Reaktorphysik

Einführung in Methoden und Probleme der Zuverlässigkeit

G. Weber

GESELLSCHAFT
FÜR
KERNFORSCHUNG M.B.H.

KARLSRUHE

KERNFORSCHUNGSZENTRUM KARLSRUHE

KFK 1811

Institut für
Angewandte Systemtechnik und Reaktorphysik

EINFÜHRUNG IN METHODEN UND PROBLEME DER ZUVERLÄSSIGKEIT

mit Beiträgen von

P.W. Becker [1], L. Caldarola [2]
W. Häfele [3], F.W. Heuser [4]
G. Nägele [3], H.J. Otway [5]
L.F. Pau [6], W. Rosenhauer [7]
D. Sellinschegg [3], G. Weber [3]

zusammengestellt von G. Weber

Gesellschaft für Kernforschung m.b.H., Karlsruhe

1) Electronics Laboratory, The Technical University of Denmark
2) Euratomdelegierter beim Projekt Schneller Brüter, Karlsruhe
3) GfK, IASR
4) Fa. Interatom, Bensberg, jetzt Institut für Reaktorsicherheit, Köln
5) IAEA, Wien
6) z.Zt. Institute of Mathematical Statistics and Operations Research The Technical University of Denmark
7) Fa. Interatom, Bensberg

Zusammenfassung

Dieser Bericht gibt die Vorträge einer Seminarreihe des IASR im Winter 1972/73 zur Einführung in Grundbegriffe, Methoden und Probleme der Zuverlässigkeit wieder. Die Stellung der Zuverlässigkeit in der heutigen Technologie wird gezeigt. Es erscheint uns als notwendig, den Rahmen der bisher üblichen Methoden zu verlassen. Dabei entstehen die echten Probleme, aber auch die Chancen der Zuverlässigkeit.

1. Die Einleitung umreißt die Bedeutung der Zuverlässigkeit in der Großforschung, indem sie Naturwissenschaft und Projektwissenschaft gegeneinander kontrastiert. Jedoch brauchen wir auch in der Projektwissenschaft Begriffsbestimmungen und Methoden, wenn sie auch in der Regel stark einer zeitlichen Entwicklung unterliegen. Der Begriff der Zuverlässigkeit wird definiert und einige grundlegende Zuverlässigkeitskenngrößen eingeführt.

2. Bei der Systemzuverlässigkeit kommen grundsätzliche und Projektbezogene Überlegungen zur Diskussion. Der Aufbau eines Fehlerbaums und seine Auswertung steht dabei im Mittelpunkt. Es gibt grundsätzlich drei Methoden zur Auswertung von Fehlerbäumen:

- analytische Auswertung
- Simulationsverfahren (Monte Carlo-Methode)
- eine Kombination der analytischen Auswertung mit Simulationsverfahren.

Zunächst werden einige Begriffe für einfache Systeme gegeben. Es kann damit gezeigt werden, daß ein System aus Komponenten, die konstante Ausfallraten besitzen, im Allgemeinen keine konstante Systemausfallrate besitzt.
Dann wird für den Fehlerbaum, der zur Verknüpfung von Ausfallereignissen eines Systems dient, eine Definition eingeführt. Dabei wird die Verknüpfung von Ereignissen durch die Logik diskutiert. Der Aufbau eines Fehlerbaums für die Stromversorgung des amerikanischen Kernkraftwerks DRESDEN-3 wird im Detail durchgeführt.

3. Die Beiträge zu projektbezogenen Anwendungen von Zuverlässigkeitsmethoden bei Interatom beschreiben zunächst Anwendungen verschiedener Simulationsprogramme und ihre Kombination mit analytischen Methoden zur Fehlerbaumauswertung. Auch die Möglichkeiten einer Markow'schen Zustandsanalyse werden diskutiert.

Darauf werden Anwendungen auf

- alternative Auslegungskonzepte für die elektrische Energieversorgung des Schnellen Brüters SNR 300 sowie
- Untersuchungen zur Nachwärmeabfuhr des SNR 300

beschrieben.

Ein Beispiel nichtprobabilistischer Untersuchungen sind die bruchmechanischen Methoden zum Integritätsnachweis für das Primärsystem des SNR - Kühlmittelkreislaufs.

4. Die Kosten-Nutzen-Risiko-Analyse für verschiedene technische Systeme wird eingeführt und die Anwendung des Risiko-Begriffs auf Reaktoren besprochen. Weiterhin bringt die Kosten-Nutzen-Risiko-Analyse einen Vergleich von Kernkraftwerken und konventionellen (ölgefeuerten) Kraftwerken. Die Bedeutung des Risikos für die Gesellschaft wird untersucht, insbesondere unter der Fragestellung: "How safe is safe enough?"

5. Ein Beispiel für die Ermittlung von Zuverlässigkeitskenngrößen ist der Lebensdauertest. Dieser kann nach verschiedenen Strategien ausgeführt werden (Festlegung des Stichprobenumfangs, der Abbruchskriterien oder Entscheidung für eine sequentielle Prozedur). Dabei ist es üblich, die aus Lebensdauerexperimenten gewonnenen Daten mittels Punktschätzungen, Konfidenzintervallschätzungen oder Hypothesentests auszuwerten. Bewertet man die möglichen Strategien durch eine Kostenfunktion, so kann man diese Funktion unter geeigneten benbedingungen minimieren und damit eine kostenminimale Strategie erhalten.

6. Die Methode der kontinuierlichen Vorhersage der Lebensdauer wird eingeführt. Mehrere Methoden zur Erhöhung der Zuverlässigkeit redundanter Systeme werden diskutiert. Es zeigt sich, daß der durch Hinzufügen einer redundanten Komponente zu einem System erzielte zusätzlich Nutzen mit der Gesamtzahl der Komponenten abnimmt. Insbesondere wird gezeigt, daß die durchschnittliche Zeit bis zum Ausfall des Systems durch Ersetzen (oder Reparieren) der Komponenten vor dem Ausfall (Instandhaltung) wesentlich verlängert werden kann, wenn man mit großer Genauigkeit den Zeitpunkt des Ausfalls jeder Komponente vorhersagen kann.

Es wird eine allgemeine Theorie der Zuverlässigkeit einer Einrichtung in Abhängigkeit von ihren Kenngrößen, ihrer Vorgeschichte, und ihrer erwarteten Betriebsbedingungen eingeführt, die zu einer neuen Definition der Zuverlässigkeit führt. Der Begriff "kontinuierliche Vorhersage der Lebensdauer" wird eingeführt, und die Grundzüge dieser allgemeinen Theorie diskutiert.

7. Ein rechnergesteuerter Entwurf (Computer Aided Design) von elektronischen Schaltkreisen kann zur Optimierung der Zuverlässigkeit verwendet werden. Für das Drift-Verhalten von Zuverlässigkeitskenngrößen wird ein mathematisches Modell eingeführt. Eine kurze Beschreibung der Methoden zur numerischen Auswertung folgt. Schließlich wird für zwei transistorierte Schaltkreise die Optimierung der Zuverlässigkeit ausgeführt.

8. Der Zweck jeder Fehler-Diagnose ist es, einen Fehler oder eine Anzahl von Fehlern zu erkennen. Dies kann folgendermaßen geschehen:

- Informationen über Vergangeheit, Einsatzbedingungen und Wartung von Komponenten werden gesammelt. Alle signifikanten Daten werden in einem Lernprozeß ausgesucht und in einer Reliability und Maintainability-Bank gespeichert. Dabei besteht die Möglichkeit, Daten kontinuierlich zu erneuern (Kapitel 6).

- Es ist auch möglich, Informationen über Ausfallursachen (im weitesten Sinn) zu sammeln. Eine systematische Beobachtung dieser Art läßt Fehlmuster erkennen (Pattern Recognition). Dabei können über das Verhalten einer einzelnen Komponente hinausgehende Gemeinsamkeiten aufgezeigt werden. Es ist somit möglich,

a) redundante Beobachtungen zu eliminieren (Data Compression),

b) eine Liste von notwendigen Anforderungen und Annahmen für die Fehlerdiagnose aufzustellen, sowie

c) eine Automation der Fehlerdiagnose sowie der Testprozeduren einzuführen.

Die Zuverlässigkeit ist eine Gebiet, das besonders stark von der Bereitschaft aller Beteiligten zur Kommunikation abhängt. Es wird uns darum jederzeit freuen, konstruktive Kritik und Hinweise für mögliche Anwendungen zu erfahren.

Summary

This report presents the talks of a seminar series of our institute (IASR) last winter (1972/73). An introduction to basic concepts, methods, and problems of reliability is given, and applications of reliability to several branches of technology are shown.

1. The introduction emphasizes the importance of reliability for technological projects. The use of clear concepts is not only required for pure science, it is also important for technology. However, in technology the concepts and methods have usually to adapt to fast changes. Some concepts of reliability are defined and simple applications discussed.

2. In the chapter on system reliability, methodological and project oriented topics are presented. The construction of a fault tree and its evaluation are shown. For evaluation, we have three methods:

- analytical evaluation
- simulation (Monte carlo methods)
- a combined use of analytical evaluation and simulation.

First, some examples of simple systems are given. It can be shown that a system with components having constant failure rates, generally has no constant system failure rate.

Then, a definition for a fault tree is introduced. The combination of primary failure events of components by means of logic is discussed. Finally, the construction of a fault tree for the emergency power system of the American nuclear power station DRESDEN-3 is explained.

3. The two contributions on project oriented applications of reliability from INTERATOM show the application of simulation programs, and the combined use of simulation and analytical evaluation for complex systems represented by fault trees. In addition, the possibilities of a Markow - analysis are discussed.
Applications of fault tree analysis on

- two alternative designs for the electric power system for the fast breeder prototype SNR 300, and
- the heat removal system (as planned for SNR 300)

are shown.

An example of a nonprobabilistic treatment is the fracture mechanical study with respect to the integrity of the primary coolant circuit of SNR 300.

4. Cost-benefit-risk analysis for several technological systems is introduced including an application for reactors. Moreover, this analysis can be used as a decision help in response to the question whether nuclear power or conventional power is preferable. The importance of risk for society is discussed, with an emphasis on the question: "How safe is safe enough"

5. An example for obtaining reliability data is the life time test. It is possible to use various strategies (e.g. by fixing the sample size, fixing the duration of tests etc.). Usually the data from life time testing are evaluated using point estimates, confidence intervals or hypothesis testing. If the different strategies can be related to cost-functions, these functions can, under reasonable constraints, be minimized, thus indicating optimal strategies.

6. The method of continous life time prediction (CLP) is introduced. First, conventional methods to increase reliability of redundant systems are discussed. It can be seen that the benefit obtained from adding another redundant component decreases as a funtion of the total number of redundant components. On the other hand, the average time to failure of the system will be considerably increased if the time to failure of all important components can be predicted with high accuracy.

A general theory of the reliability of such a component as function of its characteristics (including history and expected operating conditions) is outlined. This theory leads to a new definition of reliability.

7. Computer aided design (CAD) of electronic circuits can be used for an optimization of reliability. A mathematical model of the drift behaviour of circuits is introduced. A short description of the methods for numerical evaluation follows. Finally, two transistorized circuits are optimized with respect to reliability. The relation of this method to production yield is indicated.

8. The purpose of each failure diagnosis is to show failures or sets of failures.

This may be done as follows:

- Information (regarding history, operating conditions, and maintenance of components) is collected, and all significant data are selected in a learning process using a reliability and maintainability - bank. Here the data are continuously updated (this is done with the CLP-method).

- Information on failure causes (in the widest sense) can be retrieved. A systematic observation shows failure patterns (pattern recognition).

Since a behaviour which may be common to different components can be realized it is possible to

a) eliminate redundant observations (data compression)

b) make a list of necessary requirements, and assumptions for failure diagnosis

c) introduce the automation of failure diagnosis and test procedures.

Reliability is a field which is strongly dependent on communication. We therefore appreciate comments on this presentation and on possible applications.

Kapitel 1 : Einleitung und Grundbegriffe

W. Häfele

Einführung zum Seminar über Zuverlässigkeitskontrolle

Institut für Angewandte Systemtechnik und Reaktorphysik

Wintersemester 1972/73

Wenn Naturwissenschaft als die Wissenschaft angesehen wird, die sich um die Erkenntnis naturgesetzlicher Zusammenhänge bemüht, dann ist Technik die Anwendung solcher Erkenntnis. Heute wissen wir deutlicher als früher, daß Naturwissenschaft, Technik und Mensch auch in einem zirkulärem Verhältnis zueinander gesehen werden müssen /1/. Jedoch ist das für die Zwecke dieses Seminars hier nicht unmittelbar von Bedeutung. Vielmehr ist es zunächst ausreichend, Technik als Anwendung der Naturwissenschaft zu verstehen.

Naturgesetzliche Zusammenhänge stellen praktisch immer eine Abstraktion dar. Im Hinblick auf den zur Untersuchung anstehenden bzw. in Rede stehenden Kausalzusammenhang ist von bestimmten Nebeneffekten abzusehen. Häufig bezeichnet der Techniker in seiner Alltagssprache solche Effekte auch als Schmutzeffekte. Der reine Kausalzusammenhang ist von dem Schmutz vordergründiger Faktizität zu lösen. Ein besonders schlagendes und historisch relevantes Beispiel dafür ist das Fallgesetz. Die tägliche Erfahrung legt es eben keineswegs nahe, daß alle Körper gleich schnell fallen. Vielmehr ist es durchgängige Erfahrung aller Buben und Mädchen, daß zum Beispiel beim winterlichen Rodeln alle Schlitten verschieden schnell am Fuße der Rodelbahn ankommen. Es war eben die Leistung Newtons, von den Schmutzeffekten der Reibung abzusehen, um auf den "Kern der Sache" des Fallgesetzes zu kommen.

Daß die Formulierung eines naturgesetzlichen Zusammenhanges auch noch in einem anderen, mehr grundsätzlichen Sinn eine Abstraktion mit sich zu bringen hat, läßt sich ebenfalls einsehen. Der Begriff Naturgesetz impliziert Allgemeingültigkeit. Das heißt, es soll der in Rede stehende naturgesetzliche Zusammenhang nicht an einen einzelnen Ort und an einen bestimmten Zeitpunkt gebunden sein (Orts, Zeit-Invarianz). Bei der Findung des naturgesetzlichen Zusammen-

hanges ist also von der Orts- und Zeitgebundenheit eines konkreten Vorganges abzusehen. In einer Mehrzahl der Fälle wird dem dadurch Rechnung getragen, daß der naturgesetzliche Zusammenhang die Form einer Differentialgleichung, meistens zweiter Ordnung, hat. Diese gilt dann allgemein. Die Rückeinbettung eines konkret zu betrachtenden einzelnen Vorganges erfordert dann neben der Lösung der Differentialgleichung auch die Berücksichtigung der Anfangs- bzw. Randbedingungen. Eben diese Anfangs- bzw. Randbedingungen vermitteln den Prozeß der Reabstraktion d.h. der Konkretisierung, es wird wieder ein konkreter Fall betrachtet. Wegen der mit dem konkreten Fall verbundenen Anfangs- bzw. Randbedingungen ist der konkrete Fall dann natürlich nicht mehr Orts/Zeit-invariant. Von daher ist es nun ganz natürlich einsehbar, daß Anfangs- bzw. Randbedingungen naturgesetzlich nicht ableitbar sind. Die eben angestellte Überlegung macht vielmehr deutlich, daß solche Anfangs- bzw. Randbedingungen vielmehr grundsätzlich eine andere Qualität als das Naturgesetz haben. Sie sind wie Leitern, die man für das Verlassen eines Flugzeuges (das abstrakte Naturgesetz) anlegt, wenn sich dieses nach der Landung an einen bestimmten Ort/Zeitpunkt wieder bindet. Anfangs- bzw. Randbedingungen haben kontingenten Charakter, sie sind nicht ableitbar sondern vielmehr je und je vorfindbar. Auf die Gleichrangigkeit naturgesetzlicher und kontingenter Elemente haben C.F. von Weizsäcker und Erhard Scheibe hingewiesen /2, 3/. Der Begriff "Kontingenz" hat eine bestimmte geistesgeschichtliche Tradition. Er leitet sich von dem griechischen ενδεχομαι her und ist aus dem Griechischen von Boetius in das Lateinische contingere übersetzt worden. Der Begriff der Kontingenz hat in der Scholastik eine gewisse Rolle gespielt. Eike Hirsch hat hierüber einen Bericht geschrieben /4/. Es zeigt sich, daß von der Geistesgeschichte des Kontingenzbegriffes her sich nur bedingt Hilfen für den hier in Rede stehenden naturwissenschaftlichen Zusammenhang ergeben.

Wenn Anfangs- und Randbedingungen vorgefunden werden müssen, ist das durch Messungen zu leisten. Messungen haben im naturwissenschaftlichen Bereich, jedenfalls im Sinne des hier vorgelegten Zusammenhangs (u.a. interessiert hier nicht die besondere begriffliche Situation des Meßprozesses in der Quantentheorie), zwei Funktionen:

1.) Messungen dienen als Hilfsmittel bei der Auffindung eines naturgesetzlichen Zusammenhanges.
2.) Messungen dienen der Bestimmung der Anfangs- bzw. Randbedingungen, wenn es um die Anwendung naturgesetzlicher Zusammenhänge auf einen konkreten

Fall, d.h. um die Lösung einer technischen Aufgabe geht.

Hier interessieren wir uns für das Letztere. Ist die Funktion der Messung für den hier vorgelegten Zusammenhang jetzt so umrissen, so hat man sich damit auseinanderzusetzen, daß bei den Messungen zur Bestimmung der kontingenten Anfangs- bzw. Randbedingungen nun wieder das Problem der Nebeneffekte bzw. Schmutzeffekte in seinem vollen Umfang in Erscheinung tritt. Wenn es um den konkreten Fall im Hier und Jetzt geht, nutzt es absolut gar nichts, einen Kausalzusammenhang "grundsätzlich" verstanden zu haben. Im konkreten Fall interessiert es überhaupt nicht, ob eine Maschine "grundsätzlich" geht. Auf diese Weise bekommt der Umgang mit Neben- und Schmutzeffekten schließlich den gleichen Rang wie Naturgesetz und die Ermittlung der kontingenten Anfangs- bzw. Randbedingungen. Der Umstand, daß es der Umgang mit Neben- und Schmutzeffekten und die Ermittlung der kontingenten Anfangs- und Randbedingungen ist, die hier neben dem Naturgesetz erscheinen, bezeichnet einen operativen Zug von Technik, während Naturwissenschaft so nicht über operative Züge verfügt (erneut soll auf die besondere Situation in der Quantentheorie im Gegensatz zur klassischen Physik hier nicht eingegangen werden, obwohl sich eben so eine direkte Verbindung von der Quantentheorie zur Technik ergeben dürfte).

Der hier entwickelte Zusammenhang wird vor allem dann wirksam, wenn technische Maschinen sehr groß werden, und wenn es um das Funktionieren solcher großen technischen Maschinen geht. Solange die funktionale Reichweite technischer Maschinen begrenzt bleibt, ist es möglich, das gelegentliche Versagen solcher Maschinen als Ausnahme und nicht eigentlich zum Wesen der Sache gehörig hinzustellen. Natürlich möchte man sich dagegen schützen. Man tut es, indem man bei der Fertigung der Teile der Maschine, bei ihrem Bau und beim Betrieb bestimmte Kontrollen durchführt. Qualitätskontrolle, Wartungen und Abnahmeprüfungen sind z.B. Begriffe, die das Vorgehen in der Vergangenheit, wo technische Maschinen eine gewisse Größe nicht überschritten, charakterisierten. Aber auch der etwas imponderable Begriff des "know-how" gehört hierher. Der so in etwa umrissene Bereich war aber in der Vergangenheit methodisch gesehen nur ein Wurmfortsatz naturwissenschaftlich/technischen Arbeitens. In gar keiner Weise erfuhr dieser Bereich das gleiche Maß geistiger Aufmerksamkeit, wie es der Bereich des Naturgesetzes und der Bereich des funktionalen Entwurfs technischer Maschinen erfuhr. Nicht geistige Anstrengungen auf der Höhe moderner

Physik sondern der Mechaniker mit der Ölkanne hatte für das sichere Funktionieren von Maschinen zu sorgen.

Wenn aber technische Maschinen sehr groß werden, erhöht sich wenigstens auch die damit verbundene funktionale Reichweite. Ein modernes Kernkraftwerk z.B. hat 1000 MWe. Eine solche Kapazität reicht aus, um ganz West-Berlin mit elektrischer Energie zu versorgen. Das technische System "Apollo" reicht bis zum Mond, und die Reichweite moderner Datenverarbeitunganlagen ist dabei, den ganzen Bereich staatlicher Administration und industrieller Tätigkeit zu umgreifen. Dann stellt sich die Frage des sicheren Funktionierens anders, als wenn es nur um das Funktionieren eines Autos oder eines elektrischen Motors oder einer Schreibmaschine geht. Beispielsweise das 'black-out' Ereignis im New Yorker Raum, bei dem Mitte der sechziger Jahre die Elektrizitätsversorgung für viele Stunden vollständig ausfiel, bezeichnet die neue Dimension der Frage nach dem sicheren Funktionieren technischer Maschinen bzw. technischer Systeme.

Um jenseits aller Zweifel das Funktionieren eines technischen Systems deterministisch sicherzustellen, ist es erforderlich, alle Anfangs- und Randbedingungen, d.h. alle kontingenten Bestimmungsstücke für alle anstehenden Kausalzusammenhänge zu kennen. Das wirklich zu bewerkstelligen, vermag nur ein Dämon, auf den Laplace sich bezogen hatte. Für Menschen ist das in einem absoluten Sinne nicht vollziehbar. Im Hinblick auf die Reichweite technischer Maschinen, um die es heute geht, soll der Gedanke der Vollziehbarkeit noch etwas weiter verfolgt werden.

Während ursprünglich der Gedanke der Vollziehbarkeit in der Physik keine besondere Rolle spielt, ist er mit der Kritik Einsteins an der bis dahin geltenden Vorstellung der Gleichzeitigkeit so in den Vordergrund gestellt worden, daß von daher die begriffliche Fundierung der Physik wesentlich geändert wurde. Von dem Bereich der Quantentheorie abgesehen ist es bei dem Gedanken der Vollziehbarkeit der Gleichzeitigkeit geblieben. Immerhin aber hat Popper bei logisch erkenntnistheoretischen Überlegungen die Vollziehbarkeit logischer Schlüsse angesprochen und sieht die Reichweite logischer Schlußfolgerungsketten durch das Kriterium der Vollziehbarkeit etwa durch mit Lichtgeschwindigkeit arbeitender elektronischer Rechenanlagen grundsätzlich begrenzt /5/.
Auch von daher erscheint es wenn nicht zwingend erforderlich, so doch naheliegend, den Gedanken der Vollziehbarkeit der Ermittlung aller Anfangs- und Rand-

bedingungen stärker als bisher in den Vordergrund zu bringen und die Konsequenzen einer Nicht-Vollziehbarkeit methodisch stärker zu untersuchen.

Bevor die sich daraus ergebenden Konsequenzen angesprochen werden, soll noch ein weiterer Gedankengang verfolgt werden: Die funktionale Reichweite moderner technologischer Systeme ist beträchtlich. Moderne Kernkraftwerke, das Unternehmen der Raumfahrt und moderne elektronische Datenverarbeitung waren als Beispiele genannt worden. Mit solcher Reichweite ergibt sich eben auch eine erhebliche Abhängigkeit von dem sicheren Funktionieren dieser Systeme. Der New Yorker black-out, und die Beinahe-Katastrophe von Apollo 13 sind Beispiele hierfür. Das ist aber in einem noch weiteren Zusammenhang zu sehen. Je stärker sich der Globus bevölkert, und je höher die Zivilisationsstufe der größer gewordenen Bevölkerung wird, desto mehr hängen Überleben und Lebensvollzug von dem sicheren Funktionieren der technischen Infrastruktur ab. Mit der Reichweite der Funktionalität eines technischen Systems geht also die Reichweite des Risikos einher. Nun gilt praktisch immer, daß das sichere Funktionieren eines technischen Systems um so mehr gewährleistet werden kann, je größer der Aufwand ist, den man dafür bereitstellt. Unter begrenzenden Bedingungen kann aber nicht unbegrenzter Aufwand getrieben werden. Somit ergibt sich bei allen technischen Systemen immer ein Restrisiko. Mehr als früher ist es erforderlich, mit dem Restrisiko quantitativ und methodisch vollkommener als bisher umzugehen. Dann ist es möglich, der Reichweite des Risikos die Reichweite technischer Zuverlässigkeit gegenüber zu stellen. Es ergeben sich also drei Dimensionen der Reichweite /6/. Es sind das die folgenden:

> Die Reichweite der Funktionalität eines technischen Systems,
> die Reichweite des Risikos,
> die Reichweite der technischen Zuverlässigkeit eines technischen Systems.

In dieser dreidimensionalen Reichweite gibt es die begrenzende Funktion der Kosten. Man mag einen Zusammenhang zu dem mehr und mehr im amerikanischen Raum sich ausbildenden Begriff risk/benefit analysis herstellen.

Nachdem durch die bisher angestellten Überlegungen die Bedeutung und der Rang methodischer Arbeiten für das sichere Funktionieren technischer Systeme klar gestellt worden ist, wenden wir uns jetzt der Frage zu, wie es um diese Methodik steht. Sie hat eine Situation unvollkommener Information über alle für

die sichere Lösung einer technischen Aufgabe relevanten Anfangs- und Randbedingungen zu behandeln. Daß diese Methodik noch nicht weit entwickelt ist, erkennt man beispielsweise an der folgenden Frage:

> Gegeben eine technischen Maschine (z.B. ein Kernkraftwerk);
> was hat man im einzelnen und als Funktion von n zu tun, um bei dieser technischen Maschine gezielt die Ausfallwahrscheinlichkeit von 10^{-n} auf $10^{-(n+1)}$ zu steigern?

In praktisch allen Fällen wird auf der Basis ingenieursmäßiger Erfahrung der sicherheitsmäßige Entwurf dadurch in qualitativer Weise verbessert, daß Sicherheitsvorkehrungen getroffen werden, die im Sinne solcher ingenieursmäßiger Erfahrung qualitativ bestimmte Forderungen mehr als abdecken. Man spricht von "over design".
Um diese Situation zu verbessern, kann man zweierlei tun:

1.) Man kann im Sinne deterministischen Vorgehens die Information über Anfangs- und Randbedingungen gezielt erhöhen.
Zum Beispiel die Arbeiten von L. Caldarola zur "Life time Prediction" gehen in diese Richtung.

2.) Man kann die Informationslücke hinsichtlich der im deterministischen Sinne vollständigen Kenntnis der Anfangs- und Randbedingungen durch Einsatz statistischer Methoden überbrücken. Man kommt zu dem Konzept der Ausfallwahrscheinlichkeit.
Zum Beispiel die Arbeiten von G. Weber zur Zuverlässigkeit technischer Systeme gehen in diese Richtung.

Das Seminar des Instituts für Angewandte Systemtechnik und Reaktorphysik über Zuverlässigkeitskontrolle soll über die heute bereitstehenden Methoden und Möglichkeiten berichten.

Schließlich sei zum Abschluß dieser Einführung noch auf einen weitergehenden Zusammenhang hingewiesen. Bisher ist die Methodik des Sichermachens eines technischen Systems auf Unfallerfahrung gewachsen. Man erinnert sich beispielsweise an den folgenden Vorgang: Wegen vieler platzender Dampfkessel war ein technisches Regelwerk zu erarbeiten. Auf der Erfahrung platzender Dampfkessel aufbauend war es der Dampfkesselüberwachungsverein, der solch Regelwerk erstellt hat. Daraus ist der Technische Überwachungsverein mit ganz breiter Aufgabenstellung hervorgegangen. "Unfallerfahrung" steht eigentlich für "Experi-

ment". Damit war bis jetzt technisches Arbeiten für die Sicherheit technischer Systeme in die Methodik naturwissenschaftlich/technischen Arbeitens eingebettet, d.h. es wurde der Iterationsprozeß: Hypothese, Experiment, verbesserte Hypothese, weiteres Experiment durchlaufen, bis der zugrundeliegende Sachverhalt erreicht war. Bei modernen technischen Systemen sehr großer Reichweite ist es aber nun nicht möglich, das umfassende Sicherheitsexperiment anzustellen, weil die Folgen zu weitreichend sind. Beispielsweise gilt das für den größten denkbaren Reaktorunfall. Aber auch im Bereich toxikologischer und genetischer Fragestellungen stoßen wir auf diesen Zusammenhang /7/. Das heißt aber, daß in solchen Fällen auf das Experiment, d.h. Unfallerfahrung verzichtet werden muß. Damit bleibt man notwendig im Bereich des Hypothetischen, wenn es darum geht, eine technische Maschine sicher zu machen. Auf die Grundsätzlichkeit dieses Vorganges und die sich daraus ergebenden Konsequenzen hat W. Häfele vor kurzem hingewiesen /8/. Um so entscheidender ist es, zu einer stark verbesserten Methodik der Zuverlässigkeitskontrolle zu kommen. Auch von daher sollte das Seminar des Instituts für Angewandte Systemtechnik und Reaktorphysik über Zuverlässigkeitskontrolle gesehen werden.

Referenzen:

/1/ siehe z.B.
A.M. Klaus Müller: "Die präparierte Zeit"
Radius Verlag, Stuttgart, 1972

/2/ C.F. v. Weizsäcker: "Komplementarität und Logik",
Die Naturwissenschaft, 42. Jg., Heft 19, S. 521
(1955)

/3/ E. Scheibe: "Die kontingenten Aussagen in der Physik"
Alheneum Verlag, Frankfurt, 1964

/4/ E. Chr. Hirsch: "Kontingenz - Erkenntnistheoretische
Probleme der Projektwissenschaft und die Theologie."
Unveröffentlichter Bericht, 1968

/5/ K.R. Popper: "Indeterminism in Quantumphysics and
in Classical Physics"
British Journal for the Philosophy of Science 1
117-33, und 173-95 (1950/51)

/6/ W. Häfele: "Ergebnis und Sinn des SEFOR-Experiments"
In: Einheit und Vielheit. Festschrift für C.F.
von Weizsäcker zum 60. Geburtstag herausgegeben von
E. Scheibe und G. Süßmann
Vanderhoeck & Ruprecht, Göttingen (1972)

/7/ D. Henschler (Würzburg): "Veränderungen der Umwelt -
Toxikologische Probleme"
Vortrag auf der 107. Versammlung der Gesellschaft
Deutscher Naturforscher und Ärzte am 10. Oktober 1972
in München

/8/ W. Häfele: "Fortschritt, Funktion und Einordnung der
Kernenergie"
Vortrag auf der 107. Versammlung der Gesellschaft
Deutscher Naturforscher und Ärzte am 10. Oktober 1972
in München

1.2 Grundbegriffe der Zuverlässigkeit

Ich möchte einige Grundbegriffe der Zuverlässigkeit (Reliability) einführen.

Dazu ist es zweckmäßig, zunächst vom Oberbegriff Qualität auszugehen. Diesem werden zwei Begriffe, Güte und Zuverlässigkeit , untergeordnet.

Diesen Begriffen können

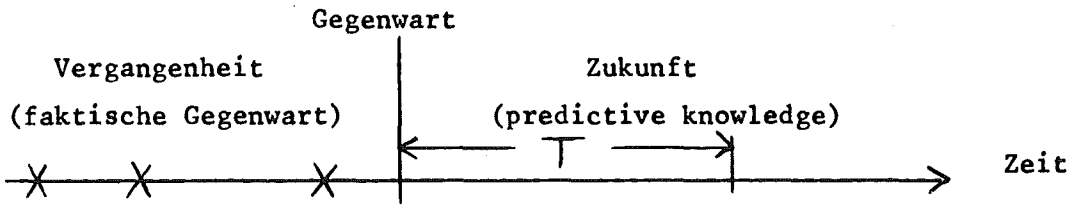
- Gütemerkmale und
- Zuverlässigkeitsmerkmale (oder Kenngrößen)

zugeordnet werden. Wir können zur Formulierung der Begriffe DIN-Normen /1/ oder VDI-Richtlinien /2/ verwenden. Entsprechende Normen gibt es z.B. für die USAEC /3/ und US-Air Force /4/.

Qualität ist die Beschaffenheit eines Erzeugnisses, die es durch den Verwendungszweck bedingten Anforderungen genügen läßt.

Gütemerkmale sind jederzeit in der Gegenwart feststellbar. Aussagen der Qualitätskontrolle, speziell auch der statistischen Qualitätskontrolle fallen in dieses Gebiet.

Zuverlässigkeit bezeichnet nicht allein Gütemerkmale, sondern Aufrechterhaltung der Gütemerkmale in der Zeit.



Wir gehen von Beobachtungen der Vergangenheit aus. Sie seien z.B. durch die Kreuze auf der Zeitachse gekennzeichnet. In der Gegenwart machen wir nun eine Voraussage für die Zukunft. Dies wird von machen Leuten auch als "predictive knowledge" bezeichnet oder als "designing of the future". Diese Voraussage ist für eine im Einzelfall festzulegende Zeitdauer T zu machen. /4/

Nach diesen absichtlich informellen Bemerkungen nun die Definition: /5/

> Zuverlässigkeit ist die Fähigkeit eines Erzeugnisses, denjenigen durch seinen Verwendungszweck bedingten Anforderungen zu genügen, die an das Verhalten während einer bestimmten Zeitdauer gestellt sind.

Ich habe hier zunächst die Methode offengelassen, die "Fähigkeit eines Erzeugnisses"anzugeben. Man kann dabei im wesentlichen 3 Typen von Aussagen unterscheiden /6/.

a) Klassifizierung als zuverlässig,
   Feststellung von Merkmalen

Beispiel: Eine Komponente ist aufgrund einer geeigneten Konstruktion als zuverlässig zu betrachten.

b) Vergleichende Aussagen,
   Vergleich von Merkmalen

Beispiel: Komponente A und Komponente B
können aufgrund einer geeigneten Konstruktion
als zuverlässig betrachtet werden.

Komponente A wurde einem Testbetrieb unterzogen, der beim Hersteller von B nicht gemacht wurde.

Komponente A ist also zuverlässiger als B.

Bei der sicher vorhandenen Bedeutung dieser Aussagen kann man jedoch nicht unmittelbar quantifizieren. Es wäre aber möglich, Überlegungen aus einem qualitativen Modell der Entscheidungstheorie zu verwenden.

c) Quantitative Aussagen über Kenngrößen

Es ist hier von besonderer Bedeutung, ein Wahrscheinlichkeitsmaß zu verwenden.
Es ist wichtig durch Verwendung aller drei Aussagetypen zu einer möglichst vollständigen Aussage zu gelangen. Es ist jedoch auch von Bedeutung, jeweils einen der Aussagetypen in verschiedener Hinsicht zu untersuchen. Dies ist in unserem Falle die durch ein Wahrscheinlichkeitsmaß quantifizierte Aussage /6/.

Dazu möchte ich einige Kenngrößen der Reliability einführen.
Diese sind

R(t)	- Zuverlässigkeitsfunktion	(Reliability)
F(t)	- Ausfallwahrscheinlichkeit	(Failure probability)
λ, μ	- Ausfallrate und Reparaturrate	(hazard rate, repair rate)
A	- Verfügbarkeit	(Availability)

Def. 1 Die Zuverlässigkeitsfunktion (Reliability) R(t) ist die Wahrscheinlichkeit, daß eine Komponente unter bestimmten Bedingungen für eine bestimmte Zeit t ihre Funktion ausübt. /1,5,7/

Diese Def. der Zuverlässigkeit ist allgemein üblich. Sie kann jedoch der Anforderung einer möglichst "vollständigen Aussage" aus verschiedenen Gründen nicht genügen. Ein Vorschlag, der meines Erachtens diesen Anforderungen gerecht wird, wird von L. Caldarola in Abschnitt 6.1 gemacht. Er wird bei der "Continuous Life Time Prediction" verwendet.

Um gegen das Fachgebiet abzugrenzen, wird diese Funktion auch bisweilen Reliability-Funktion genannt. Die Zuverlässigkeitsfunktion ist eine Kenngröße der Zuverlässigkeit. R(t) ist eine im weiteren Sinn monoton abfallende Funktion von t. (Abb. 1)
Sie nimmt stets die Werte

$$R(o) = 1 \qquad \text{und } R(\infty) = 0$$

an. Diese Aussage gilt, wenn wir eine nicht reparierbare Komponente voraussetzen. Man kann im Zusammenhang mit der Informationstheorie auf eine grundsätzlich andere Kenngröße kommen. Sie wird auf Grund einer Konvention auch als Reliability bezeichnet.

Def. 2 Die Ausfallwahrscheinlichkeit F(t) ist die Wahrscheinlichkeit, daß eine Komponente bis zur Zeit t ausfällt.

Abb. 1 (Ausfallwahrscheinlichkeit)

Dies ist - ebenfalls für nicht reparierbare Komponenten - eine im weiteren Sinne ansteigende Funktion. Es ist eine Aufgabe der Reliability

- festzustellen, durch welche Mittel ein unkontrolliertes Ansteigen von F(t) verhindert werden kann.

- Dieses unkontrollierte Risiko kann z.B. durch Reparatur und durch Wartungsmaßnahmen eingeschränkt werden.
  (preventive maintenance)/7,8/

Def. 3 Die Ausfallrate läßt sich mit Hilfe der Zuverlässigkeitsfunktion definieren:

$$\lambda(t) := -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt}$$

Nun kann die Ausfallrate jedoch folgendermaßen als bedingte Wahrscheinlichkeit interpretiert werden:

$\lambda(t)\,dt = P\{$Komponente fällt aus in$(t, t+dt)$, unter der Bedingung, daß sie bis zur Zeit t nicht ausgefallen ist$\}$

Es ist $F(t) = 1-R(t)$ nach unserer Definition

also $dF(t) = -dR(t)$

Die Normierung von $-dR(t)$ durch $R(t)$ führt zu

$$\lambda(t)\,dt,$$

einem Ausdruck, den wir als bedingte Wahrscheinlichkeit interpretieren können.

Eng mit der Ausfallrate verbunden ist die

Mittlere Lebensdauer $\bar{t}$. Sie ist als

$$\bar{t} := \int_0^\infty t f(t)\,dt$$

definiert.

Dabei setzen wir voraus, daß die Ausfallwahrscheinlichkeit F(t) auch eine Dichte f(t) hat.

Es scheint mir besonders wichtig zu sein, darauf hinzuweisen, daß Ausfallrate und mittlere Lebensdauer in Frequenzeinheiten (hr^{-1}) bzw. Zeiteinheiten (hr) angegeben werden. Reliability, Ausfallwahrscheinlichkeit und Verfügbarkeit sind dimensionslose Kenngrößen. Auf die Tests zur Schätzung bzw. Voraussage dieser Kenngrößen will ich hier nicht eingehen. Es ist jedoch nötig, einiges zur Verwendung der Ausfallrate zu sagen .

Es ist in vielen Fällen notwendig, den soeben definierten Begriff der Ausfallrate zu verallgemeinern.

Nehmen wir an, ein Schalter sei die dabei betrachtete Komponente.

Er kann durch zwei Größen gekennzeichnet werden, die als "partial Failure rates" bezeichnet werden /8/.

λ_1 gibt die Zahl der Ausfälle pro 10^6 h

λ_2 gibt die Zahl der Ausfälle pro 10^6 Schaltoperationen,

z.B. $\lambda_2 = 0{,}5$ failures/10^6 operations

Wissen wir die durchschnittliche Zahl der Schaltungen pro Stunde, z.B. 30/h, so können wir

$$\lambda'_2 = 30 \text{ operations/hour} \times 0{,}5 \text{ failures}/10^6 \text{ operations}$$

$$= 15 \text{ failures}/10^6 \text{ hours}$$

erhalten:

$$\lambda_{\text{gesamt}} = \lambda_1 + \lambda'_2$$

Wir stellen dabei fest, daß der Beitrag von λ_1 (partial failures rate) klein gegen den durch die Anzahl der Schaltoperationen stark modifizierten Beitrag von λ_2 (partial failures rate) ist. Es ist somit von erstrangiger Bedeutung, die Zahl der Schaltoperationen wenigstens größenordnungsmäßig zu kennen.

Dazu kommen noch Faktoren, die von Folgendem abhängen können:

- Schockbeanspruchung
- Vibrationsbeanspruchung
- Mittel des Herstellers zur Qualitätskontrolle
- Art des Gebrauchs und Dauer des Einsatzes

Diese Einzelheiten sind aus einem offiziellen Dokument des amerikanischen Department of Defence, dem MIL HDBK 217A /8/, verkürzt übernommen. Sie sollen den grundsätzlichen Ausführungen zur Statistik und zum Lifetime-Predictor nicht vorgreifen /9/.

Wir wollen nun eine weitere Kenngröße definieren:

Die Reparaturrate

Dabei gehen wir von einer ähnlichen Überlegung aus, wie es bei der Interpretation von $\lambda(t)$, der Ausfallrate, gemacht wurde,

$$\mu(t)dt = P\{\text{Komponente wird repariert in } (t,t+dt), \text{unter der Bedingung, daß sie bis zur Zeit t nicht ersetzt wurde.}\}$$

Selbstverständlich nehmen wir hier einen anderen Ursprung 0 unserer Zeitachse, nämlich den Zeitpunkt, für den die Komponente ausfiel.

Wir wollen in diesem Zusammenhang einen interessanten Spezialfall betrachten.

Wir nehmen an

- die Ausfallrate und
- die Reparaturrate seien konstant.

Die Annahmen werden in der Praxis sehr oft gemacht und liegen einem Teil unserer Seminarreihe zugrunde. Wir können jedoch leicht zu Fällen gelangen, in denen keine Konstante zu erwarten ist. Einen dieser Fälle werde ich bei unseren Beispielen zeigen. (2.1)

Ich möchte nun eine Komponente beschreiben, die reparierbar ist. Sie kann in zwei Zuständen sein. Wir bezeichnen mit

"1" den Zustand der Funktionsfähigkeit (dieser Komponente) und mit

"0" den Ausfallzustand (dieser Komponente)

Das Ereignis des Ausfalls kann als Übergang $1 \longrightarrow 0$ beschrieben werden.

Das Ereignis der Reparatur kann als Übergang $0 \longrightarrow 1$ beschrieben werden.

$1 \longrightarrow 0$ sei durch eine konstante Ausfallrate λ gekennzeichnet.

$0 \longrightarrow 1$ sei durch eine konstante Reparaturrate μ gekennzeichnet.

Dies kann immer so verstanden werden, daß das System durch bedingte Wahrscheinlichkeiten beschrieben werden kann, die nur vom vorherigen Zustand abhängen. Sie hängen nicht von der Vergangenheit ab.

Wir erhalten lineare Differentialgleichungen mit konstanten Koeffizienten.

Ihre Lösung sind

$$P_{11}(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$$P_{01}(t) = \frac{\mu}{\lambda+\mu} - \frac{\mu}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$$P_{00}(t) = \frac{\lambda}{\lambda+\mu} + \frac{\mu}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$$P_{10}(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

Geht nun $t \longrightarrow \infty$, so erhalten wir (Abb. 2) :

$$\lim_{t \to \infty} P_{11} = \lim_{t \to \infty} P_{01} = \frac{\mu}{\lambda+\mu} = A_{\infty} \qquad x)$$

Wir definieren

$$A(t) = P_{11}(t) \quad \text{und} \quad A_{\infty} = \frac{\mu}{\lambda + \mu}$$

als Verfügbarkeit. Haben wir konstante λ, μ, so ist eine unmittelbare einleuchtende Interpretation möglich. Sei

$\bar{t}_b = \frac{1}{\mu}$ die mittlere Zeit,

für die eine Komponente in Betrieb ist

$\bar{t}_r = \frac{1}{\mu}$ die mittlere Zeit,

für die eine Komponente ausgefallen
(d.h. in Reparatur ist)

Dan gilt

$$A_{\infty} = \frac{\bar{t}_b}{\bar{t}_b + \bar{t}_r} \qquad /10/.$$

A_{∞} bezeichnet die Verfügbarkeit für den stationären Zustand.

---

x) Anmerkung: /11/

$P_{ij}(t)$ ist die Wahrscheinlichkeit, daß eine Komponente zum Zeitpunkt im Zustand j ist, unter der Bedingung, daß sie zum Zeitpunkt t = 0 im Zustand i war.
Für große t " vergißt" die Komponente ihren Ausgangszustand. Darum ist es plausibel, daß die Größen, die sich nur durch ihren Anfangszustand unterscheiden, auf den gleichen Grenzwert A_{∞} konvergieren. Dies ist auch aus den Differentialgleichungen zu entnehmen.

Die Verfügbarkeit ist hier derjenige Bruchteil der gesamten zu betrachtenden Zeit, für den eine Komponente in Betrieb ist.

Die Verfügbarkeit wird manchmal ohne Wahrscheinlichkeit betrachtet. Sie macht dann keine Vorhersage, sondern gibt ein an einem System beobachtetes Merkmal. /13,14/

1.3 Serien- und Prallelschaltungen

Wir zeigen die Zuverlässigkeit von Serien- und Parallelschaltungen von Komponenten (siehe auch 2.1 Systemreliability). Damit wird der Grund zu einigen Fragen der Redundanztechnik und Systemreliability gelegt.

Ein System aus n Komponenten sei folgendermaßen definiert:

Serienschaltung:

Ein System, das genau dann funktioniert, wenn alle n Komponenten funktionieren.

Parallelschaltung:

Ein System, das dann funktioniert, wenn wenigstens eine der n Komponenten funktioniert.

Das zu betrachtende System bestehe zunächst aus 2 Komponenten, A, B.

Wir werden bei Serien- und Parallelschaltungen allgemein feststellen, daß die Reihenfolge des Ausfalls (A vor B, B vor A) nichts ausmacht.

1. Wir nehmen ein System an, das genau dann funktioniert, wenn A und B funktionieren (Serienschaltung), (Abb. 3).

a_1) Unter der Bedingung 'A ausgefallen vor t'
ist

$$P\{\text{Funktion des Systems bis t/A ausgefallen vor t}\} = 0$$

b_1) Unter der Bedingung 'A nicht ausgefallen vor t'
ist

$$P\{\text{Funktion des Systems bis t/A nicht ausgefallen vor t}\}$$

$$= P\{\text{B nicht ausgefallen vor t}\} = R_B(t)$$

Zu a_1 : Für eine ausgefallene Komponente A
ist (Serienschaltung angenommen) das System ausgefallen.

Zu b_1 : Für eine nicht ausgefallene Komponente A hängt (Serienschaltung angenommen) der Systemausfall nur noch von B ab.

Also :

$$R_s(t) = 0 \cdot (1 - R_A(t)) + R_B(t) \cdot R_A(t)$$

$$= R_A(t) \cdot R_B(t)$$

Daraus kann man ersehen, daß ein System, in gleicher Weise von der Funktion von A und B abhängt.

Aus Symmetriegründen wollen wir dieselben Überlegungen auch mit Komponente B ausführen.

a_2) Unter der Bedingung 'B ausgefallen vor t'
ist

$$P\{\text{Funktion des Systems bis t/B ausgefallen vor t}\} = 0$$

b_2) Unter der Bedingung 'B nicht ausgefallen vor t' ist

$$P\{\text{Funktion des Systems bis t/B nicht ausgefallen vor t}\}$$

$$= P\{\text{A nicht ausgefallen vor t}\} = R_A(t)$$

Zu a_2) und b_2) gelten die Aussagen von a_1) und b_1) <u>wenn</u> wir A und B vertauschen.

Also:

$$R_s(t) = 0 \cdot (1 - R_B(t)) + R_A(t) \cdot R_B(t)$$

$$= R_A(t) \cdot R_B(t)$$

Wir kommen also - unabhängig von der Reihenfolge des Ausfalls- auf dieselben Werte für die Systemreliability $R_s(t)$.

2. Wir nehmen ein System an, das dann funktioniert, wenn <u>wenigstens eine</u> seiner Komponenten A,B funktioniert (Parallelschaltung),(Abb. 4).

a_1) Unter der Bedingung 'A ausgefallen vor t' ist

$$P\{\text{Funktion des Systems bis t/A ausgefallen vor t}\} = R_B(t)$$

b_1) Unter der Bedingung 'A nicht ausgefallen vor t' ist

$$P\{\text{Funktion des Systems bis t/A nicht ausgefallen vor t}\} = 1$$

Zu a_1: Für eine ausgefallene Komponente A ist (Parallelschaltung angnommen) die Funktion des Systems nur noch von der Funktion der Komponente B abhängt.

Zu b_1 : Für eine nicht ausgefallene Komponente A ist (Parallelschaltung angenommen) ist die Funktion des Systems gesichert. (Es funktioniert mit Wahrscheinlichkeit 1).

Sei nun

$$P\{A \text{ ausgefallen vor } t\} = 1 - R_A(t),$$

dann gilt:

$$R_s(t) = R_B(1-R_A(t)) + 1 \cdot R_A(t)$$

$$= 1 - (1-R_A(t)) \cdot (1 - R_B(t))$$

Dies ist als die Systemzuverlässigkeit einer Parallelschaltung zu bezeichnen.

Aus Symmmetriegründen gilt weiterhin:

a_2) Unter der Bedingung 'B ausgefallen vor t' ist

$$P\{\text{Funktion des Systems bis t/B ausgefallen vor t}\} = R_A(t)$$

b_2) Unter der Bedingung 'B nicht ausgefallen vor t' ist

$$P\{\text{Funktion des Systems bis t/B nicht ausgefallen vor t}\} = 1$$

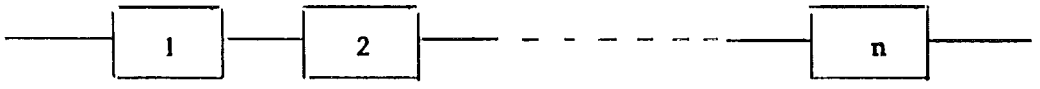
Diese für zwei Komponenten ausgeführten Überlegungen wollen wir nun auf

- Serienschaltungen bzw.
- Parallelschaltungen

von n Komponenten erweitern.

Dies ist ein weiterer Schritt zur Systemreliability. Wir werden dabei auch sehen, daß die Zuverlässigkeitsfunktion stark von der Zahl der durch sie beschriebenen Komponenten abhängt.

In einer <u>Serienschaltung</u> können wir sagen, daß das System dann funktioniert wenn alle Komponenten funktionieren.



Nehmen wir nun noch an, daß für alle einzelnen Komponenten die Reliability-Funktion gleich ist,

$$R(t),$$

so erhalten wir

$$R_s(t) = (R(t))^n$$

in einer offensichtlichen Verallgemeinerung des Beispiels Nr. 1.

Eine hinreichend lange Serienschaltung kann die Systemzuverlässigkeit klein gegen R(der Einzelkomponente) machen. Diese Gefahr muß mit geeigneten Mitteln aus dem Wege geräumt werden. D.h. es sind Redundanzen oder andere Mittel zur Zuverlässigkeitssicherung zu verwenden.

In einer Parallelschaltung können wir sagen, daß das System immer funktionsfähig bleibt, solange wenigstens eine der n Komponenten funktioniert. Als Systemzuverlässigkeit erhalten wir

$$R_s(t) = 1 - (1 - R(t))^n$$

Dies gilt wieder unter der Annahme, daß für alle Komponenten dieselbe Zuverlässigkeit vorliegt. Durch eine hinreichende Erhöhung der Redundanz können wir die Zuverlässigkeit beliebig nahe an 1 bringen.

Dies ist meist ein sehr kostspieliges Verfahren. Man kann aber zeigen, daß

- wenn die Kosten linear ansteigen
- sich die Ausfallwahrscheinlichkeit annähernd exponentiell verkleinert.

Diese angenehmen Eigenschaften der Redundanz sind jedoch nicht mehr vorhanden, wenn 2 Typen von Fehlern möglich sind. Dann werden andere Methoden der Zuverlässigkeitssicherung erforderlich /13/.

Sie gelten überdies nur für nichtreparierbare Komponenten. Wie in Kap. 3 und 6 gezeigt wird, treten bei reparierbaren Komponenten andere Eigenschaften in den Vordergrund.

Literaturverzeichnis und Anmerkungen zu 1.2, 1.3

1. DIN-Norm 40041, Zuverlässigkeit elektronischer Bauelemente, Begriffsbestimmungen

2. VDI-Richtlinien, z.B. VDI 4004, Blatt 2, (Entwurf), November 1972

   Die VDI-Richtlinien werden in einem VDI-Handbuch "Zuverlässigkeit" (Herausgeber Dr. H.J. Keller, Messerschmidt-Bölkow-Blom) zusammengefaßt.

3. U.S. Atomic Energy Commission, Reliability Standards Committee: RDT-Standard for Reliability and Maintainability (Oakridge), siehe auch Compilation of United States Nuclear Standards, ORNL-NSIC-57, UC80 Reactor Technology, W.B. Cottrell, NSB-Special Committee, 1968

4. J.J. Naresky (Rome Air Development Center), Reliability Definitions, IEEE-Trans.on Reliability Vol. R 19, no. 4 (November 1970)

5. DIN-Norm 40041 und
   W. Görke, Zuverlässigkeitsprobleme elektronischer Schaltungen, B.I., Mannheim 1969

6. W. Stegmüller, R. Carnap, Induktive Logik und Wahrscheinlichkeit, Wien 1958

7. R.E. Barlow und F. Proschan
   Mathematical Theory of Reliability, John Wiley (1965)

8. MIL - HDBK - 217A:
   Military Standardisation Handbook, Reliability Stress and Failure Rate Data for Electronic Equipment,
   Department of Defense, Washington D.C., December 1965

9. In einem besonderen Kapitel (Continuous Life Time Predictor) wird auf ein allgemeines Modell zur Behandlung von Ausfallraten unter Stress eingegangen (L. Caldarola). Hier ist zunächst festzuhalten, daß eine Nichtbeachtung zu unsinnigen Werten führen könnte. Ohne theoretische Begründung wurde dieser Gesichtspunkt auch in der Arbeit Dr. Heusers aufgenommen.

10. Die Verfügbarkeit, als Quotient von $\bar{t}_b$ [hr] und ($\bar{t}_b + \bar{t}_r$) [hr] ist dimensionslos.

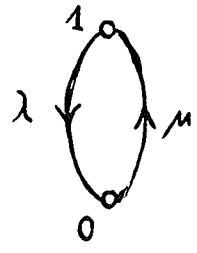
11. W. Feller, An Introduction to Probability Theory and its Applications,
Third Ed., Vol. 1
John Wiley & Sons, Inc., New York 1968

12. Zur Verfügbarkeit

Aus den Wahrscheinlichkeiten für die Zustände 1,0 und den Raten λ, μ

$P_1(t + h) = (1 - \lambda)\, h\, P_1(t) + \mu h\, P_o(t) + O(h)$

$P_o(t + h) = \mu h\, P_1(t) + (1 - \lambda)\, h\, P_o(t) + O(h)$ erhält man folgende Differentialgleichungen:



$$\frac{d\,P_1(t)}{dt} = -\lambda P_1(t) + \mu P_o(t)$$

$$\frac{d\,P_o(t)}{dt} = \lambda P_1(t) - \mu P_o(t)$$

Diese werden durch Laplace-Transformation in lineare Gleichungen umgewandelt. Wir erhalten:

$$\begin{pmatrix} P_1(0) \\ P_o(0) \end{pmatrix} = \begin{pmatrix} s+\lambda & -\mu \\ -\lambda & s+\mu \end{pmatrix} \cdot \begin{pmatrix} L\{P_1\} \\ L\{P_o\} \end{pmatrix}$$

Zum Zeitpunkt t=0 möge das Geräte mit der Wahrscheinlichkeit α in Ordnung sein. Damit haben wir als Anfangsbedingungen:

$$P_1(0) = \alpha$$
$$P_o(0) = 1 - \alpha \qquad 0 \leq \alpha \leq 1$$

Wir erhalten, nach Rücktransformation, folgende Lösung:

$$P_1(t) = \frac{\mu}{\mu + \lambda} \left(\alpha - \frac{\mu}{\mu+\lambda}\right) e^{-(\lambda+\mu)t}$$

Mit $\alpha_1 = 1$, bzw. $\alpha_o = 0$, also

$$P_{11}(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda}\, e^{-(\lambda+\mu)t}$$

$$P_{01}(t) = \frac{\mu}{\mu+\lambda} - \frac{\lambda}{\mu+\lambda}\, e^{-(\lambda+\mu)t}$$

13. L. Caldarola, G. Weber, KFK 640,

General Criteria to Optimize the Operation of a Power Plant with Special Considerations to its Safety Requirements, Karlsruhe, August 1967

14. Dr. Vetter, Verfügbarkeitsuntersuchungen für Grundlastkraftwerke, Mitt. d. Ver. der Großkesselbesitzer e.V., Heft 96, Juni 1965, S. 135

sowie

W. Fehndrich, W. Hlubek, D. Vetterkind
Zuverlässigkeitsprobleme von der Planung bis zum Betrieb thermischer Kraftwerke
Tagung "Technische Zuverlässigkeit 1973", Nürnberg, Tagungsheft p. 86-89

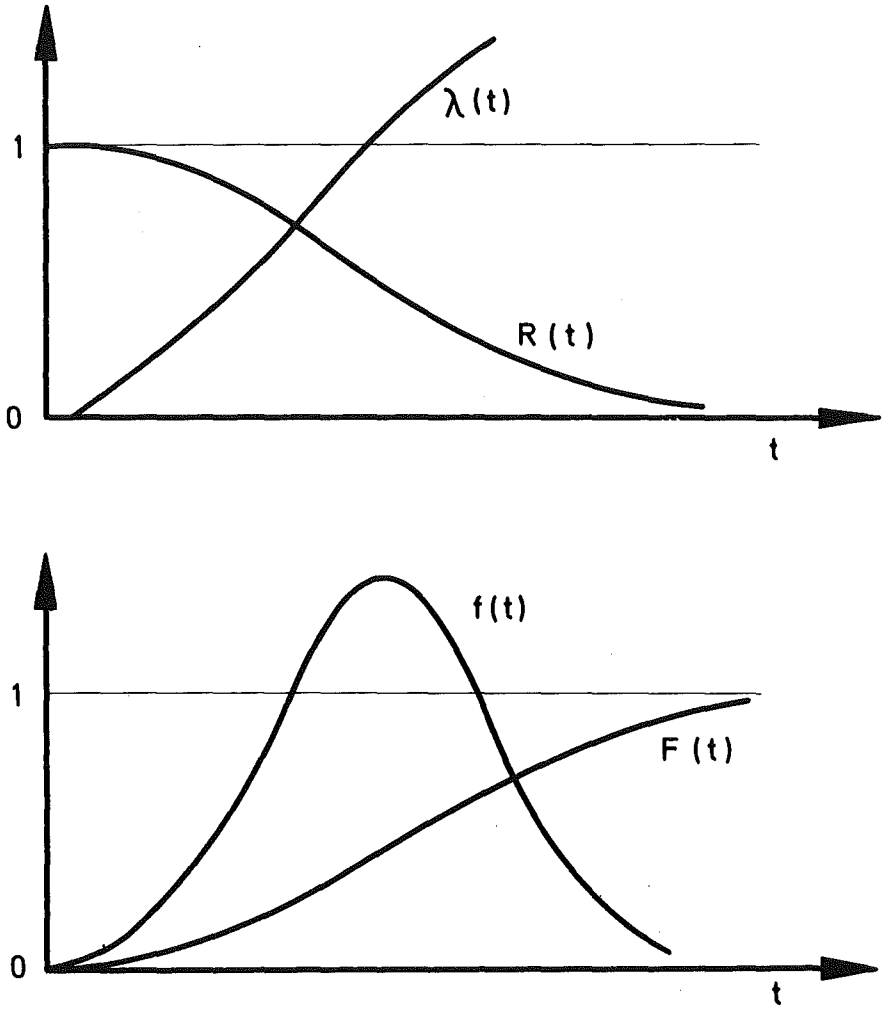


Abb. 1

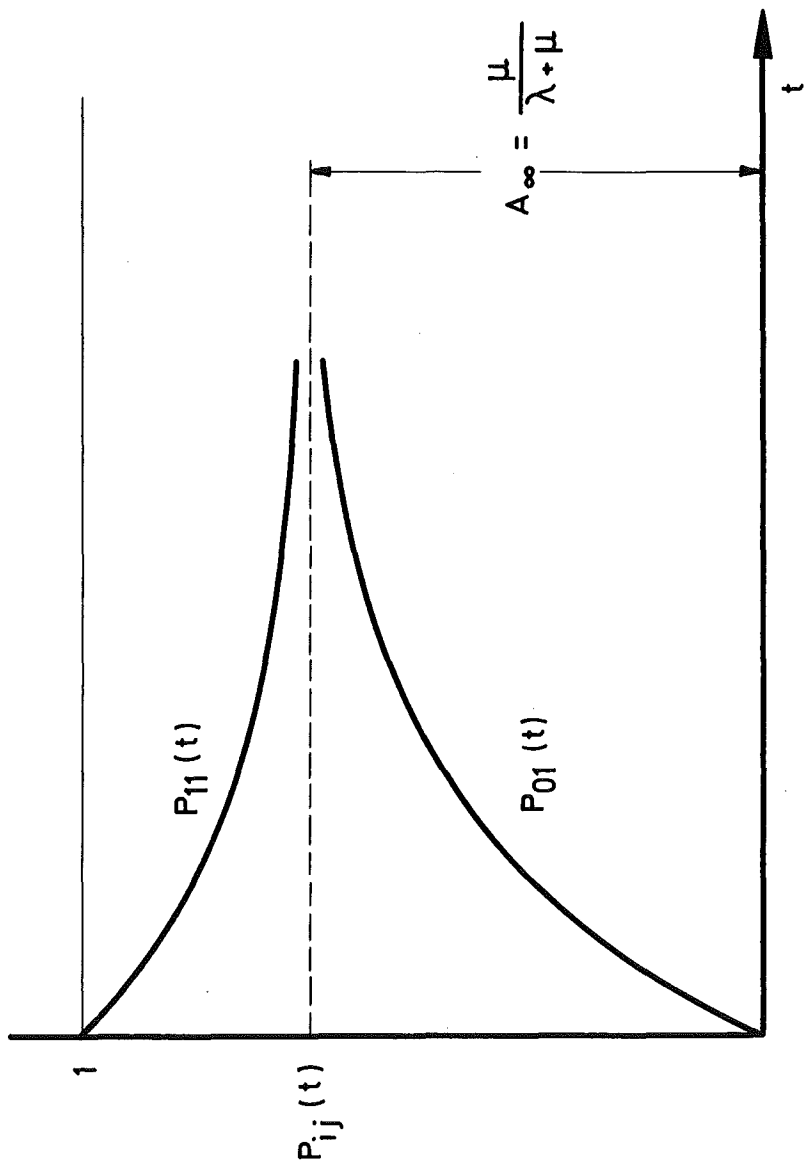
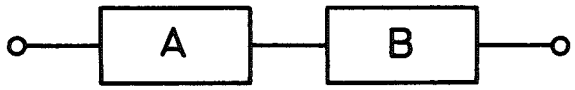


Abb. 2

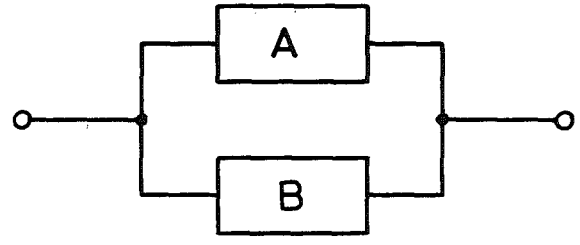


$$R_S = R_{S,A} \cdot R_A + R_{S,\bar{A}} \quad (1 - R_A)$$

$$= R_{S,B} \cdot R_B + R_{S,\bar{B}} \quad (1 - R_B)$$

$$= R_A \cdot R_B + 0 \quad (1 - R_A)$$

Abb. 3



$$R_S = R_{S,A}\, R_A + R_{S,\bar{A}}\,(1 - R_A)$$

$$= 1 \cdot R_A + R_B\,(1 - R_A)$$

$$= 1 - (1 - R_A)\,(1 - R_B)$$

Abb. 4

Kapitel 2 : Systemreliability

G. Weber

2. Systemreliability

2.1 Einfache Beispiele

Wir wollen nun mit den Grundbegriffen einige Zuverlässigkeitsaussagen über einfache Systeme machen.

Dabei setzen wir voraus:

Jede Komponente kann genau zwei Zustände annehmen:

(1) funktionsfähigkeit und

(0) ausgefallen

Die Komponenten können an zufälligen Zeitpunkten von (1) nach (0) übergehen.

Eine Reparatur findet nicht statt.

Jeden Übergang von einem Zustand in einen anderen nennen wir ein Ereignis.

> Wir verknüpfen die zufälligen Ereignisse nach den Regeln der Logik und werten diese Ereignisse nach den Regeln der Wahrscheinlichkeitsrechnung aus.

Es kann darüberhinaus gesagt werden, ob die Ausfallrate monoton ist. Diese Fragen sind von Bedeutung für eine Entscheidung, ob eine sogenannte präventive Maintenance (Wartung) Kostenmäßig Vorteile oder Nachteile bringt. Nur wenn die Ausfallrate ansteigt ist eine präventive Maintencance kostenmäßig von Vorteil.

Wenn Komponenten eine konstante Ausfallrate haben, ist eine präventive Maintenance, genauer ein präventives Ersetzen eines Bauteils ohne kostenmäßige Vorteile gegenüber einer Reparatur.

Ich möchte nun ein System zeigen, das aus zwei verschiedenen Komponenten mit konstanten Ausfallraten zusammengesetzt ist.

1. Serienschaltung

Zwei Komponenten A,B seien in Serie geschaltet,(vgl.1.3).Der Ausfall einer Komponente ist dann der Systemausfall.

Ihre Dichten f_A, f_B, bzw. Ausfallwahrscheinlichkeiten F_A, F_B sind

$$f_A(t) = \lambda_A e^{-\lambda_A t} \quad , \quad F_A(t) = 1 - e^{-\lambda_A t}$$

$$f_B(t) = {}_B e^{-\lambda_B t} \quad , \quad F_B(t) = 1 - e^{-\lambda_B t}$$

Damit erhalten wir für die Zuverlässigkeit des Systems

$$R_s(t) = e^{-(\lambda_A + \lambda_B)t}$$

und für die Ausfallrate des Systems

$$\lambda_S = -\frac{1}{R_S(t)} \quad \frac{dR_S(t)}{dt} = \lambda_A + \lambda_B$$

2. Prallelschaltung (Redundanz)

Zwei Komponenten A,B seien parallel- geschaltet (vgl.1.3) . Der Ausfall von A und B ist der Systemausfall.

Die Ausfallraten λ_A, λ_B seien gleich,

$$\lambda_A = \lambda_B = \lambda$$

Ihre Dichten f_A, f_B bzw. Ausfallwahrscheinlichkeiten F_A, F_B sind

$$f_A(t) = f_A(t) = \lambda e^{-\lambda t} \quad , \quad F_A(t) = F_B(t) = 1 - e^{-\lambda t}$$

Damit erhalten wir für die Zuverlässigkeit des Systems

$$R_s(t) = e^{-\lambda t} + e^{-\lambda t} - e^{-\lambda t} \cdot e^{-\lambda t}$$

und für die Ausfallrate des Systems

$$\lambda_S(t) = -\frac{1}{R_s(t)} \cdot \frac{dR_s(t)}{dt} = -\frac{2(-\lambda e^{-\lambda t}) + 2\lambda e^{-2\lambda t}}{2e^{-\lambda t} - e^{-2\lambda t}}$$

$$= \frac{2\lambda - 2\lambda e^{-\lambda t}}{2 - e^{-\lambda t}}$$

Damit ist die System-Ausfallrate nicht mehr konstant. Sie konvergiert jedoch gegen λ, d.h. bei hinreichender Größe von t (Zeit) ist das System defakto nur noch von der länger lebenden Komponente bestimmt. Eine Aussage welche Komponente hier vermutlich länger lebt ist nicht möglich (Folge von $\lambda_A = \lambda_B$).

Im Folgenden seien die Ausfallraten verschieden.

Zwei Komponenten, 1,2, seien wieder parallel geschaltet.
Der Ausfall von beiden Komponenten ist der Systemausfall.
Die Ausfallraten seien

$$\lambda_1 = 1/\text{Jahr}$$

$$\lambda_2 = 2/\text{Jahr}$$

Ihre Dichten f_i bzw. Ausfallwahrscheinlichkeiten F_i sind:

$$f_1(t) = e^{-t} \qquad F_1(t) = 1-e^{-t}$$

bzw.

$$f_2(t) = e^{-2t} \qquad F_2(t) = 1-e^{-2t}$$

Damit erhalten wir für die Zuverlässigkeit des Systems

$$R_s(t) = e^{-t} + e^{-2t} - e^{-t} \cdot e^{-2t}$$

und für die Ausfallrate des Systems

$$\lambda_s(t) = \frac{1}{R_s} \cdot \frac{dR_s}{dt} = \frac{e^{-t}\left[1+2e^{-t} - 3e^{-2t}\right]}{e^{-t}\left[1 + e^{-t} - e^{-2t}\right]}$$

Das damit beschriebene λ_s steigt offenbar an und fällt später wieder ab.

Wir haben eine Ausfallrate, die von 0 ansteigt, jedoch später wieder absinkt und asymptotisch gegen 1 geht. Dies bedeutet, daß das System auf lange Sicht sich wie eine Einzelkomponente verhält. 1/Jahr ist die Ausfallrate der durchschnittlich länger lebenden Komponente. Die Frage der Maintenance eines Systems ist jedoch anders als die der Einzelkomponente zu beurteilen.

Das heißt: Im Anfang der Verwendung des Systems ist eine Maintenance auf Systemebene auf jeden Fall gerechtfertigt.

2.2 Definition des Fehlerbaums, Ereignisverknüpfung und Logik

Diese Einführung in die System-Reliability setzt Abschnitt 2.1 voraus. Dazu sollen jedoch - insbesondere im Hinblick auf komplexe Systeme- allgemeine Begriffe eingeführt werden.

Unter Verwendung einiger Begriffe aus der Graphentheorie soll der Fehlerbaum definiert werden. Damit sind sehr wirksame Methoden zur Verknüpfung vieler Einzelereignisse möglich geworden.

Um die Art dieser Verknüpfungen besser zu verstehen, ist es von Bedeutung, eine Einführung in einen Zweig der formalen Logik zu geben. Dies ist die Aussagenlogik.

Danach wird die Anwendung der Aussagenlogik auf Fehlerbäume gezeigt. Der Zusammenhang mit einem kombinatorischen Netzwerk kommt hier herein.

2.21 Definition des Fehlerbaums

Graphentheoretische Begriffe

Für die Definition des Fehlerbaums ist es notwendig, einige Begriffe aus der Graphentheorie (oder aus der Theorie der Inzidenzstrukturen) zu verwenden.

Die notwendigen Grundbegriffe werden mit Abb.1 und Abb. 2 erläutert.

Abb. 1 zeigt ein Beispiel eines gerichteten Graphen. Er besteht aus Ecken und Kanten.

- Die Ecken (vertices) sind nummeriert (Abb. 1, 2) (von 1 bis 10).

- Die Kanten (arcs) verbinden je zwei Ecken (z.B. 2 und 8).(Abb. 1, 2). Alle Kanten sind gerichtet. Dieser Richtung entsprechend reden wir auch von einer Anfangsecke und einer Schlußecke einer Kante.

  Die Anfangsecke ist unmittelbarer Vorgänger der Schlußecke (predecessor). Z.B. ist 1 predecessor von 7.

  Die Schlußecke ist unmittelbarer Nachfolger der Anfangsecke (successor). Z.B. ist 8 successor von 2.

Der Begriff des Pfades (Abb. 1) sei so erklärt:

Ein Pfad ist eine Folge von einer oder mehreren Ecken, so daß eine gerichtete Kante zwischen jedem geordneten Paar von Ecken besteht. Ein in sich geschlossener Pfad heißt Schlinge (circuit). Bei ihm ist die Anfangsecke gleich der Schlußecke.

2, 8, 10 ist ein Pfad
2, 1, 7 ist kein Pfad

Wir sehen, daß 5 der Ecken ohne Vorgänger sind (Nr. 1-5). Diese werden als Input des Fault-Trees bezeichnet. Sie sind Ausfallereignissen an Komponenten zugeordnet.

Ein Pfad, für den Anfangsecke und Schlußecke zusammenfallen, heißt Schlinge. In Abb. 3 ist mit dem Pfad, der über die Ecken

1, 2, 1

geht, eine Schlinge gezeigt.

Definition des Fehlerbaums

Def.: Ein Fehlerbaum (Fault Tree) ist ein endlicher, gerichteter Graph ohne Schlingen. Jede Ecke kann einen von mehreren Zuständen repräsentieren. Für jede Ecke ist eine Funktion definiert, welche diesen Zustand angibt. Dieser Zustand hängt von allen Vorgängern der Ecke ab.

a) Die Ecken ohne Vorgänger repräsentieren einen von mehreren Zuständen von Komponenten.

b) Die Ecke ohne Nachfolger repräsentiert einen von mehreren Zuständen des Systems.

Ecken ohne Vorgänger sind in Abb. 1: 1, 2, 3, 4, 5.
Wir suchen damit den Zustand aller anderer Ecken zu ermitteln. Besonderes Interesse verdient jedoch diejenige Ecke, welche keine Nachfolger hat. Sie ist der Output des fault trees. Sie bezeichnet das Funktionieren oder Ausfallen des Systems.

Wir beschränken uns in diesem Zusammenhang auf genau zwei Zustände für jede Ecke. (Es ist auch möglich, fault-trees mit mehr als 2 Zuständen pro Ecke auszuwerten.) Haben wir jedoch genau zwei Zustände (z.B. ausgefallen und funktionsfähig), so ist die Anwendung der Aussagenlogik oder boolescher Techniken möglich. Es ist damit z.B. möglich, eine Vereinfachung des fault trees zu machen. Wir werden ein Beispiel einer sehr starken Vereinfachung weiter unten angeben.

Es ist hier anzumerken, daß diese Definition eines Fault-trees einem kombinatorischen Netzwerk (combinatorial switching network) entspricht. Die Forderung, daß dieses Netzwerk ohne Schlingen sein soll, kann folgendermaßen interpretiert werden: Der jeweilige Output dieses Netzwerks ist ausschließlich durch den jeweiligen input bestimmt. Eine Speicherung (memory) früherer Inputs findet nicht statt. Wir werden eine andere Bedingung im 2. Teil dieser Einführung haben. Dort will ich sequentielle Netzwerke besprechen, für die eine Speicherung möglich ist.

Wir beschränken uns im folgenden auf einen von jeweils genau zwei möglichen Zuständen für jede Ecke.

Die Forderung, daß dieses Netzwerk ohne Schlingen sein soll, werde ich an einem Beispiel untersuchen. Der Fehlerbaum repräsentiert ein Netzwerk, für das keine Speicherung (memory) früherer Inputs stattfindet.

Mehrere Outputs

Wir können die in 2.21 gegebene Definition des Fehlerbaums ohne grundsätzliche Schwierigkeiten auf einen Graphen mit mehreren Ecken ohne Nachfolger ausdehnen. Diese Ecken ohne Nachfolger werden gewöhnlich als Wurzeln (roots) bezeichnet. (Abb. 4 gibt ein Beispiel mit 3 Wurzeln.)

Wir können die Definition ohne begriffliche Schwierigkeiten zu einem gerichteten Graphen mit mehreren Wurzeln ausdehnen.

Def. Ein gerichteter Graph hat eine oder mehrere Ecken, genannt Wurzeln (roots), die speziell ausgezeichnet sind von den übrigen Ecken durch die Existenz von Vorgängern (predecessors), die aber keine Nachfolger (successors) haben.

Lassen wir diese Def. eines gerichteten Graphen zu, so können sinngemäß alle Aussagen der Fehlerbaumdefinition übernommen werden. Es ist jedoch zu beachten, daß wir nun mehrere Ecken ohne Nachfolger haben. Ich halte darum eine unkritische Übernahme des Namens "Fehlerbaum" nicht für eine sinnvolle Bezeichnung. Das ist keine grundsätzliche Einschränkung. In der Theorie der kombinatorischen Netzwerke ist ein Graph mit mehreren Wurzeln keine Ausnahme.

Bilden die Komponenten 1 bis 9 ein System (Abb. 4), so können wir durch 3 Wurzeln drei verschiedene Teilsystem-Ausfälle darstellen. Dies sei am Rande vermerkt, da es noch wenig angewandt wurde.

Logische Verknüpfungen

Einführung

Der Fehlerbaum ermöglicht eine Verknüpfung von vielen Einzelereignissen. Diese Verknüpfung soll exakt und effizient sein. Dazu wollen wir einen für diese Verknüpfung geeigneten Formalismus einführen. Auch ein Formalismus ist auf dem Boden der natürlichen Sprache gewachsen. Man wird dabei den Aufbau eines Formalismus besser verstehen, wenn man weiß, welche Züge der Umgangssprache dieser wiedergibt, und in welcher Weise er dies tut. Am besten lernt man dies dadurch, daß man sich darin übt, umgangssprachliche Aussagen in die formale Sprache zu übersetzen, mit anderen Worten, diese Aussagen zu symbolisieren /5,6,7/.

Dazu werden zunächst drei logische Verknüpfungen definiert. Dann sollen einige wichtige Relationen gezeigt werden, die bei der praktischen Arbeit mit Fehlerbäumen häufig verwendet werden. An einem einfachen Beispiel wird der Aufbau eines Fehlerbaumes demonstriert. Dann wollen wir den Aufbau eines Fehlerbaumes für die Stromversorgung eines Kernkraftwerks zeigen (2.3)

Wir führen hier die folgenden Verknüpfungen ein:

1. Verneinung (Negation)
2. UND - Verknüpfung (Konjunktion)
3. ODER - Verknüpfung (Disjunktion)
4. Äquivalenz

1. Negation

x bezeichne eine Aussage.
Ist x wahr, dann ist $\overline{x}$ (seine Negation) falsch (und umgekehrt).

Bezeichnet x ein Ereignis, das eintritt, dann bezeichnet $\overline{x}$ ein Ereignis, das nicht eintritt.

Beispiel:

x_1 = "Komponente 1 fällt aus".

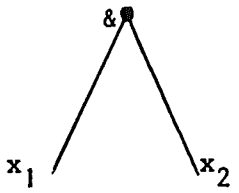
$\overline{x}_1$ = "Komponente 1 fällt nicht aus".

2. UND - Verknüpfung (Konjunktion)

Die Konjunktion wird als "x_1 & x_2" geschrieben.

Die Konjunktion ist dann und nur dann wahr, wenn x_1 und x_2 wahr sind.

Graphische Darstellung:



UND

Dabei sei:

x_1 = "Komponente 1 fällt aus"

x_2 = "Komponente 2 fällt aus"

Dies bedeutet, daß ein System (allgemeiner, ein Untersystem) vorliegt, das aus Komponenten 1,2 besteht, welches dann und nur dann ausfällt, wenn 1 und 2

ausfallen.

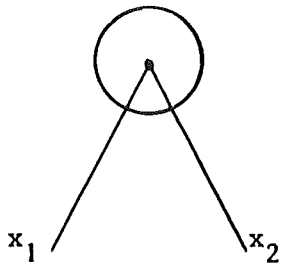
(Die Konjunktion wird in der Fehlerbaumterminologie auch als "UND"-Tor bezeichnet. Sie wird u.A. als $x_1 \wedge x_2$ geschrieben.)

3. ODER - Verknüpfung (Disjunktion)

Die Disjunktion (das nicht - exklusive ODER) wird als "$x_1 \vee x_2$" geschrieben. Die Disjunktion ist dann und nur dann falsch, wenn

"x_1 und x_2" falsch sind.

Graphische Darstellung:



ODER

Dabei sei

x_1 = "Komponente 1 fällt aus"

x_2 = "Komponente 2 fällt aus"

Dies bedeutet, daß ein System (allgemeiner, ein Untersystem) vorliegt, das aus Komponente 1,2 besteht, welches dann und nur dann nicht ausfällt, wenn 1 und 2 nicht ausfallen.

(Die Disjunktion wird in der Fehlerbaumterminologie auch als "ODER"-Tor bezeichnet).

4. Äquivalenz

Die Äquivalenz wird $x_1 \longleftrightarrow x_2$ geschrieben. Sie ist dann und nur dann wahr, wenn entweder x_1 und x_2 wahr, oder x_1 und x_2 falsch sind.

Es gibt noch andere aussagenlogische Verknüpfungen, die jedoch an dieser Stelle nicht ausführlich behandelt werden.

Gesetzte der Aussagenlogik

Wir führen einige Gesetzte der Aussagenlogik an, welche für Überlegungen an Fehlerbäumen verwendet werden.

1.) $x_1 \vee x_2 \longleftrightarrow \overline{\overline{x}_1 \,\&\, \overline{x}_2}$ DeMorgan'sches Gesetz

Beispiel: Komponente 1 oder Komponente 2 fällt aus.
Dies ist folgender Aussage äquivalent:

Es ist nicht wahr, daß (Komponente 1 nicht ausfällt und Komponente 2 nicht ausfällt)

Ein Beweis des Gesetzes kann z.B. mittels Wahrheitstafeln ausgeführt werden.

2.) $x_1 \vee (x_1 \vee x_2) \longleftrightarrow x_1 \vee x_2$ 1. Absorptionsgesetzt

Beispiel: Komponente 1 fällt aus oder (Komponente 1 fällt aus oder Komponente 2 fällt aus). Dies ist folgender Aussage äquivalent:

Komponente 1 fällt aus oder Komponente 2 fällt aus.

Ein Beweis kann mittels Wahrheitstafeln ausgeführt werden.

3.) 2. Absorptionsgesetz

$x_1 \vee (x_1 \,\&\, x_2) \longleftrightarrow x_1$

Beispiel: Komponente 1 fällt aus oder (Komponente 1 fällt aus und Komponente 2 fällt aus).

Dies ist folgender Aussage äquivalent:

Komponente 1 fällt aus.

Wir geben damit 3 Gesetze der Aussagenlogik als Beispiele.

Zur Semantik des Fehlerbaums

Die Auswahl dieser Symbole ist nicht zwingend. Es gibt eine Anzahl anderer Möglichkeiten. In anderen Arbeiten werden z.B. exklusives ODER (entweder,....., oder) u.a. Symbole verwendet.

Die hier genannten haben immerhin die folgenden Eigenschaften:

1. Sie können eine vollständige Aussagenlogik definieren.

2. Durch Negation,
   UND
   ODER
   sind sie einer Deutung relativ leicht zugänglich /4,6/.

Wir können jedoch folgendes feststellen:

Jeder Fehlerbaum mit 2 Zuständen pro Ecke muß der Aussagenlogik gehorchen. Aber nicht jede Formel der Aussagenlogik ergibt einen Fehlerbaum.

a) Es gibt Formeln der Aussagenlogik, die selten oder nie in der heutigen Fehlerbaum-Terminologie gebraucht werden. Dies trifft z.B. für die Implikation zu [1]. Dies ist jedoch keine grundsätzliche Einschränkung.

b) Es gibt Formeln der Aussagenlogik, deren Grundzeichen aus völlig verschiedenen Systemen kommende Zustände repräsentieren.

   "2 · 2 = 5 oder Komponente 5 ist ausgefallen."

   Dies ist aussagenlogisch nicht anfechtbar. Man wird es jedoch nicht in einen Fehlerbaum bringen.

---

1) In dem eng verwandten Gebiet kombinatorischer Schaltungen spielt die Implikation dagegen eine wichtige Rolle.

c) Es gibt Aussagen, die immer wahr oder immer falsch sind (Tautologien). Diese sind nicht annehmbar für einen Fehlerbaum z.B. x_1 : = "Komp. 1 ist ausgefallen" ergibt

$$x_1 \vee \overline{x_1}$$

Dies ist, da stets wenigstens eine Aussage wahr ist, immer wahr. Die Aussagenkombination

$$x_1 \ \& \ \overline{x_1}$$

ist immer falsch.

Diese Kombinationen liefern keinen Beitrag zu einem Fehlerbaum: Es kann keine Zustandsänderung (Ereignis) eintreten.

Der Aufbau eines einfachen Fehlerbaums

Zeigen wir kurz den Aufbau eines Fehlerbaums am Beispiel einer im Blockdiagramm angegebenen Serien-Parallel-Schaltung: Wie man sieht, wird dort ein Signal über irgendeine geeignete Kombination von Schaltelementen von A nach B übertragen. Wir sehen (Abb. 5)

1. Das Signal kommt nicht mehr von A nach B, wenn die zwei parallelen Untersysteme ausfallen. Diesem Ereignis entspricht das oberste "UND"-Tor des Fehlerbaums.

2. Das eine der Untersysteme ist ausgefallen, wenn die Komponenten 1 und 2 oder 3 ausgefallen sind, was auf dem Fehlerbaum zu sehen ist.

3. Das andere Untersystem ist ausgefallen, wenn Komponente 4 oder 5 ausgefallen ist.

Man beachte bei dem so entstandenen Fehlerbaum /8/:

- Jede Komponente kann in genau zwei Zuständen sein: ausgefallen oder nicht ausgefallen.

- Die UND- bzw. ODER-Tore geben an, in welchem Zusammenhang Komponenten zum Ausfall beitragen können. So verursachen die Ausfälle der Komponenten 4 oder 5 den Ausfall eines der Untersysteme unserer Serien-Parallel-Schaltung.

- Eine wichtige Eigenschaft des Fehlerbaums ist seine Orientierung im Gegensatz zur Serien-Parallel-Schaltung. Die Orientierung entspricht der Tatsache, daß der Ausfall einer Komponente begrifflich dem Ausfall eines Untersystems vorangehen muß.

Der Fehlerbaum kann zur Ermittlung der Ausfallwahrscheinlichkeit des Systems durch Simulation oder analytische Auswertung verwendet werden.

Vereinfachung

Wir vereinfachen einen gegebenen Fehlerbaum:

Ein aussagenlogischer Ausdruck für den hier dargestellten Fehlerbaum ist: (Abb.6)

$$(x_1 \vee x_2) \;\&\; (x_2 \vee (x_3 \& x_4 \vee x_4 \& x_5 \vee x_3 \& x_5))$$

Es sei $f_{2/3} \equiv x_3 \& x_4 \vee x_4 \& x_5 \vee x_3 \& x_5$

($f_{2/3}$ entspricht dem Ausfall einer 2 von 3 - Schaltung).

Damit erhalten wir:

$$(x_1 \vee x_2) \;\&\; (x_2 \vee f_{2/3})$$

$$x_1 \& x_2 \vee x_1 \& f_{2/3} \vee x_2 \& x_2 \vee x_2 \& f_{2/3}$$

$x_2 \& x_2 \longleftrightarrow x_2$ (Idempotenz der Konjunktion)

$x_1 \& x_2 \vee x_2 \longleftrightarrow x_2$ (Absorption)

$x_2 \& f_{2/3} \vee x_2 \longleftrightarrow x_2$ (Absorption)

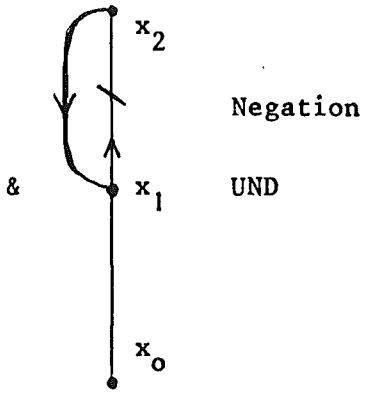
damit bleibt als Ausdruck

$x_2 \vee x_1 \& f_{2/3}$ (Abb. 7)

Der vereinfachte Fehlerbaum hat keine Verzweigung vorzuweisen. Dies ist für die analytische Auswertung nützlich. /8/

Analyse einer Schlinge

Bei der Definition des Fehlerbaums wurde gefordert, daß dieser ohne Schlingen sein soll. Durch ein Beispiel kann gezeigt werden, daß eine Schlinge in der Tat zu Widersprüchen führen würde.



Wir erhalten zunächst

$x_1 \longleftrightarrow x_o \ \& \ x_2$.

Weiter erhalten wir x_2 als Negation von x_1:

$$x_2 \longleftrightarrow \overline{x}_1$$

Also, durch einsetzen,

$$x_1 \longleftrightarrow x_o \ \& \ \overline{x}_1$$

Die Konjunktion ist genau dann wahr, wenn x_o und $\overline{x}_1$ wahr sind. Sie ist jedoch auch x_1 äquivalent.

Nun nehmen wir an daß x_o wahr sei.
Dann hängt die Wahrheit der Konjunktion nur noch von $\overline{x}_1$ ab.
Das bedeutet also:

x_1 ist dann und nur dann wahr wenn $\overline{x}_1$ wahr ist.
Dies ist ein Widerspruch.
Um solche Widersprüche zu vermeiden, müssen wir in der Definition des Fehlerbaums annehmen, daß er keine Schlingen enthält.
Es gibt auch andere Schlingen, bei denen ebenfalls logische Fehler auftreten, die ein logisches Arbeiten mit Fehlerbäumen unmöglich machen: Wir erhalten einen Ausdruck, der immer wahr ist (Tautologie).

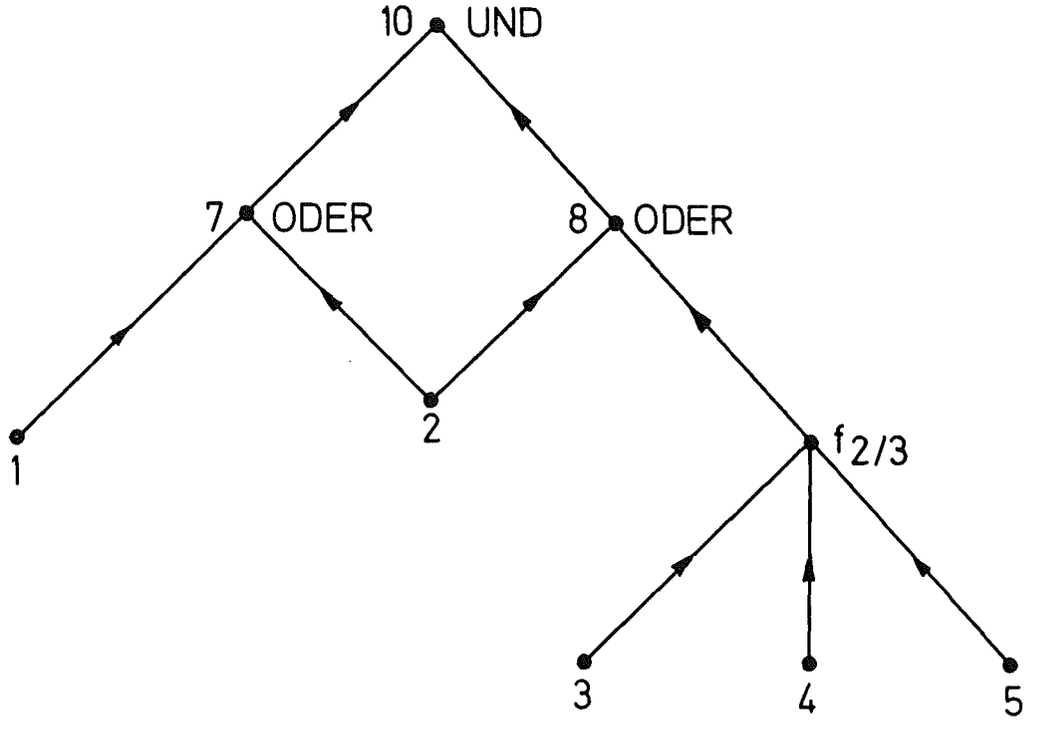


Abb.1

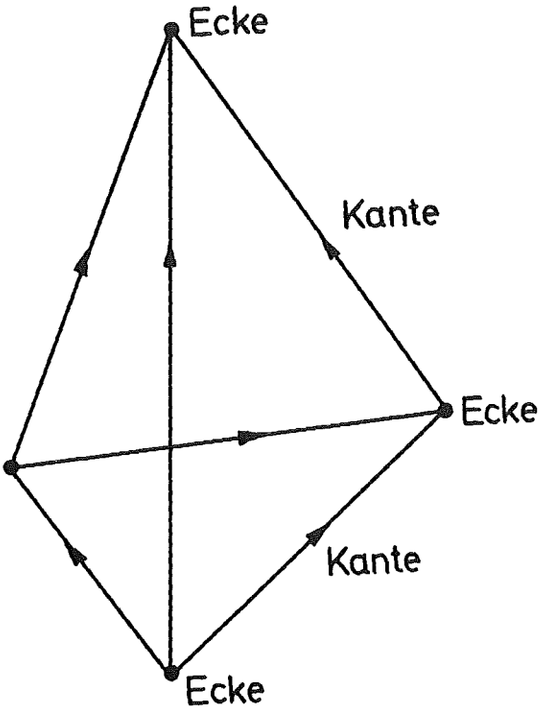


Abb. 2

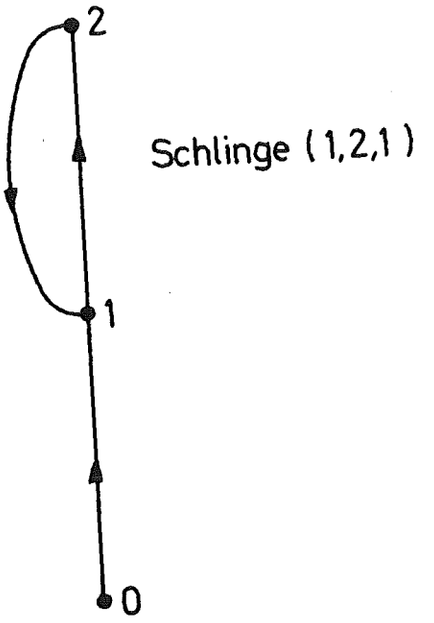


Abb. 3 Schlinge

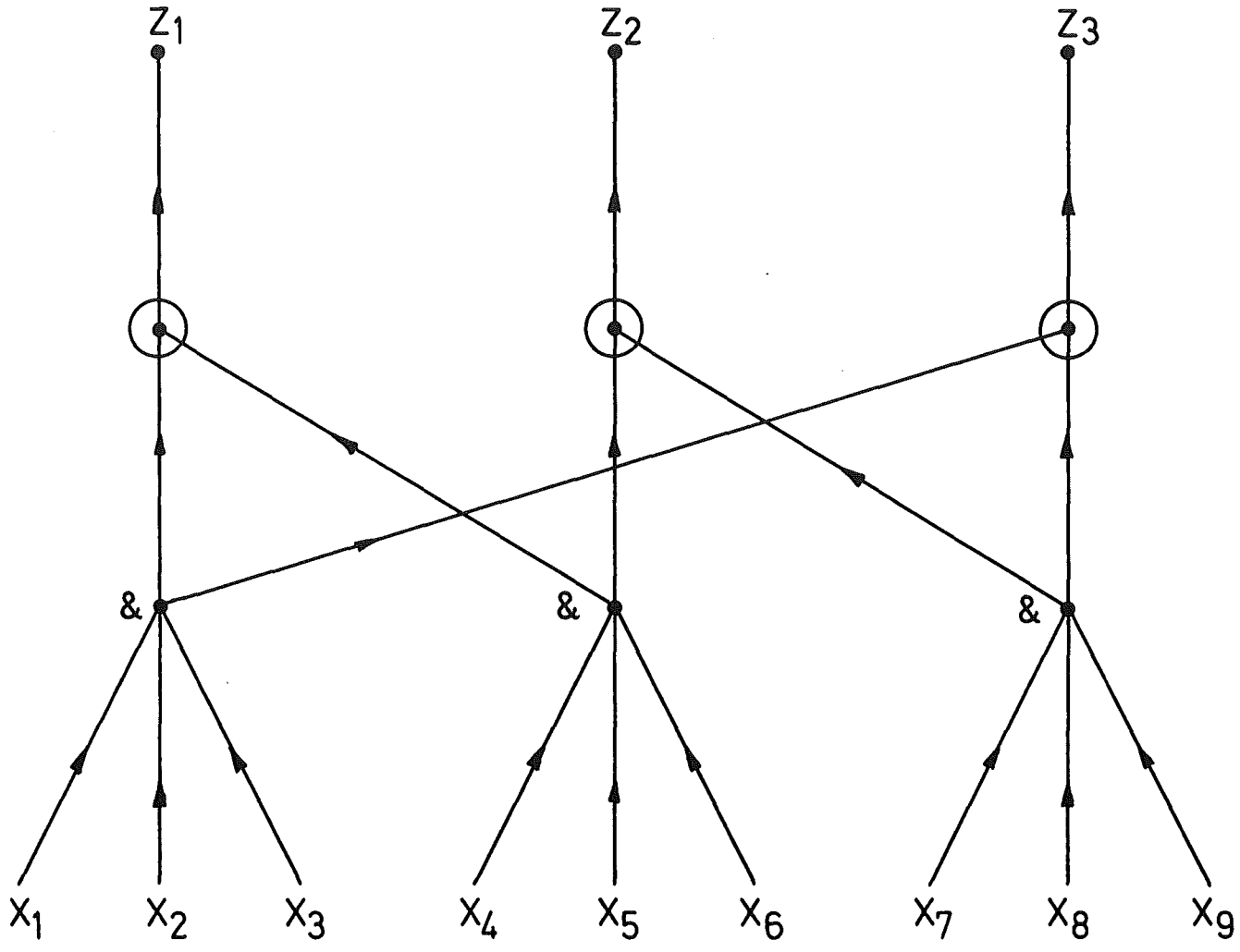


Abb. 4

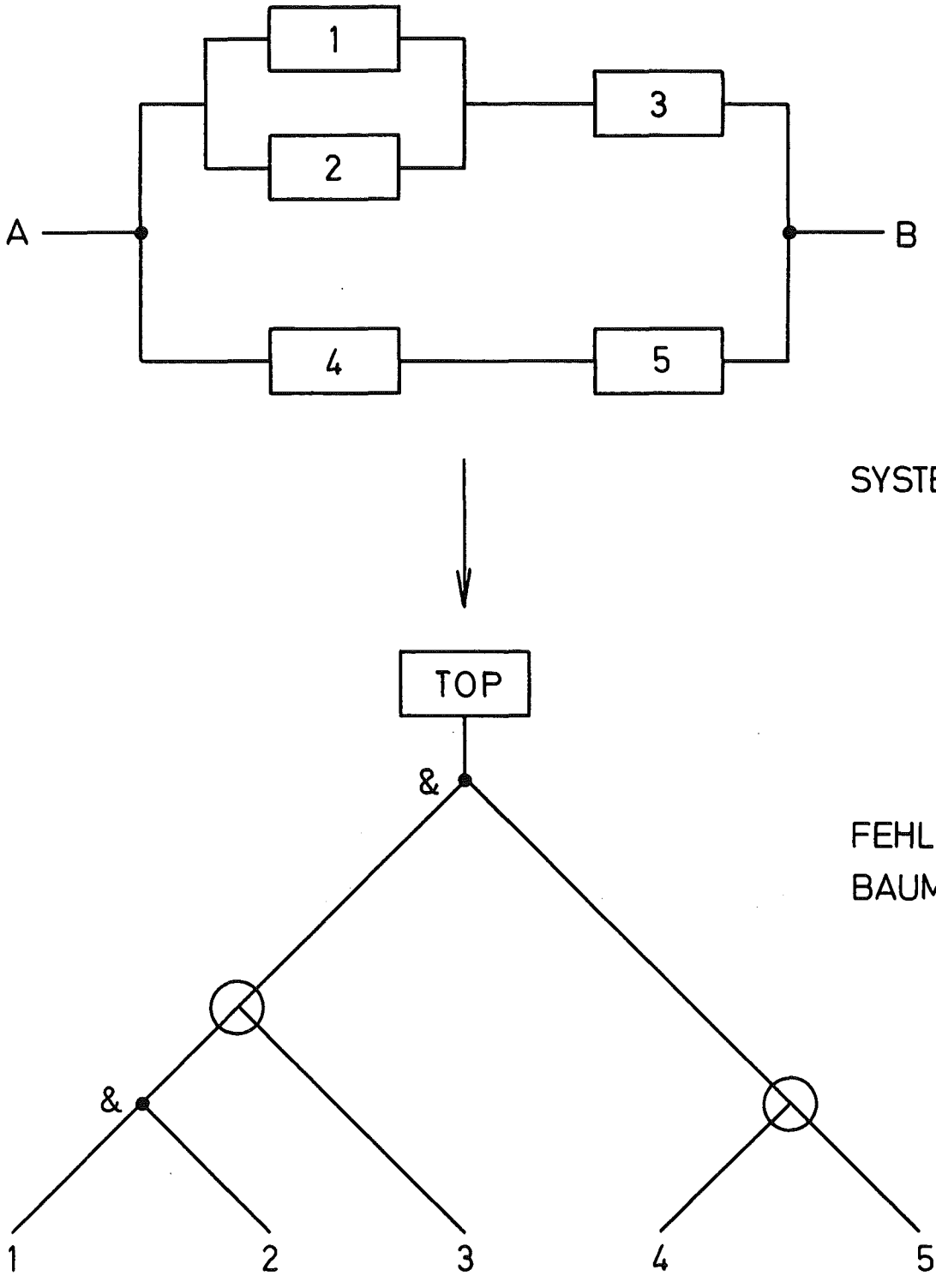
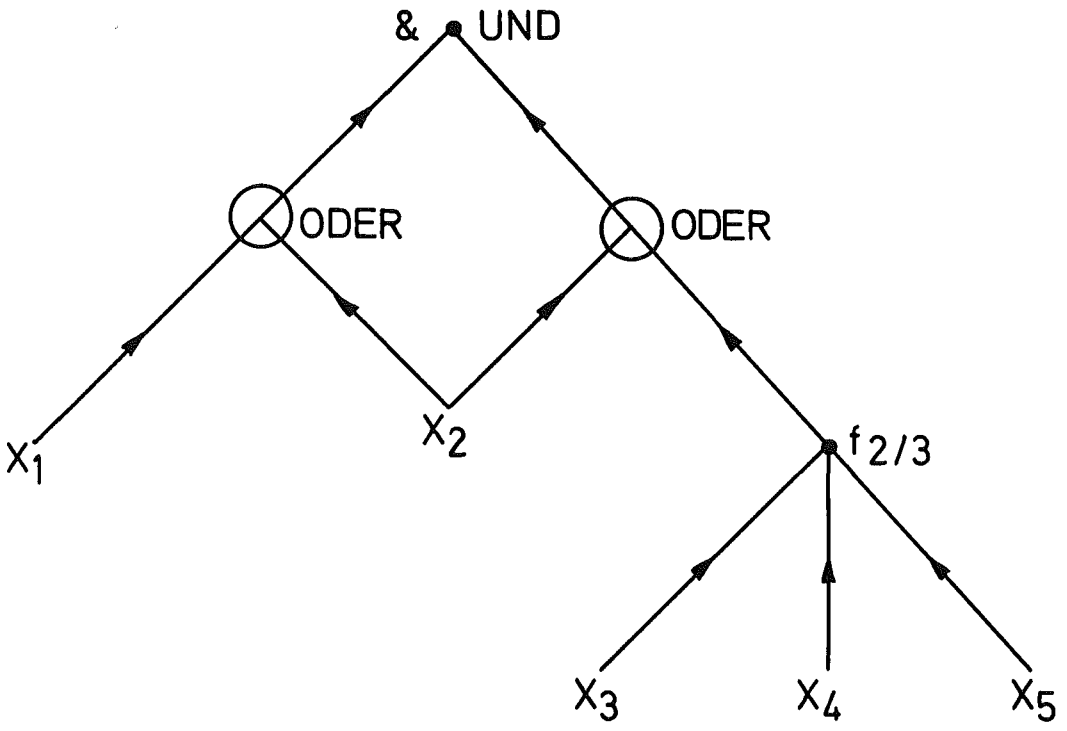


Abb. 5



(mit $f_{2/3} \equiv X_3 \,\&\, X_4 \;\vee\; X_4 \,\&\, X_5 \vee X_3 \,\&\, X_5$)

Abb. 6

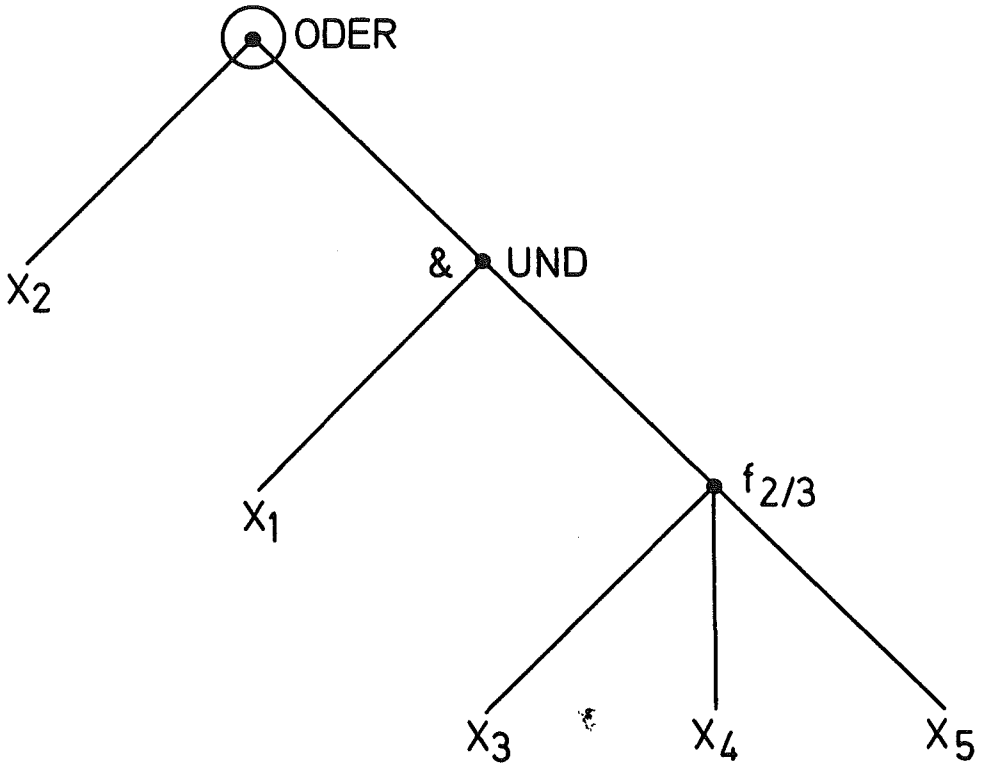


Abb. 7

2.3 Aufbau eines Fehlerbaumes

Einleitung

In diesem Seminar wende ich die in den vorhergehenden Seminaren entwickelte Begriffsbildung (aus Graphentheorie und Aussagenlogik) auf ein Modell eines wirklichen Systems an. Dieses Modell beschreibt die wichtigsten Komponenten, Stromversorgung und Notstromanlage eines Kernkraftwerks, der "DRESDEN Nuclear Power Station" (im Staate Illinois)./9/

Über die Vollständigkeit dieser Beschreibung soll zunächst noch nichts gesagt werden. Es ist jedoch notwendig, am Ende des Fehlerbaumaufbaus darauf zurückzukommen.

Der Zweck der Fehlerbaumanalyse ist die Untersuchung der Ursache von Störfällen an Systemen, bevor das System solche Störfälle erleidet. /4/

Das Ziel der Fehlerbaumanalyse ist die Systembeurteilung im Hinblick auf Zuverlässigkeit, Verfügbarkeit und Sicherheit, Ziele der Analyse sind im einzelnen:

a) die systematische Identifizierung aller möglichen Ursachen, die zu einem vorgegebenen Systemausfall führen, insbesondere Aufbau eines Fehlerbaums an einem gegebenen Modell,

b) die Ermittlung der Eintrittswahrscheinlichkeiten dieser Ursachen und der Eintrittswahrscheinlichkeit des Systemausfalls, insbesondere Fehlerbaumauswertung,

c) die Ermittlung von Beurteilungskriterien zur Systemauslegung, Verwendung einer Analyse zur Beurteilung der Auslegung.

Hier möchte ich das Ziel (a) verfolgen.
Herr Dr. Rosenhauer (INTERATOM) wird sich im folgenden Seminar mit Ziel(b) beschäftigen und Herr Dr. Heuser wird sich auf die Beurteilung der Auslegung konzentrieren (c).

SYSTEM - BESCHREIBUNG

Die Beschreibung des Systems kann hier relativ kurz und informell sein. Das System wird daraufhin in Abb. 8 und in der Beschreibung der Komponentenausfälle ausgeführt.

Ein Kernkraftwerk produziert Energie, es ist jedoch gleichzeitig ein Verbraucher. Manche Funktionen in Betrieb, wie z.B. Kühlung durch Pumpen, die Steuerung des normalen Betriebs, insbesondere jedoch sicherheitsbedingte Funktionen (Abschalten, Notkühlung), aber auch alle Meß-und automatischen Kontrollgeräte bedürfen einer zuverlässigen Versorgung. Wegen der Vielfalt der eingesetzten Komponenten ist es zweckmäßig, verschiedene "Schienen" zur Stromversorgung zur Verfügung zu haben.

Die "Dresden-Power-Station" ist zur Absicherung dieser verschiedenartigen Anforderungen mit folgenden grundsätzlich austauschbaren Stromversorgungen ausgestattet.

- Die normale Stromversorgung (Abb. 8)

  Sie besteht aus

  a) der Versorgung aus dem eigenen Kraftwerk,

  b) einem Anschluß an das Verbundnetz der Commonwealth-Edison Co.

- Die Notstromversorgung (Abb. 8)

  Wenn die normale Stromversorgung nicht verfügbar ist, stehen drei Typen der Notstromversorgung zur Verfügung:

a) Ein Dieselgenerator mit einer Leistung von 500 kW,

b) ein 34,5 - kV - Netz, das nicht von Commonwealth-Edison betrieben wird (und darum nicht in Phase mit der 345 kV-Schiene ist),

c) eine (redundant ausgelegte) 125-Volt-Batterie (die für besonders wichtige Funktionen der Steuerung und Messung vorgesehen ist),

Diese Batterie ist nicht in dem zugrundegelegten Modell (Blockdiagramm) enthalten und wird auch nicht in dem aufzubauenden Fehlerbaum berücksichtigt.

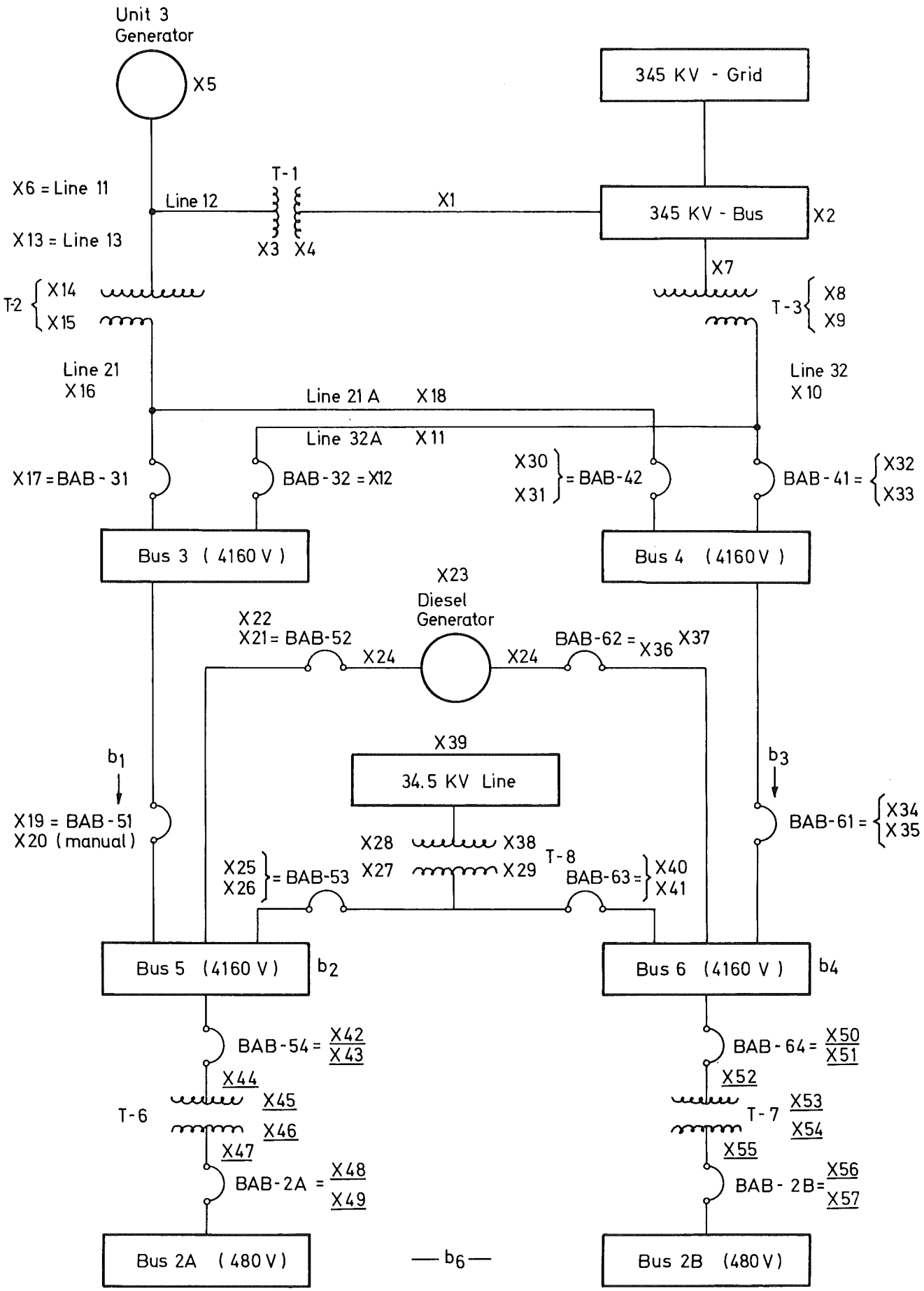


Abb. 8: Stromversorgung der Dresden-Power-Station

Aufbau des Fehlerbaums

Aus dem in Abb. 8 gegebenen Modell (Blockdiagramm) entwickeln wir den Fehlerbaum in Schritten:

1. Drei Subsysteme werden definiert.

2. Die zum Ausfall des Subsystems beitragenden Komponentenausfälle werden im Blockdiagramm eingezeichnet und in einer Liste zusammengefaßt.

3. Im ersten Subsystem wird durch eine kurze Beschreibung das Entstehen der logischen Verknüpfungen verdeutlicht.

4. Der dem jeweiligen Subsystem entsprechende Fehlerbaum wird ausführlich gezeigt.

5. Eine zur Auswertung geeignete Kurzfassung des Fehlerbaums für dieses Subsystem wird hinzugefügt.

Haben wir diese Schritte ausgeführt, so müssen wir uns fragen, ob wir das Ziel unserer Analyse, "die systematische Identifizierung aller möglichen Ursachen" erreicht haben.

Zu 1. Wir unterteilen das System folgendermaßen:

1.1 Notstromversorgung (mit Dieselgenerator und 34,5kV Hochspannung)

1.2 Bus 3 und Bus 5 (linke Seite der Normalversorgung)

1.3 Bus 4 und Bus 6 (rechte Seite der Normalversorgung)

Aus diesen Subsystemen läßt sich ein Fehlerbaum aufbauen.

Zu 2.

Die Ausfälle, die eine Unterbrechung der Versorgung verursachen werden in ein weiteres Blockdiagramm eingezeichnet.

Wir erhalten:

2.1 Notstromversorgung kann an folgenden Stellen unterbrochen werden:

a_{21}, a_{20}, a_{23}

a_{33}, a_{25}, a_{36} (Abb. 9)

Diese Unterbrechungen kommen als logische Verknüpfungen von Einzelereignissen zustande. Sie werden in 3.1 und im dazugehörigen Unterbaum beschrieben (Abb. 10, S. 73).

2.2 Bus 5 kann an folgenden Stellen die Verbindung mit der Normalversorgung verlieren:

a_{18}, c, x_{11}, d, x_{17} (Abb. 11).

Diese Unterbrechungen kommen wieder als logische Verknüpfungen von Einzelereignissen zustande. Sie werden im zugehörigen Unterbaum beschrieben (Abb. 12).

2.3 Bus 6 kann an folgenden Stellen die Verbindung mit der Normalversorgung verlieren:

x_2, a_{31}, d, x_{18}, a_{27}, c, a_{29} (Abb. 13, Abb. 14, S. 77)

Bezüglich Verknüpfungen von Einzelereignissen siehe 2.2.

Zu 3. Das erste Subsystem bestehend aus

- Dieselgenerator und
- 34,5 kV-Netz

kann Bus 5 und Bus 6 nicht mehr versorgen, wenn

Diesel keine Leistung abgibt oder (Leistungsschalter BAB 62 und Leistungsschalter BAB 52 ausgefallen sind)
und

T-8 (Transformator von 34.5 kV-Netz keine Leistung abgibt) oder (Leistungsschalter BAB 53 und Leistungsschalter BAB 63 ausgefallen sind).

Dieser Satz wird in übersichtlicher Weise im ersten Unterbaum dargestellt. Dabei werden die in dieser Aussage stehenden Ereignisse als Verknüpfung von Einzelereignissen dargestellt (Abb. 9 und 10). Damit ist der Übergang "Modell ⟶ Fehlerbaum" ausgeführt.

Zu 4. Die folgenden Seiten zeigen einen Übergang der weiteren ausgewählten Untersysteme, jeweils mit ausführlichem Fehlerbaum (Abb. 11 und 12 sowie 13 und 14).

Zu 5. Der ausführlichen Form wird eine zur analytischen Auswertung geeignete Kurzfassung angefügt (Abb. 15, 16, 17).

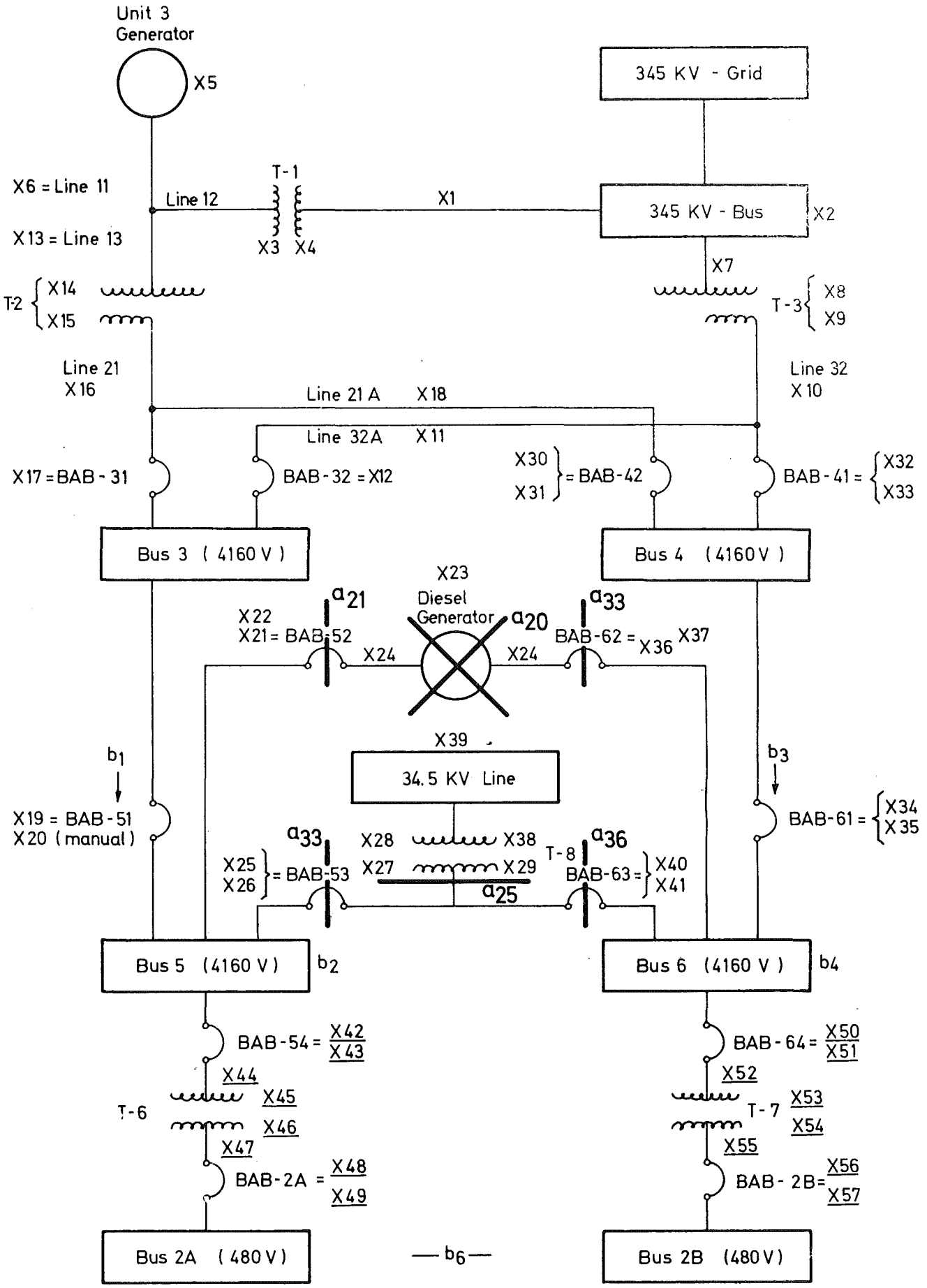
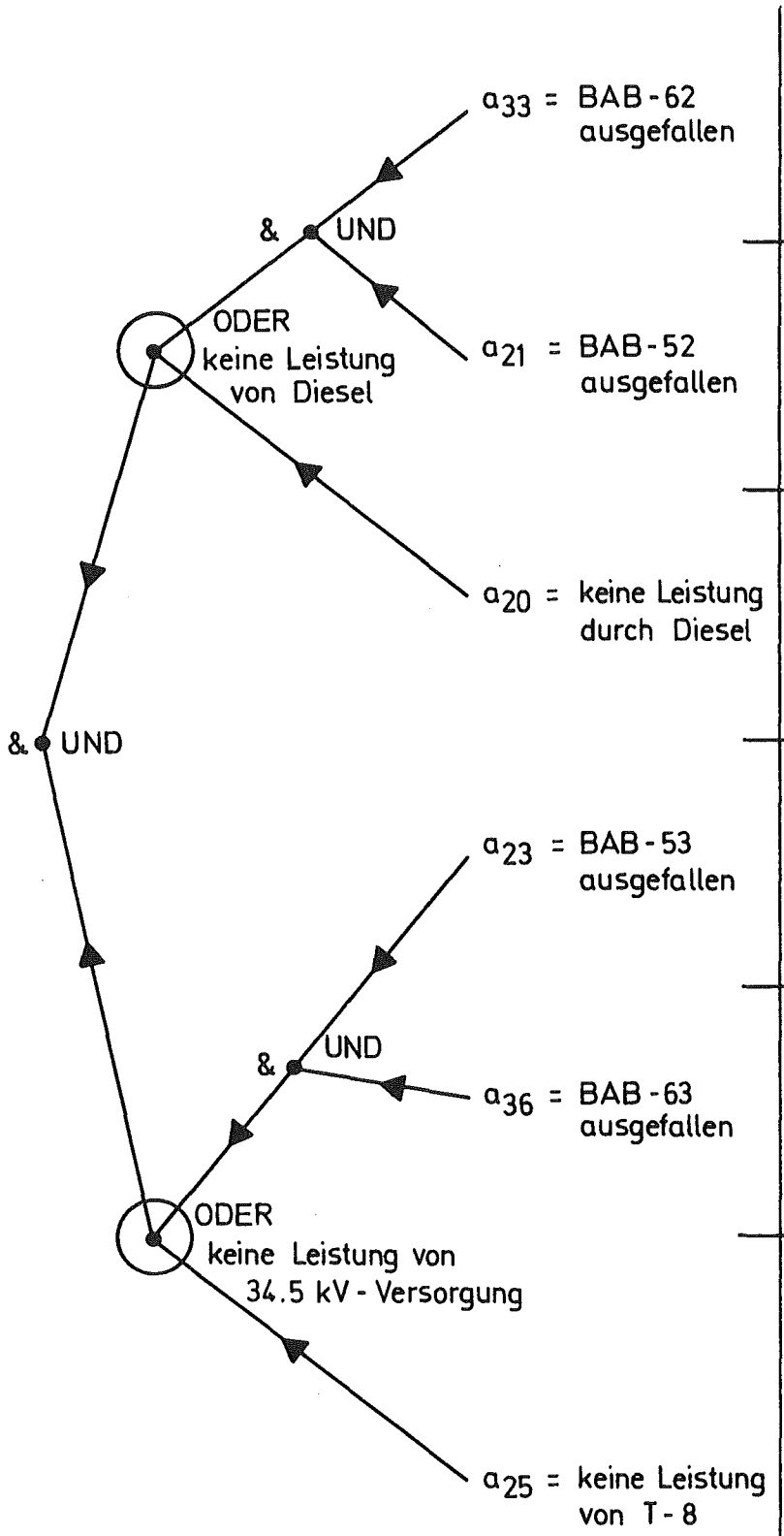


Abb. 9: Ausfall der Notstromversorgung



a_{33} = Leistungsschalter BAB-62 offen (X 36) oder

Schaltautomatik BAB-62 fällt aus (X 37)

---

a_{21} = Leistungsschalter BAB-52 offen (X 21) oder

Schaltautomatik BAB-52 fällt aus (X 22)

---

a_{20} = Diesel-Generator fällt aus (X 23) oder

Leitung zum Diesel-Generator ausgefallen (X 24)

---

a_{23} = Schaltautomatik BAB-53 fällt aus (X 25) oder

Leistungsschalter BAB-53 offen (X 26)

---

a_{36} = Leistungsschalter BAB-63 offen (X 40) oder

Schaltautomatik BAB-63 fällt aus (X 41)

---

a_{25} = T-8 Sekundärwicklung offen (X 27) oder

T-8 Primärwicklung offen (X 28) oder

Leitung von T-8 ausgefallen (X 29) oder

Untererde-Speiseleitung zu T-8 ausgefallen (X 38) oder

34,5 kV-Versorgung des Kraftwerks ausgefallen (X 39)

Abb. 10: Fehlerbaum zum Ausfall der Notstromversorgung

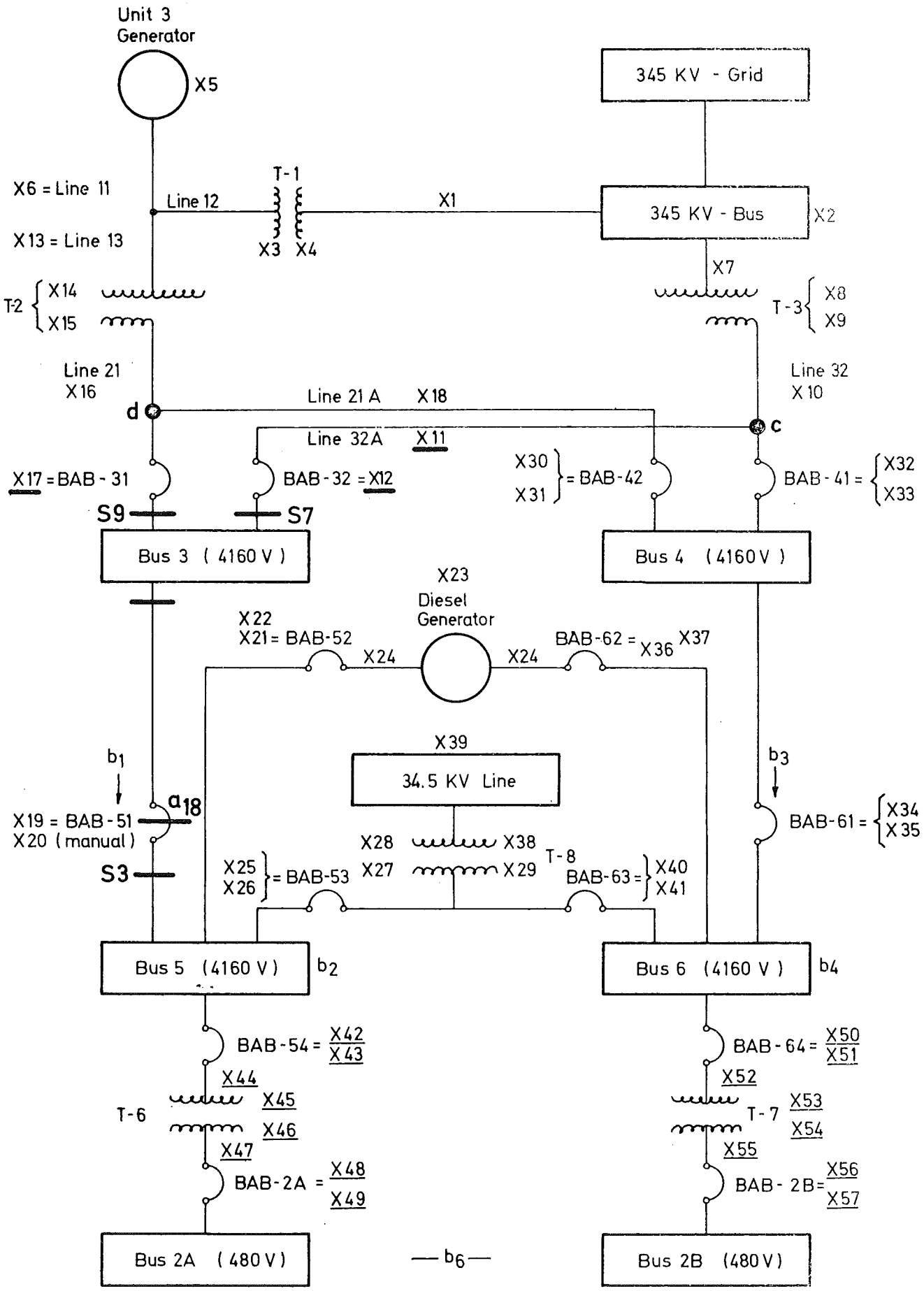


Abb. 11: Ausfall der normalen Versorgung von Bus 5

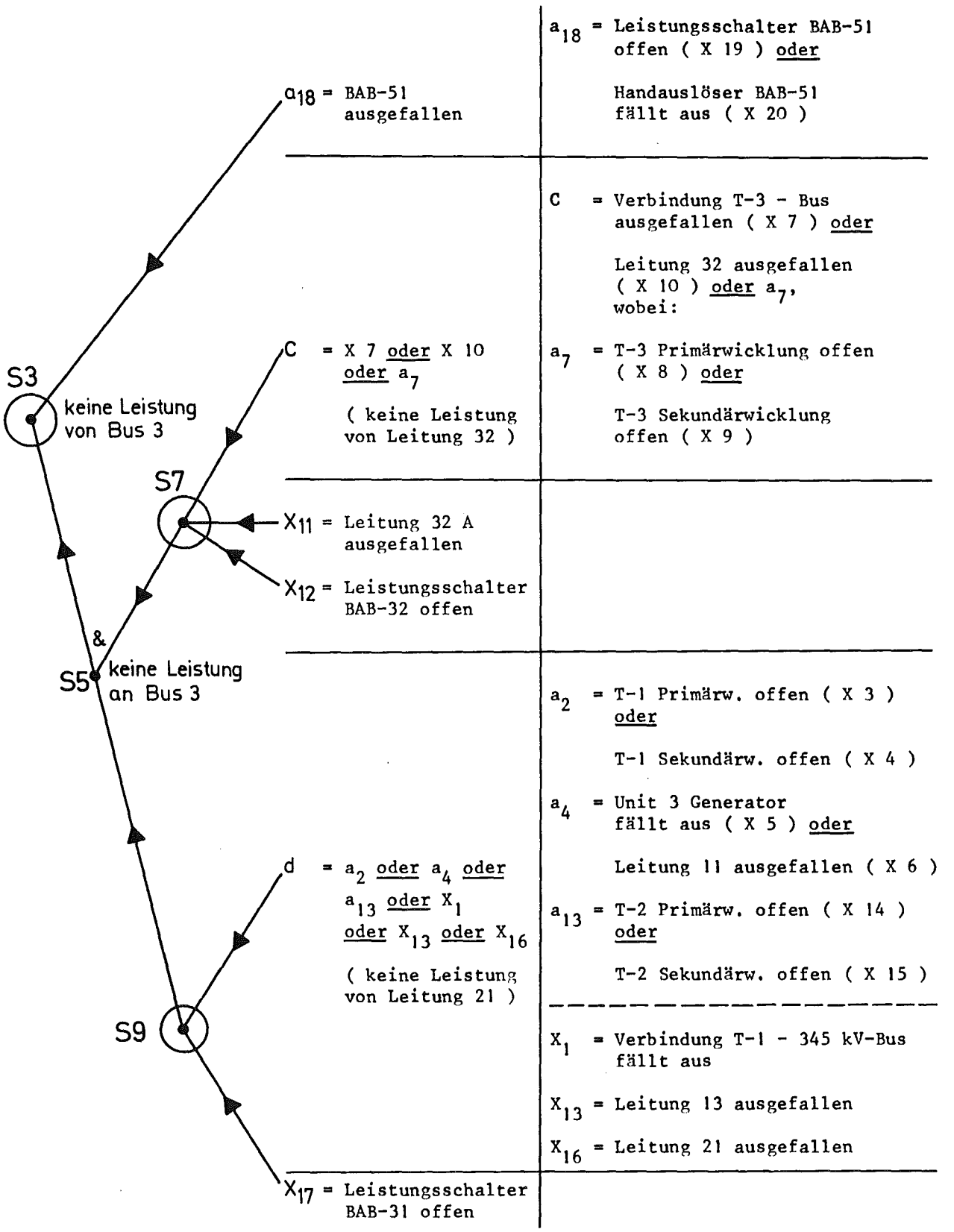


Abb. 12: Fehlerbaum zum Ausfall der normalen Versorgung von Bus 5

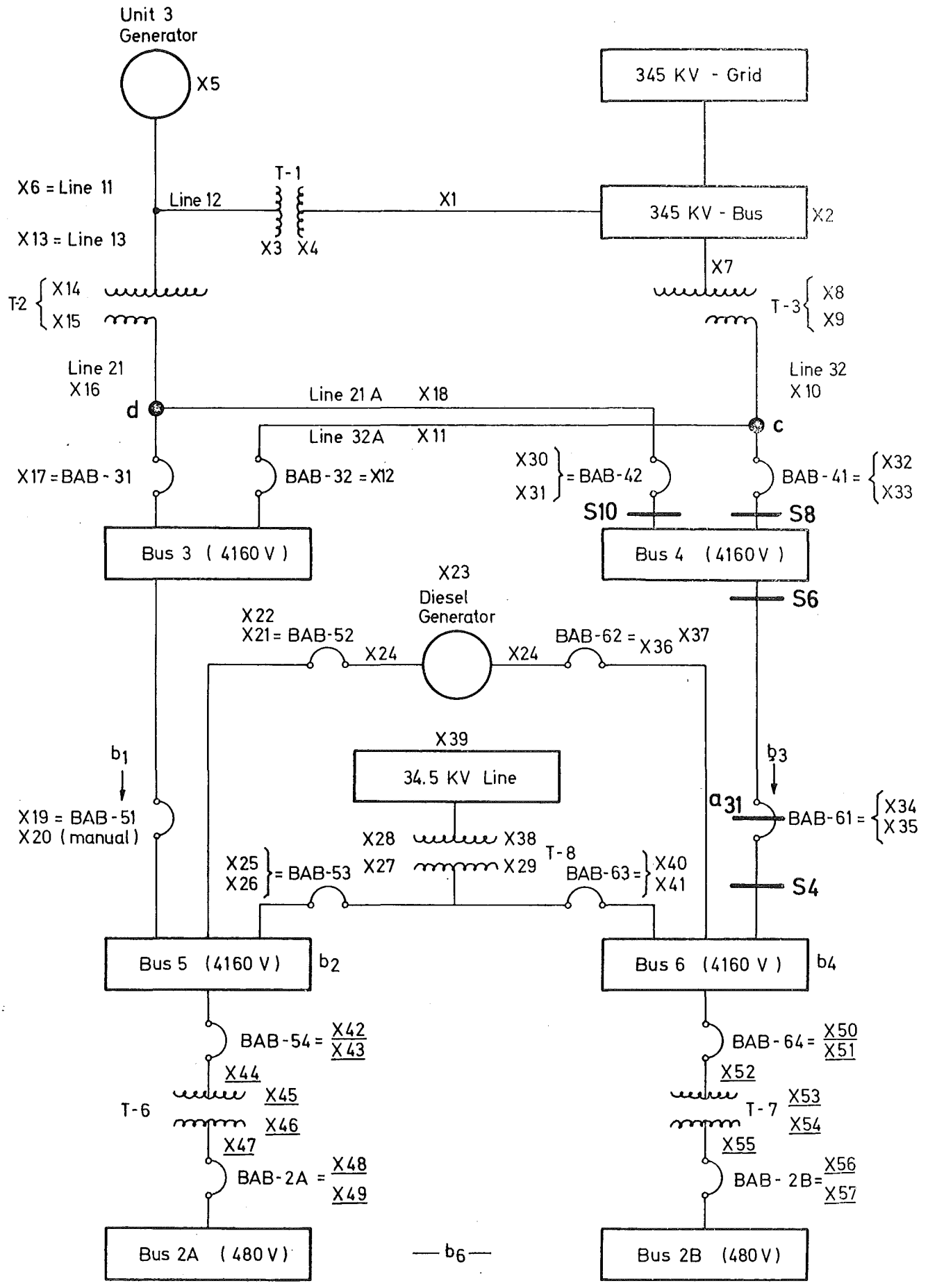


Abb. 13: Ausfall der normalen Versorgung von Bus 6

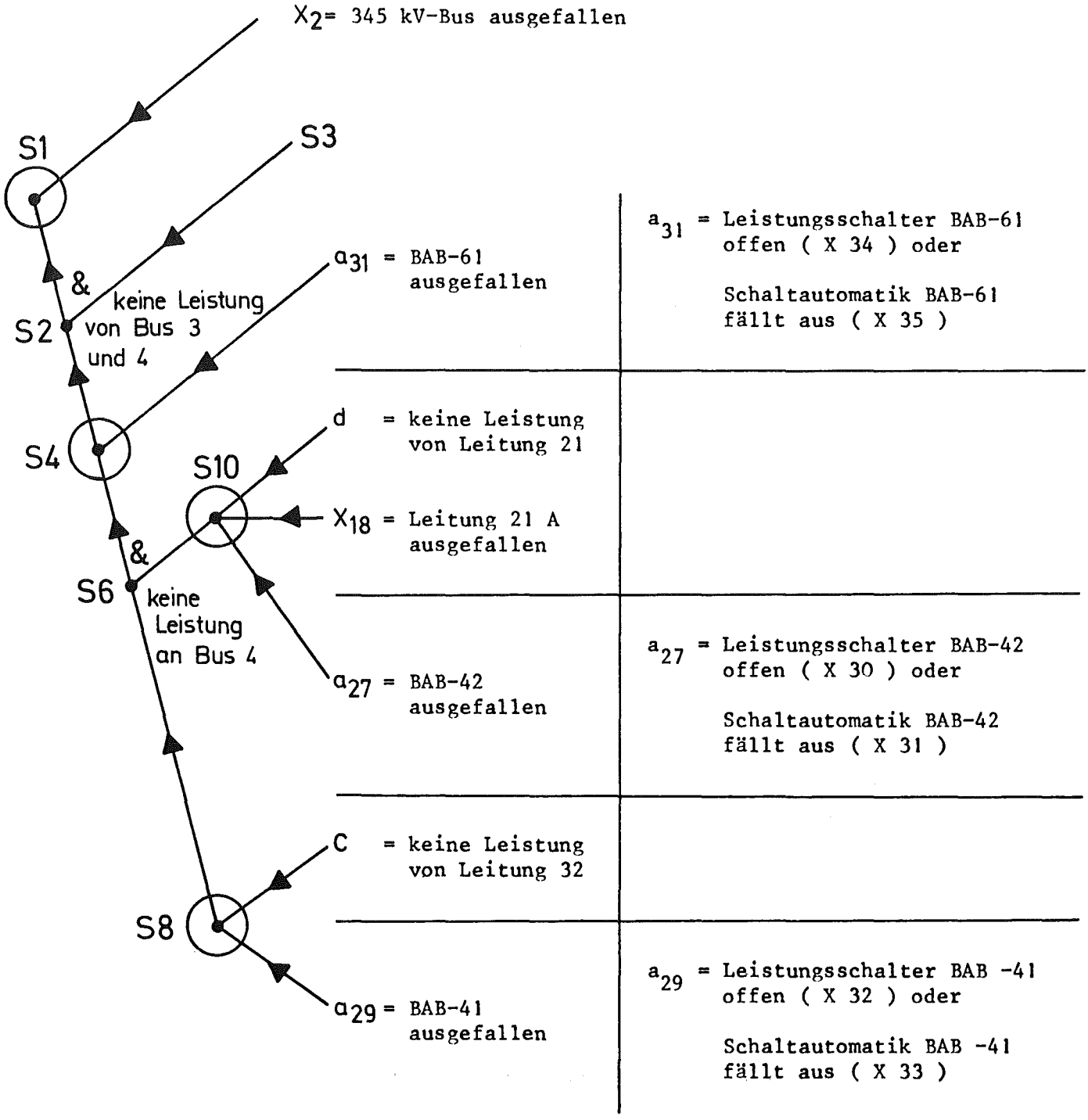


Abb. 14: Fehlerbaum zum Ausfall der normalen Versorgung von Bus 6

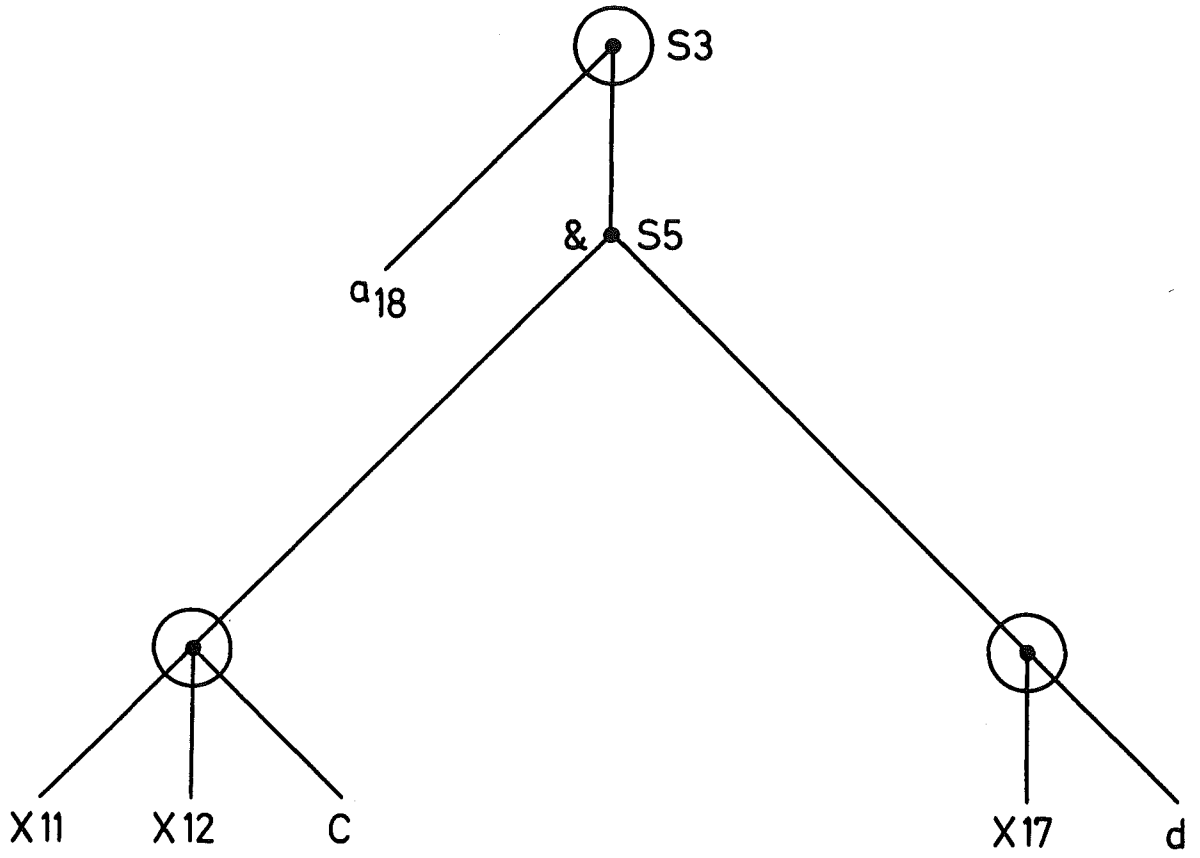


Abb. 15: Zusammenfassung des Unterbaums von Abb. 12

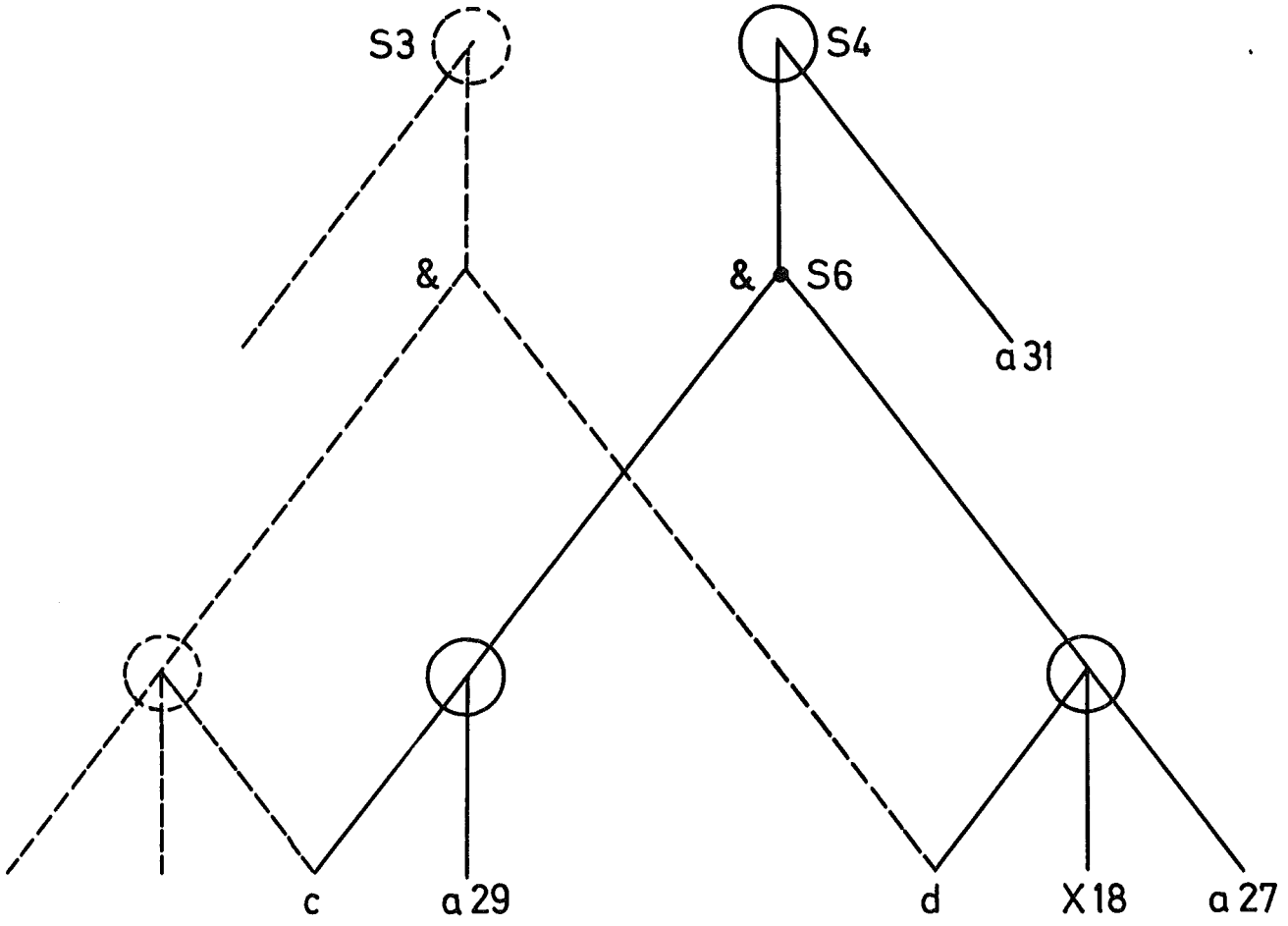


Abb. 16: Hinzufügen des Fehlerbaums von Abb. 14

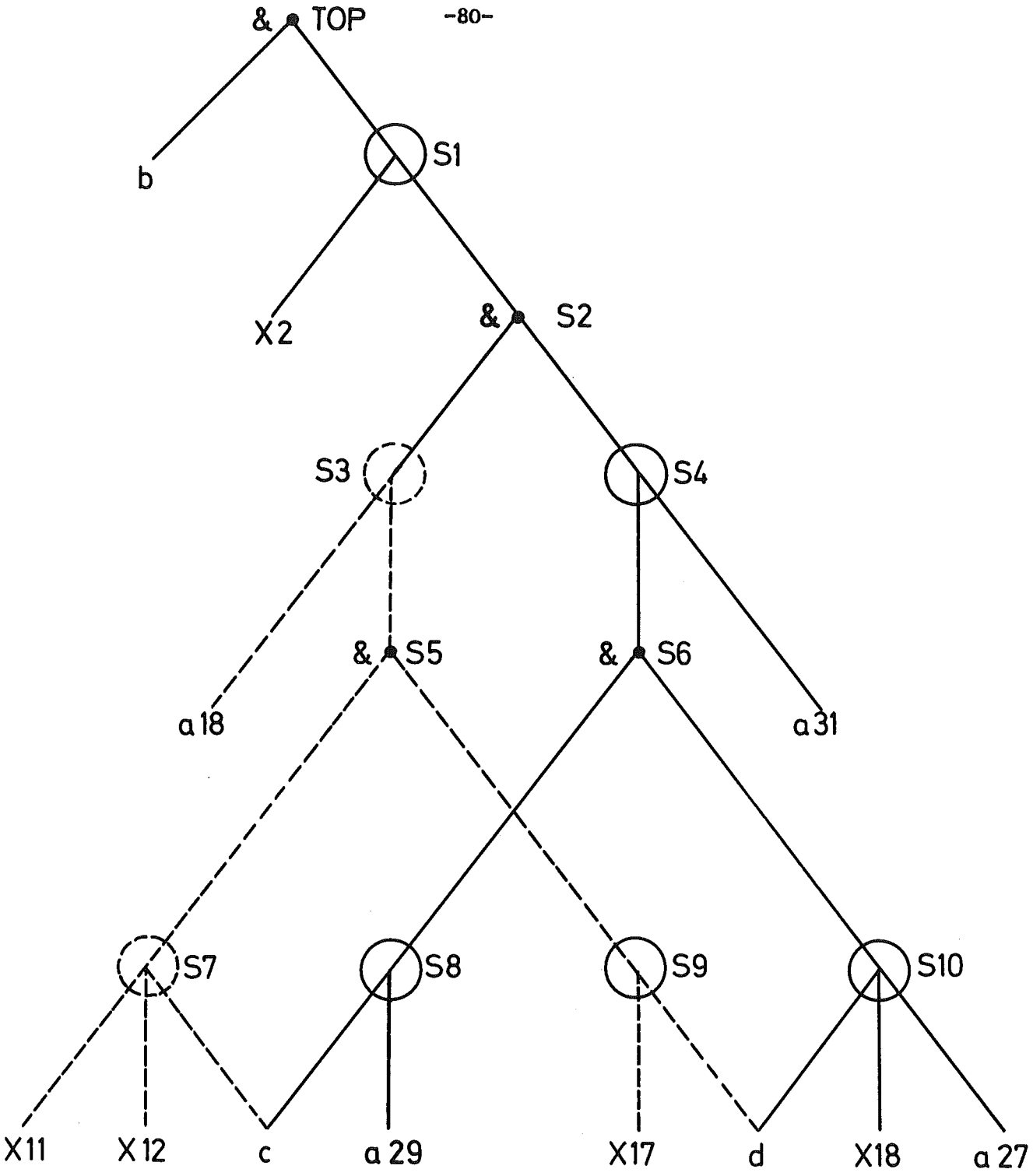


Abb. 17: Zusammenfassung des gesamten Fehlerbaums

Anmerkung: Nach Aufbau eines Fehlerbaums ist es notwendig, seine Vollständigkeit und Widerspruchsfreiheit zu prüfen. Dazu gibt es keine allgemein anerkannten Methoden.

a) Für die Frage der logischen Widerspruchsfreiheit des Fehlerbaums können Methoden der Logik und/oder Boole'sche Techniken eingesetzt werden /2/.

b) Eine zweite Gruppe von Fehlern kann durch Übersehen oder Fehlinterpretation einiger Ausfallvorgänge entstehen. Dafür gibt es keine Kriterien. Es ist ratsam, den Fehlerbaum ein zweites Mal aufzustellen /4/.

Literaturverzeichnis und Anmerkungen

1. C. Berge(transl. A. Doig), The Theory of Graphs, Methuen and John Wiley (1962)

J. W. Essam, M. E. Fisher, Some Basic Definitions in Graph Theory, Reviews of Modern Physics, 42, Supplement, (April 1970), p. 271-288

2. J.D. Murchland, G.G. Weber, A Moment Method for the Calculation of A Confidence Interval for the Failure Probability of a System, Proc. 1972 Annual Symposium on Reliability and Maintainability, San Francisco (1972) p. 565-577

3. D. Schulte, Kombinatorische und Sequentielle Netzwerke, (Grundlagen und Anwendungen der Automatentheorie), R. Oldenbourg, München (1967)

4. Normenentwurf "Fehlerbaumanalyse" (Fachnormenausschuss Kerntechnik, FNKe 3.3, (1972) Dieser Entwurf wurde unter Beteiligung von Dr. Rosenhauer (INTERATOM), Dr. Heuser (INTERATOM), Dr. Weber (GfK) überarbeitet.

5. A. Tarski, Einführung in die mathematische Logik, (Moderne Mathematik in elementarer Darstellung), Vandenhoek & Ruprecht, Göttingen, (1966)

6. H. Hermes, Einführung in die mathematische Logik (Mathematische Leitfäden) B. G. Teubner, Stuttgart, (1963)

7. W. Leinfellner, Einführung in die Erkenntnis- und Wissenschaftstheorie, B.I. - Hochschultaschenbücher, Mannheim, (1965)
Hier ist insbesondere auf die Darstellung der Aussagenlogik zu verweisen: p. 28 - 36

8. G. Weber, Methoden der Zuverlässigkeitsanalyse von Systemen (Vortrag auf der Tagung "Technische Zuverlässigkeit", 1971, Nürnberg)

9. B.J. Garrick, W. C. Gekler et al., Reliability Analysis of Nuclear Power Plant Protective Systems, Holmes & Narver, Inc., Nuclear Division, HN - 190 (1967)

Kapitel 3 : Projektbezogene Anwendung von Zuverlässigkeitsmethoden bei INTERATOM

Projektbezogene Anwendung von Zuverlässigkeitsmethoden bei INTERATOM

1. Teil

W. Rosenhauer, Bensberg

1. Überblick

Bevor ich auf einzelne Systeme und die entsprechenden anwendungsorientierten Methoden eingehe, möchte ich zunächst einen kurzen Überblick über das Konzept geben, Abb. 1, nach dem die Tätigkeiten auf dem Gebiet der Zuverlässigkeit bei INTERATOM ablaufen.

Projektbegleitende Zuverlässigkeitsuntersuchungen beginnen mit einer Analyse der Anlagenstörfälle. Die Untersuchung des mit dem Betrieb der Gesamtanlage verbundenen Risikos ist ein sehr wichtiger Schritt. Sie liefert qualitativ, welche Teilsysteme wichtig für die Sicherheit sind. Sie liefert darüberhinaus die quantitativen Anforderungen, die kompatibel mit einem angenommenen Gesamtrisiko sind, wodurch nichtoptimale Auslegungen aufgrund isolierter Betrachtungsweisen vermieden werden.

Die Störfallanalysen stehen in engem Zusammenhang mit den Zuverlässigkeitsuntersuchungen von Teilsystemen, mit denen nachgewiesen werden muß, ob die zu stellenden Anforderungen erfüllt sind. In meinem Teil des Vortrags werde ich mehr auf die in diesem Zusammenhang verwendeten Methoden eingehen. Im 2. Teil wird mehr über wichtige Ergebnisse berichtet.

Ein weiterer Tätigkeitsschwerpunkt sind die Untersuchungen zum Ausfallverhalten der Strukturwerkstoffe, über die im 2. Teil ausführlicher berichtet wird. Ich möchte nur darauf hinweisen, daß Auslegungen, die Ausfallmechanismen der Werkstoffe vermeiden, effektiv die Zuverlässigkeit erhöhen.
Worum es geht, ist aus der Anmerkung "Integritätsnachweis des Primärsystems" ersichtlich. Die Pfeile sollen lose einige Zusammenhänge und zeitliche Abläufe der einzelnen Tätigkeiten wiedergeben.

Die systemanalytischen Untersuchungen von Teilsystemen werden ergänzt durch Zuverlässigkeitsspezifikationen und Testprogramme für einzelne Komponenten. Dazu gehört z.B. ein Lebensdauertest für Meßsonden mit Thermoelementen, der wichtige Daten für den Betrieb der Zusatzinstrumentierung SNR liefern soll.

Hiermit ist schon der nächste Punkt, Ausfalldaten, Schadenserfassung angesprochen. Dabei geht es natürlich auch um die Erfassung von Reparaturdaten. Die Schadenserfassung bei KNK in Zusammenarbeit mit dem Betreiber und bei den INTERATOM-Versuchsanlagen ist angelaufen.

Verfügbarkeitsanalysen stehen in engem Zusammenhang mit Sicherheitsanforderungen. Es wurden auch rein wirtschaftliche Systeme bezüglich ihrer Verfügbarkeit zum Zwecke der Kostenoptimierung untersucht, ohne daß Sicherheitsfragen berührt waren, da die bei INTERATOM entwickelten Rechenmethoden hierfür sehr geeignet waren.

Methodenentwicklung war bei allen aufgeführten Tätigkeitsschwerpunkten erforderlich. Bei den Methoden zur Ermittlung von Zuverlässigkeit bzw. Verfügbarkeit, auf die sich mein Vortrag beschränkt, werde ich weniger auf wissenschaftliche Aspekte und mehr auf Anwendungsprobleme eingehen.

2. Pumpensystem (2 v. 3), systemspezifische technische Bedingungen

Der erste Schritt zur Berechnung einer Systemausfallwahrscheinlichkeit ist die genaue Definition des unerwünschten Ereignisses TOP. Die logischen Bedingungen an Untersysteme bzw. Komponenten, für die TOP vorliegt, werden gewöhnlich als Fehlerbaum gezeichnet - daher die Bezeichnung TOP. Hierzu gehört eine genaue Kenntnis und Analyse von Funktion und Ausfallmöglichkeiten der Systemkomponenten, was großes technisches Verständnis und vor allen Dingen engen Kontakt mit den Auslegern voraussetzt. Die Analyse des Systems muß nicht nur die Ausfalllogik, d.h. den Fehlerbaum, liefern, sondern die wichtigen in der Betriebsweise liegenden technischen Sonderbedingungen erfassen.

Zur Erläuterung möchte ich ein in 2v. 3 - Redundanz ausgelegtes Pumpensystem betrachten, das für diesen Zweck sehr stark schematisiert dargestellt wurde, Abb. 2. Der Fehlerbaum ist in diesem Fall leicht zu zeichnen, Abb. 3. Die Wahrscheinlichkeiten für TOP läßt sich mit den Rechenregeln der Wahrscheinlichkeit

$$P(A \vee B) = P(A) + P(B) - P(A \wedge B)$$
$$P(A \wedge B) = P(A) \cdot P(B) \qquad (A, B \text{ unabhängig})$$

aus den Ausfallwahrscheinlichkeiten der Stränge ausrechnen, wenn die gezeichnete Boole'sche Form noch so umgeformt wird, daß die Glieder mit dem gemeinsamen Ausfallereignis in der $\vee$-Formel wegfallen.

Die auf diese Weise gewonnene Lösung geht am technischen Problem jedoch völlig vorbei, und zwar aus einer ganzen Reihe von Gründen:

- Die Stränge haben gemeinsame Komponenten bzw. common mode -Fehler (Ventilsteuerung, gemeinsame Leitung, Energieversorgung etc.), so daß die Multiplikationsregel nicht anwendbar ist (Abhängigkeit der Eingänge am UND-Tor, Vermaschung). Dies ist eine allgemein auftretende Schwierigkeit, weil uneingeschränkte Redundanz technisch nicht realisierbar ist.

- Das wichtigste technische Kennzeichen des Systems ist die Reparaturmöglichkeit ausgefallener Komponenten, wodurch ebenfalls die einfachen Rechenregeln verlorengehen. Die Reparatur hat für die Zuverlässigkeit im Reaktorbau eine ganz andere Bedeutung als z.B. in Luft- und Raumfahrt, weil es um Einsatzzeiten von 20 Jahren geht und nicht um kurze Zeiten wie etwa die Flugdauer einer Rakete.

- In der kalten Phase haben einzelne Komponenten andere Ausfallwahrscheinlichkeiten als im Betrieb. Technisch ist es wichtig, daß viele Komponenten und Systeme mehrere Phasen haben (Standby).

- Bei Umschaltungen oder Reparaturen benötigte Ventile fallen auf Anforderung aus; es sind abhängige Komponenten.

Solche und andere systemspezifische Bedingungen seien im folgenden mit "Reparatur etc." bezeichnet. Zuverlässigkeitsergebnisse können nur dann Entscheidungshilfen bei der Festlegung von Betriebsweisen und Auslegungsmerkmalen sein, wenn die genannten wesentlichen Einflüsse in den Rechnungen berücksichtigt sind.

Ehe ich auf Berechnungsmethoden für die Ausfallwahrscheinlichkeiten mit Reparatur etc. eingehe, möchte ich anhand eines anderen technischen Systems noch ein weiteres grundsätzliches Problem behandeln.

3. Zusatzinstrumentierung, Definition und Anwendung der Größen Zuverlässigkeit und Verfügbarkeit

Ich möchte einige für das System Zusatzinstrumentierung/Sicherheitsrechner SNR besonders wichtige prinzipielle Aspekte betrachten.

Zum System: Die Möglichkeit läßt sich nicht ausschließen, daß lokale Störungen in einem Brennelement (BE) zu Schäden in benachbarten BE's führen und daß eine solche Schadenspropagation wesentliche Teile des Cores erfaßt. Rechtzeitige Gegenmaßnahmen könnten durch eine Zusatzinstrumentierung über jedem BE-Austritt eingeleitet werden, deren Signale von Sicherheitsrechnern im closed loop ausgewertet werden. Bei der Auslegung und der Handhabung des Systems sind folgende Punkte zu berücksichtigen:

- Ein entsprechender Störfall in einem BE muß rechtzeitig die Gegenmaßnahme (zur Vereinfachung: scram) bewirken.

- Unnötige Abschaltungen des Reaktors wegen Instrumentierungs- und Rechnerausfällen bedeuten u.U. erhebliche Stillstandszeiten und betriebliche Schwierigkeiten für die Anlage.

- Unnötige Abschaltungen beeinflussen das mit der Anlage verbundene Sicherheitsrisiko, z.B. weil Nachwärmeabfuhr nötig wird.

Auf die mehr physikalischen Probleme, z.B. auf die Frage, welche Störungen von dem intakten Überwachungssystem überhaupt erkannt werden, welche Reaktionszeiten des Systems sichergestellt werden müssen u.a., möchte ich nicht eingehen und sie als gelöst voraussetzen. Vorsorgliche Abschaltungen sind durch Betriebsvorschriften zu erwarten, z.B. für den Fall, daß BE's wegen Instrumentierungsausfällen unüberwacht sind.

Die genannten Anforderungen sind gegenläufig. Für Entscheidungen zwischen alternativen Konzepten, eine Optimierung des ausgewählten Konzepts und schließlich

den Nachweis, daß die Forderungen genügend gut erfüllt sind, müssen quantitative Zuerlässigkeitsmethoden angewendet werden.

Als unentbehrlich für die Anwendung quantitativer Methoden hat sich eine klare mathematisch strenge Definition der zu berechnenden Grundgrößen erwiesen, die auch bei reparierbaren oder inspizierbaren Systemen, bei Systemen mit mehreren Betriebsphasen (Standby), Umschaltungen und anderen in der Praxis auftretenden spezifischen Bedingungen brauchbar ist. Bei der Beurteilung eines unerwünschten Ereignisses TOP ist es sehr wichtig, zwischen der (mathematischen) Zuverlässigkeit und der (mathematischen) Verfügbarkeit genau zu unterscheiden:

- Die Zuverlässigkeitsfunktion R(t) ist die auf eine Betriebsdauer (Zeitintervall $[0, t]$) bezogene Wahrscheinlichkeit dafür, daß das Ereignis TOP während der Betriebszeit t nicht auftritt.

- Die Verfügbarkeit A(t) ist die auf einen Zeitpunkt t bezogene Wahrscheinlichkeit (temporäre Wahrscheinlichkeit), daß zum Zeitpunkt t das Ereignis TOP nicht vorliegt.

  Die Verfügbarkeit erreicht für t in der Größenordnung der mittleren Reparaturzeit des Systems einen zeitunabhängigen Wert, da das System dann genauso gut schon repariert wie noch oder wieder ausgefallen sein kann.

  Ohne Reparatur etc. liegt zu einem Zeitpunkt t das Ereignis TOP genau dann nicht vor, wenn es während des Betriebsintervalls (0, t) nicht aufgetreten ist: Zuverlässigkeit und Verfügbarkeit für das gleiche Ereignis TOP sind ohne Reparatur etc. identisch. Allgemein sind Zuverlässigkeit und Verfügbarkeit völlig verschiedene Größen. Die Verfügbarkeit ist nicht etwa irgendein Differential der Zuverlässigkeit, sondern ist im technischen Zusammenhang völlig andersartig zu berechnen. Dies sei durch die Anwendung auf die Zusatzinstrumentierung erläutert.

  Für die Sicherheit bei Auftreten einer BE-Störung ist offensichtlich maßgebend, ob zum Störfallzeitpunkt das Überwachungssystem arbeitet oder nicht. Gefragt ist die Verfügbarkeit. Wie häufig unnötige Abschaltungen sind, kann man mit

der Wahrscheinlichkeit dafür abschätzen, daß in einem bestimmten Betriebszeitintervall kein Grund für eine Abschaltung vorliegt. Gefragt ist die Zuverlässigkeit.

Genauso wichtig wie die Wahl der richtigen mathematischen Größe ist natürlich die Definition des unerwünschten Ereignisses TOP. Dies wird völlig klar, wenn man bedenkt, daß in das unerwünschte Ereignis TOP(A) für die Unverfügbarkeit beim BE-Störfall nur die Instrumentierung des gestörten BE's eingeht, während in TOP(R) für vorsorgliche Abschaltung Fehler der Instrumentierungen aller BE's zu berücksichtigen sind.

Schließlich möchte ich noch auf den großen zahlenmäßigen Unterschied der beiden Größen hinweisen. Betrachtet man nur den durch die vorgesehene Thermoelementinstrumentierung hervorgerufenen Anteil, so liegen die Ergebnisse für die Unverfügbarkeit 1-A(t) je nach Voraussetzungen im Bereich 10^{-4} bis einige 10^{-7}, Abb. 4 (UF, EF: unentdeckbare bzw. entdeckbare Thermoelementfehler).

Die Wahrscheinlichkeit 1-R(1a) für unnötige Abschaltungen liegt dicht bei 1,so daß es zweckmäßig ist, eine mittlere Zeit zwischen solchen Abschaltungen anzugeben (je nach Voraussetzungen 1a oder mehr):

$$MTTA = \int_0^\infty R(t)\, dt$$

Bei der Schnellbrütertagung in Karlsruhe /1/ wurde von größenordnungsmäßig 10 vorsorglichen Abschaltungen pro Jahr gesprochen. Es ist - nicht nur aus kommerziellen Gründen - nötig, eine einseitige Auslegung im Hinblick auf genügende oder sogar überhöhte Verfügbarkeit beim BE-Störfall zu vermeiden. Die wichtigsten Entscheidungen,an denen wir in diesem Zusammenhang mitgewirkt haben, waren, ein viertes Thermoelement als Reserve in der Instrumentierungssonde vorzusehen und einen Lebensdauertest für Thermoelemente in Sonden durchzuführen, sowie abgeschwächte Fehlerreaktionsvorschriften ins Auge zu fassen.

Mit diesen Hinweisen möchte ich die Zusatzinstrumentierung verlassen und lieber auf die Methoden eingehen, die zur Berechnung der oben definierten Größen verwendet werden.

3. Monte-Carlo-Simulation, INTERATOM-Rechenprogramme

Die hauptsächlich bei INTERATOM verwendete Methode ist die Monte-Carlo-Simualtion. Die Methode kann man mit Hilfe der Formeln zum Bernoulli-Versuch sehr schnell verstehen. Es sei p die zu ermittelnde Systemwahrscheinlichkeit. Wenn das System N mal über die Betriebszeit TMAX durchgespielt (simuliert) wird, so ist die Wahrscheinlichkeit für n Ausfälle durch die Bernoulli-Verteilung gegeben:

$$W_N(n) = \binom{N}{n} \; p^n \; (1-p)^{N-n}$$

Der Erwartungswert für die Zahl der Ausfälle ist $< n > = Np$. Ein Maß dafür, wie weit die Zahl der Ausfälle von diesem Erwartungswert abweichen kann, ist die Streuung σ:

$$\sigma = \sqrt{(n- < n >)^2} \; = \; \sqrt{Np(1-p)}$$

Dies bedeutet, daß man mit n als beobachteter Ausfallzahl n/N als Schätzwert für die Wahrscheinlichkeit p hat, den man für $n \geqslant 4$ in die Formel für σ einsetzen kann,/2/, was nicht exakt ist, sich in der Praxis aber sehr bewährt hat. Das Ergebnis ist für $p \ll 1$:

$$p \simeq \frac{n \pm \sqrt{n}}{N}$$

Will man z.B. $p = 10^{-4}$ mit einer Genauigkeit von 50 % nachweisen, so muß man n = 4 Ausfallspiele bei N = 40000 Systemsimulationen erzielen.

Das Grundschema für die Simulation eines Systems sieht folgendermaßen aus, Abb. 5. Der Rechner liefert auf dem Intervall $\underline{/}\,0,1\,\underline{/}$ gleichverteilte Zufallszahlen. Mit Hilfe der Lebensdauerverteilung F(t) - der Wahrscheinlichkeit dafür, daß die Lebensdauer kleiner als t ist - wird gemäß z = F(TTF) mit der Zufallszahl z der Ausfallzeitpunkt TTF einer Komponente bestimmt. Solche Erstausfallzeitpunkte werden für alle Komponenten ausgespielt, es sind "Ereignispunkte". Der Rechner geht von Ereignispunkt zu Ereignispunkt, Abb. 6, stellt fest, ob TOP vorliegt und bewirkt notwendige Maßnahmen: Umschaltungen werden vorgenommen, Systeme werden reparierbar oder gehen in Betrieb, Abklingzeiten werden aufaddiert, und andere systemspezifische Bedingungen werden realisiert, oder es wird ganz analog zur Lebensdauer eine

mittlere Totzeit der Komponente ausgespielt. Der Wiederintaktzeitpunkt ist ein neuer Ereignispunkt, an dem wieder ein neuer Ausfallzeitpunkt ermittelt wird, usw. Der Rechner registriert, ob TOP erreicht wird und ordnet die erzielten Systemausfälle noch zeitlich. Dies kommt einem Verschieben von TMAX gleich, so daß man als Ausdruck schließlich die kumulative Ausfallwahrscheinlichkeit in Abhängigkeit von der Zeit erhält. Einige solche Ergebnisse werden im 2. Teil des Vortrags gezeigt.

Das oben angeführte Zahlenbeispiel - Nachweis einer Wahrscheinlichkeit von 10^{-4} - zeigt gleichzeitig die praktische Grenze für die Anwendung reiner Simulationsprogramme (bei INTERATOM FEBA-1, FEBA-2)auf komplizierte oder größere Systeme (z.B. mehr als 100 Komponenten), die für uns erreicht ist, wenn ein Rechenlauf länger als 30 Minuten (CDC 6400) dauert. Die elektrische Energieversorgung des SNR und andere Systeme, die Sicherheitsanforderungen zu erfüllen hatten, lagen mit nichtpessimistischen Reparaturdaten um Größenordnungen besser, also jenseits der angegebenen Nachweisgrenze.

Das Problem wurde durch die Erstellung des INTERATOM-Programms SAP (Struktur-Analyse-Programm) gelöst /3/, in dem analytische Methoden und Simulation kombiniert verwendet werden. Analytisch wird die Ausfallwahrscheinlichkeit $F_{o.R.}(t)$ ohne Berücksichtigung von Reparatur etc. mit vorgegebener Genauigkeit berechnet. Simulativ wird nur noch der Faktor Rep(t) ermittelt, um den sich das Ergebnis ohne Reparatur durch Reparatur etc. verbessert:

$$F_{m.R.}(t) = F_{o.R.}(TMAX) \cdot \frac{F_{m.R_o}(t)}{F_{o.R_o}(TMAX)} = F_{o.R.}(TMAX) \cdot Rep(t)$$

Wollte man z.B. $F_{m.R.} = 10^{-6}$ mit einer Genauigkeit von 50 % nachweisen, so müßte man 4 Millionen Spiele machen, wobei nur 4 Spiele Informationen über das Ausfallverhalten des Systems liefern würden. Der Nachweis ist schon aus technischen Gründen nicht durchführbar, weil größenordnungsmäßig 150 Stunden Rechenzeit (CDC 6400) erforderlich wären, und auch nicht sinnvoll. Der Rechenzeitgewinn mit SAP ist ungefähr durch die Ausfallwahrscheinlichkeit ohne Reparatur etc. gegeben, z.B. $F_{o.R.} = 10^{-3}$. Es werden nur noch solche Spiele gemacht, die ohne Reparatur etc. einen Systemausfall brächten, und das sind nur 4000 Spiele. Die analytische Berechnung von $F_{o.R.}$ benötigt natürlich auch Rechenzeit; insgesamt kommt man zu Rechenläufen von 15-20 Minuten Dauer.

4. Zustandsanalyse und Markovprozesse

Analytische Verfahren ohne Verwendung der Monte-Carlo-Simulation haben sich für größere Systeme als unzweckmäßig erwiesen, da bei Anwendungssystemen immer wieder neue systemspezifische Bedingungen auftraten, die analytisch nur sehr mühsam - wenn überhaupt - hätten behandelt werden können. Für kleinere Systeme jedoch war es möglich, mit Hilfe der Zustandsanalyse Ergebnisse mit Reparatur etc. als formelmäßige Lösungen von Markov-Prozessen zu gewinnen. Die Methode eignet sich auch für mittlere Systeme /4/, für die unter Verwendung von Programmen zur Lösung von linearen Differentialgleichungssystemen numerische analytische Ergebnisse gewonnen werden. Bei der Bestimmung von Anforderungen an die Na-Pumpen des SNR während der Nachwärmeabfuhr jedoch war es z.B. sehr wichtig, über numerische Ergebnisse hinaus eine Formel aufzustellen, aus der die Parameterabhängigkeiten klar ersichtlich sind /5/.

Statt allgemeiner theoretischer Überlegungen möchte ich die geschlossene Lösung für ein 2 v. 3 System identischer Komponenten mit Reparatur vorführen. Der wichtigste Schritt ist die Aufstellung der technisch relevanten exklusiven und vollständigen Systemzustände, die Zustandsanalyse:

Z1: Alle drei Komponenten intakt
Z2: Genau eine Komponente ausgefallen
Z3: Mehr als eine Komponente ausgefallen

Der Zustand Z3 beschreibt das unerwünschte Ereignis. Die Zustände müssen so definiert werden, daß Übergangsraten $\lambda_{ij}(t)$ zwischen ihnen angebbar sind:

$$\lambda_{ij}(t)dt = W \text{ (System zu t in i und zu t + dt in j)}$$

Ausfallrate λ = 1/MTTF und Reparaturrate r = 1/MTTR einer Komponente seien als konstant vorausgesetzt (Exponentialstatistik), Abb. 7.

Zu berechnen sind die Wahrscheinlichkeiten $P_i(t)$ dafür, zum Zeitpunkt t das System im Zustand i anzutreffen. Wichtig ist, daß zur Berechnung der Zuverlässigkeit Z3 ein absorbierender Zustand ist. Nur dann ist die Wahrscheinlichkeit, das System zum Zeitpunkt t in Z3 zu finden, identisch mit der Wahrscheinlichkeit, daß das System im Zeitintervall $\overline{0, t}$ nach Z3 gekommen ist:

$$R(t) = 1 - P_3(t) = P_1(t) + P_2(t)$$

Wollte man die Verfügbarkeit berechnen, so wäre auch Z3 ein reparierbarer Zustand, der aufgespalten werden müßte, um die Übergangsraten angeben zu können. Es sei nur angemerkt, daß die Verfügbarkeit für den vorliegenden Fall über die disjunktive Normalform der Strukturfunktion sehr viel einfacher zu bekommen ist.

Die $P_i(t)$ erhält man als Lösung des Markov-Dgl.-Systems

$$\dot{P}_1(t) = -3\lambda P_1(t) + rP_2(t)$$

$$\dot{P}_2(t) = 3\lambda P_1(t) - (2\lambda+r)P_2(t)$$

$$\dot{P}_3(t) = 2\lambda P_2(t)$$

$$P_1(0) = 1,\ P_2(0) = P_3(0) = 0$$

Es genügt, die beiden ersten Gleichungen zu betrachten. Die Lösung ist

$$R(t) = (1-c)e^{-t\alpha(-)} + ce^{-t\alpha(+)}$$

$$\alpha(\pm) = \frac{1}{2}\left(r+5\lambda \pm \sqrt{r+10\lambda+\lambda^2}\right)$$

$$c = \frac{1}{2}\left(1 - \frac{r+5\lambda}{\sqrt{r+10\lambda+\lambda^2}}\right)$$

In den meisten technischen Systemen ist die mittlere Lebensdauer MTTF groß gegen die mittlere Reparaturzeit:

$$\rho = \text{MTTR} / \text{MTTF} = \lambda/r << 1$$

Entwicklungen nach ρ oder anderen Parametern dürfen jedoch nur sehr vorsichtig gemacht werden, weil die Konvergenz durch im Komplexen liegende wesentliche Singularitäten beschränkt wird. Im vorliegenden Fall z.B. funktioniert die Entwicklung nur für $\rho<0,1$. Nimmt man außerdem $t>>\text{MTTR}$ und $t\lesssim\text{MTTF}$ an, so erhält man für die Ausfallwahrscheinlichkeit eine anwendungsfreundliche Formel:

$$1-R(t) \simeq 6\,\frac{\lambda^2}{r}\,t$$

Im Zusammenhang mit diesen Formeln möchte ich noch eine Bemerkung zum importance sampling machen. Um mit reinen Simulationsprogrammen mehr Ausfälle zu erhalten, werden die Fehlerraten und evtl. die Reparaturraten durch hinzugesetzte Faktoren verschlechtert. Das Simulationsergebnis muß analytisch korrigiert werden. Schon bei dem sehr einfachen angegebenen Beispiel hängt das Ergebnis über transzendente Funktionen von den Raten ab, so daß zumindest über für importance-Faktoren interessante größere Bereiche kein einfacher - etwa ein linearer - Zusammenhang gegeben ist. Die obige exakte Formel zeigt, daß die Rückrechnung von importance-Faktoren äußerst problematisch und mit überschaubaren Fehlern fast so schwierig ist wie die Lösung des Problems selbst.

Abb. 8 zeigt zum Abschluß eine Übersicht über Anwendungsbereiche und Art der Ergebnisse für die einzelnen bei INTERATOM verwendeten Rechenmethoden.

Referenzen

/1/ R.D. Smith (UKAEA)
"Protective Instrumentation for Fast Reactors".
International Conference on Engineering of Fast Reactors for Safe and Reliable Operation, Karlsruhe, Oct. 1972

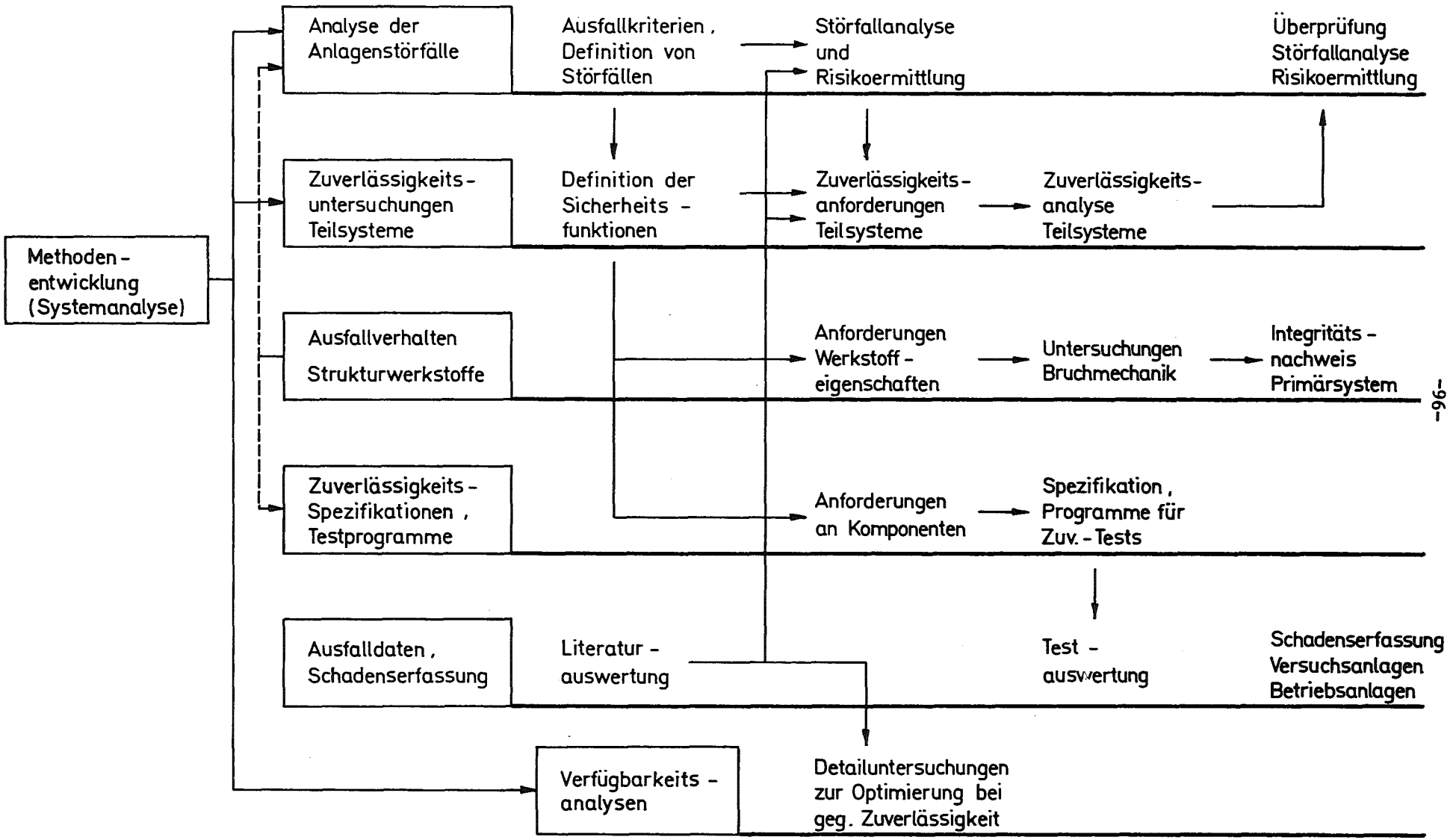
/2/ B.L. van der Waerden
"Mathematische Statistik"
S. 28, Springer-Verlag, Berlin 1971

/3/ F.W. Heuser, W. Rosenhauer
"SAP-1 - Ein neues Programm zur Berechnung von Zuverlässigkeitsgrößen komplexer Systeme".
Atomwirtschaft 17, 2
(1972) 81

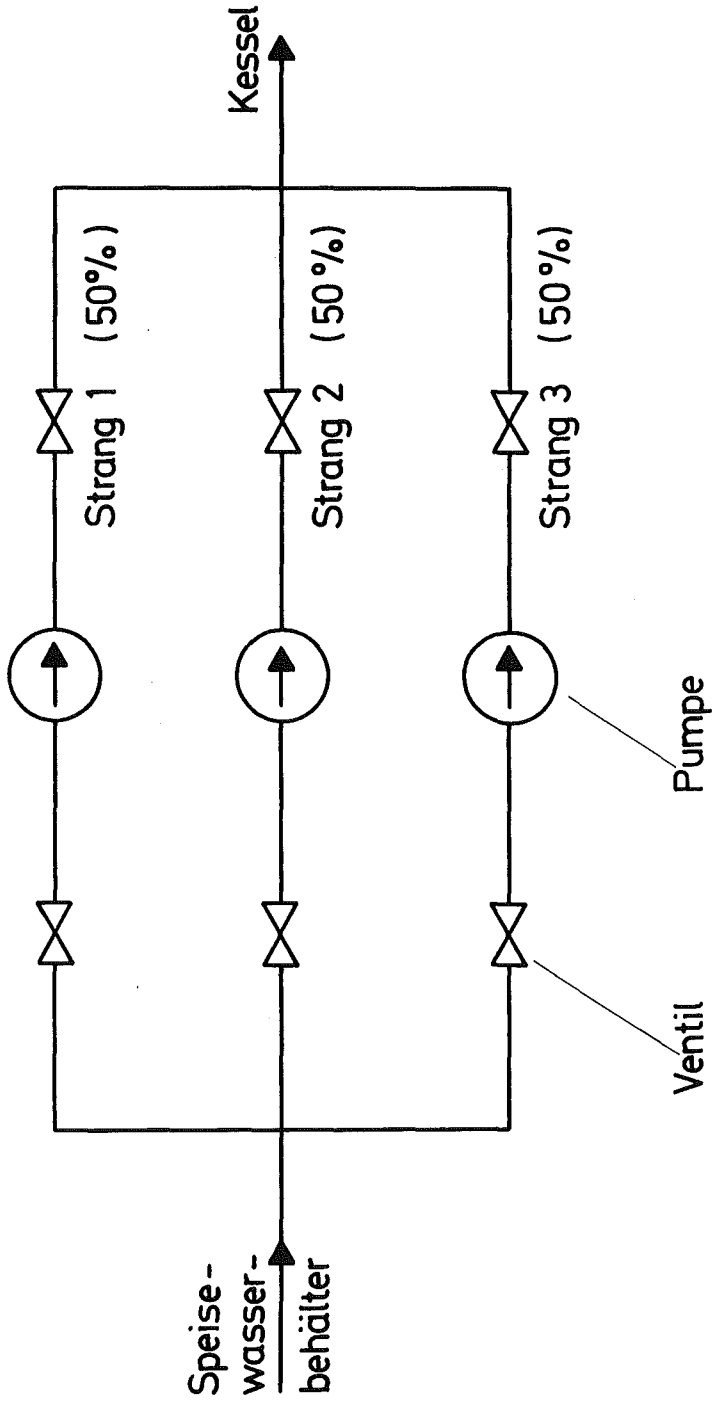
/4/ H. Zeibig, E. Valentin
"Anwendung von Markoff-Prozessen zur Zuverlässigkeitsanalyse für ein Stellstabantriebsystem".
Kerntechnik 13, 9 (1971) 387

/5/ H. Zeibig, J. Blombach, F.W. Heuser, W. Rosenhauer
"Reliability Analysis of the Decay Heat Removal for SNR".
1972 (wie /1/)

Abb. 1



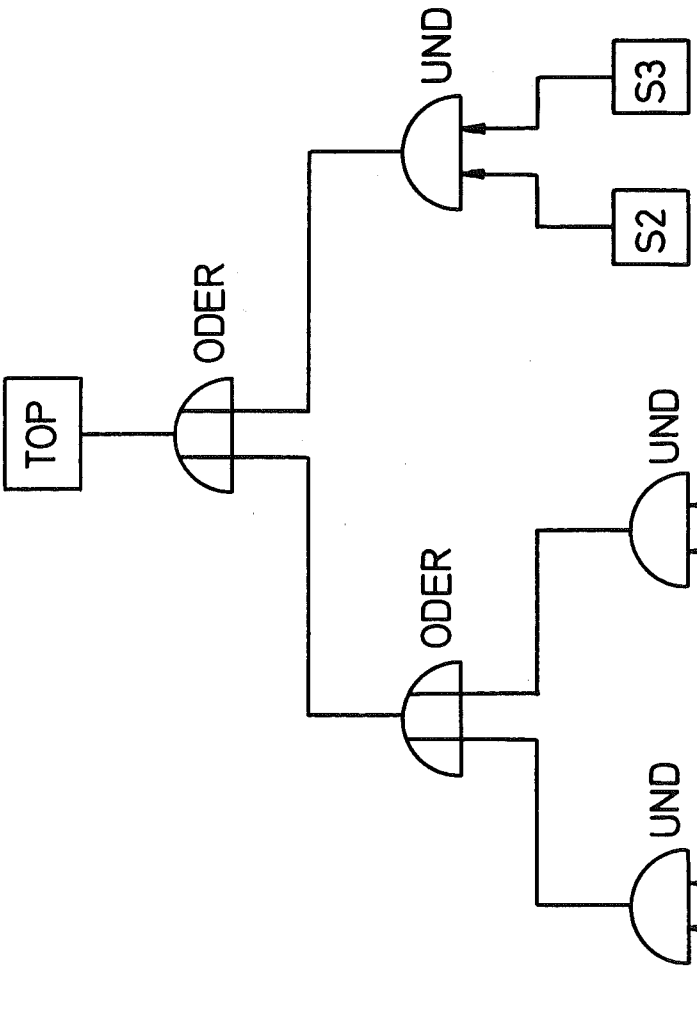
Übersicht Zuverlässigkeitstätigkeiten bei Interatom



2 von 3 Pumpensystem

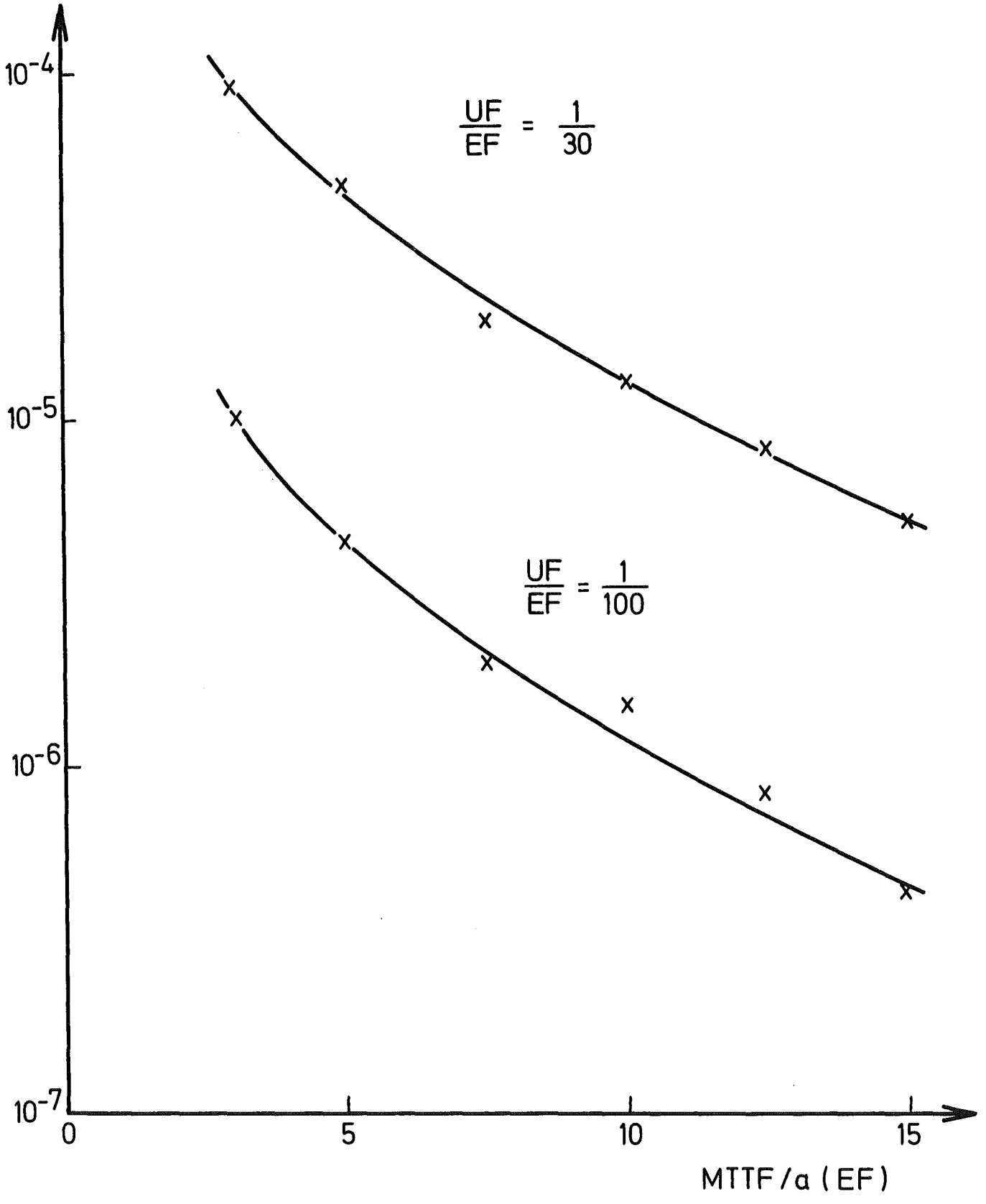
Abb. 2

TOP: zwei oder drei Stränge ausgefallen



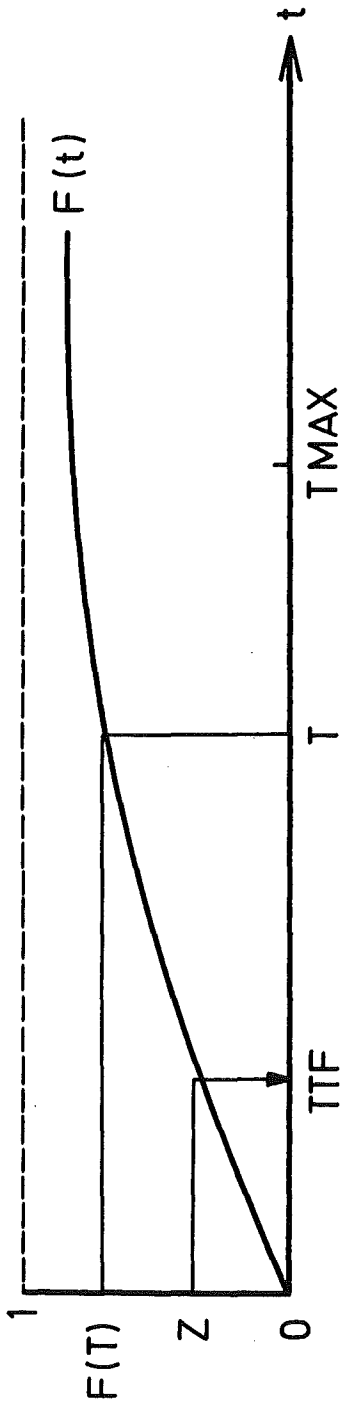
Fehlerbaum 2 von 3 - System

Abb. 3



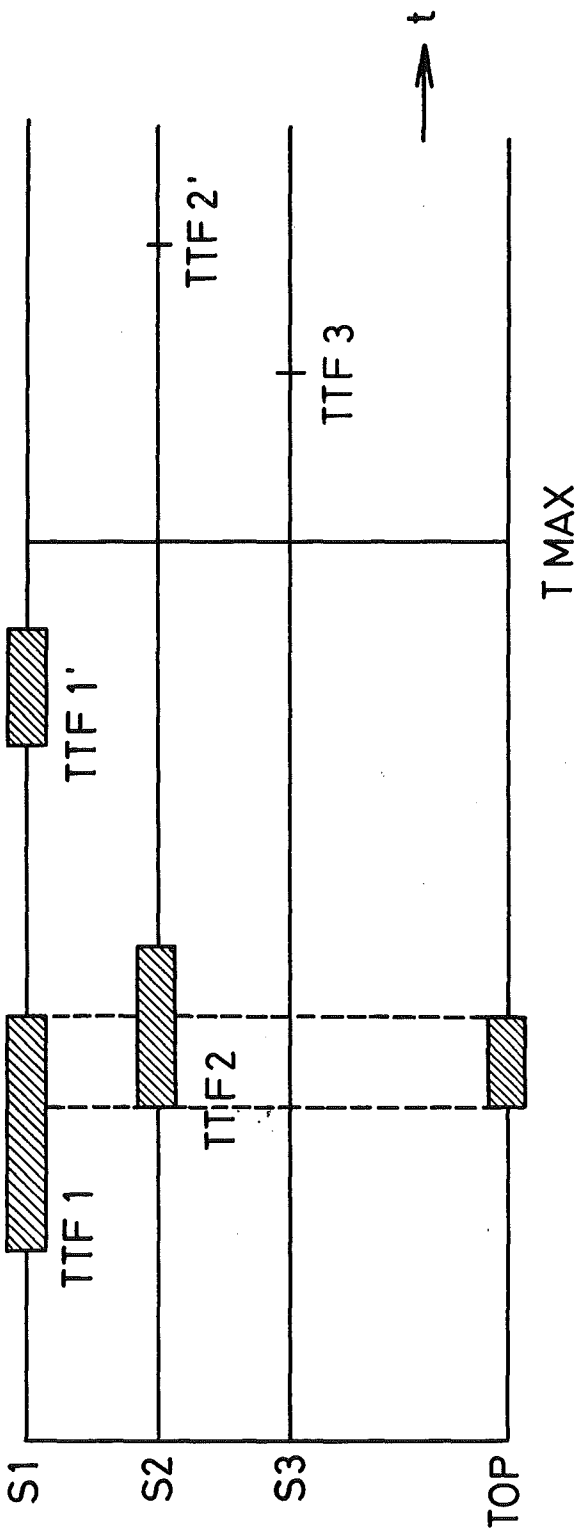
Unverfügbarkeit der TE's einer Meßsonde

Abb.4



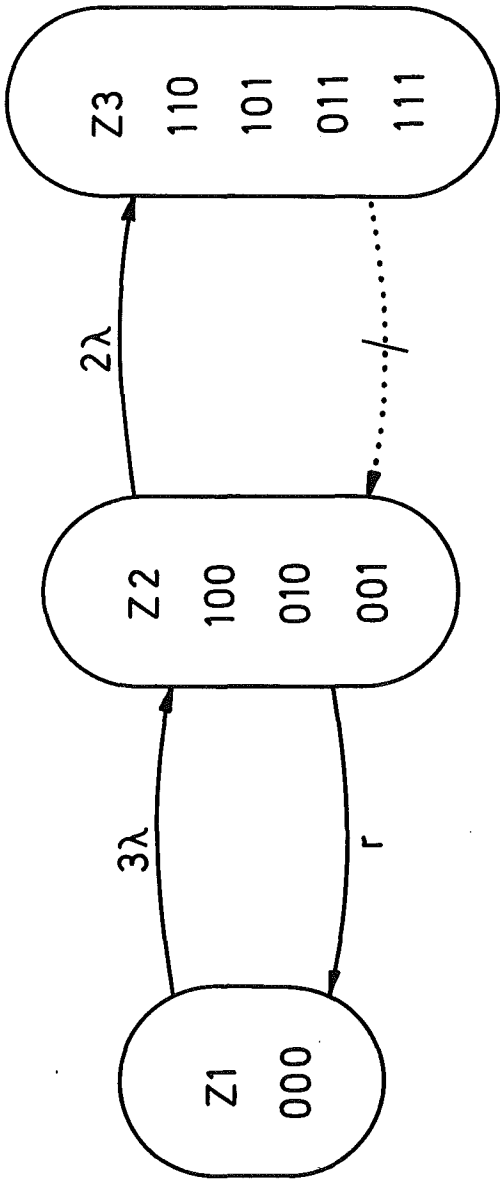
Bestimmung der TTF's mit Hilfe von Zufallszahlen Z

Abb.5



Zeitlicher Ablauf der Simulation

Abb.6



Zustandsdiagramm Zuverlässigkeit (2 von 3)

Abb.7

Abb. 8

Systeme mit Reparatur etc.	Zustandsanalyse / Markov: Hand-rechn.	Zustandsanalyse / Markov: Eigenw. progr.	Zustandsanalyse / Markov: Dgl. syst. progr.	Reine Sim. Progr.: FEBA-1 SAP	Reine Sim. Progr.: FEBA-2	Anal. / Sim. pr.: SAP
Kleine : $< 10^1$ Zustände	FPa	FPn	Na	Ns	Ns Standby	Ns
Mittlere : $\sim 10^2$ Zustände		FPn / Na	Na	Ns	Ns Standby	Ns
Größere : ~300 Komp. $W \lesssim 10^{-4}$				Ns	Ns Standby	Ns
Größere : ~300 Komp. W beliebig, Rep $\lesssim 10^{-4}$						Ns

F Formel , P Parameter, a analytisch , s simulativ

N Numerische Ergebnisse

Übersicht über die bei INTERATOM verwendeten Zuverlässigkeits - Rechenmethoden und die Ergebnisqualitäten

Projektbezogene Anwendung von Zuverlässigkeitsmethoden bei INTERATOM

2. Teil

F.W. Heuser, Bensberg

Nachdem im ersten Teil des Vortrags im wesentlichen die methodischen Grundlagen und Entwicklungen zu den bei INTERATOM durchgeführten Zuverlässigkeitsuntersuchungen behandelt worden sind, werden im zweiten Teil des Vortrags einige Anwendungen und Ergebnisse besprochen. Dabei handelt es sich um drei Problemstellungen:

1. Eine Zuverlässigkeitsanalyse zu zwei alternativen Auslegungskonzepten für die elektrische Energieversorgung SNR /1/,
2. Zuverlässigkeitsuntersuchungen zur Nachwärmeabfuhr SNR /2/ und
3. Bruchmechanische Untersuchungen zum Integritätsnachweis für das Primärsystem /3/.

Zur Einordnung dieser Probleme in einen umfassenden Zusammenhang zeigt Abb. 1 noch einmal das Übersichtsbild zu dem bei INTERATOM verfolgten Konzept für projektbegleitende Zuverlässigkeitsuntersuchungen.

Die ersten beiden Punkte stehen unmittelbar im Zusammenhang mit einer Analyse aller Anlagenstörfälle /4/, /5/. Die Zuverlässigkeitsanforderungen, die an die elektrische Energieversorgung und an die Systeme zur Nachwärmeabfuhr zu stellen sind, sind aus einer wahrscheinlichkeitstheoretischen Störfallanalyse abgeleitet worden, mit der alle Störfälle, die zu dem mit der Anlage verbundenen Risiko beitragen können, untersucht worden sind. So haben die Ergebnisse der Störfallanalyse gezeigt, daß die Zuverlässigkeitsanforderungen für die elektrische Energieversorgung ganz wesentlich von den Forderungen bestimmt werden, die für

eine sichere Nachwärmeabfuhr zu erfüllen sind. Es handelt sich hierbei um Anforderungen, die nach jeder Reaktorabschaltung auftreten, d.h. nach jeder geplanten Abschaltung (z.B. für Brennelementwechsel), mit jeder ungewollten Abschaltung (spurious scram) und natürlich zu jedem mit Reaktorschnellschluß verbundenen Störfall.

Es sind genau die Maßnahmen zur Beherrschung leichter, aber häufiger Störfälle und nicht die Anforderungen zur Beherrschung schwerer, jedoch seltener Störfallereignisse, die die Zuverlässigkeitsanforderungen an die Energieversorgung bestimmen. Zu jeder Reaktorabschaltung, d.h. zu jedem Übergang vom Leistungsbetrieb auf Nachscrambetrieb sind Maßnahmen zur Sicherstellung der Nachwärmeabfuhr, bzw. danach auch zur Aufrechterhaltung der Energieversorgung für die Dauer der Nachwärmeabfuhr, zu gewährleisten.

1. Zuverlässigkeitsanalysen zu zwei alternativen Auslegungskonzepten für die elektrische Energieversorgung SNR /1/

   Abb. 2 zeigt die elektrotechnischen Grundschaltungen zu den untersuchten Alternativkonzepten für die elektrische Energieversorgung SNR. Die linke Seite des Bildes zeigt das für die Anlage vorgesehene Referenzkonzept (Konzept 1). Im normalen Leistungsbetrieb wird die für den Eigenbedarf benötigte Leistung von der Einspeisung in das 220 kV-Versorgungsnetz abgezweigt und über den Eigenbedarfstransformator der 2-fach geteilten 6 kV-Eigenbedarfsanlage zugeführt.

   Für generatorseitige Störungen, d.h. zu jedem Reaktorschnellschluß oder aber auch bei Ausfall des Turbo-Generators selbst, wird der Generator mit Öffnen des 21 kV-Leistungsschalters von der Anlage abgetrennt. Die Eigenbedarfsanlage wird dann aus dem 220 kV-Versorgungsnetz eingespeist. Für netzseitige Störungen, d.h. für Störungen im 220 kV-Versorgungsnetz oder auch in der Ableitung zum Versorgungsnetz (Maschinentransformatoren) wird der netzseitige Leistungsschalter geöffnet. Der Generator muß dann auf Eigenbedarf abgefangen werden, damit die Anlage im Inselbetrieb weiter versorgt werden kann.

Störungen im Eigenbedarfsabzweig - und das ist ein entscheidender Nachteil dieses Konzepts - können nicht mehr mit einer anderen Einspeisung für die Eigenbedarfsanlage überbrückt werden. Ein Fehler in der Generatorableitung oder ein Ausfall der Eigenbedarfsversorgung bedeutet dann sofort Anforderung der Dieselnotstromaggregate zur Versorgung der 6 kV-Notstromverteilung.

Genau an dieser Stelle wurde das Referenzkonzept von den Genehmigungsbehörden als unzureichend angesehen,da diese Störungen nicht mit einer weiteren Netzeinspeisung überbrückt werden können. Darüberhinaus wurde von den Genehmigungsbehörden die Funktionstüchtigkeit der 21 kV-Leistungsschalter und ihr Einfluß auf das Ausfallverhalten der Gesamtanlage als kritisch angesehen. (Es handelt sich hierbei um neu entwickelte 21 kV-Leistungsschalter, die in der Lage sind, auch hohe Abschaltleistungen, z.B. bei Kurzschluß, zu schalten.)

Entsprechend den USAEC-Sicherheitskriterien /6/ und den vom IRS herausgegebenen Empfehlungen "Sicherheitskriterien für Kernkraftwerke" /7/, nach denen mindestens zwei voneinander unabhängige Anlagen zur Versorgung der Eigenbedarfsanlage gefordert werden, wurde von den Gutachtern das auf der rechten Seite von Abb. 2 gezeigte Alternativkonzept für die Energieversorgung vorgeschlagen.

In diesem Konzept wird auf die Abtrennung der generatorseitigen Störungen über dieLeistungsschalter verzichtet. Zur redundanten Einspeisung auf die 6 kV-Eigenbedarfsanlage steht vielmehr ein gesondertes Anfahrnetz auf einer anderen Spannungsebene als der des 220 kV-Versorgungsnetzes zur Verfügung.

Prinzipiell können die Schwierigkeiten des Referenzkonzepts mit dieser Alternativlösung überwunden werden, doch hat auch dieses Konzept besondere Schwachstellen und Nachteile:

- Die Unabhängigkeit beider Spannungsebenen kann nicht unbedingt vorausgesetzt werden,

- Während für den Anschluß an die 220 kV-Schaltstation des Versorgungsnetzes nur 2 km Freileitung notwendig sind, sind für den 110 kV-Anschluß des Anfahrnetzes ca. 20 km Freileitung zu installieren,

- Jede Störung im Blockbereich (Versorgung über den Eigenbedarfstransformator) fordert eine Eigenbedarfsumschaltung zwischen der Einspeisung vom Turbo-Generator und vom Anfahrnetz. (Eine besondere Schwierigkeit der Umschaltung ergibt sich aus der Eigenart der in einem Kernkraftwerk angeschlossenen Verbraucher, das Verhältnis von trägen Massen zu Motorleistungen kann bei einer Umschaltung so ungünstig liegen, daß eine stoßfreie Schnellumschaltung erschwert wird.)

Die Notstromanlage besteht aus einer 3-fach geteilten Notstromschiene, in der jeder einzelne Schienenabschnitt von je einem Dieselaggregat versorgt wird. Leistungsmäßig ist die Notstromanlage so ausgelegt, daß ein Dieselaggregat die volle Notstromleistung aufbringen kann, die zur Nachwärmeabfuhr notwendig ist. Andererseits kann beim SNR die Nachwärme bereits über eine der drei vorhandenen Kühlkreisketten abgeführt werden. Mit der 3-fach Aufteilung der Notstromanalge erreicht man dann eine konsequent eindeutige Zuordnung zwischen der elektrischen Versorgung und den Notstromverbrauchern in den einzelnen Kühlkreisketten. Dieses Konzept der unvermaschten Versorgungsstränge verfügt über eine hohe Unabhängigkeit der einzelnen Versorgungen (Einfluß von common mode failures) und bei entsprechender räumlicher Aufteilung auch über eine räumliche Redundanz gegenüber äußeren Störfalleinwirkungen (Flugzeugabsturz etc.). Die Notstromanlage entspricht damit weitgehend der USAEC-Sicherheitsvorschrift Nr. 6 zur Unabhängigkeit zwischen redundanten Energieversorgungsquellen (Notstromaggregate) und ihren Verteilungssystemen (Notstromverteilung) /8/.

Ausfall der Notstromverteilung liegt vor, wenn alle drei Schienenabschnitte der Verteilung ausgefallen sind und nicht mehr mit Strom versorgt werden können.

Hersteller und Betreiber sind - nicht zuletzt aus Kostengründen - natürlich an der Beibehaltung des Referenzkonzepts interessiert. Die Gutachter halten dieses Konzept jedoch nur dann für vertretbar, wenn mit einer Zuverlässigkeitsanalyse nachgewiesen wird, daß die Zuverlässigkeit des Konzepts 1 in derselben Größenordnung liegt wie für das vorgeschlagene Alternativkonzept (Konzept 2) mit Anfahrnetz.

Zu beiden Konzepten wurde eine Fehlerbaumanalyse vorgenommen, mit der das Ausfallverhalten von mehr als 100 Komponenten (je Konzept) berücksichtigt wird. Der Fehlerbaum wurde im einzelnen mit den Gutachtern abgesprochen. Abb. 3 zeigt ein Übersichtsbild für diesen Fehlerbaum. Für Konzept 1, das über kein Anfahrnetz verfügt, muß man sich dabei die in dem Bild eingetragene Umschalteinrichtung (US) zur Umschaltung auf das Anfahrnetz als ständig ausgefallen vorstellen. Entsprechend gilt für Konzept 2, in dem in der Generatorableitung keine Leistungsschalter zum Abtrennen einer Generator- bzw. Netzstörung vorgesehen sind, daß die Fehlerbaumeingänge der Ereignisse "Abtrennen des Generators" und "Abfangen des Generators" als ständig ausgefallen zu bewerten sind.

Neben der Frage der zu berücksichtigenden Ausfallmodi und Ausfallraten, die im wesentlichen der VDEW-Statistik /9/ entnommen worden sind,hat in den Gesprächen mit den Genehmigungsbehörden die Festlegung von Reparatur- und Inspektionszeiten für die einzelnen Komponenten eine entscheidende Rolle gespielt. Als Totzeit für die Komponenten wurden neben den tatsächlichen Reparaturzeiten auch die für die Anlage vorgesehenen Inspektionszeiten berücksichtigt.

Für die Rechnung erfaßt man damit den Einfluß der unentdeckbaren Ausfälle von Anforderungskomponenten, die ja nur in ganz bestimmten Betriebssituationen angefordert werden, und damit auf "intakt" oder "ausgefallen" erkannt werden können. Als Maß für die mittlere Entdeckungszeit für den Ausfall einer Anforderungskomponente wurde dabei die halbe Inspektionszeit angesetzt. Eine direkte Simulation von Anforderungskomponenten, wie sie mit dem Rechenprogramm SAP /10/ ohne weiteres durchgeführt werden kann, konnte nicht vorgenommen werden, da die vorliegenden Ausfallstatistiken, i.b. /9/, keine Ausfallwahrscheinlichkeiten per Anforderung enthalten.

Zur Diskussion der Ergebnisse möchte ich ein Splittingverfahren besprechen, mit dem der Einfluß einzelner Teil- bzw. Untersysteme auf das Ausfallverhalten des Gesamtsystems quantitativ beurteilt werden kann.

Zu beiden Konzepten sucht man eine Zerlegung des Gesamtergebnisses "Totalausfall der Energieversorgung auf der 6 kV-Notstromverteilung" nach sich gegenseitig ausschließenden Zuständen, "ausgefallen" oder "intakt" der 6 kV-Eigenbedarfsanlage

$$P(TOP) = P(TOP \wedge EB) + P(TOP \wedge \overline{EB}) \quad ,$$

zur multiplikativen Aufsplittung erhält man weiter mit der Einführung bedingter Wahrscheinlichkeiten

$$P(TOP) = P(TOP/_{EB}) * P(EB) + P(TOP/_{\overline{EB}}) * P(\overline{EB}) \quad .$$

(Mit dem Zeichen * soll angedeutet werden, daß die einfache Multiplikation der einzelnen Terme nur richtig ist, wenn die Splittinggleichung zur Ermittlung einer momentanen Wahrscheinlichkeit, z.B. der Verfügbarkeit oder der kumulativen Ausfallwahrscheinlichkeit ohne Berücksichtigung der Reparatur benutzt wird.)

Die einzelnen Terme dieser Aufsplittung lassen sich einfach deuten:

$P(EB)$ ist die Ausfallwahrscheinlichkeit der Eigenbedarfsanlage selbst,

$P(TOP/_{EB})$ ist die Ausfallwahrscheinlichkeit der Notstromverteilung unter der Voraussetzung, daß die Eigenbedarfsanlage bereits ausgefallen ist, d.h. $P(TOP_{/EB}) = P$ (Diesel),

$P(TOP/_{\overline{EB}})$ ist die Ausfallwahrscheinlichkeit der Notstromverteilung unter der Voraussetzung, daß die Eigenbedarfsanlage intakt ist, d.h. der Term enthält nur Fehleranteile in Kabelverbindungen, Schienenfehler etc., die zum Ausfall der Notstromverteilung führen, d.h. $P(TOP/_{EB}) = P$ (Verbindung).

Schließlich ist $P(\overline{EB}) = 1 - P(EB) \simeq 1$.

Die Splittingformel schreibt man dann zu

$$P(TOP) = P(Diesel) * P(EB) + P(Verb.) \quad ^{1)} \quad .$$

---

[1] Für die einzelnen Rechnungen ist die Splittingformel nicht einfach nach verschiedenen Zuständen für die Eigenbedarfsanlage, sondern etwas genauer nach verschiedenen sich gegenseitig ausschließenden Zustandskombinationen für die beiden Schienenabschnitte EBA und EBB der Eigenbedarfsanlage weiterzuführen.

Eine Aufspaltung nach dem Splittingverfahren ist natürlich nur dann sinnvoll, wenn das additive Splitting exklusiv und die multiplikativen Splittingterme voneinander unabhängig sind. Eine ausführlichere Beschreibung des Splittingverfahrens wird in /1/, Abschnitt 2.3, gegeben.

In der bisher gegebenen Splittingformel ist der Einfluß der Reparatur noch nicht berücksichtigt worden, z.B. liegt für den ersten, multiplikativen Anteil zur Ausfallwahrscheinlichkeit der Ausfall des Gesamtsystems nur mit dem gleichzeitigen Ausfall beider Teilsysteme (Ausfall der Eigenbedarfsversorgung und der Dieselnotstromversorgung) vor. Dieser Einfluß ist im multiplikativen Splittingterm mit einem Reparaturkoinzidenzfaktor C für gleichzeitigen Ausfall beider Teilsysteme (Überlappung von Reparatur- bzw. Totzeitintervallen) zu berücksichtigen. Es gilt dann allgemeiner

$$P(TOP) = P(Diesel).P(EB).C(Diesel, EB) + P(Verb.) \ .$$

In einer einfachen Abschätzung für den Reparaturkoinzidenzfaktor C zwischen zwei Teilsystemen a und b ist C(a, b) gleich der Summe der mittleren Reparaturzeiten Tr,a und Tr,b beider Teilsysteme bezogen auf die betrachtete Betriebszeit des Gesamtsystems

$$C(a,b) = \frac{Tr,a + Tr,b}{T_{max}} \ .$$

Diese Abschätzung kann mit einfachen Überlegungen zur Verfügbarkeit des Zweitsystems bei Ausfall des Erstsystems anschaulich erläutert werden. Eine exakte Begründung für diese Abschätzung kann mit einer analytischen Berechnung von C(a,b) über die Markowsche Zustandsanalyse erreicht werden. Man ermittelt hierzu die Wahrscheinlichkeit für gleichzeitigen Ausfall zweier Teilsysteme a und b, die mit den Fehlerraten λ_a, λ_b und den Reparaturraten r_a, r_b beschrieben werden.

Mit dem Splittingverfahren hat man für die praktische Anwendung ein Verfahren zur Hand, um den Einfluß einzelner Untersysteme auf das Ausfallverhalten eines Gesamtsystems quantitativ zu beurteilen. Dieses analytische Verfahren ist vor allem im Blick auf Parameterdiskussionen vielen statistischen Auswertungen von Simulationsprogrammen zur Einflußermittlung einzelner Komponenten auf das Gesamtausfallverhalten eines Systems, sowohl im Aufwand als auch in der Aussage wesentlich überlegen.

Die für die Analyse notwendigen Rechnungen wurden mit dem Rechenprogramm SAP (Struktur - Analyse - Programm) /10/ vorgenommen. Die Rechnungen zeigen, daß der entscheidende Anteil zur Ausfallwahrscheinlichkeit des Gesamtsystems vom ersten Splittingterm kommt, d.h. das Ergebnis wird im wesentlichen von der Zuverlässigkeit der Versorgungsquellen und ihrer Einspeisewege bestimmt, nicht aber von Ausfällen innerhalb der Verteilungsanlage selbst.

Ausfall-ereignis	Beschreibung	Ausfallwahr-scheinlichkeit	mittlere Ausfallzeit /h/
EB	Eigenbedarfs-anlage	Konzept 1 $(7{,}5 \pm 0{,}8).10^{-2}$ Konzept 2 $(3{,}4 \pm 0{,}6).10^{-2}$	14 ± 2 16 ± 3
TOP $\overline{EB}$	Dieselnotstrom-anlage	$(3{,}3 \pm 0{,}8).10^{-3}$	58 ± 9
TOP $\cap$ $\overline{EB}$	Ausfall über Kabel, Schienen etc.	$< 10^{-8}$	

Tabelle: Die kumulativen Ausfallwahrscheinlichkeiten für die einzelnen Teilsysteme nach einer Betriebszeit von 10^4 Stunden und die mittleren Reparaturzeiten für die einzelnen Teilsysteme

Die in den Rechnungen ermittelten Ergebnisse sind in der Tabelle 1 zusammengestellt worden. Angegeben werden die kumulativen Ausfallwahrscheinlichkeiten der einzelnen Teilsysteme nach einer Betriebszeit von 10^4 Stunden und zur Berechnung des Reparaturkoinzidenzfaktors die in den Simulationsläufen ermittelten mittleren Reparaturzeiten der einzelnen Teilsysteme. Die in der Tabelle angegebenen Unschärfen entsprechen dabei den mit den Simulationsrechnungen verbundenen Unsicherheiten. Als Maß dieser Unsicherheit wurde jeweils die Standardabweichung angegeben.

Die konzeptspezifischen Unterschiede sind allein schon mit P(EB), der Ausfallwahrscheinlichkeit für die Eigenbedarfsanlage gegeben. Der Unterschied in beiden Konzepten beträgt etwa einen Faktor 2. Für das Referenzkonzept (Konzept 1) liegt man damit in den von den Genehmigungsbehörden geforderten Nachweisgrenzen. Abb. 4 zeigt das aus den Splittingrechnungen ermittelte Gesamtergebnis für beide Konzepte. Aufgetragen wurde die kumulative Ausfallwahrscheinlichkeit für die 6 kV-Notstromverteilung in Abhängigkeit von der Zeit.

Die für beide Konzepte unterschiedlichen Ergebnisse sollen an der Ausfallwahrscheinlichkeit für die 6 kV-Eigenbedarfsanlage noch genauer diskutiert werden. Hierzu wurden je 2000 Simulationsspiele zu jedem Konzept ausgeführt und in Schadensprotokollen, die vom Programm entsprechend dem Simulationsablauf ausgedruckt werden, ausgewertet. Ausgehend vom normalen Betriebszustand der Anlage (Leistungsbetrieb) sind mit den für die Rechnungen angesetzten Ausfalldaten in 2000 Simulationsspielen

ca.	16000	generatorseitige Störungen (darin enthalten ca. 6 Scrams pro Jahr) ,
	400	netzseitige Störungen
und	60	Störungen im Eigenbedarfsabzweig

zu erwarten.

Gefragt wird nach dem Einfluß dieser Primärstörungen auf das Ausfallverhalten der 6 kV-Eigenbedarfsanlage. Die Anzahl der mit diesen Störungen simulierten Ausfälle der 6 kV-Eigenbedarfsanlage sind für beide Konzepte in der nachfolgenden Tabelle 2 zusammengestellt.

Anzahl Primärstörungen	Beschreibung	Konzept 1		Konzept 2	
		Anzahl Ausfälle	Ursache	Anzahl Ausfälle	Ursache
16000	Generator (einschl. Scram)	20	Netzstörungen	50	Störungen Anfahrnetz
		4	Generator-schalter	20	EB-Umschaltung
400	Ableitung zum 220 kV-Netz	60	Abfangen des Generators		-
60	Eigenbedarfsabzweig	60	(Störung selbst)	1	EB-Umschaltung

Tabelle 2: Anzahl der Ausfälle der 6 kV-Eigenbedarfsanlage für 2000 Simulationsspiele zu beiden Konzepten
- aufgeteilt nach Primärstörungen in verschiedenen Anlagenbereichen.

An den in der Tabelle zusammengestellten Ergebnissen sieht man die ganze Problematik beider Konzepte. Die Qualitäten des Konzepts 1 liegen ganz entscheidend in der sicheren Beherrschung generatorseitiger Störungen durch Öffnen des generatorseitigen Leistungsschalters und relativ sicherer Versorgung aus dem 220 kV-Netz. Für Konzept 2 erweist sich dagegen die mit der Störung angeforderte Umschaltung auf das Anfahrnetz als kritisch. Darüberhinaus fällt die relativ hohe Anzahl von Störungen im Anfahrnetz auf. Sie ist begründet mit der wesentlich längeren Freileitung zur 110 kV-Schaltstation als der zur 220 kV-Schaltstation im Versorgungsnetz.

Natürlich sind die zu den Rechnungen verwendeten Daten mit Unsicherheiten behaftet, doch die diskutierten Ergebnisse zeigen, daß zum Vergleich beider Konzepte nicht ohne weiteres Ergebnisse erzielt werden können, die sich um eine Größenordnung oder noch mehr voneinander unterscheiden.

Es soll noch darauf hingewiesen werden, daß die Genehmigungsbehörden unabhängig von unserer Fehlerbaum-Analyse und unseren Rechnungen zu gleichen Ergebnissen gekommen sind. Damit kann die von den Genehmigungsbehörden gemachte Auflage, die Zuverlässigkeit des Referenzkonzepts nachzuweisen, als erfüllt angesehen werden, so daß die Installation eines Anfahrnetzes nicht erforderlich ist.

2. Zuverlässigkeitsuntersuchungen zur Nachwärmeabfuhr SNR /2/

Neben dem Einfluß der Energieversorgung sind zur Beurteilung der Nachwärmeabfuhr eine ganze Reihe von Auslegungsgesichtspunkten und Zuverlässigkeitsanforderungen zu berücksichtigen. Bevor wir diese Anforderungen im einzelnen diskutieren, soll zunächst eine kurze Systembeschreibung zum Konzept der Nachwärmeabfuhr beim SNR gegeben werden. Abb. 5 zeigt hierzu ein Übersichtsbild zu den Systemen, über die die Nachwärme abgeführt werden kann.

Anders als in Wasserreaktoren wird im SNR die Nachwärme grundsätzlich über die Hauptkühlkreisketten an die Wärmesenke im Wasser-Dampf-System geführt. Zur Wärmeübertragung stehen dabei die drei parallelen Kühlkreisketten, bestehend aus Primär- und Sekundärnatriumkreis, sowie dem tertiären Wasser-Damps-Kreis zur Verfügung. Das Übersichtsbild in Abb. 5 zeigt eine dieser drei Wärmeübertragungsketten.

Ausgehend vom Reaktortank wird die Wärme über den Zwischenwärmetauscher (3) zwischen Primär- und Sekundärkreis und über den Dampferzeuger (5) an das Wasser-Dampf-System übertragen. Zur Speisewasserversorgung stehen im Tertiärkreis drei Speisewasserpumpen (12) zu je 50 % Fördermenge (Leistungsbetrieb) und vier Notspeisepumpen (19) zu je 100 % Fördermenge (Nachwärmebetrieb) zur Verfügung. Von den vier Notspeisepumpen ist jeweils eine einem Dampferzeugersystem zugeordnet, während die vierte Pumpe im Bedarfsfall wahlweise auf jede Wärmeübertragungskette aufgeschaltet werden kann. Die Rückkühlung des Speisewassers erfolgt in der ersten Phase der Nachwärmeabfuhr über die Kondensationsanlage (9) des Turbosatzes (6). In der zweiten Phase, oder im Notstromfall von Anfang an, wird die Nachwärme über die strangspezifischen Nachwärmekondensatoren (16) abgeführt. Zusätzlich zur Nachwärmeabfuhr über die Hauptkühlkreise kann die Nachwärme auch über ein Notkühlsystem abgeführt werden. Dieses System besteht aus sechs Tauchkühlern im Reaktortank, über sechs mit EM.Pumpen (21) getriebene Natriumkreisläufe wird die Nachwärme an zwei als Naturzug-Luftkühler (20) ausgebildete Wärmesenken abgegeben.

Mit der kurz gegebenen Systembeschreibung sind die Einrichtungen zur Nachwärmeabfuhr nach folgenden Gesichtspunkten ausgelegt:

- die Nachwärme kann bereits über eine der drei vorhandenen Kühlkreisketten abgeführt werden,
- nach Kühlmittelverluststörfällen ist die Nachwärmeabfuhr über die Hauptkühlkreise gewährleistet,
- bei Ausfall der Pumpen in den Primär- und Sekundärkreisen wird die Nachwärme im Naturumlauf an das Wasser-Dampf-System übertragen,
- bei Störungen im Tertiärsystem ist die Nachwärmeabfuhr über wenigstens zwei der drei Kühlkreisketten möglich.

Aus diesen Punkten ergeben sich im einzelnen eine Reihe von Auslegungsanforderungen, die hier nicht weiter erörtert werden können, es soll hier nur eine aktive Maßnahme erwähnt werden:

Um zu dem seltenen, aber schweren Störfall "Leckage im Primärkreis" im Reaktortank den Notspiegel des Kühlmittels nicht zu unterschreiten, ist es erforderlich, die Primärpumpen sicher auf eine Drehzahl kleiner 5 % der Nenndrehzahl abzufangen. Bei höherer Drehzahl der Pumpen wird der Notspiegel unterschritten, die Nachwärme kann dann nicht mehr über die Hauptkühlkreise, sondern nur noch über das Notkühlsystem abgeführt werden.

Nachdem das Sicherheitskonzept zur Nachwärmeabfuhr in seinen wesentlichen Punkten skizziert worden ist, sollen im zweiten Schritt die Zuverlässigkeitsanforderungen zur Nachwärmeabfuhr besprochen werden.

In der Analyse aller Anlagenstörfälle ermittelte man die kumulative Eintrittswahrscheinlichkeit für einen Schaden mit radiologischen Auswirkungen zu etwa 10^{-8} bezogen auf 1 Jahr. Akzeptiert man diese Zahl als ein für die Anlage tolerierbares Risiko, so entsprechen die zunächst in der Störfallanalyse angesetzten Schätzwerte nun Zuverlässigkeitsanforderungen, die an die einzelnen Untersysteme zu stellen sind. Diese Anforderungen sind in Detailanalysen nachzuweisen. Für die Nachwärmeabfuhr sind dabei Anforderungen an

das Primär- und Sekundärsystem,
die Energieversorgung,
das Wasser-Dampf-System
und das Notkühlsystem

nachzuweisen.

Zuverlässigkeitsanforderungen an das Primär- und Sekundärsystem:

Unter der pessimistischen Annahme, daß die Nachwärmeabfuhr in einer Kühlkreiskette blockiert ist, wird aus der Analyse aller Anlagenstörfälle für das Primär- und Sekundärsystem gefordert, daß die Ausfallwahrscheinlichkeit der Nachwärmeabfuhr im Zwangsumlauf kleiner als 8.10^{-6} ist /4/, /5/. Aus dieser Forderung für Primär- und Sekundärsystem lassen sich nun einzelne Anforderungen für die Na-Pumpen ableiten. Für eine erste Übersichtsrechnung wurde hierzu für die Pumpenanordnung im Primär- und Sekundärkreis eine Markowsche Zustandsanalyse vorgenommen. Der Einfachheit halber wurde für diese Analyse vorausgesetzt, daß alle Pumpen die gleichen Ausfallraten und Reparaturdaten haben. Abb. 6 zeigt die Zustände, die für eine Analyse des Pumpensystems

festzulegen sind,

Z1 - alle Pumpen sind intakt,

Z2 - genau eine Pumpe in einer der beiden Kühlkreisketten ist ausgefallen,

Z3 - Primär- und Sekundärpumpe einer Kühlkreiskette sind ausgefallen,

Z4 - in jeder der beiden Kühlkreisketten ist mindestens eine Pumpe ausgefallen.

Das System ist durch die Definition dieser vier Zustände vollständig festgelegt und mit einem Markow-Prozeß beschreibbar. Die Übergangswahrscheinlichkeiten zwischen den festgelegten Zuständen sind durch die Ausfall- und Reparaturraten λ und r einer Pumpe gegeben. Der Zustand Z4 charakterisiert den Ausfall der Nachwärmeabfuhr. Für die hier vorgenommene Zuverlässigkeitsanalyse muß vorausgesetzt werden, daß das System im Zustand Z4 nicht mehr repariert werden kann.

Setzt man voraus, daß die mittlere Zeit zwischen zwei Fehlern groß ist gegenüber der erforderlichen Reparaturzeit, d.h. $\rho = \lambda/r << 1$, so erhält man für die Ausfallwahrscheinlichkeit des Systems (Wahrscheinlichkeit für Z4) zu Zeiten t, die groß sind gegenüber der mittleren Systemreparaturzeit,

$$P_4(t) \approx 8\,\rho^2 rt \quad \text{mit} \quad \rho = \lambda/r \ .$$

Fordert man im analytischen Ergebnis für die Ausfallwahrscheinlichkeit $P_4 = 8.10^{-6}$, so erhält man mit einer vorgegebenen Dauer der Nachwärmeabfuhr und einer vorgegebenen Reparaturzeit MTTR = $\frac{1}{r}$ eine Zuverlässigkeitsanforderung für die Pumpe selbst. Mit $t = 10^3$ h zur Dauer der Nachwärmeabfuhr und MTTR = 10 h für die Reparaturzeit an einer Pumpe erhält man $\lambda = 10^{-5}\ h^{-1}$ als Ausfallrate einer Pumpe. Das ist ein Wert, der durchaus mit bisherigen Betriebserfahrungen für Natrium-Pumpen übereinstimmt.

Zuverlässigkeitsanforderungen an die Energieversorgung:

Im Zusammenhang mit der Nachwärmeabfuhr müssen für die Energieversorgung natürlich die Anforderungen bei Nachscrambetrieb (und nicht im Leistungsbetrieb) nachgewiesen werden, da nach Reaktorschnellschluß der Generator als Einspeisung nicht mehr zur Verfügung steht.

In Abb. 7 ist die Ausfallwahrscheinlichkeit der 6 kV-Notstromverteilung für Nachscrambetrieb über der Zeit aufgetragen worden.

Die mit den offenen Kreisen gegebene Kurve entspricht dabei Rechnungen zum Referenzkonzept (Konzept 1, ohne Anfahrnetz) für die Energieversorgung. Setzt man zur Dauer der Nachwärmeabfuhr eine Zeit $t = 2.10^3$ h an, so erhält man für die Zuverlässigkeit der Energieversorgung $P \lesssim 10^{-6}$ als Ausfallwahrscheinlichkeit.

Der Einfluß der Energieversorgung ist im Fehlerbaum für die Nachwärmeabfuhr stark vereinfacht berücksichtigt worden, die ganze Energieversorgung wird darin nur mit einigen Komponenten beschrieben,
einer Normalversorgung,
den Startanregungen für die Dieselaggregate
und den Dieselaggregaten selbst, unterschieden nach Standby- und Betriebsverhalten.

Ausfall- und Reparaturdaten dieser Komponenten mußten so gewählt werden, daß die für die Nachwärmeabfuhr vorgenommenen Vereinfachungen mit den Ergebnissen der genauen Rechnung (Abb. 7, offene Kreise) gut übereinstimmen. Die mit den geschlossenen Kreisen in Abb. 7 gegebene Kurve entspricht den Ergebnissen dieser vereinfachten Rechnung.

Zuverlässigkeitsanforderungen an das Wasser-Dampf-System und an das Notkühlsystem:

Die Zuverlässigkeitsanforderungen an das Wasser-Dampf-System und an das Notkühlsystem können grundsätzlich nach folgenden Gesichtspunkten diskutiert werden:

- Für das Wasser-Dampf-System:

  Die Nachwärme muß mit der gleichen Zuverlässigkeit abgeführt werden, wie sie vom Sekundärsystem angeboten wird. Betrachtet man in den Na-Systemen nur den Zwangsumlauf, so entspricht dies einer Minimalanforderung an das Wasser-Dampf-System.

- Für das Notkühlsystem:

  Das Notkühlsystem selbst soll nur die unwahrscheinlichen Fälle abdecken, in denen eine Nachwärmeabfuhr über die Hauptkühlkreise nicht möglich ist.

Dem derzeitigen Auslegungsstand entsprechend soll in einem ersten Schritt zunächst nur eine Übersicht über die grundlegende Zuordnung von Zuverlässigkeitsanforderungen zu den verschiedenen Teilsystemen gefunden werden. Für die Zuverlässigkeitsanalyse zur Beurteilung der Nachwärmeabfuhr ist darum zunächst ein sehr vereinfachter Fehlerbaum ausgearbeitet worden. Allerdings, und darauf kam es wesentlich an, sollten für diese Untersuchungen verschiedene Bedingungen zur Betriebsstrategie (z.B. Einfluß des Standby-Verhaltens der Dieselnotstromaggregate, spezielle Anforderungsbedingungen für das Notkühlsystem) realistisch erfaßt werden.

Abb. 8 zeigt den Fehlerbaum zum Ausfall der Nachwärmeabfuhr, hier für den Fall, daß eine Kühlkreiskette bereits ausgefallen ist und die Nachwärme nur über zwei Kühlkreisketten abgeführt werden kann. Der entsprechende Fehlerbaum für die Nachwärmeabfuhr über drei Kühlkreisketten ist in Abb. 9 wiedergegeben. Tabelle 3 (hinter Abb. 9) enthält eine Liste der in den Fehlerbäumen berücksichtigten Komponenten mit den für die Rechnungen angesetzten Ausfall- und Reparaturdaten.

Im folgenden soll der Fehlerbaum zur Nachwärmeabfuhr über zwei Hauptkühlkreisketten (Abb. 8) kurz besprochen werden. Mit diesem Fehlerbaum beschreibt man das Verhalten der Anlage nach kreisspezifischen Störfällen in den Wärmeübertragungsketten. Für die Analyse geht man dabei von der Annahme aus, daß der gestörte Kühlkreis während der ganzen Nachwärmeabfuhrphase nicht mehr zur Verfügung steht.

Auf der rechten Seite des Bildes (Abb. 8) sind die beiden Hauptkühlkreisketten mit den Primär- und Sekundärpumpensystemen (1), (2) und (5), (6), sowie den kreisspezifischen Komponenten des Wasser-Dampf-Systems (3) und (7) zu sehen. (11) bezeichnet die normale Energieversorgung, d.h. Einspeisung der Notstromverteilung vom 220 kV-Versorgungsnetz über die Eigenbedarfsanlage. Der Fehlerbaum ist aufgeteilt (gesplittet) nach sich gegenseitig ausschließenden Ausfallkombinationen zu intakter und ausgefallener Normalversorgung. Ausfall der Nachwärmeabfuhr liegt z.B. dann vor, wenn bei intakter Normalversorgung (11 intakt) zwei Hauptkühlkreisketten ausgefallen sind und das über T17 (T17 auf "1") angeforderte Notkühlsystem mit der Anforderung (15*) "Umschaltung auf Notkühlsystem" ausfällt.

Die Einzelheiten aller Ausfallkombinationen, i.b. die zu ausgefallener Normalversorgung (11 ausgefallen), möchte ich nicht besprechen, dafür aber jedoch kurz auf die in dem Fehlerbaum verarbeitete Betriebsstrategie eingehen. Mit dem Ausfall der Normalversorgung (11 auf "1") werden die Anforderungen zum Start der Dieselaggregate (13*), (14*) aufgerufen. Für die Dieselaggregate wird ein Ausfall sowohl im Bereitschaftszustand (vor der Startanforderung) als auch im Betriebszustand (nach der Startanforderung) erfaßt. Bereitschafts- und Betriebszustand werden dabei mit unterschiedlichen Ausfallraten, Reparatur- und Inspektionszeiten beschrieben. Neben der Anforderung für das Notkühlsystem (15*) wird zur Notstromversorgung für das Notkühlsystem eine Diesel-Fortschaltung von D1 über D2 nach D3 mit Komponenten (16*) und (18*) berücksichtigt. In Abb. 10 sind einige Ergebnisse zu den Rechnungen für die Nachwärmeabfuhr über zwei Hauptkühlkreisketten wiedergegeben. Aufgetragen ist die Ausfallwahrscheinlichkeit zur Nachwärmeabfuhr über eine Zeitdauer $T_{max} = 3.10^3 h$. Die mittlere Kurve entspricht dem vorgesehenen Auslegungsstand, Nachwärmeabfuhr über die Hauptkühlkreise und über das Notkühlsystem. Die obere Kurve zeigt die Ausfallwahrscheinlichkeit zur Nachwärmeabfuhr allein über die Hauptkühlkreise. Sie ist ungefähr um einen Faktor 10 größer als in der mittleren Kurve zum vorgesehenen Auslegungsstand. Andererseits ist mit einer ideal guten Energieversorgung für das Notkühlsystem (untere Kurve) die Ausfallwahrscheinlichkeit um einen Faktor 3 bis 5 niedriger als die zum Referenzkonzept.

Abb. 11 zeigt die entsprechenden Ergebnisse zur Nachwärmeabfuhr über drei Hauptkühlkreise. Diese Situation liegt vor zu Störfällen, die nicht in den

Wärmeübertragungsketten liegen (z.B. ungewollte Reaktorabschaltung). Die mittlere Kurve zeigt wieder das Ausfallverhalten für das Referenzkonzept, Nachwärmeabfuhr über die Hauptkühlkreise und das Notkühlsystem. Die Ausfallwahrscheinlichkeit für die Nachwärmeabfuhr allein über die Hauptkühlkreise(ohne Notkühlsystem) ist unwesentlich größer. Das liegt einfach daran, daß hier das Gesamtergebnis gegen die Zuverlässigkeit der Energieversorgung aufläuft. Die hohe Redundanz der Kühlkreisketten kommt erst mit der unteren Kurve voll zur Geltung, in der für das Notkühlsystem wieder eine eigene, ideal gute Energieversorgung vorausgesetzt worden ist.

3. Bruchmechanische Untersuchungen zum Integritätsnachweis für das Primärsystem /3/

Zur Sicherheitsbeurteilung von Reaktoren kommt dem Integritätsnachweis für das Primärsystem eine ganz entscheidende Bedeutung zu. Zuverlässigkeitsanalysen auf der Grundlage zahlenmäßiger Erfahrungswerte und wahrscheinlichkeitstheoretische Ansätze sind für diesen Nachweis jedoch nicht ohne weiteres möglich. Eine effektive Erhöhung der Zuverlässigkeit aber, z.B. von Rohrleitungen, kann jedoch damit erreicht werden, daß man Materialeigenschaften und Ausfallmechanismen, oder anders gesagt, das Ausfallverhalten von Strukturwerkstoffen, untersucht.

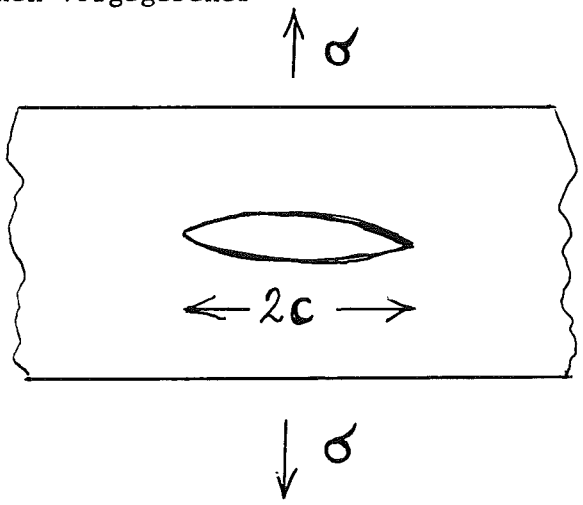
In diesem Zusammenhang möchte ich über die bei INTERATOM durchgeführten Arbeiten auf dem Gebiet der Bruchmechanik berichten. Es handelt sich hierbei um Berstversuche an Rohrproben, bruchmechanische Untersuchungen zu Längs- und Umfangrissen an KNK-Rohren des Primärsystems mit Originalabmessungen. Die Untersuchungen führen zur Aufstellung eines Leck vor Bruch-Kriteriums, man zeigt, daß es mit dem Anriß eines Rohres nicht unmittelbar zum prompten Abriß des vollen Rohrquerschnitts oder zum totalen Aufriß eines Rohres kommen kann, sondern immer erst zu einer begrenzten Leckage, bevor promptes, d.h. überkritisches Rißwachstum überhaupt einsetzen kann.

Diese Untersuchungen haben im Genehmigungsverfahren für KNK eine entscheidende Rolle gespielt. Aufgrund der experimentell vorliegenden Ergebnisse zu Berstversuchen an KNK-Rohren konnte erreicht werden, daß für das Doppelrohr zwischen dem Eintrittsstutzen am Reaktortank und den Absperrarmaturen in den Kreisläufen das Außenrohr nicht auf promptes Aufreißen des Innenrohres ausgelegt werden muß.

Die Grundüberlegungen dieser Versuche bauen auf neueren Entwicklungen der Bruchmechanik zur Bestimmung eines kritischen Spannungsintensitätsfaktors K_c auf. Wichtig dabei ist, daß dieser Spannungsintensitätsfaktor eine von der Versuchsanordnung, Probengeometrie, Versuchsdurchführung unabhängige Materialkonstante ist, mit der das Rißverhalten in einem Werkstoff in Abhängigkeit von einer äußeren Spannung beschrieben werden kann. Für eine allgemeine verständliche Einführung in die Grundzüge dieses Konzepts wird auf /11/ verwiesen.

Ich will versuchen, den Grundgedanken dieses Konzepts in seiner einfachsten Form verständlich zu machen.

Man betrachtet eine unendlich ausgedehnte Platte, in die unter der Zugspannung σ ein Riß der Länge 2c eingebracht wird. Überlegungen zur Bilanz der an einem Rißwachstum beteiligten Energien führen zu einem Bruchkriterium, d.h. zu einer Beziehung zwischen vorgegebener



Rißlänge und kritischer Spannung σ_t für promptes Rißwachstum. Bei der Einbringung eines Risses der Länge 2c in den unter Zug beanspruchten Körper wird eine elastische Energie $U_{el} \simeq \frac{\Pi^2 c^2 \sigma^2}{E}$ freigesetzt, andererseits ist zur Bildung des Risses der Länge 2c eine Rißbildungsenergie $U_G \simeq 4cG$ aufzubringen (E ist der Elastizitätsmodul und G die spezifische Rißbildungsenergie pro Flächeneinheit). Die Bilanz dieser Energien führt zu einem Stabilitätskriterium, das in seiner einfachsten Form für Sprödbruchverhalten

$$\sigma_c = \sqrt{\frac{EG}{\Pi c}}$$

von Griffith (1920) angegeben worden ist. Zu einer vorgegebenen Rißlänge c

ist σ_c die von außen angreifende Spannung, oberhalb der prompte Rißausbreitung einsetzt.

Neuere Arbeiten zur Spannungsanalyse an der Rißspitze (Irvine et al., 1948 ff) führten zur Entwicklung des Konzepts für einen kritischen Spannungsintensitätsfaktor K_c. Die mit einer Spannungsanalyse ermittelte Lösung für die Spannung in der Umgebung der Rißspitze zeigte, daß die in der Rißspitze auftretenden Spannungen über einen Spannungsintensitätsfaktor K mit

$$K = \sigma \sqrt{\pi c}$$

in Beziehung zur äußeren Zugspannung σ gesetzt werden können. Setzt man $\sigma = \sigma_c$ (kritische Spannung für Rißwachstum) so erhält man mit $K = K_c$

$$K_c^2 = E \cdot G \ ,$$

d.h. der kritische Spannungsintensitätsfaktor K_c kann als eine Materialkonstante zum bruchmechanischen Verhalten eines Werkstoffs gedeutet werden. Über die Beziehung zur Rißbildungsenergie oder Rißzähigkeit G sieht man: K_c ist ein Maß für die Bruchzähigkeit eines Werkstoffes. Die für K_c (in ihrer einfachsten Form) angegebene Beziehung bildet den Ausgangspunkt aller bruchmechanischen Untersuchungen auf der Basis des kritischen Spannungsintensitätsfaktors.

Für die uns interessierenden Werkstoffe liegen die tatsächlichen Verhältnisse jedoch wesentlich komplizierter als hier skizziert worden ist. Von technischem Interesse sind hochzähe Werkstoffe, die plastische Verformungen aufnehmen. So kommt es über zunehmender Spannung vor dem Rißgrund zur Ausbildung einer mehr oder weniger großen plastischen Zone, es kommt zu einer Einschnürung an der Rißspitze, das Material beginnt zu fließen, bevor es zur weiteren Rißausbreitung, zum überkritischen Rißwachstum kommt. Man kann sagen, K_c ist ein Maß für die plastische Verformungsenergie, die zu überwinden ist, damit Rißwachstum eintreten kann. Dieser Effekt der plastischen Verformung ist sowohl in der Theorie als auch experimentell für den kritischen Spannungsintensitätsfaktor zu berücksichtigen. So muß die Ausdehnung einer plastischen Zone natürlich von einer Probenabmessung aufgenommen werden. Hier kommt es unter Umständen zu sehr aufwendigen Versuchsbedingungen.

Eine besondere Schwierigkeit besteht auch darin, im Experiment wirklich zu konservativ abgesicherten K_c-Werten zu kommen, d.h. den niedrigsten K_c-Wert zu ermitteln, mit dem Dehnungsbehinderungen, wie sie in technischen Bauteilen auftreten, auch berücksichtigt werden. Um K_c mit seinem tatsächlichen Wert als Materialkonstante experimentell zu ermitteln, hat man unbedingt darauf zu achten, daß in der Probe der ebene Dehnungszustand vorliegt, mit dem mögliche Dehnungsbehinderungen gegen plastische Verformung (die einen Bruch tendentiell begünstigen) auch erfaßt werden.

In den bei INTERATOM durchgeführten Berstversuchen an Rohrproben werden die Schwierigkeiten damit überwunden, daß die Versuche an Originalbauteilen vorgenommen werden. Die Versuche werden zu künstlich angebrachten Längs- und Umfangsrissen verschiedener Längen unternommen /3/. Nachdem der künstlich eingebrachte Riß mit einer Metallfolie abgedichtet worden ist, wird im Inneren des Rohres hydraulisch ein Druck aufgebaut. Beobachtet wird das Rißverhalten über ansteigendem Druck, bzw. über ansteigender äußerer Spannung. Ermittelt wird die Spannung, zu der Rißwachstum einsetzt und beobachtet werden kann.

Abb. 12 enthält einige experimentelle Ergebnisse zu den an KNK-Rohrproben durchgeführten Berstversuchen. Aufgetragen ist der Zusammenhang zwischen kritischer Rißlänge 2c und der äußeren angelegten Spannung σ, hier zu verschiedenen Ansätzen zur Ermittlung des kritischen Spannungsintensitätsfaktors bei Rohrgeometrie /3/, /12/. Eingetragen sind die Versuchsergebnisse zu verschiedenen Längsrissen in KNK-Rohrproben.

Sieht man von den numerischen Unterschieden in den verschieden ermittelten K_c-Werten ab (sie sind hauptsächlich von theoretischem Interesse zur Beurteilung der verschiedenen zur Auswertung herangezogenen Ansätze), so zeigen die experimentellen Ergebnisse eine äußerst gute Übereinstimmung mit den hier angesetzten Auswertungen /3/, /12/. Wichtig ist, daß zu den hier interessierenden Betriebsspannungen σ_v kritische Rißlängen mit $2c \approx 40$ cm ermittelt werden. Dieses Ergebnis zeigt deutlich, daß es zu den in den Rohrleitungen vorliegenden Betriebsbedingungen bei Rißbildungen immer erst zu entdeckbaren Leckagen kommen wird, bevor ein vorhandener Riß instabil wird und Rißwachstum einsetzt.

Die Abb. 13a-e zeigen einige Aufnahmen, die in einem Berstversuch mit Längsriß über zunehmendem Druck- bzw. Spannungsaufbau gemacht worden sind. Abb. 13a zeigt die Ausgangssituation des vorgefertigten Risses mit einem im Pulsbetrieb erzeugten natürlichen Anriß in der Rißspitze. Die weiteren Abbildungen zeigen die über zunehmender Spannung sich ausbildende plastische Zone und Einschnürung vor der Rißspitze. Darüber hinaus kann in den Abb. 13c und d das über dem Spannungsaufbau einsetzende Rißwachstum verfolgt werden, bis schließlich in Abb. 13e das Rißwachstum über mehrere Markierungen (Abstand 1 mm) mit starker Einschnürung vor der Rißfront beobachtet wird.

Literaturangaben

/1/ F.W. Heuser, H. Werner
Zuverlässigkeitsuntersuchung der elektrischen Energieversorgung SNR 300, INTERATOM
Technischer Bericht ITB 72.44 (1972)

/2/ H. Zeibig, J. Blombach, F.W. Heuser, W. Rosenhauer
Reliability Analysis of the Decay Heat Removal for SNR.
International Conference on Engineering of Fast Reactors for Safe and Reliable Operation, Karlsruhe, Germany, October 1972

/3/ H. Zeibig, E. Fortmann
Fracture Behavior Investigations of 10 CrMoNiNb 910 Steel Pipes.
First Int. Conf. on Structural Mechanics in Reactor Technology, Berlin, September 1971

/4/ H.W. zur Horst
Wahrscheinlichkeitstheoretische Störfallanalyse SNR.
INTERATOM-Arbeitsbericht 70/2, Teil 1, April 1970

/5/ J. Wehling
Wahrscheinlichkeitstheoretische Störfallanalyse SNR.
INTERATOM Technischer Bericht ITB 72.26
April 1972

/6/ General Design Criteria For Nuclear Power Plants.
Atomic Energy Commission, 10 CFK part 50,
Appendix A-Federal Register Vol. 36, No. 35,
Febr. 1971 - siehe auch IRS-Kurzinformation 71/40/C

/7/ Sicherheitskriterien für Kernkraftwerke
IRS-R-2, 1969

/8/ Safety Guide 6
Independence between redundant standby (onsite) power sources and between their distribution systems.
Atomic Energy Commission,
Oct. 1971 - siehe auch IRS-Kurzinformation 71/34/C

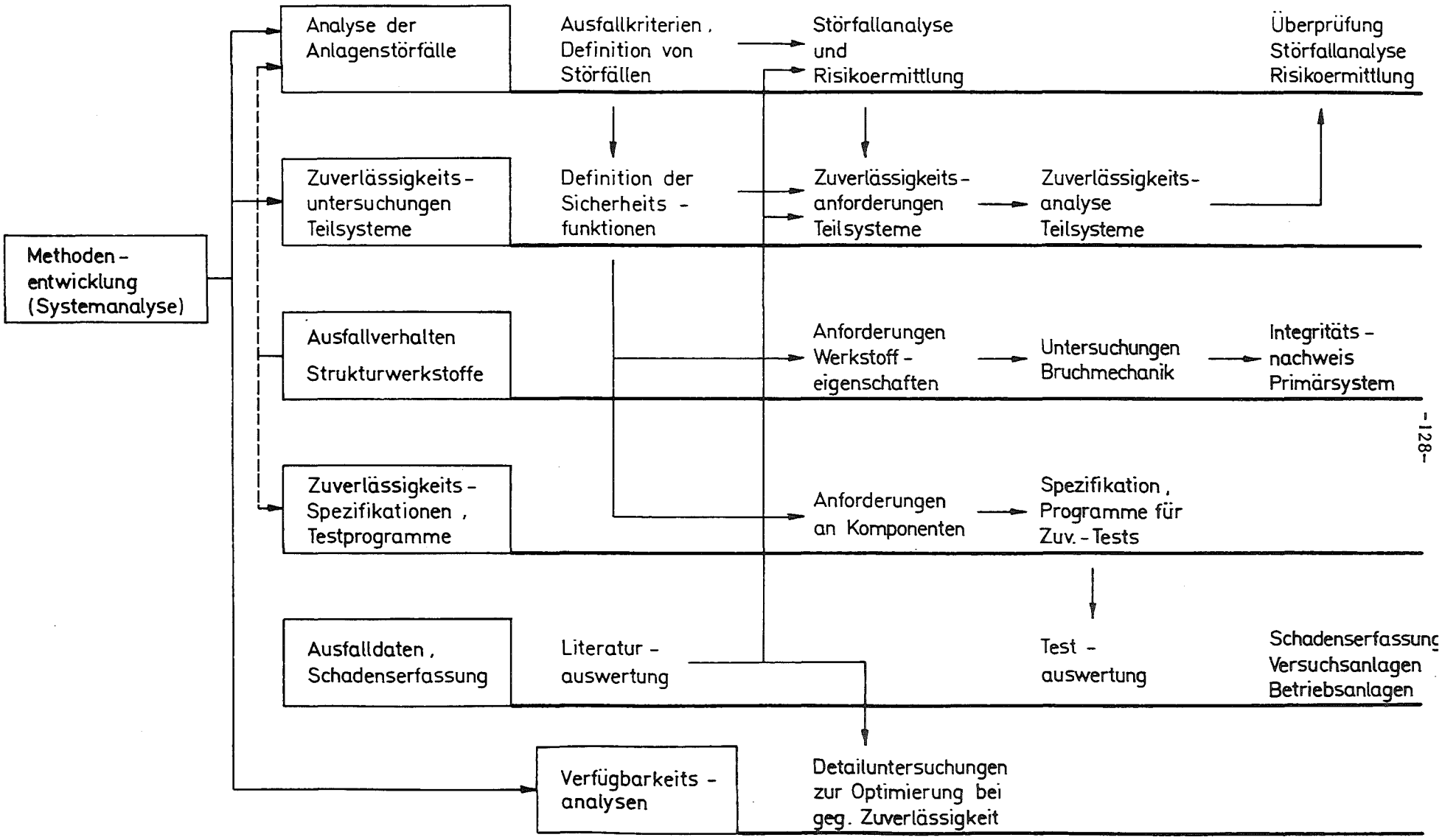
/9/ VDEW Störungs- und Schadensstatistik, 1969
herausgegeben von der Vereinigung Deutscher Elektrizitätswerke
- VDEW e.V., Frankfurt/M.

/10/ F.W. Heuser, W. Rosenhauer
SAP-1 . Ein neues Programm zur Berechnung von Zuverlässigkeitsgrößen komplexer Systeme.
Atomwirtschaft 17, Heft 2, 1972

/11/ W. Dahl
Grundlagen und Anwendungsmöglichkeiten der Bruchmechanik bei der Sprödbruchprüfung.
Zeitschrift für Metallkunde, Bd. 61, 1970, S. 794 ff.

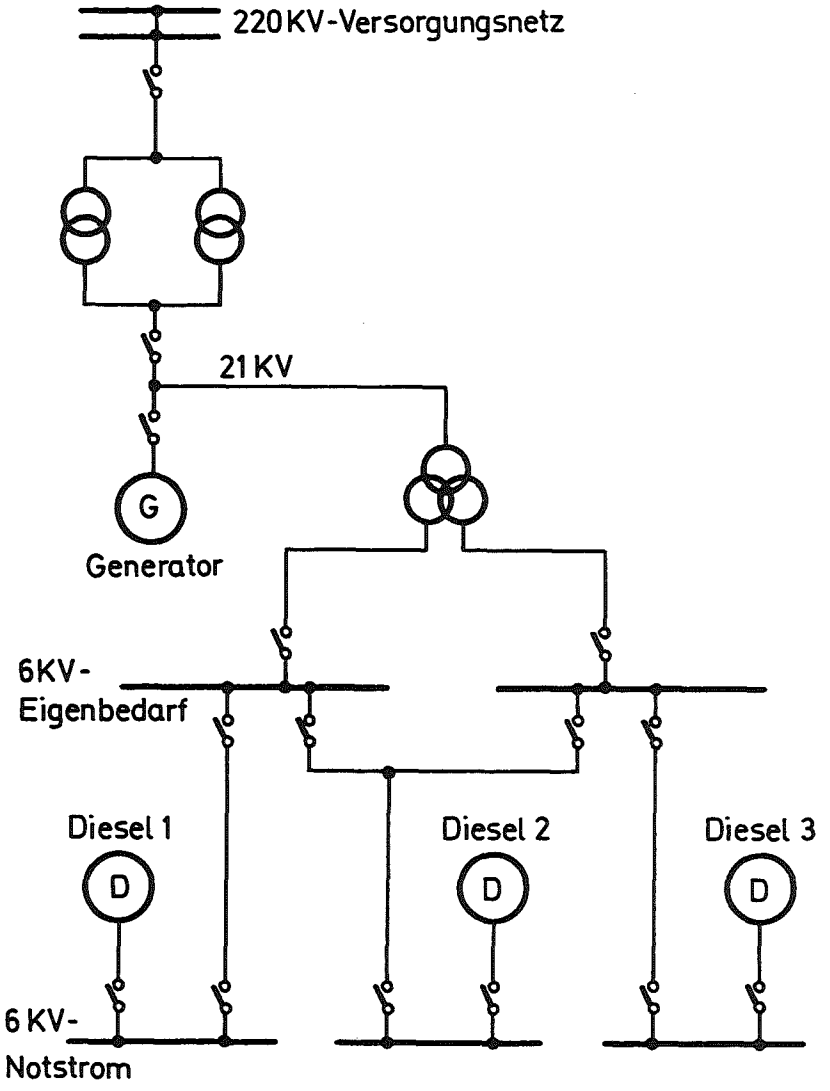
/12/ Duffy, A.R., et al.
"Fracture", Vol. 5, edited by Liebowitz, H., Academic Press, New York (1969)

Abb. 1

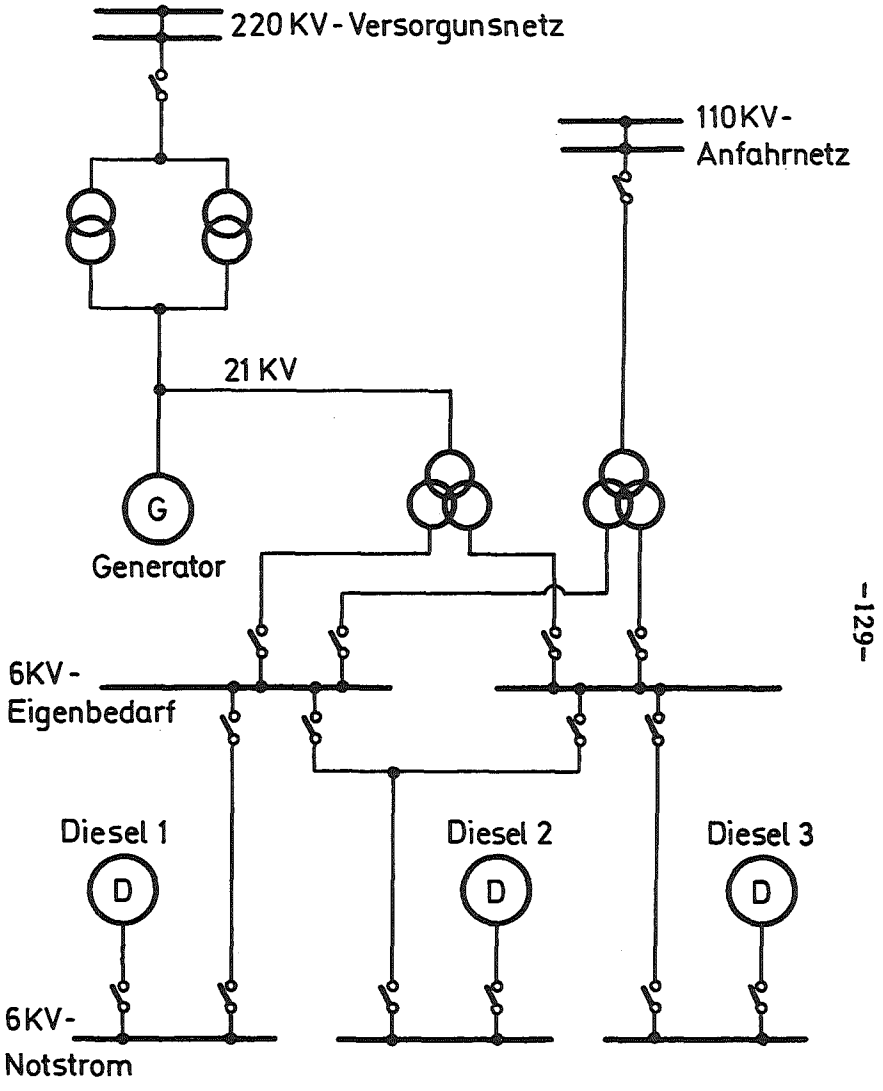


Übersicht Zuverlässigkeitstätigkeiten bei Interatom

Abb. 2

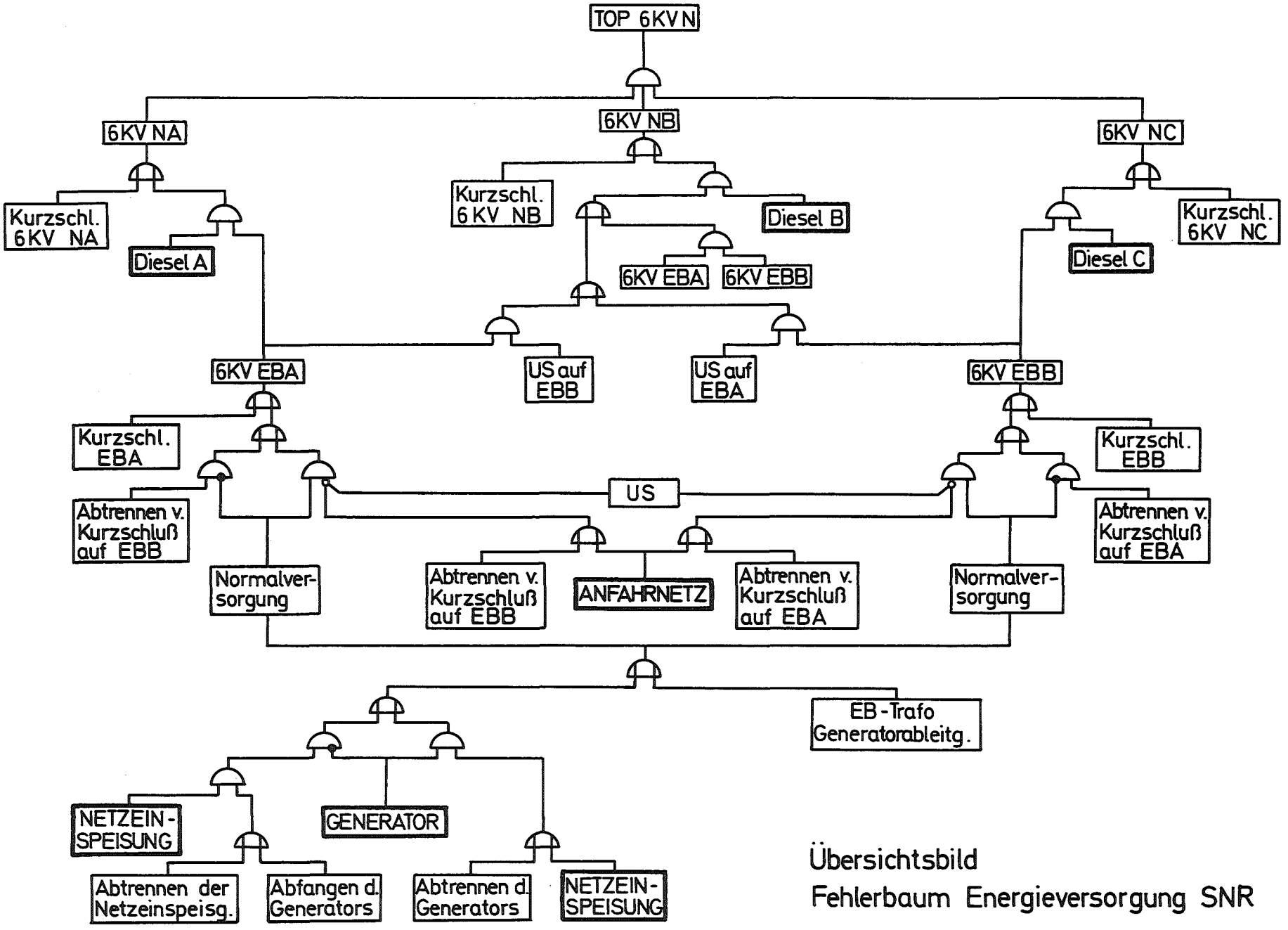


Referenzkonzept zur Energieversorgung des SNR 300 (ohne Anfahrnetz), Konzept 1



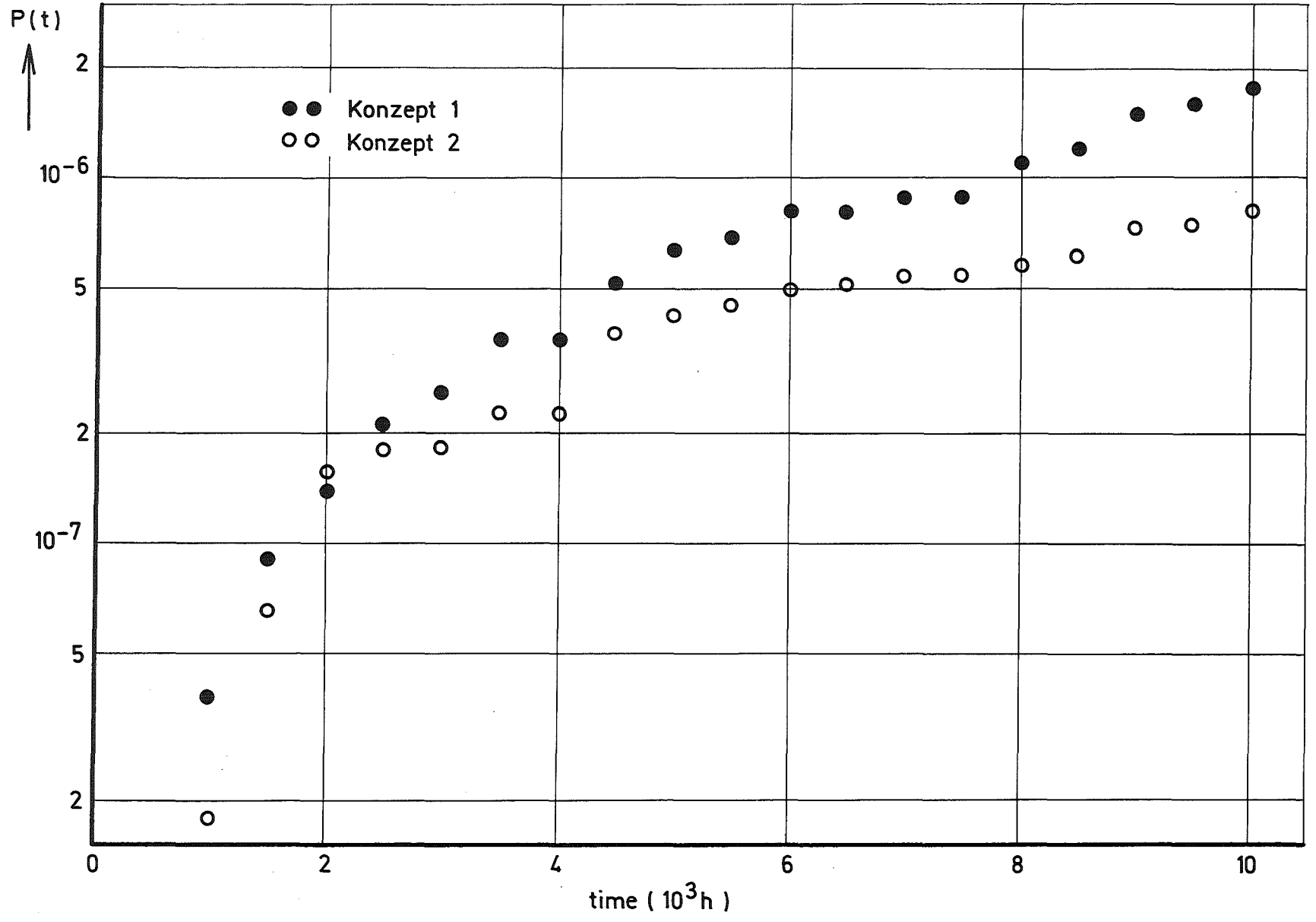
Alternativkonzept zur Energieversorgung des SNR 300 (mit Anfahrnetz), Konzept 2

Abb. 3

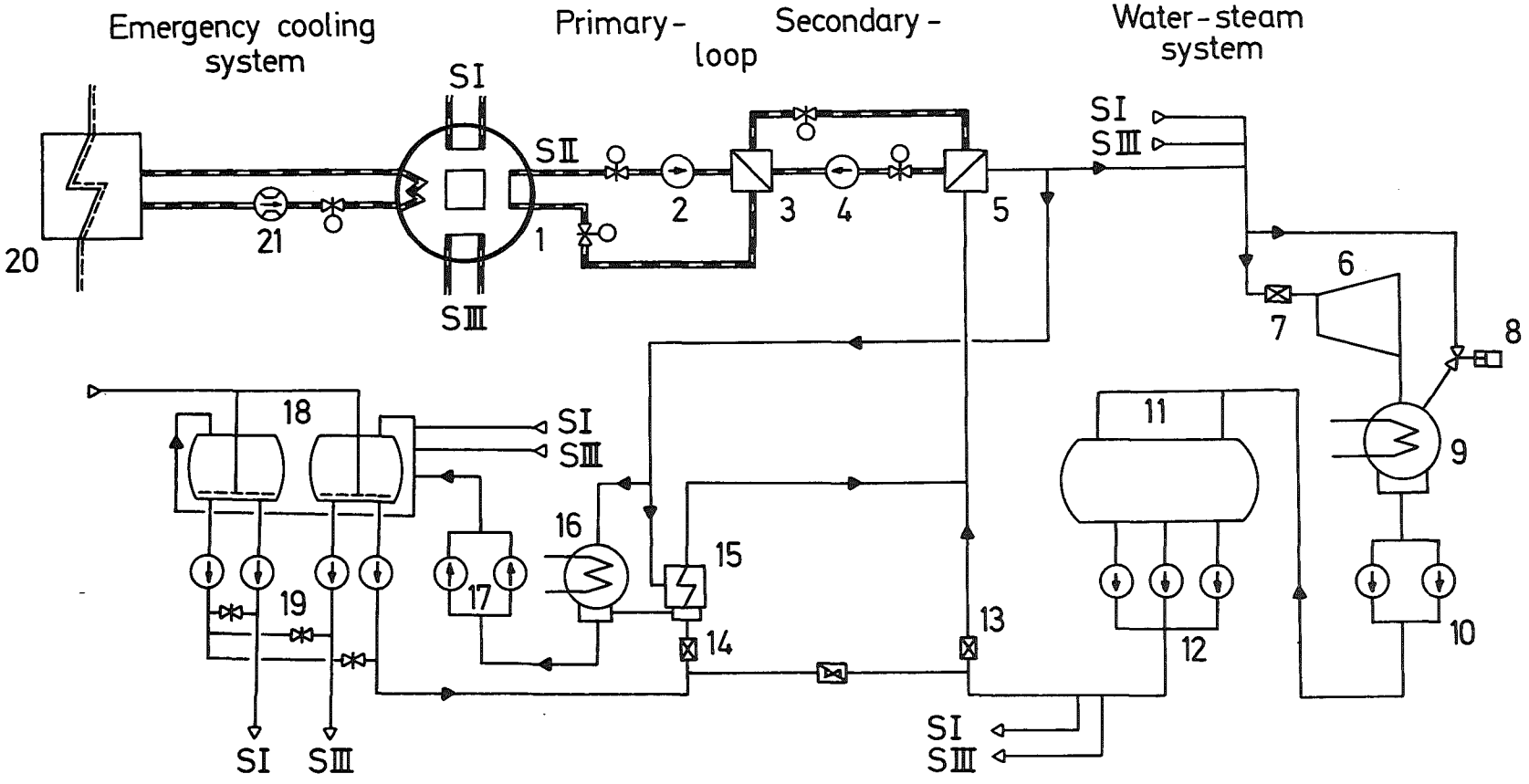


Übersichtsbild
Fehlerbaum Energieversorgung SNR

Abb. 4



Kumulative Ausfallwahrscheinlichkeit der 6KV - Notstromverteilung SNR 300

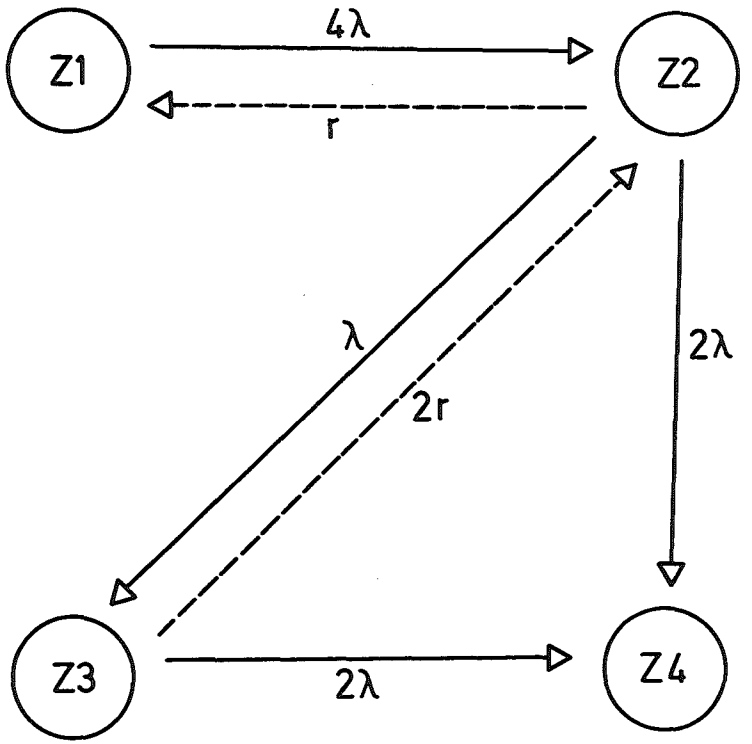


Legend

1 Reactor
2 Primary pump (sodium)
3 Intermediate heat exchanger
4 Secondary pump (sodium)
5 Steam generator
6 Turbine
7 Turbine valve
8 Pressure reduction station
9 Main condenser
10 Main condensate pumps
11 Feedwater tank
12 Main feedwater pumps
13 Feedwater controlling valve
14 Feedwater contr. valve (low load)
15 Feedwater preheater
16 Decay heat condenser
17 Decay heat condensate pumps
18 Hot water tank
19 Emergency feed pumps
20 Air cooler
21 EM - pump

SNR DECAY HEAT REMOVAL

Abb.6



Z1 alle Pumpen intakt

Z2 eine Pumpe ausgefallen

Z3 zwei Pumpen in einer Kühlkreiskette ausgefallen

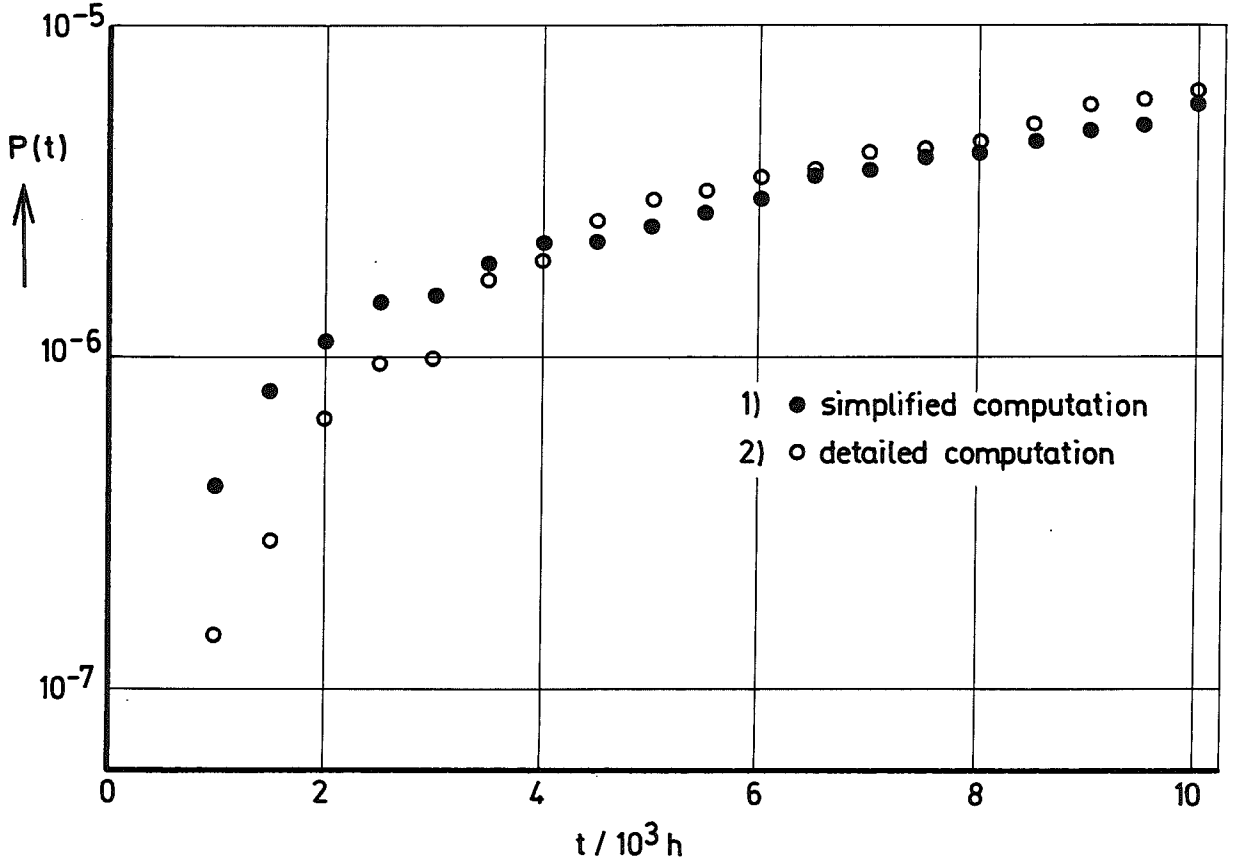
Z4 mindestens eine Pumpe in jeder Kühlkreiskette ausgefallen

$P(1) \approx g_{g^2 r t}$ mit $g = \frac{\lambda}{r} \ll 1$

und $MTTR_{System} \ll t$

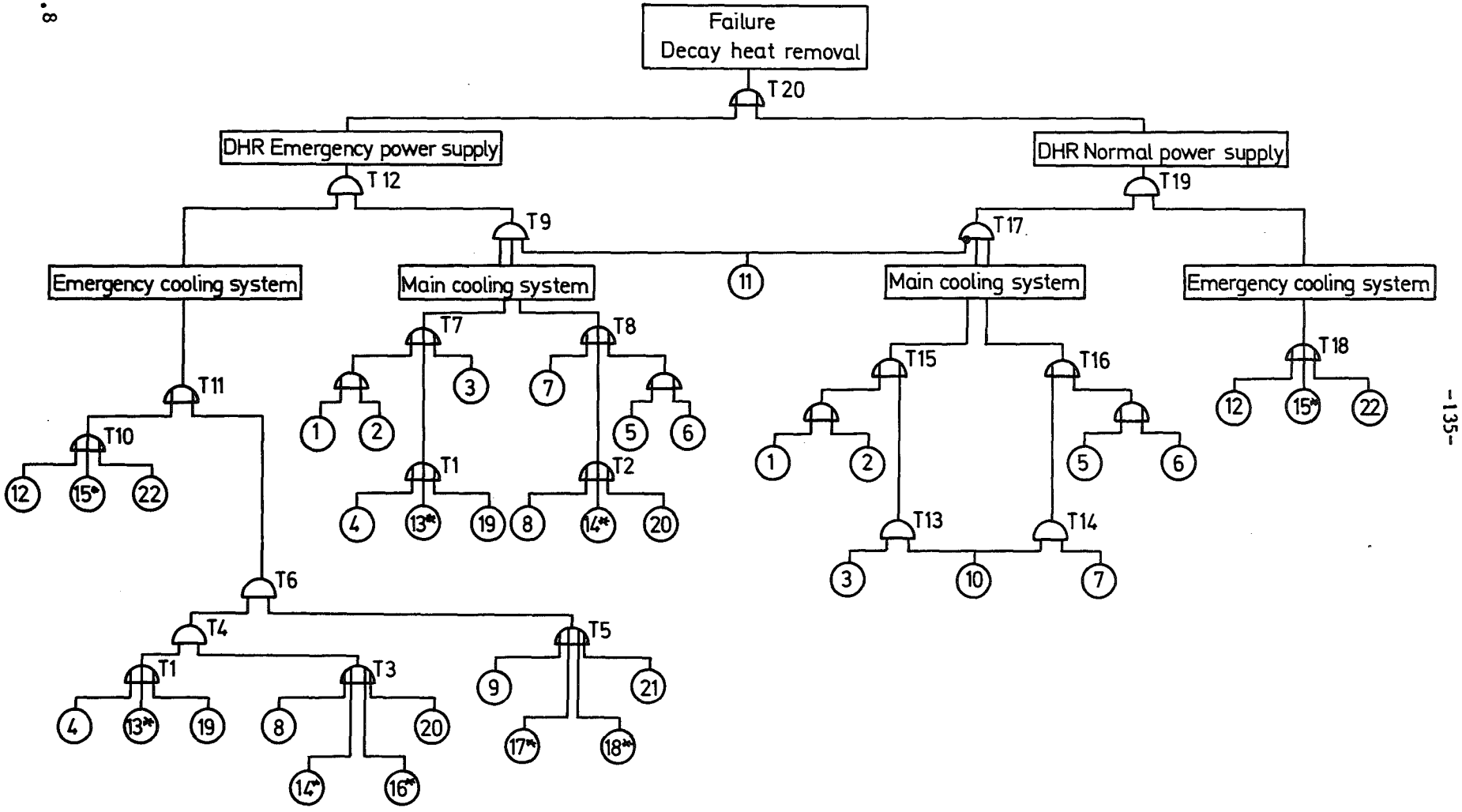
Zustandsanalyse zu den Na - Pumpensystemen

Abb. 7



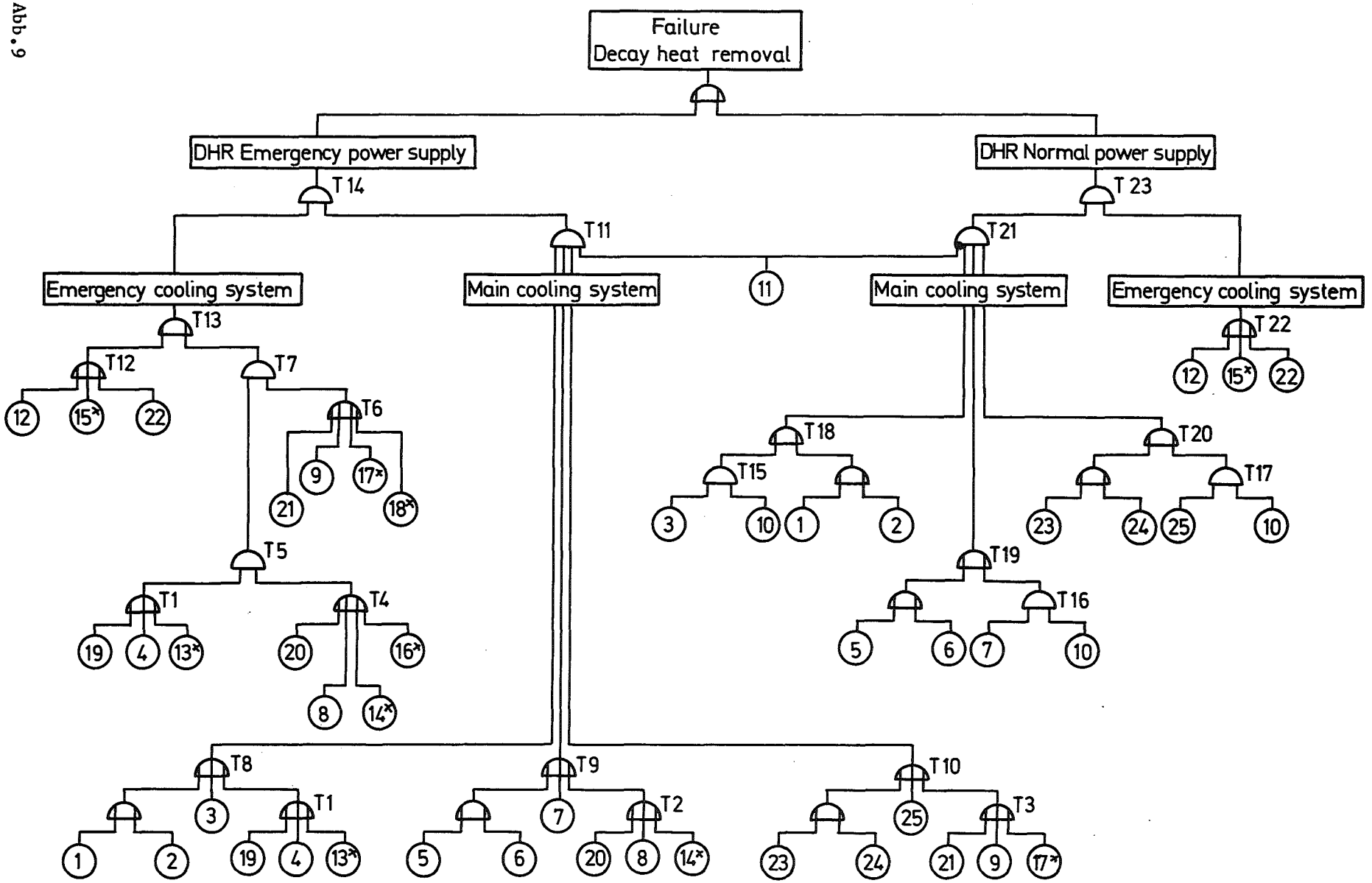
Failure probability power supply after scram

Abb. 8



Decay heat removal fault tree (two loops)

Abb. 9



Decay heat removal fault tree (three loops)

Tabelle 3

List of Components and Failure Data

No	Component	MTTF/10^6h	MTTR/h
1	Pump 1, Primary System	0.5	100
2	Pump 1, Secondary System	0.5	100
3	Water-Steam System 1	0.05	100
4	Diesel Supply 1, stand-by	0.06	400
5	Pump 2, Primary System	0.5	100
6	Pump 2, Secondary System	0.5	100
7	Water-Steam System 2	0.05	100
8	Diesel Supply 2, stand-by	0.06	400
9	Diesel Supply 3, stand-by	0.06	400
10	Water-Steam System, general	0.05	100
11	Power Supply Grid	0.05	30
12	Emergency Cooling System, stand-by	0.1	1 000
13+	Diesel 1, demand	10^{-2}	40
14+	Diesel 2, demand	10^{-2}	40
15+	Emergency Cooling System, demand	10^{-2}	10 000
16+	Change-Over demand, from diesel 1 to diesel 2 for Emergency Cooling System	10^{-2}	40
17+	Diesel 3, demand	10^{-2}	40
18+	Change-Over demand, from diesel 2 to diesel 3 for Emergency Cooling System	10^{-1}	100
19	Diesel Supply 1, Operating	0.0077	200
20	Diesel Supply 2, Operating	0.0077	200
21	Diesel Supply 3, Operating	0.0077	200
22	Emergency Cooling System, Operating	0.01	10 000
23	Pump 3, Primary System	0.5	100
24	Pump 3, Secondary System	0.5	100
25	Water-Steam System 3	0.05	100

The index + of the numbers 13 to 18 indicates, that these components do not have a "Mean Time to Failure" (MTTF) but a failure probability at demand.

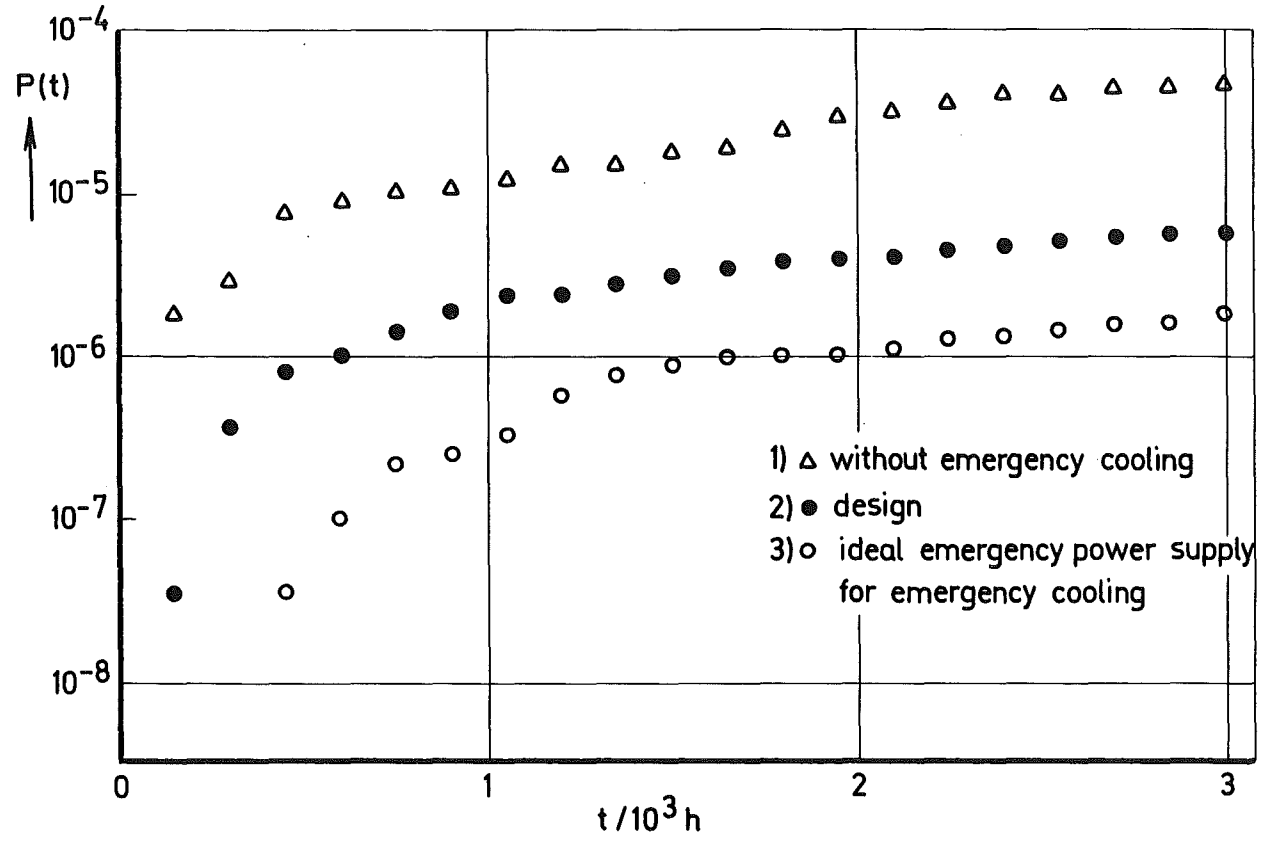


Abb. 10 Failure probability two loops DHR

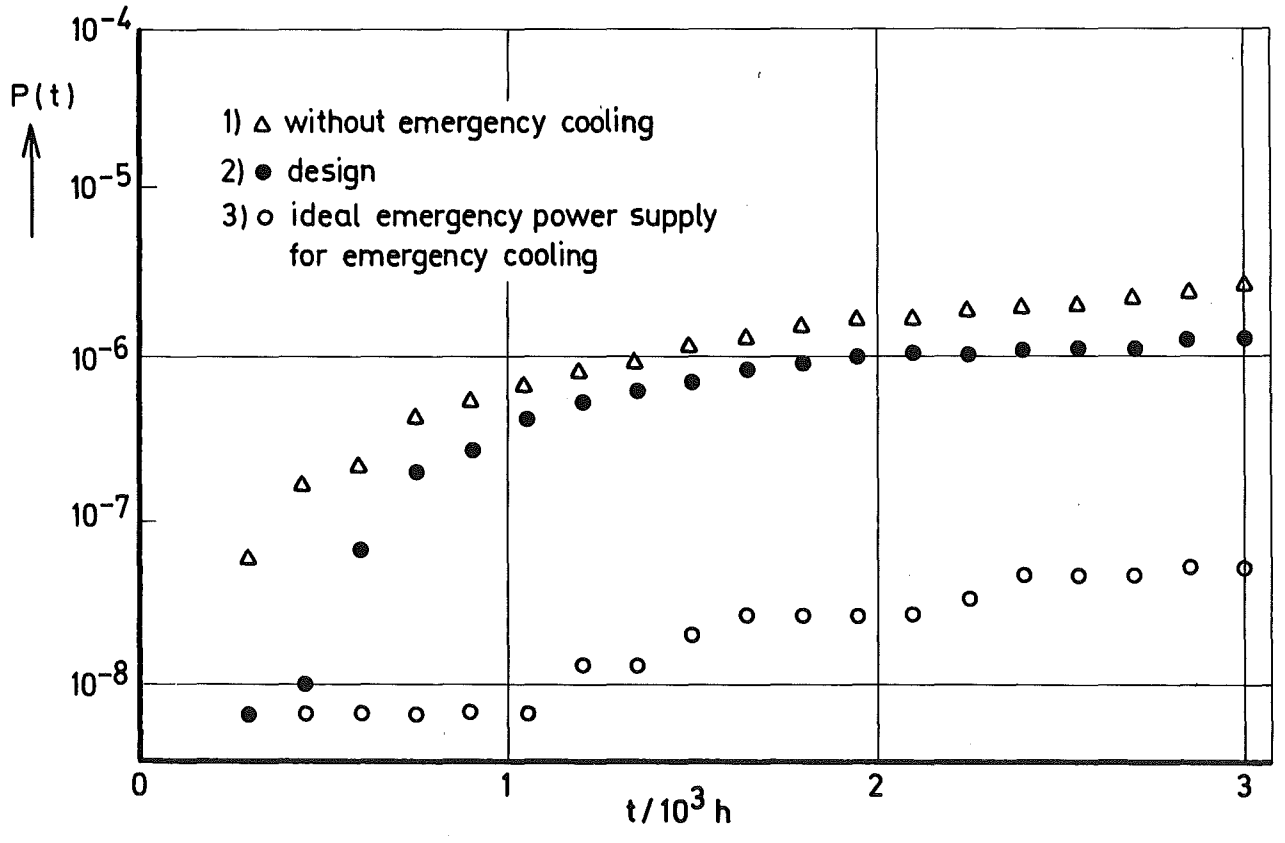
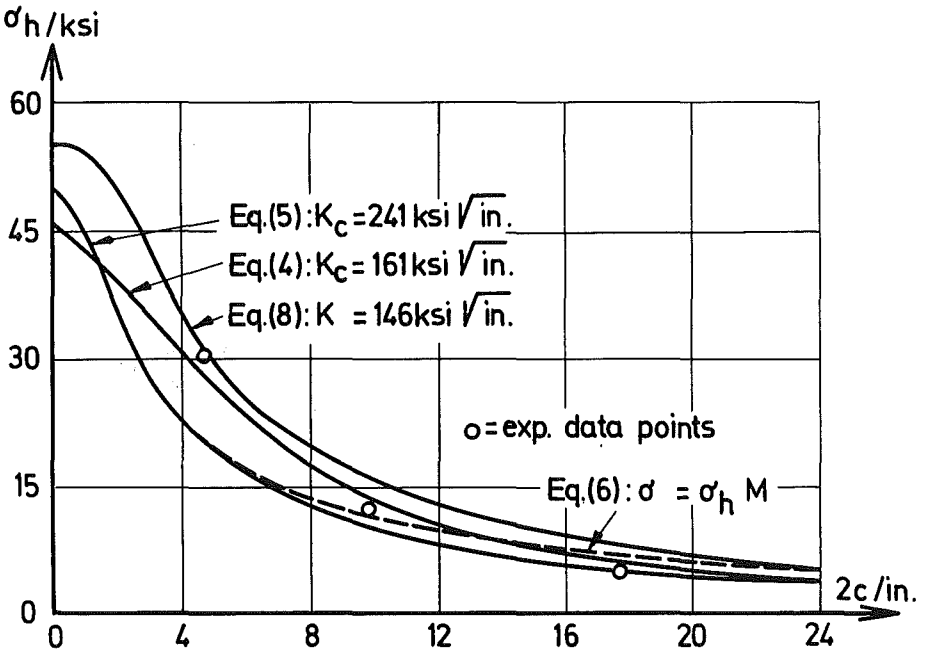


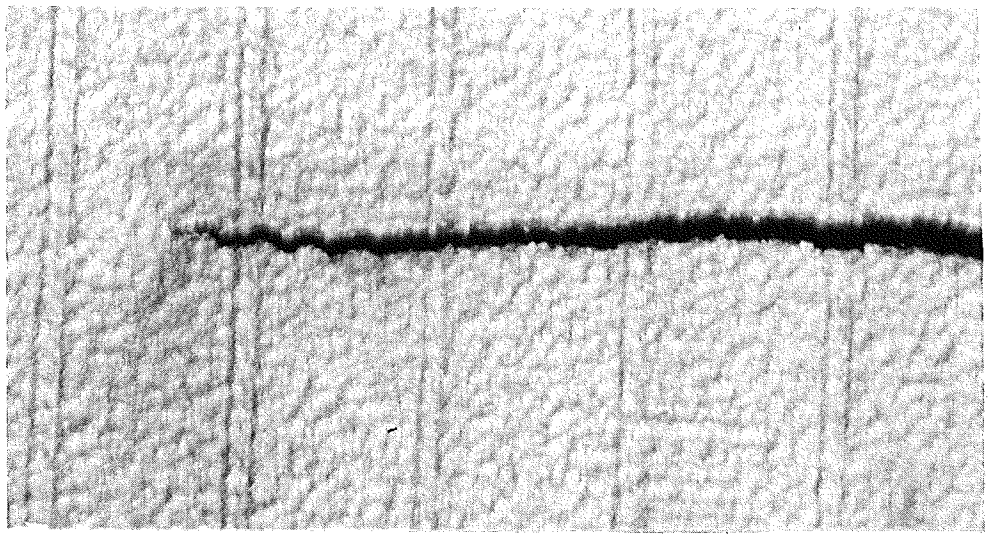
Abb. 11 Failure probability three loops DHR



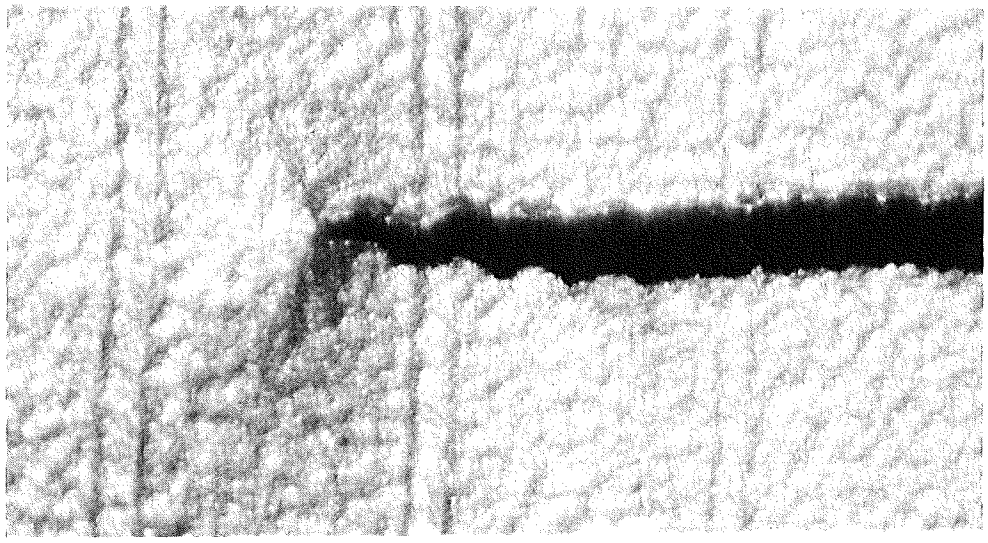
Failure stress curves and experimental data on 10 Cr Mo Ni Nb 910 steel pipes

Abb. 12

a



b



c

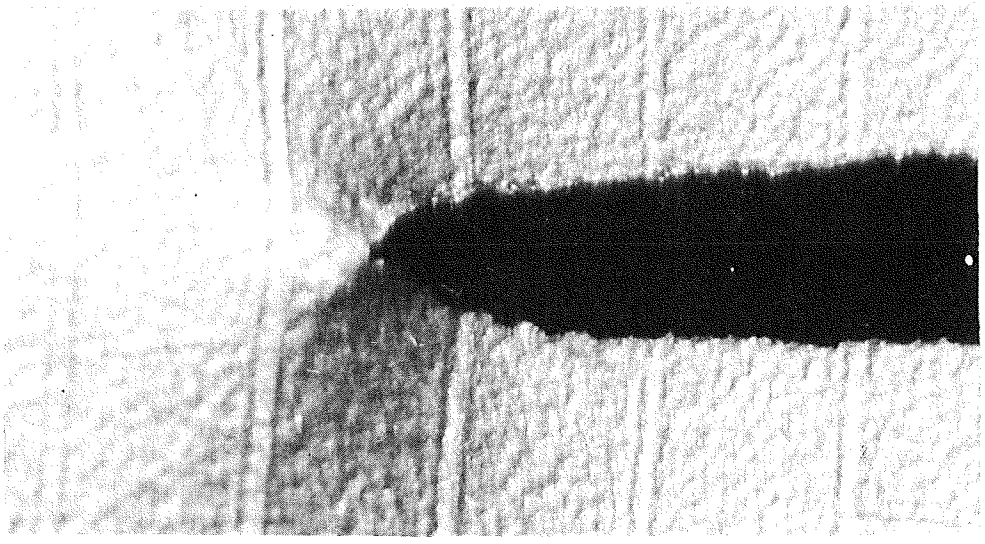
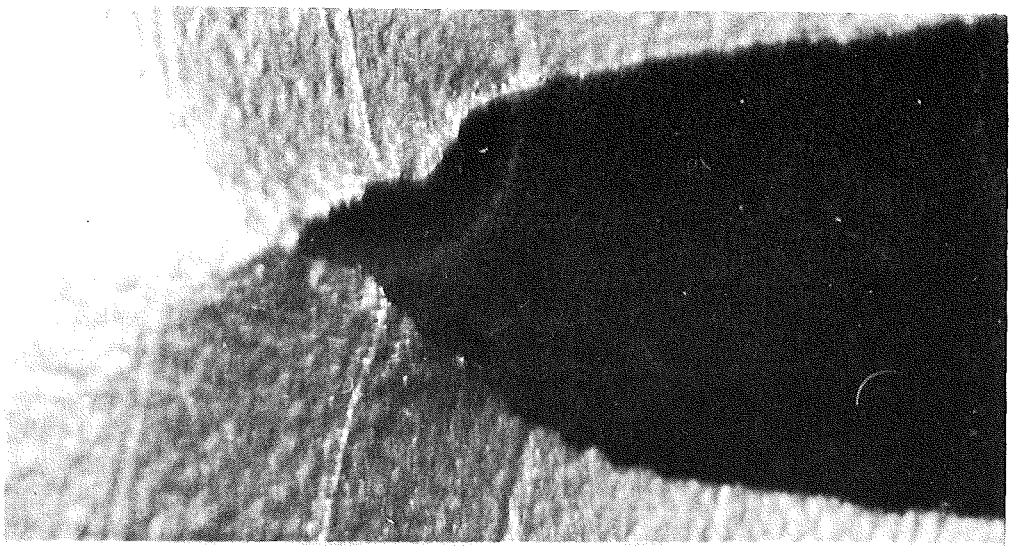


Abb. 13: (Abstand der Markierungsstriche 1 mm)

d



e

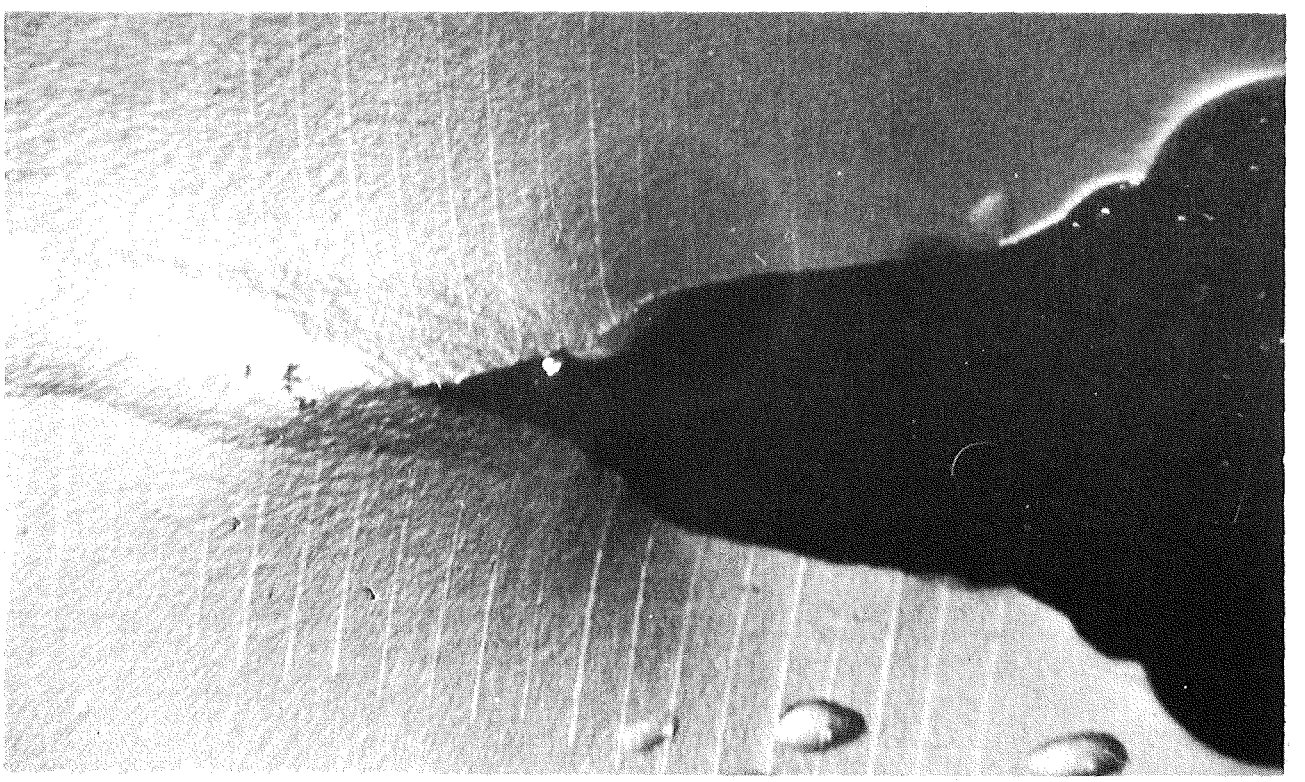


Abb. 13

Kapitel 4 : Cost-Benefit-Risk-Assessment for a number of Technological Systems

H. J. Otway

Literaturverzeichnis

COST BENEFIT ASSESSMENT

by

Harry J. Otway

Thank you very much for the invitation to participate in your seminar to-day. Professor Häfele has asked me to summarise some of my own work on the subject of applying cost (or risk) -benefit concepts to nuclear power plant and reactor assessment. I will also review some of Starr's work on the risks from fossil-fueled power plants. I would like to apologise in advance for spending so much time on my own work; others have done very good work on these problems but I will concentrate on my own material because it is more familiar to me.

The material to be covered here breaks into five broad subject areas: (I) a brief discussion of some cost-benefit concepts, (II) a sample risk assessment for a nuclear reactor, (III) a summary of Starr's work comparing the impacts of fossil-fueled and nuclear power plants, (IV) some material on assessing the relative importance of some social values, and (V) comments on the validity of some of my earlier work and speculation as to how future work might proceed.

This paper summarises the work of several other papers and, therefore, it has been necessary to be rather brief. Those wishing more details are referred to the original references.

I. SOME COST-BENEFIT CONCEPTS

In many of the routine activities of life there exists the possibility of sudden death or injury, yet we continue to participate in these activities. The reason, of course, is that the participant derives some benefit that, to him, outweighs the risk involved. A

common example might be automobile travel. In the U.S., more than 55,000 people are killed annually in automobile accidents, more than two million are injured, and the automobile is a major contributor to atmospheric pollution and resource consumption. Yet we continue to drive, because, as a society, we have subjectively and collectively decided that the benefits of personal transportation outweigh these well-known risks.

There are many examples of how we make, usually subconsciously, risk-benefit trade-offs in our private lives. A simple example might be that of a man living in the city who decides, partly because of the rising crime rate, that life in the city is no longer "safe". He may then decide to move his family to the suburbs where life is "safer" and then accept an additional risk of death or injury by commuting to the city. He has decided subjectively that, on balance, the risk of being harmed due to urban crime is more than the risk of being harmed due to his additional freeway exposure. Of course, there are many other, even more subjective factors, which are even harder to measure. He may personally prefer injury in an automobile accident to injury by mugging. The cleaner air in the suburbs represents a lessening in health risk as well as an aesthetic benefit. Our cultural system also would place value upon the protection of his family even at his own increased risk. However, the point is that a risk-benefit evaluation, however informal, has been made. It is also important to note that this cost-benefit judgment has been almost entirely intuitive rather than quantitative in nature. When speaking of social group decisions as opposed to individual decisions, this intuitive approach is no longer adequate. Quantification, where possible, often allows us to eliminate some of the variables involved which simplifies the decision-making process.

Figure 1 shows a crude, and somewhat arbitrary, approximation of the procedures involved in making a cost-benefit quantification. The first step shown is that of enumerating the positive (benefits) and

negative (cost/risks) aspects of the proposed process. For a nuclear power plant the negative aspects might include nuclear effluents, both routine and accidental, the discharge of hot water and an aesthetic or psychic detriment. Some efforts have been made to assess the risks from routine reactor effluents and from accidental releases, as a function of probability, from reactors. These will be discussed later in this paper. The primary beneficial aspect would be the power produced. The next consideration would be determining the distribution through the ecosphere in terms of space, time and biological species. Here we would also consider the distribution of the benefits in terms of population, space, and time.

Next, one must estimate the integrated effects of the risk and benefits. Risk examples here might be the radiation doses to humans and the effects of thermal effluents upon aquatic life. On the benefit side, one must consider the net effect of additional supplies of electricity, and the possibility of increased soil productivity through warm water irrigation. Increased electricity could be positive, in the case of life-lengthening in an underdeveloped country, or perhaps negative in supplying unnecessary labour-saving devices to an already under-exercised, power-rich people. The effects upon both the local and national economies must also be considered here. Quantification of negative effects would include, for human radiological exposure, the morbidity-mortality probabilities following exposure and the perceived effect of aesthetic detriment upon those affected. The upper limit of the dose-response relationship for irradiation of humans is reasonably well known. Some work has been done on estimating the carcinogenic effects of atmospheric pollutants through analogy with known carcinogens and through analysis of epidemiological data. There are still many uncertainties in these latter relationships.

Note that as the calculational process in Figure 1 moves from left to right, there is a continuous change in the disciplines required. The

design of the process is mostly a function of physical scientists and technologists while the determination of distribution and effects falls to biological scientists and economists. The estimation of aesthetic effects and, perhaps conversion of units, tends toward the behavioral sciences. A thorough analysis of a risk-benefit problem is truly an interdisciplinary effort and no one discipline can hope to cope with the whole process.

In addition to providing the input to decision making as shown in Figure 1, there is a second very important function served by the analysis. There has been much discussion of involving the public in decisions affecting the environment. There have been suggestions that the "public" might participate in hearings held specifically for this purpose. This concept is useful however, only if this "public" can make informed input or criticism. Most members of the public, including scientists, are not able to understand the consequences of, say, 1 man-rem radiation dose or 10 ppm of SO_2 in the air. The benefit-cost quantification and conversion of units in the last two steps in Figure 1 might help people understand the relative magnitude of the individual risks and may help to bring the perceived or "felt" risks more nearly in line with the actual risks. The fear of the unknown is a significant factor here and well done cost-benefit analysis could help move some of the unknowns toward the known.

II. A REACTOR RISK ESTIMATE

The work summarised here [1] is an estimate of the public risk, due to accidental release of fission products from the Omega West Reactor (OWR), an 8 MW(th) tank-type research reactor operated by the Los Alamos Scientific Laboratory at Los Alamos, New Nexico, U.S. A. The method used is a refinement and extension of earlier work estimating the public risk from a 1000 MW nuclear power plant.[2]

The risk estimate for the OWR was performed to support an application

for an increase in operating power from 5 to 8 MW (th). There is no evidence that this analysis had any bearing whatever upon the outcome of this application

Risk, as used here, is the probability of an individual meeting a given fate from a particular cause. Specifically, it would be the probability of death from a reactor accident and would include the probability of the accident occuring, the probability of radioactive material being carried to one's location, and the probability of dying after receiving the radiation dose. The specific risks considered here are the somatic risk of death (both early and late) from thyroid carcinoma (iodine isotopes) and neoplastic diseases due to whole-body irradiation, the genetic risk, and non-specific life-shortening risk. The individual risk, as a function of distance and direction from the reactor, was estimated as well as the total detriment to the community from operation of the reactor.

THE METHOD

It is difficult to identify each possible accident in an analysis such as this. There may be combinations of system failures that do not enter the thinking of the people doing the analysis; there may be unexpected interactions within or between systems such as common mode failures. The problem is to find a relationship between accident consequence and accident probability to be used as a source term in an estimate of risk. Our approach in this case was to take a sample of the complete accident population and to use this sample as a basis for establishing a probability density function of fission product release for the reactor. In this case the complete accident population consists of all accidents, in all combinations of systems or component failure, which could result in an external release of fission products. Our sample of this population consisted of all of the accidents which we could imagine that might lead to an external fission product release. This sample is inherently limited by the facilities of the human imagination and cannot, of course, result in a statistically random sample

since those potential accidents that we cannot imagine, as well as those involving significant common mode interaction, are unavailable to be sampled. However, this sample, while not random, is also not intentionally biased, so we are approximating a random sample of all possible accidents by a sample based on recognizable accidents. We feel this assumption is not unreasonable because there is a great effort to bias against common mode failures through careful design.

Many of the failure rates used in this analysis, especially for emergency systems, were calculated based on OWR test data or operating history. The effect of certain types of common mode interactions is included in these data. These data were collected over a period of years on the actual systems so that any designed-in common mode interactions within a system or between systems are included in the data and, consequently, in the statistical estimates of failure rates. Of course, these data do not include common mode interactions which might appear only under accident conditions, such as damage due to flying missiles generated during the accident or accident generation temperature or humidity conditions.

We have further attempted to make some allowance for common mode failures within systems by using conservative values for system failure rates. For example, when failure rates based on test data or operating history were used, the 90% confidence value for the system failure rate in question was employed in calculating the nominal probabilities of specific accidents. If no failure was noted, the 99.9% confidence value for system failure rates was used for the 90% confidence level calculations of specific accident probabilities. For this analysis, all emergency system failure rates were calculated based on actual data from the OWR.

The results of a more formal calculation of common mode interactions between primary and emergency systems are mentioned later. These results did not differ greatly from those where these interactions were not included.

RISK

THE CONCEPT OF RISK

We can try to gain an appreciation for numerical values of risk by considering the values of some risks that are commonly accepted. Because the reactor risk discussed here is that due to accidents, comparison with other accident risks is helpful. Table I shows selected U.S. accident figures from 1966. People are not equally exposed to all these hazards and, indeed, some are not exposed to some hazards at all, but many of these accidents are common in society, so the risks they provide are representative of the "average" risk to the "average" person. These statistics may also be indicative of how we form our subjective feelings about certain hazards. If an accident is improbable, as shown in Table I, it is typically less known, and the chance of the "average" person knowing of someone suffering this particular fate is also small

Fatal accidents providing hazards on the order of 10^{-3} per person/year are uncommon. When a risk approaches this level, immediate action is taken to reduce the hazard. This level of risk appears unacceptable to everyone.

At an accident level of 10^{-4} per person/year, people spend money, especially public money, to control the cause. Money is spent for traffic signs and control, and police and fire departments are maintained with public funds. Safety slogans popularized for accidents in this category show an element of fear, e.g., "The life you save may be your own".

Mortality risks at the level of 10^{-5} per person/year are still considered by society. Mothers warn their children about most of these hazards (playing with fire, drowning, firearms, poisons), and some people accept a degree of inconvenience, such as not travelling by air, to avoid them. Safety slogans for these risks have a precautionary ring "Never swim alone", "Never point a gun at another person", "Keep medicines out of children's reach".

Accidents with a probability of about 10^{-6} per person/year are not of great concern to the average person. He may be aware of them, but he feels they will never happen to him. Phrases associated with these occurrences have an element of resignation: "Lightning never strikes twice....", "An act of God".

The intent of this discussion is to point out that there is a general lack of concern about accidents having averaged mortality risks of 10^{-6}/year. This will provide a numerical comparison for evaluation of the results of the OWR risk analysis.

The Risks Considered

We have conservatively assumed that the consequences of irradiation are linear with dose, that there are no threshold or rate effects, and that there is no repair of radiation damage. We do not suggest that these conditions represent reality - only that they provide an upper limit of risk. It appears that threshold, rate, and repair effects do exist and make the actual risks lower than those suggested here. Numerical values of the probability of death per unit dose and the sources of these estimates follow.

Whole Body Somatic Risk. The risks included in whole body somatic risk are death from leukemia and from carcinomas other than of the thyroid. For doses up to 150 rad, a linear relationship of 30×10^{-6} per person/rad has been used as the probability of death from each of these.[3] For higher doses, the response would be based on the acute effects of radiation.

Thyroid Carcinoma. Assuming that the product of morbidity and mortality is roughly constant for all ages, the chance of death from internal ^{131}I irradiation of the thyroid has been taken as 1×10^{-6} per person/rad.[3]

Nonspecific Life Shortening. After radiation exposure of animal populations, increased mortality is noted, which is not associated any single disease but seems as though the animals had undergone accelerated physiological aging. An estimated 7% lifespan reduction per 100 rad is used here as an approximate upper limit of risk. This may also be expressed as a mortality probability of 700×10^{-6} per person/rad.[4]

Genetic Risk. In predicting genetic risk, the term "genetic death" is used. A genetic death may be defined as the eventual extinction of a gene lineage. This might occur through the reduced fertility or sterility of someone carrying the gene or through stillbirth, abortion, or early embryonic or prereproductive death. The term is somewhat misleading in that a genetic death may not represent a somatic death; a genetic death (sterility, for example) may not have an associated corpse. Therefore, calculation of radiation-induced mutation frequency is meaningful only in comparison with the natural rate of mutation. The natural genetic death rate, based on normal mutation rates and genetic equilibrium, may be estimated as 200 000 x 10^{-6} per person/generation.[4] We have chosen 7200 x 10^{-6} genetic deaths/rad as a conservative value for radiation-induced mutations. About 2.5% of this would be expected in the first generation.

RESULTS

This section outlines the results of applying the method described to the Omega West Reactor.

Determination of the Accident Envelope

The accident envelope (Fig.2) may be generated by assessing the probability of a primary system failing in conjunction with the failure of any combination of other systems during the time interval (before or after the primary system failure) in which they would be needed. The fission-product release value for the assumed accident situation constitutes one point in the accident envelope. This procedure may be repeated for different combinations of system failures to produce additional points and does not restrict one to consideration of spontaneous failure of a primary system as the initiating event. For example, loss of electrical power or an operator error might conceivably initiate failure of the reactor cooling system. One must then assess

the probability that power failure or operator error will cause failure of the cooling system in the manner postulated, then use this probability to generate a point in the accident envelope.

Fission Product Release vs Probability

The source term for this risk assessment is the probability density function of fission-product release formed from the release-probability envelope shown in Fig. 1 using a nonlinear least squares computer programme. The equation of this density function is

$$f(X) = \frac{1}{\sqrt{2\pi} \times \sigma} \exp-[(\ln X - \mu)/\sigma]^2$$

where, for this fit,

μ = -5.93

σ = 2.64

The accidents considered and the failure rates used for some systems and components are found in Ref. 1. The fission-product releases shown in Fig. 2 are in terms of curies of ^{131}I released. However, in performing the dispersion and dose calculations, account is taken of all iodine isotopes and other fission products released in each accident.

There are five general sources of system and component reliability data

1) component reliability measurements
2) reactor operating history
3) specific systems tests
4) largely intuitive assessment of reliability
5) calculated reliabilities (e.g. fault tree).

We have used all these, although 4 and 5 overlap somewhat. The statistical treatment used to obtain confidence levels and failure probabilities from OWR operating history and test data is summarized in the next section.

Risk vs Distance and Direction

A sample risk vs distance result for Pasquill F weather (down-canyon wind) is shown in Fig. 3. This is one of a group of curves that results from the calculations described earlier, that is, before the probability of occurrence of the various Pasquill conditions has been included.

Local meteorology is important in considering the OWR which is located in the bottom of a long, narrow canyon. The local meteorology enters in as a series of weighting probabilities applied to the curves represented by Fig. 3 to obtain Fig. 4 which shows lines of constant somatic mortality risk (thyroid carcinoma, leukemia, and other carcinomas) superimposed on a schematic plan of Los Alamos. The warehouse immediately northwest of OWR is the nearest uncontrolled structure. The highest individual somatic risk to the population is about 5×10^{-10}/year which, relative to the values discussed earlier, is negligible. The risk added by the OWR would increase the chance of accidental death for an "average" person with "average" accident exposure by 0.0001%. Based on "typical" values of hazard pay a person exposed to the somatic risk of 5×10^{-10}/year would be entitled to receive about $0.01 per hundred years of compensation. The nonspecific life shortening at the point of highest individual risk may be expressed as 25 sec/year of continuous exposure.

The Total Risk

The total risk, based on a 30-year reactor lifetime can be expressed as a detriment over all generations of 1.4×10^{-2} death. This figure is

conservative because it also contains genetic deaths and the equivalent of nonspecific life shortening. The total risks (30-year reactor operation) are compared to some other common risks in Table II.

Based on 30 years of reactor operation, the total risk figure in this table could also be expressed as about 4.5×10^{-4} death per year. For comparison, a community this size (~13 000 excluding suburban areas remote from the OWR) would have about 2600 natural genetic deaths per generation, assuming natural mutation rates and genetic equilibrium. On the basis of national accident statistics, one would expect about 270 accidental deaths in the community in a 30-year period.

ESTIMATION OF FAILURE RATES

After identifying the largest possible sample of accidents, the main problem encountered is in determining a failure rate for each component or system involved in these postulated accidents. The least rigorous method of estimating failure rates is for someone familiar with the system, or similar systems, to make an estimate based on his experience and judgement. When forced to use this source one must use a pessimistic estimate so that, if bias were introduced, it would be toward a higher risk.

A better method of estimation is to search the literature for experimentally determined failure rates for the components of interest. Two problems encountered in this type of estimation are (a) that the component may be similar but not identical to the component of interest, and (b) that the failure rate may have been determined in an environment different from that in which the component operates.

A more mathematically pleasing method for estimating failure rates is to use data from the operating history of the reactor or similar type reactors. This has the desirable property of estimating the failure rates of the hardware in its working environment, although

admittedly not an accident environment. Another advantage is that designed-in common mode interactions within a system, or between different systems, are included in the data that have been collected. These data do not, of course, include common mode interactions that would be apparent only under accident conditions (such as flying missiles, for example) but common mode failures which result from design inadequacies would result in higher calculated failure rates. This method can be used if we assume that the failures are distributed as a Poisson process with gamma-distributed waiting times to failure and exponentially distributed interarrival times. These assumptions are valid if it can be assumed that maintenance and repair result in negligible wear-out effect.

The degree of accuracy obtained in estimating a failure rate is directly related to the amount of operating data available. If a component doesn't fail in 15 years, there is some difficulty encountered in estimating its failure rate. However, it seems reasonable to assume that its failure rate is less than that for a component that failed once in 15 years. Using the above concept and the distribution theory assumed previously, one is able to put an upper confidence limit on a component that has no observed failures in an observation time T. The lower 1- confidence interval on the population failure rate given as a probability statement is

$$P\left[\ 0 \leq v \leq \frac{X^2_{1-\alpha}\ (2n+2)}{2T}\ \right] = 1 - \alpha,$$

where

α = probability that an observation from the hypothesized population will randomly occur outside the confidence interval

n = number of failures observed in time interval T

$X^2_{1-\alpha}\ (2n+2)$ = $1 - \alpha$ percentile of a chi-square distribution with $2n + 2$ deg of freedom

v = population value of the failure rate per year.

Sample calculations, a discussion of failure rates, and an estimate of common-mode failure effects may be found in Ref.1.

CONCLUSIONS

The basic conclusion of this study was that the indefinite operation of the OWR at a power level of 8 MW(th) presents no undue risk to the community in which it is sited.

An interesting development was that the source term for the OWR analysis, the probability density function of release formed from the envelope of Fig. 2, was almost identical with that found for the 1000 MWe PWR analysed in Ref.2. Two inferences could be made from this. One is that the accident source terms for most thermal reactors as presently designed and sited might be quite similar. Another is that this similarity may give a very crude measure of the effectiveness of some of the PWR safeguards. Namely, the PWR containment and atmospheric cooling and spray systems may account for an effective power reduction from 3200 to 8 MW(th), a factor of 400. This statement must be viewed cautiously because there are many other basic differences in design between a PWR and a tank-type research reactor. For a given design, this approach might enable evaluation of specific safeguard systems in terms of equivalent power reduction. Of course, we had only compared two reactors so this apparent source term similarity might also be pure coincidence. However, a more recent probabilistic analysis of a fast breeder reactor, done at Atomic International Inc.,* also produced the same source term. It is still difficult to say if this could be meaningful or not. But it does seem reasonable that different reactor types, designed to meet the same regulatory requirements, could present about the same public risk when viewed from a probabilistic standpoint.

---

* Private communication. Chancey Starr.

III A COMPARISON: NUCLEAR vs OIL FIRED PLANTS

This section will briefly summarise the work of Starr, et al[5] which draws a comparison between the public health risks from nuclear and oil-fired power plants. Again, those interested in a more detailed treatment are referred to the original work.

Risks were estimated for both types of facility under conditions of continuous operation at existing U.S. federal regulatory limits, and for accidents. The risks considered were primarily the risks of somatic death from radiation in the case of the nuclear plant or from inhalation of SO_2 and particulates for the oil-fired plant.

Pollutants and Effects

Figure 5 shows U.S. federal regulatory limits for exposure to radiation, SO_2 and NO_2 along with the thresholds for medically percievable effects and natural background levels. Figure 6 shows a relationship between SO_2 (with particulates) concentration, time of exposure and morbidity-mortality in man and animals. This figure provided a basis for estimating the probability of death, due primarily to respiratory complications, from exposure to SO_2. The effects of other oil-fired plant effluents such as NO_2, hydrocarbons, CO, heavy metals, radon, etc. were not considered for this study (and are not very well known) - causing an under-estimate in risk. Data for morbidity-mortality due to radiation exposures were taken from Ref. 3.

Risks From Steady-State Effluents

For a basin containing a fixed volume of air, a calculation was made to determine how many 1000 MWe power plants of each type would be required to cause atmospheric pollution to reach allowable concentration limits. Meteorological factors and removal factors were neglected in all cases and the contaminants compared were SO_2, NO_2 and radioactivity. Table III summarises results of this comparison, which indicate that on this basis

far more nuclear plants could be operated. Note that this calculation only compares operation at allowable air quality levels so is therefore only meaningful if all other factors are equal and health effects are similarly proportional to federal standards. Figure 4 shows that the health effects of radiation at federal limits are considerably less than those of SO_2 or NO_2 at their corresponding limits.

If the effects of large scale accidents are weighted by their respective probabilities the public impacts of episodic releases may be compared. For a 100 MWe nuclear power plant the source term relationship between fission product release and accident probability was taken from Ref. 2. The corresponding relationship for fires in oil-storage facilities is shown in Fig. 7. These source-terms are compared on a common probability scale in Fig. 8. Morbidity-mortality relationships for radiation exposure were taken from Ref. 3 while the corresponding risk from SO_2 exposure, fitted to the curve of Fig. 5, was taken to be

$4 \times 10^{-5} \times (SPt)^{1/2}$ mortality risk (death due to respiratory cause only) per person exposed to S (ppm) of SO_2, P (gm/m^3) of particulate matter for t (years) down to 10^{-4} (ppm-(gm/m^3)-year) which is a routine urban exposure.

Based upon the same site and weather conditions the cumulative mortality risks as a function of distance from the plant are shown in Fig. 9. This indicates that, on an accidental release basis, the risk from the nuclear power plant is about a factor of 10 or so less than that from the oil-fired plant.

Summary

A comparison of the public risks for both types of plant for continuous and accidental exposures is shown in Table IV. In both cases the risks from accidents appear negligible when compared to risks from continuous operation at regulatory limits. In this latter case the nuclear plant risk is estimated to be about 1/60 of that from the oil-fired plant.

IV. SOCIAL VALUES

In the previous sections we have talked about the quantification of biological risk. This is a complex problem but is still a relatively straightforward procedure. In trying to do a more comprehensive cost-benefit calculation, such as that discussed in Section I, the question of assessing the relative importance of subjective values arises. This is a far more difficult problem, but still worthwhile attempting because, if conservative estimates of the magnitudes of some of these additional variables indicates they are small in comparison to others, they may then be eliminated from further consideration in the decision-making process.

Life Values

A classical problem in attempting any kind of cost-benefit analysis is that, for even a very simple problem, risk and benefit are not in consistent units. For example, risk may be expressed in units of death, injury or radiation exposure while benefits might be in monetary value. The comparison of results in these dissimilar units is a complex study in value judgement.

As a society, we place a far different value upon a statistically expected loss of life as opposed to a psecific identified life. For example, large sums of money are often spent to find a lost child or to rescue survivors of a mining disaster, shipwreck or aeroplane crash. However, we are far more casual about a statistically expected loss of life, such as the appropriation of funds to provide a traffic signal at a dangerous intersection where someone (unidentified as yet) is sure to be killed. This is true of many public safety measures where the future victims are anonymous.

In a situation where risks are involuntarily allocated to the public it is necessary that a relatively large segment of the population be affected by the proposed activity, and that the maximum risk assumed

by any population group or individual not be unduly large. In this way the risk-benefit distributions may be viewed statistically to attempt a maximisation of net societal benefit.

Many investigators have attempted to place actuarial values upon human life. Others have estimated monetary values per man-rad of radiation exposure. If we accept the premise that radiation exposure causes a certain risk then, in principle, a monetary value for radiation exposure implies a life-value also. Some of these values are compared in Table V. For comparison, they have all been converted to units of U.S. dollars per man-rad using a (upper-limit) conversion factor of 10^{-3} mortality probability per rad dose and ignoring any dose rate or threshold effects.

These figures could also have been converted into units of dollars per statistical life. The point is that for such a completely subjective assessment the values found are in reasonably good agreement and an upper-limit value for these difficult judgements could be found that allows at least a rough comparison of risks and benefits in the same units. For brevity references and details of the estimates are not given here but may be found in Ref. 6.

The Perception of Risk

Another important question is that of how various risks are perceived by people. This is very important because people react to any given risk by how great they <u>think</u> it is, not how great it <u>actually</u> is - partly because they usually have no idea of the actual magnitudes of various risks nor could they be expected to easily put them into proper perspective. This factor has played a decisive role in many of the controversies surrounding the public acceptance of various technologies - nuclear power being perhaps one case. An extreme example of the importance of perception may be seen in the hypochondriac,

physically well, who perceives his health as being so precarious that he is unable to function.

Studies have been made on the perceived threat from extreme geophysical events. In a survey of people in 496 urban locations[7] an approximate log-normal distribution was postulated to describe the perception of flood hazard. That is, persons living in locations of intermediate measured flood frequence had a higher relative perception of flood hazard than those of places experiencing either more frequent or less frequent flooding. This is not what one would expect when actual flood risk is considered.

Another area in which subjective factors can be very important is in the perception of physical illness. Wyler [8], through the use of survey techniques, has attempted to quantify the subjective aspects of illness from a gestalt point of view. For this survey, the concept of seriousness of illness included such factors as prognosis, duration, threat to life, etc.; but, more important, it also included the emotional and aesthetic factors which influence one's perception of how serious a particular illness is. In this study, a list of 126 disease items was shown to a sample of medical out-patients. They were then asked to rate these diseases in a quantitative manner using a given illness as a modulus item. The quantitative rankings given by out-patients to various diseases were also compared to the results of the same survey applied to a group of physicians, whose knowledge of disease might lead them to rank disease items in a different manner than the general public. The differences in ranking between the two groups, the general public out-patients and the group of physicians, turned out to be very small. The Spearman rank order correlation coefficient between the two groups was a highly significant 0.947. The geometric means of quantitative rankings of these disease items was used to form the Seriousness of Illness Rating Scale (SIRS). This survey was later tried with a second group of physicians to check reproducibility with excellent results; and as a further check, the cross-cultural consistency was estimated by

testing groups in Ireland and Spain again with resultant high correlation coefficients.

In asking the sample groups to rate illnesses, peptic ulcer was given an arbitrary value of 500 points. The respondants were asked to compare the seriousness of each of the remaining illnesses to that of peptic ulcer. That is, to rate the relative seriousness, using all their experience - direct and indirect, objective and subjective, - in arriving at an answer. It is important to note that this method of ranking definitely includes the emotional aesthetic and moral prejudices associated with various diseases. A sample of some of the diseases included in the SIRS and their mean ratings is shown in Table VI.

Note that the subjective impressions of various diseases have indeed been quantified. Syphilis, for example, which has high negative moral connotations in our society, but which is seldom fatal if treated promptly, was given slightly less than half the rating given cancer. Sexual inability, with an obvious emotional loading, was rated about half as serious as heart attack - although it is never fatal of itself. Such items as bad breath and dandruff may appear to be overvalued, even ridiculous, when compared to other disease items. However, if advertising is any indicator, the fear of bad breath and dandruff have generated a sizable industry involving large sums of money in many countries. The point here is that it appears that it is indeed possible to attach some quantitative significance to the emotional, moral and aesthetic factors attached by people to various ailments. These techniques have also been used to quantify the perceived importance of a number of life-change events which require some degree of individual social adaptation.[9]

The examples of the quantification of subjective values given here have little direct relationship to the use of risk-benefit principles for technology assessment or standard setting, but the techniques used could be applied in other fields. The problem of the quantification of aesthetic values for risk-benefit assessment does not

seem an insurmountable one. The use of appropriate survey techniques could help eliminate some of the difficulty in evaluating phrases such as "people just don't seem to like it". Indeed, even a semi-quantitative ranking of the public perception of various alternatives could be most helpful in decision making. A sample cost-benefit calculation (for a PNE project) which attempts to make monetary estimates of some of these subjective factors may be found in Ref. 10.

How Safe is Safe Enough

In addition to the methodology of making cost benefit assessments one must also consider the determination of exactly what cost-benefit relationships are acceptable to society. Starr [5] has suggested the relationship of Fig. 10 between the per capita benefits of a given system and mortality probability. He postulates that risks at a level below that presented by natural events such as lightning, earthquakes, etc. (about 10^{-6} per person per year) are acceptable without regard to the corresponding benefits. This is almost certainly true because below this level people are essentially unaware of the risk because it is so small.

For an upper limit of involuntarily exposure risks, the average death rate from disease in the U.S. population was suggested. While there certainly is some level above which risks are unacceptable to the social group, regardless of compensation, the average death rate for disease does not necessarily appear to be a "magic" criteria. The averaged U.S. death rate from disease of 10^{-2} per person per year turns out to be the exact death probability for a man around 55 years of age. It seems unlikely that people would be intuiively aware of this rate and base their acceptance or rejection of a given risk accordingly. It is clear, however, that above some risk level a large group will not willingly accept involuntary exposure even if the benefit is large. Between these two extremes a linear relationship is suggested with higher risk levels corresponding to increased benefits. There is no system which is "safe" in the absolute sense but the curve of Fig. 10 defines a

conservative and reasonable approach to determining goals for the acceptability of involuntary exposure to technological risks.*

There has been some discussion in the literature about the relationship between the acceptance of voluntary and involuntary risks. It seems clear that people will expose themselves to much higher risk than they will accept on an involuntary basis. Phychological experiments [11,12] have shown that people tend to be overconfident in predicting the outcome of events over which they can exert some control. These differences have been quantified to some extent. This is analogous to the apparent readiness to accept higher voluntary risks where the degree of participation can be controlled. On the other hand, evidence indicates that people tend to be underconfident when facing uncertainties of external origin [13]. This verifies the apparent over-estimation of vague risks of an environmental or technological nature which must be accepted involuntarily by the public. This is another example of one of the recurring problems in interdisciplary problems such as cost-benefit assessment - the unknowns in one discipline sometimes turn out to be well understood in another. The importance of an interdisciplary approach should not be underestimated.

V. MISCELLANEOUS COMMENTS

Some of the work discussed earlier especially that of Ref. 2 has received a fair amount of attention in the last year or so. I have been asked many times how I feel about it at this point in time. This work was done in 1968 and early 1969 and now, with the benefit of some four years hindsight, I see it somewhat differently myself.

To begin with, we live now in a quite different time. Many events which seemed incredible a few years ago are now commonplace.

---

* It is interesting to note that the life values represented by the curve of Fig. 10 are in the range of 10^7 to 10^8 dollars - the suggested dividing line therefore seems to provide a reasonable conservatism in comparison with the life-value estimates discussed earlier.

For example, last fall a senior-level U.S. Civil Servant robbed a bank and sky-jacked an aeroplane to Cuba. An extremist group threatened to crash a sky-jacked aeroplane in their control into a nuclear facility. These seemingly incredible events occurred in the same week. Indeed, the events of the 1972 Olympic Games still seem incredible. The point is that the question of sabotage, both external and internal, was not considered in the earlier work - and such events are likely of higher probability now than they were at the time this work was done. I don't know if this is significant in comparison with other risks but I'm sure it can no longer be discounted out-of-hand as "incredible". I also think that with an appropriate effort the magnitude of this risk could be estimated.

At the time of the original work the controversy about emergency core cooling systems had not yet started. In all probability the physics involved are not as mysterious as some people would have us believe. However, until this is finally known it is difficult to know what sort of failure rates to assign these systems. My work, of course, assumed that if such systems surmounted the start-up failure rate they would operate as designed. This must still be confirmed.

This sort of work in attempting to quantify the risks from technology is very important and people should be encouraged to further develop methods for making such analysis. The approach of Refs. 1 and 2, the detailed probabilistic analysis of each possible accident sequence, is very difficult, although perhaps valid for reactors, such as OWR, where sufficient operating and test data exist.

It is known that loss function for all sorts of events display the same mathematical form. Figures 11 and 12 show these distributions for fire and aeroplane crash losses, and Figure 13 shows a comparison between natural events and accidents. These plots can be made for dozens of different activities. Note that one point and a slope are enough to define these distributions. A cursory investigation of these data tends to indicate that the slopes are related to the measure taken (i.e. safeguards systems) to either prevent accidents

or to minimize their consequences should they occur. Further, these loss functions include all losses. For example, aeroplane crashes are also sometimes caused by common-made failures or sabotage - yet the loss functions maintain the same form.

Were I now to attempt a risk estimate for a nuclear power plant I would first try to make an upper limit estimate of risk using this loss function approach. If this estimate showed risks to be acceptably low, the problem is essentially solved. I have done some preliminary work on this and believe that meaningful results are possible.

VI. SUMMARY

The field of technology assessment, of which cost-benefit analysis is one methodology, is an important one to-day. It is especially important in the area of energy policies. Here all aternatives must be examined on a timely basis because the energy problems facing much of the world are not merely theoretical.

It appears that the analysis of various types of energy sources is technically possible if an appropriate expenditure in money and manpower is made. This has not really been done to date. Such analyses could be an important input in decision making to select the appropriate policies for various geographical and political situations. The quantification of variables, where possible, can be a great help in reducing a problem to a more understandable form.

The determination of acceptable levels of risk, which can ultimately be translated into reliability design goals, also deserves more attention. A preliminary rough look at this indicates, for example, that the economic loss to a reactor operation might be a more stringent criteria than the biological risk to the public.[14] This should also be examined in more detail.

I have tried to give several examples of research where the unknowns in one discipline represented the "conventional wisdom" in another. An analysis of these problems can only be meaningful and complete if done on an interdisciplinary basis independent from the sponsorship, and resultant pressures, by any particular type of technology or industry.

REFERENCES

1. H.J. Otway, R.K. Lohrding and M.E. Battat, "A Risk Estimate for an Urban-Sited Reactor" Nuclear Technology, 12, 173 (1971).

2. H.J. Otway and Robert C. Erdmann, "Reactor Siting and Design from a Risk Viewpoint," Nuclear Engineering Design, 13, 365 (1970).

3. H.J. Otway and Robert C. Erdmann, "Leukemia and Thyroid Carcinoma: a Comparison of the Late Mortality Risks from Reactor Accidents", Nuclear Safety, 11, 462 (1970).

4. H.J. Otway, Morris E. Battat, Ronald K. Lohrding, Robert D. Turner, and Richard L. Cubitt, "A Risk Analysis of the Omega West Reactor" LA-4449, Los Alamos Scientific Laboratory report (1970).

5. C. Starr, M.A. Greenfield and D. F. Hausknecht, "A Comparison of Public Health Risks: Nuclear vs Oil-Fired Power Plants," Nuclear News, 15, 37 (1972).

6. H.J. Otway "The Quantification of Social Values" in "Risk vs Benefit: Solution or Dream" H.J. Otway, Editor, Los Alamos Scientific Laboratory report LA-4860-MS, February 1972,

7. I. Burton, R.W. Kates and G.F. White, "The Human Ecology of Extreme Geophysical Events" Natural Hazard Research Working Paper No. 1, Department of Geography, University of Toronto, (1968).

8. A.R. Wyler, M. Masuda, T.H. Holmes, "Seriousness of Illness Rating Scale" Journal of Phychosomatic Research, 11, 363, (1968).

9. T.H. Holmes and R.H. Rahe, "The Social Readjustment Rating Scale" Journal of Phychosomatic Research, 11, 213 (1967).

10. H.J. Otway, L. van der Harst and G.H. Higgins, "Socioeconomic Aspects of a Plowshare Project" Nuclear Technology 17, 58, (1972).

11. W.C. Howell, "An Evaluation of Subjective Probability in a Visual Discrimination Task" Journal of Experimental Psychology, 75, 479,(1967).

12. W.C. Howell, "Uncertainty from Internal and External Sources: A Clear Case of Overconfidence" Journal of Experimental Psychology, 89, 240 (1971).

13. C.R. Peterson and L.R. Beach, "Man as an Intuitive Statistician", Psychological Review, 68, 29, (1967).

14. H.J. Otway, J.B. Burnham and R.K. Lohrding, "Economic vs Biological Risk as Reactor Design Criteria" IEEE Transactions on Nuclear Science, Vol. NS-18, No.1, 451 (1971)

TABLE I

SOME U.S. ACCIDENTAL DEATH STATISTICS FOR 1966

Type of Accident	Total Deaths	Probability of Death per Person Per Year
Motor Vehicle	53,041	2.7×10^{-4}
Falls	20,066	1.0×10^{-4}
Fire and Explosion	8,084	4.0×10^{-5}
Drowning	5,687	2.8×10^{-5}
Firearms	2,558	1.3×10^{-5}
Poisoning		
Solids and Liquids	2,283	1.1×10^{-5}
Gases and Vapors	1,648	8.2×10^{-6}
Machinery	2,070	1.0×10^{-5}
Water Transport	1,630	8.1×10^{-6}
Aircraft	1,510	7.5×10^{-6}
Inhalation and Ingestion of Food	1,464	7.3×10^{-6}
Falling or Projected Object	1,459	7.3×10^{-6}
Mechanical Suffocation	1,263	6.3×10^{-6}
Therapeutic Medical and Surgical Procedures	1,087	5.5×10^{-6}
Railway (Except Motor Vehicle)	1,027	5.1×10^{-6}
Electric Current	1,026	5.1×10^{-6}
Hot Substance, Corrosive Liquid, Steam	408	2.0×10^{-6}
Animals (Nonvenomous)	131	6.6×10^{-7}
Lightning	110	5.5×10^{-7}
Venomous Animals and Insects	48	2.4×10^{-7}
Streetcar	9	4.5×10^{-8}
Radiation	1	-

TABLE II

POPULATION RISKS*

RISKS FROM OWR		SOME COMPARISON RISKS	
Neoplastic Disease	5.1×10^{-5} death	525 deaths	Naturally Occurring Neoplastic Disease
Non-Specific Life Shortening	1.2×10^{-3} death	270 deaths	Accidents (All causes)
Genetic Risk			
1st Generation	3×10^{y} g. death	2,600 $\frac{\text{Genetic deaths}}{\text{Generation}}$	Natural genetic death rate
Subsequent Generations	1.2×10^{-2} g.death		

* Based upon 13,000 people at risk for a 30 year period

TABLE III

TOLERABLE NUMBERS OF POWER PLANTS AS IMPLIED BY CURRENT PRACTICES IN LOS ANGELES COUNTY*

Plant Type	Critical Pollutant	Tolerable Number of 1,000-Mwe Plants (Exclusive of Pollutants from Other Sources)
Oil	SO_2	10
Natural gas	NO_2	23
Nuclear reactor (LWR)	Radioactive gases	160,000

* Based on the following assumptions:

1. Unspecified mixture of radioactive isotopes released from nuclear plant (Most restrictive assumption based on 1 mrem).
2. Compliance with 0.5 percent by weight sulfur content for oil.
3. Air volume of Los Angeles County was assumed to be 3,165 $km,^3$ which implies a mean inversion height of 300 m.
4. Ventilation of this volume requires one day.
5. Effluent volume rate for 1,000-MWe reactor is taken as 0.5×10^6 cfm which is an estimated upper limit.

TABLE IV

PUBLIC RISK COMPARISON

Plant Type	Expected Annual Averages (Deaths per 10 million population per 1,000-MWe plant per year)	
	Continuous Operation at Regulated Exposure Limits	Total Risk from Accidents
Nuclear reactor (cancer deaths)	1	Negligible (0.00006)
Oil-fired plant (respiratory deaths)	60	Negligible (0.0002)

TABLE V

VALUE OF RADIATION RISK

	$/Man-Rad
Cohen	$250
Hedgran and Lindell	$200
Dunster	~$10
Lederberg	$100-$600
Otway	$200*
Jury Awards	~$250*
Future Earnings	~$200*
Hazard Pay	$135-$980*
FAA Estimate	$373*

*Inferred from life value estimates

TABLE VI

SOME ITEMS FROM THE SERIOUSNESS OF ILLNESS RATING SCALE

	Mean Score
Leukemia	1080
Cancer	1020
Multiple Sclerosis	875
Heart Attack	855
Muscular Dystrophy	785
Stroke	774
Blindness	737
Chest Pain	609
Peptic Ulcer*	500*
Syphilis	474
Sexual Inability	382
Pneumonia	338
Irregular Heart Beats	302
Whooping Cough	230
Measles	159
Acne	98
Common Cold	62
Bad Breath	49
Dandruff	21

* Modulus Item

Figures

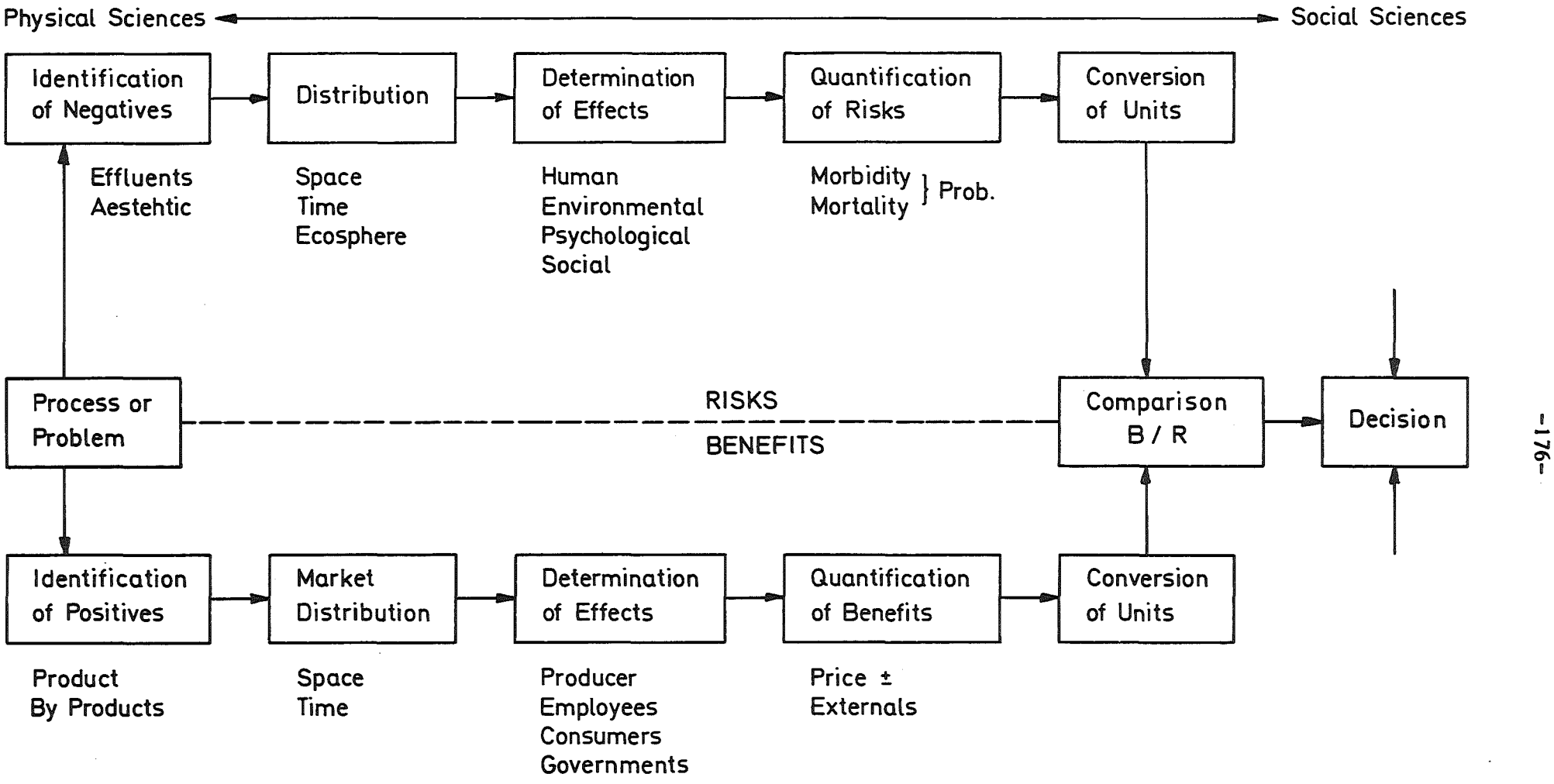


Fig. 1 The Risk - Benefit Process

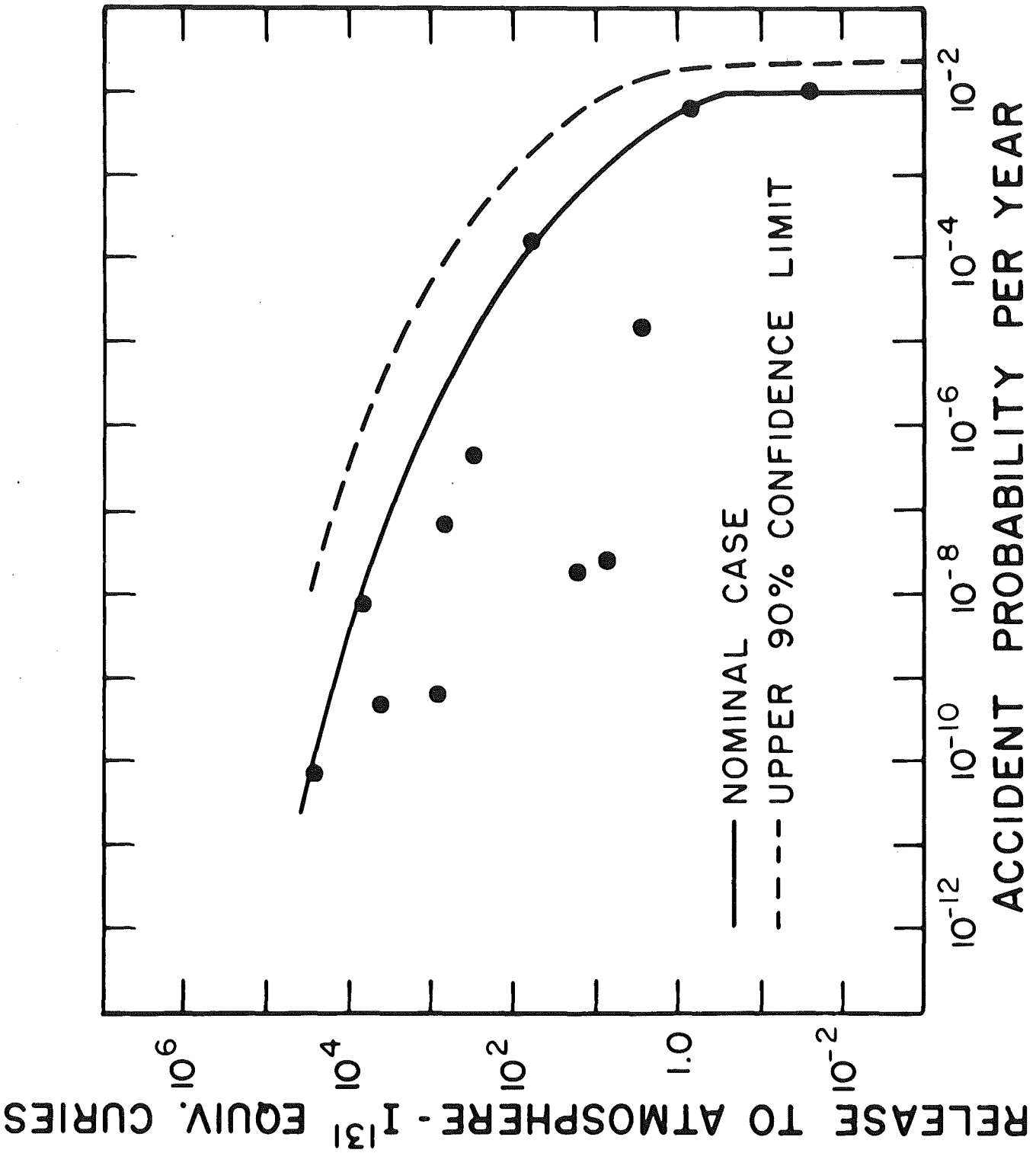

RELEASE TO ATMOSPHERE - I^{131} EQUIV. CURIES
10^{6}
10^{4}
10^{2}
1.0
10^{-2}
ACCIDENT PROBABILITY PER YEAR
10^{-12}
10^{-10}
10^{-8}
10^{-6}
10^{-4}
10^{-2}
NOMINAL CASE
UPPER 90% CONFIDENCE LIMIT

Fig.2

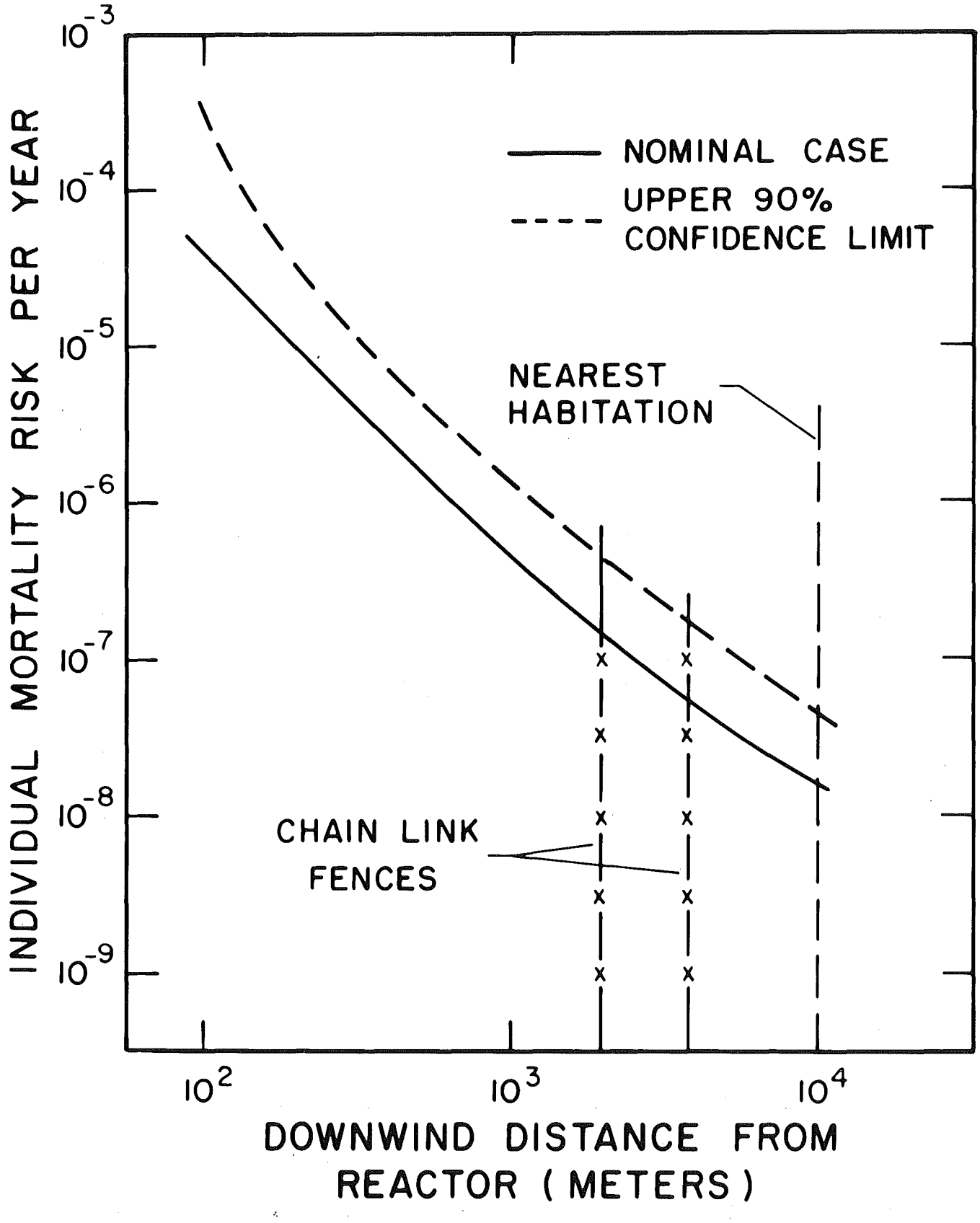
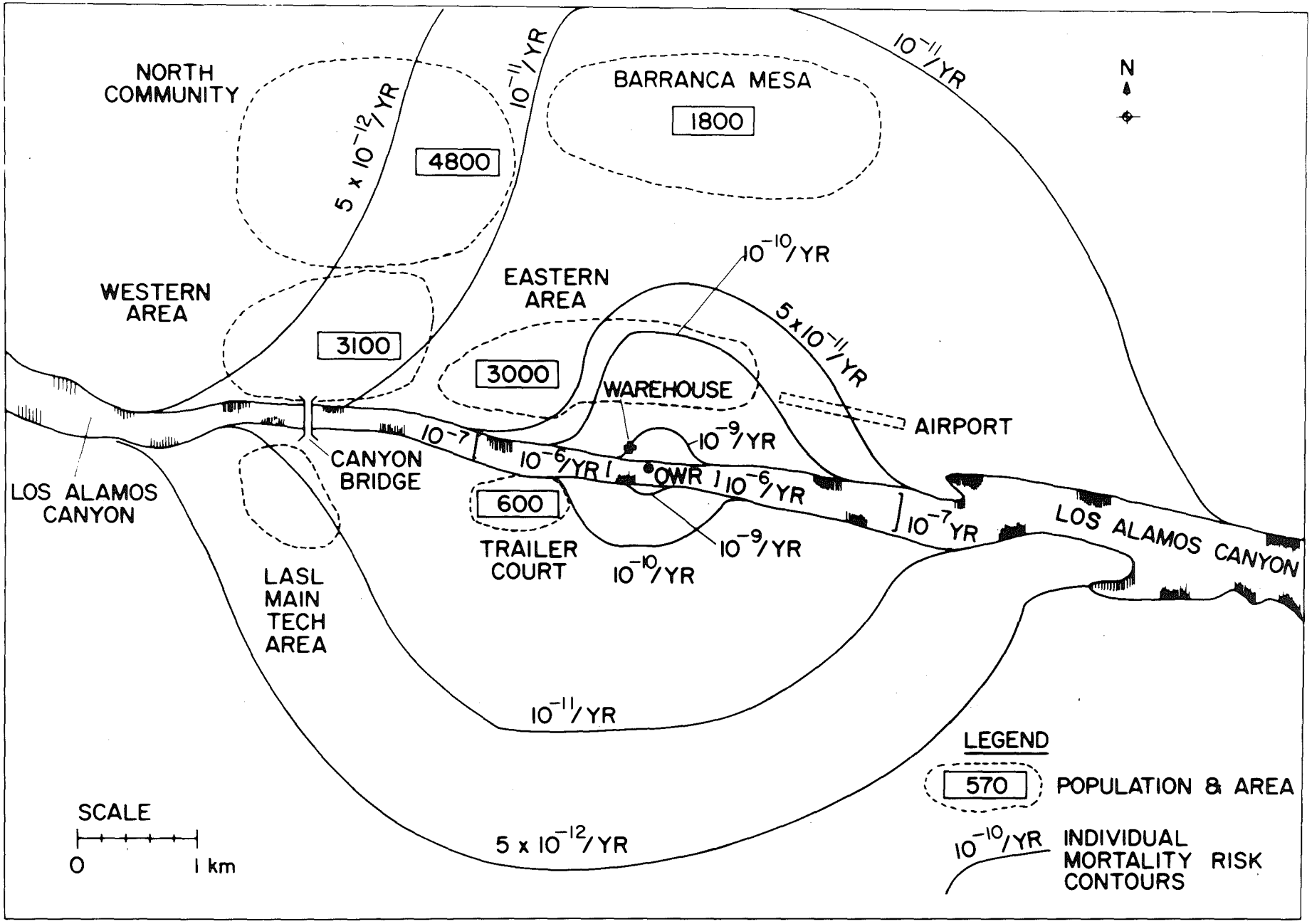
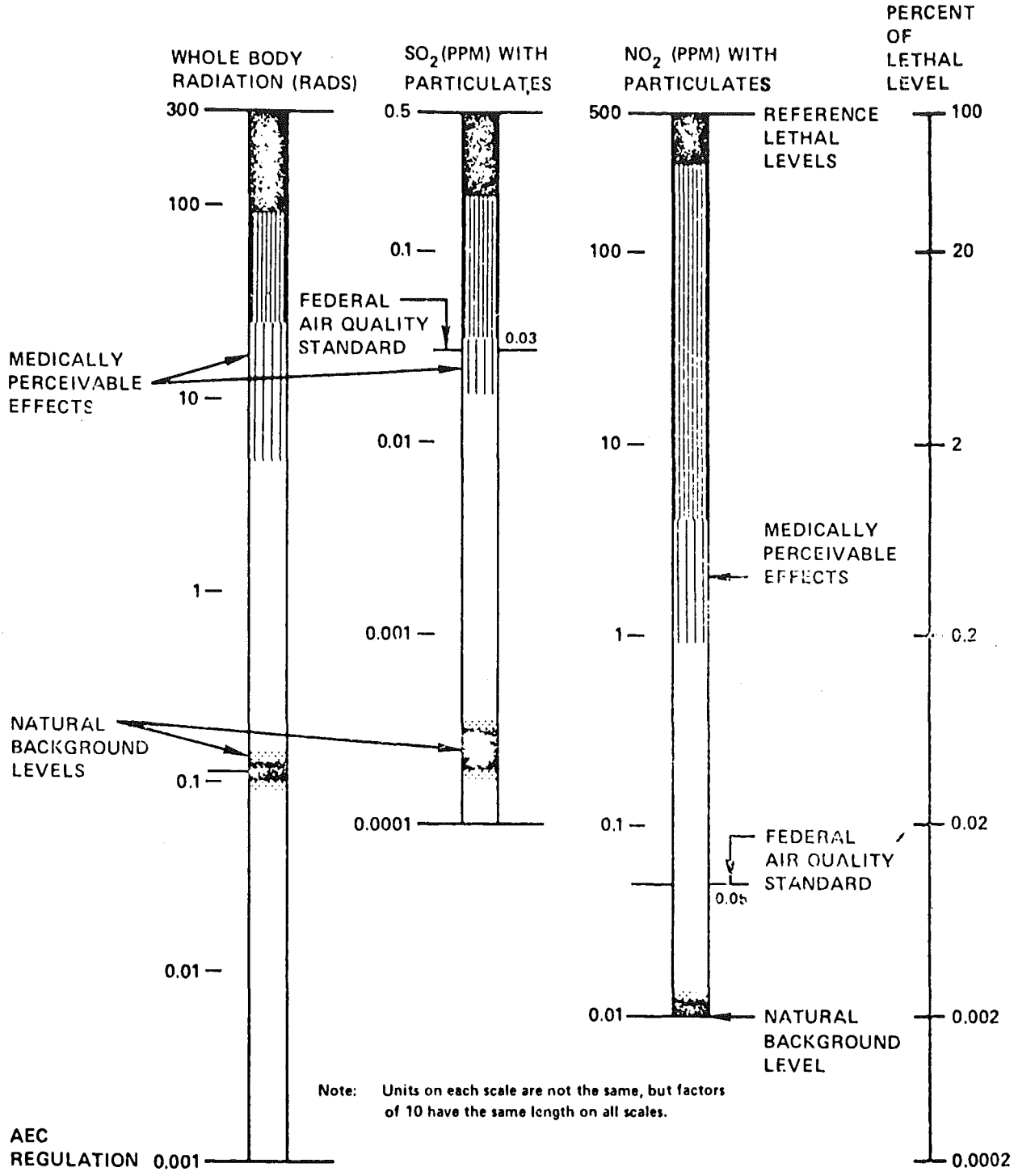

INDIVIDUAL MORTALITY RISK PER YEAR
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-9}
NOMINAL CASE
UPPER 90% CONFIDENCE LIMIT
NEAREST HABITATION
CHAIN LINK FENCES
10^{2}
10^{3}
10^{4}
DOWNWIND DISTANCE FROM REACTOR (METERS)

Fig.3

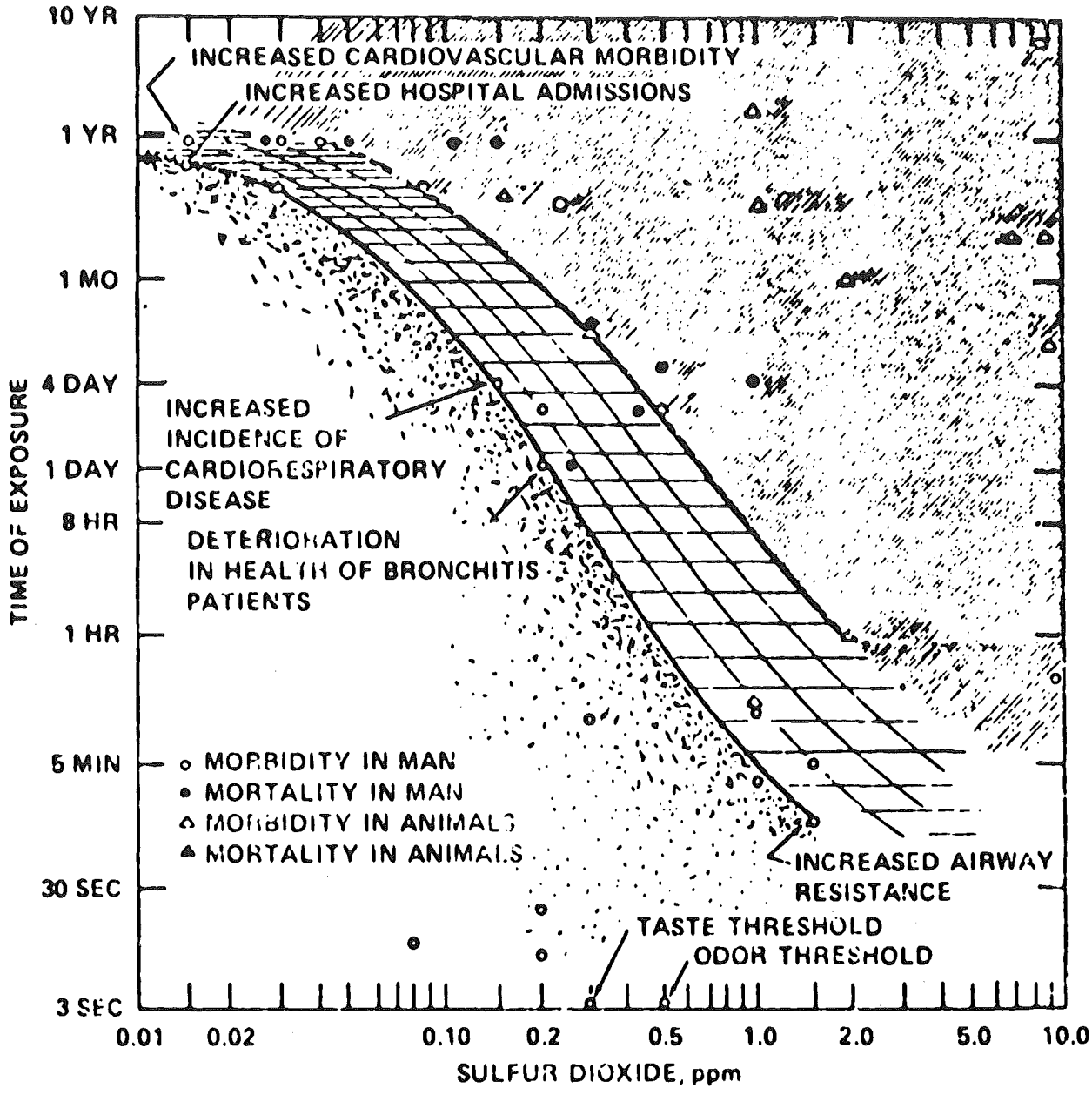
Fig. 4


NORTH COMMUNITY
4800
5 x 10⁻¹²/YR
10⁻¹¹/YR
BARRANCA MESA
1800
10⁻¹¹/YR
N
WESTERN AREA
3100
EASTERN AREA
3000
10⁻¹⁰/YR
5x10⁻¹¹/YR
WAREHOUSE
AIRPORT
10⁻⁹/YR
10⁻⁷
10⁻⁶/YR
OWR
10⁻⁶/YR
10⁻⁷YR
LOS ALAMOS CANYON
CANYON BRIDGE
LOS ALAMOS CANYON
600
TRAILER COURT
10⁻⁹/YR
10⁻¹⁰/YR
LASL MAIN TECH AREA
10⁻¹¹/YR
LEGEND
570
POPULATION & AREA
10⁻¹⁰/YR
INDIVIDUAL MORTALITY RISK CONTOURS
SCALE
0
1 km
5 x 10⁻¹²/YR



Observed Pollutant Effects on Physiological Function of Humans

Fig.5



RANGE OF CONCENTRATIONS AND EXPOSURE TIMES IN WHICH SIGNIFICANT HEALTH EFFECTS HAVE BEEN REPORTED

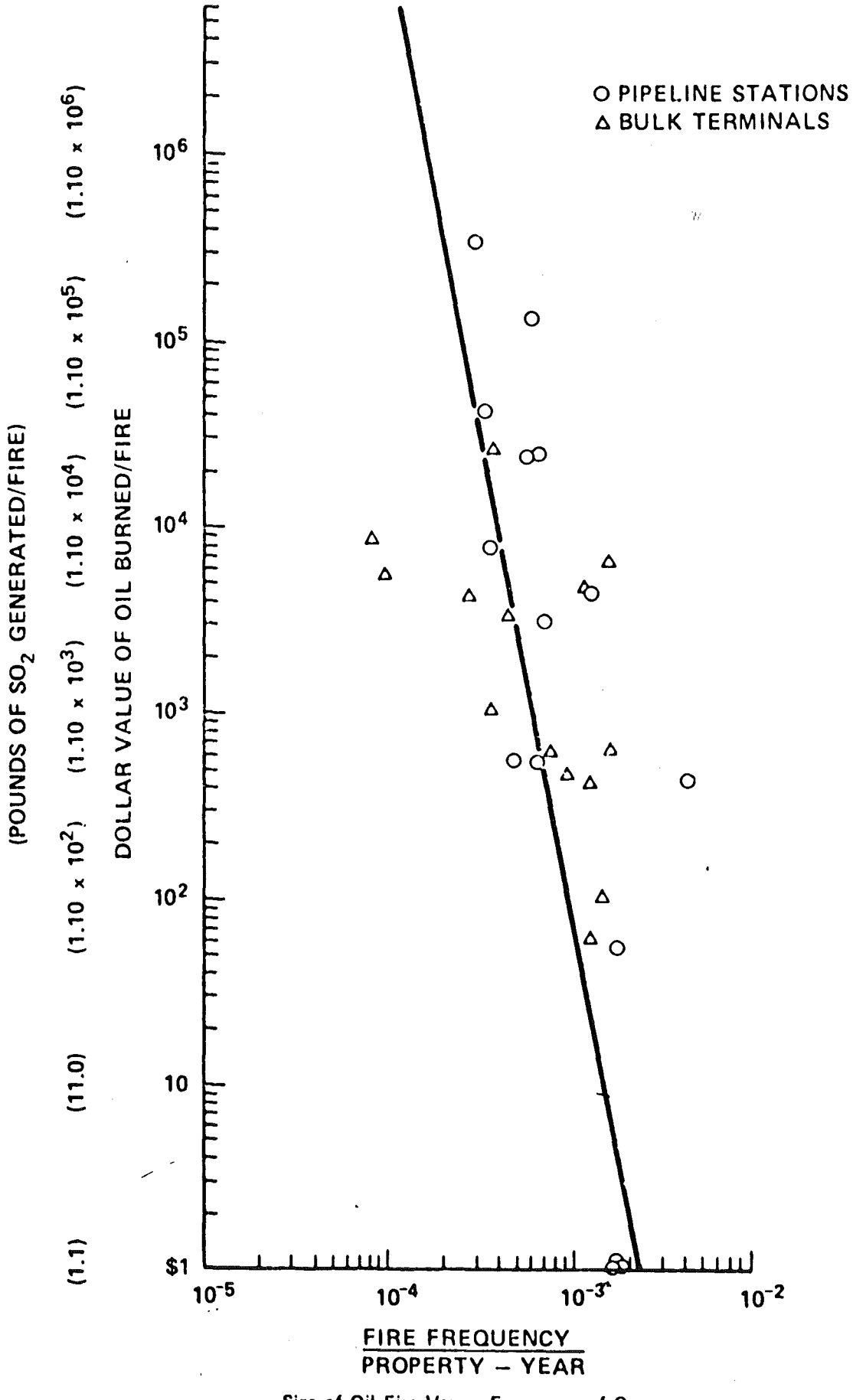
RANGE OF CONCENTRATIONS AND EXPOSURE TIMES IN WHICH DEATHS HAVE BEEN REPORTED IN EXCESS OF NORMAL EXPECTATION

RANGES OF CONCENTRATIONS AND EXPOSURE TIMES IN WHICH HEALTH EFFECTS ARE SUSPECTED

Effects of Sulphur Dioxide-Pollution on Health

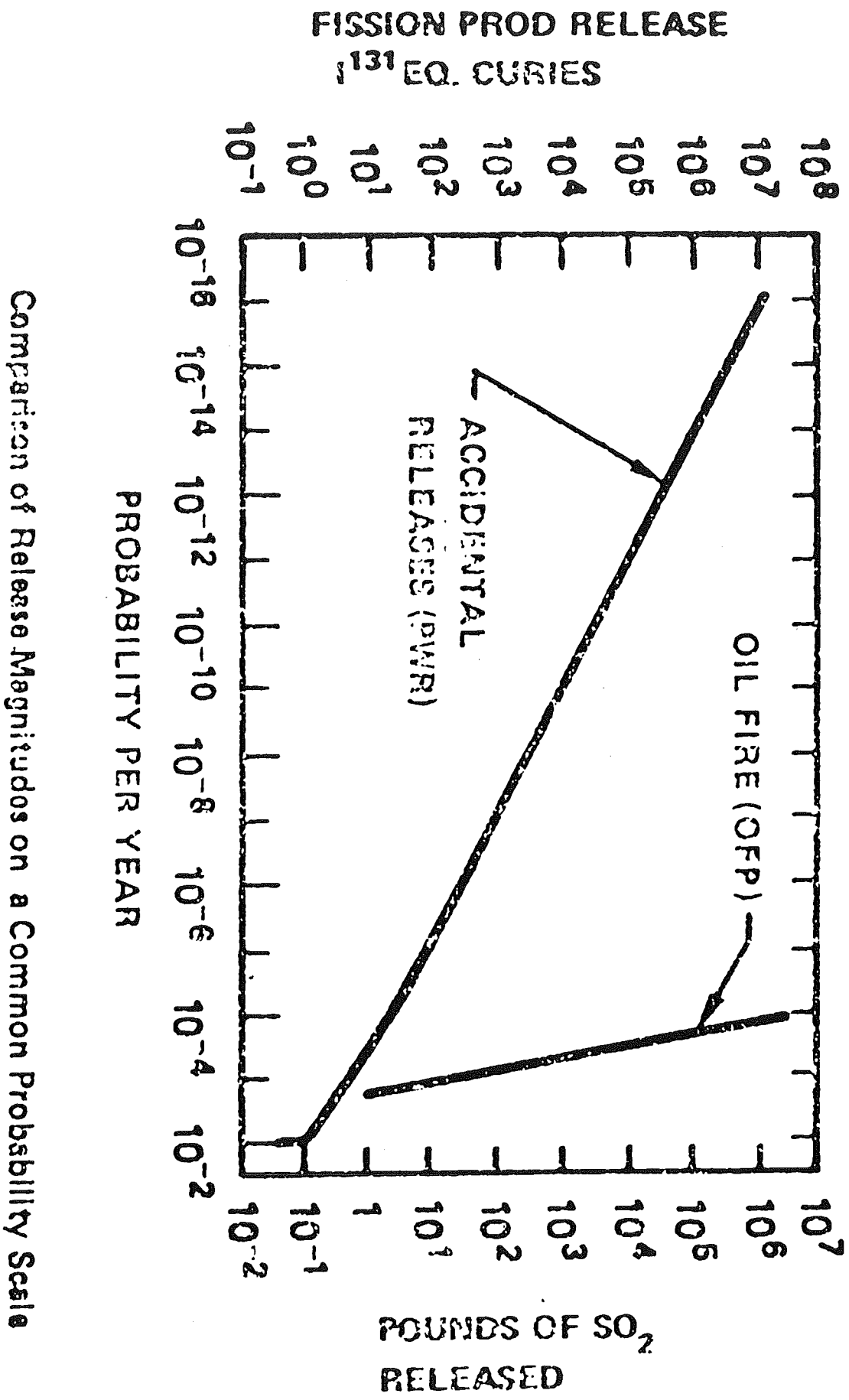
Taken From "Air Quality Criteria for Sulfur Dioxides"
a Talk by Bernard E. Conley, Ph.D.
Chief, Air Quality Criteria – National
Center for Air Pollution Control

Fig.6



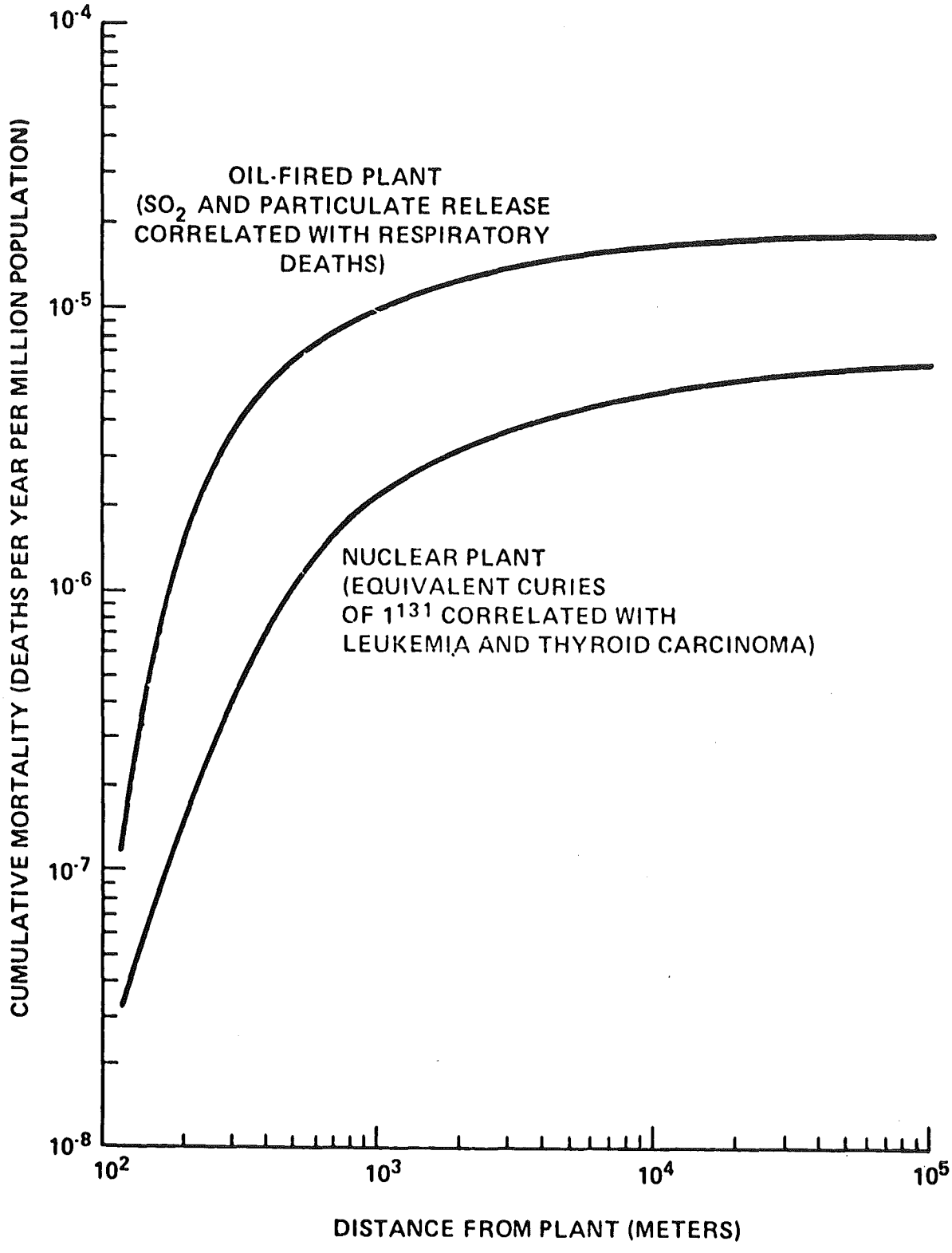
Size of Oil Fire Versus Frequency of Occurrence

Fig.7



Comparison of Release Magnitudes on a Common Probability Scale

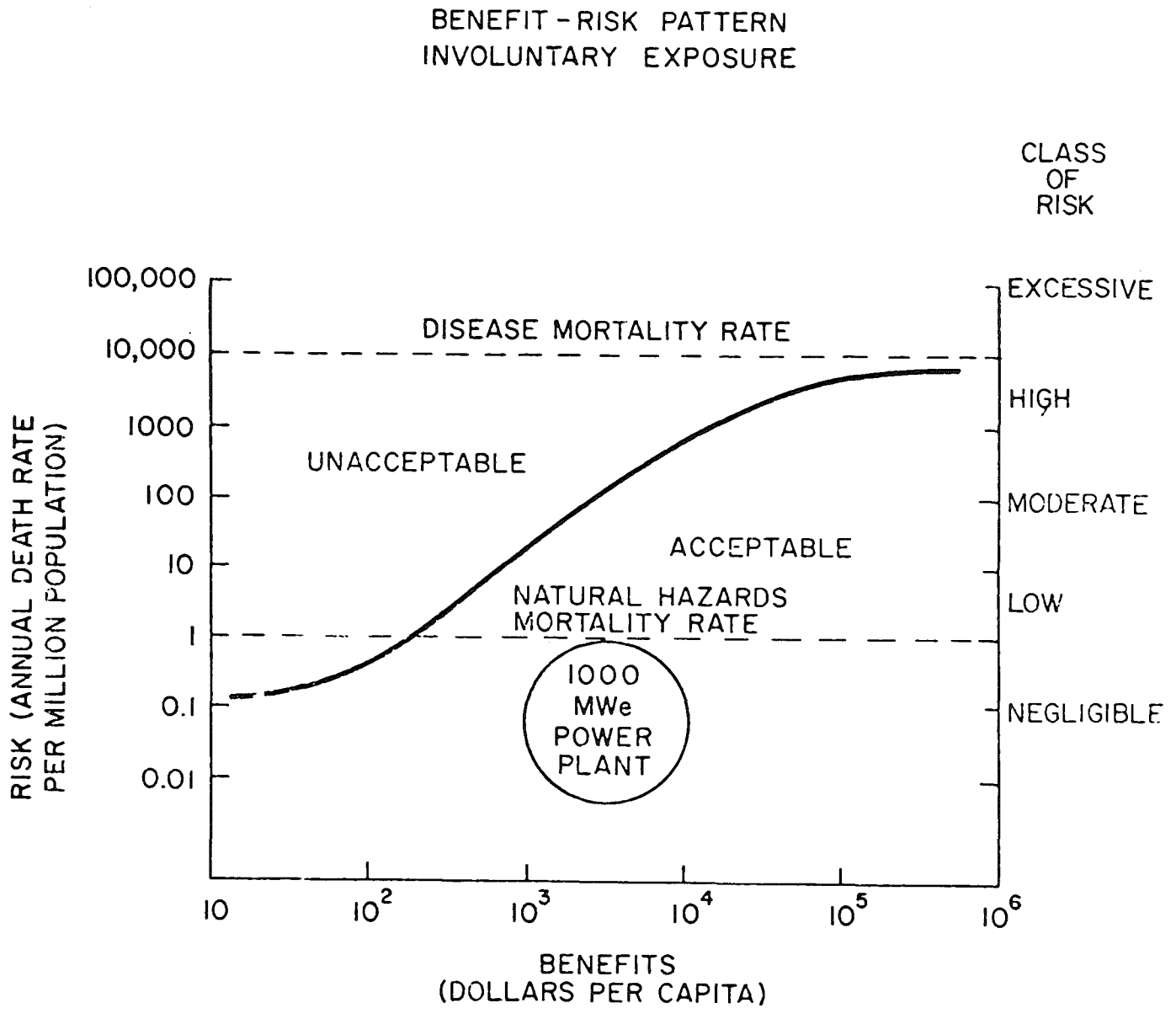
Fig.8



Cumulative Accident Mortality with Distance

Fig.9

Fig. 10



Benefit-risk Pattern for Involuntary Exposure

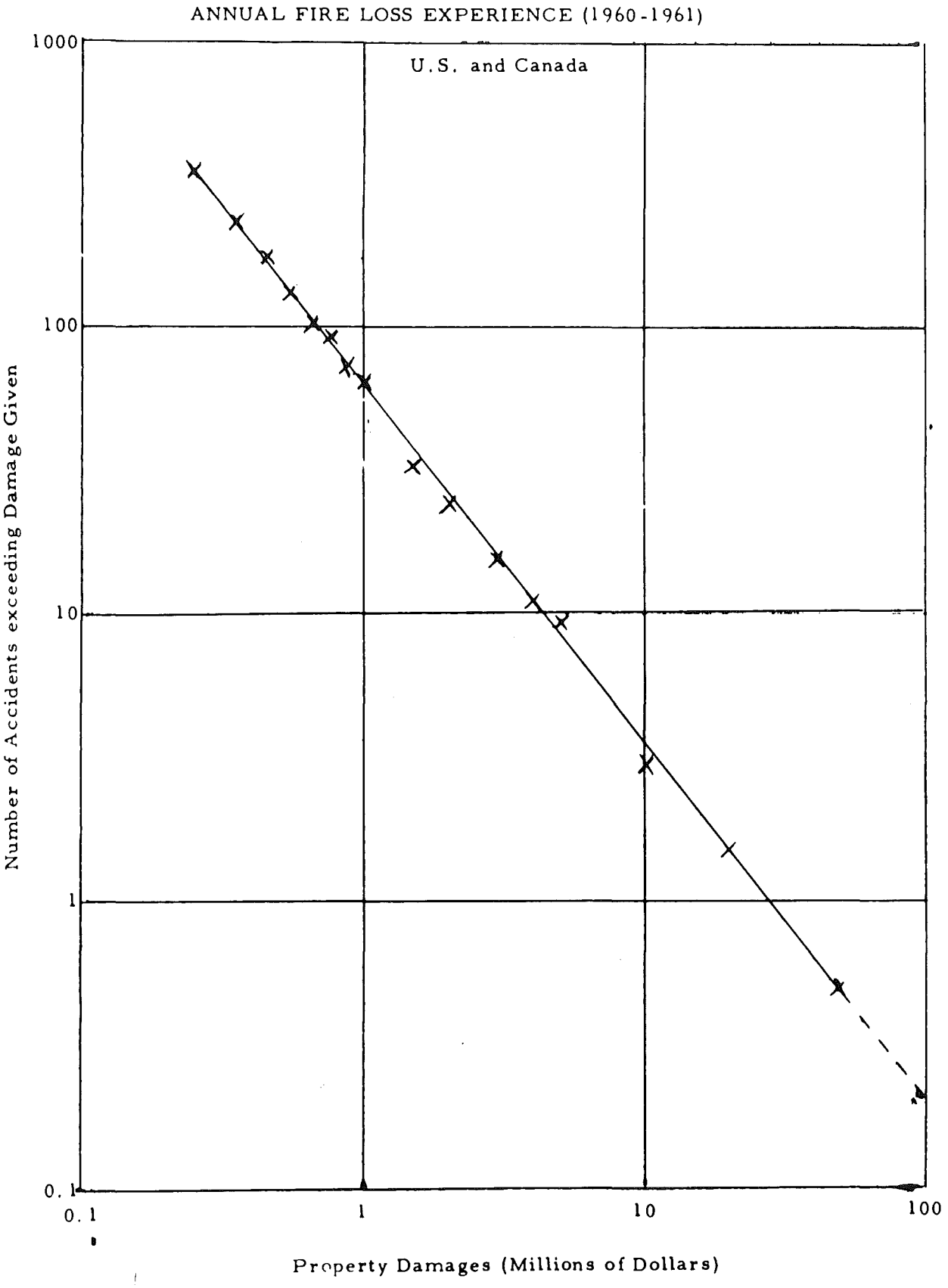

ANNUAL FIRE LOSS EXPERIENCE (1960-1961)
U.S. and Canada
1000
100
10
1
0.1
0.1
1
10
100
Number of Accidents exceeding Damage Given
Property Damages (Millions of Dollars)

Fig. 11

AIRCRAFT DEATHS IN THREE
ACCIDENT CATEGORIES

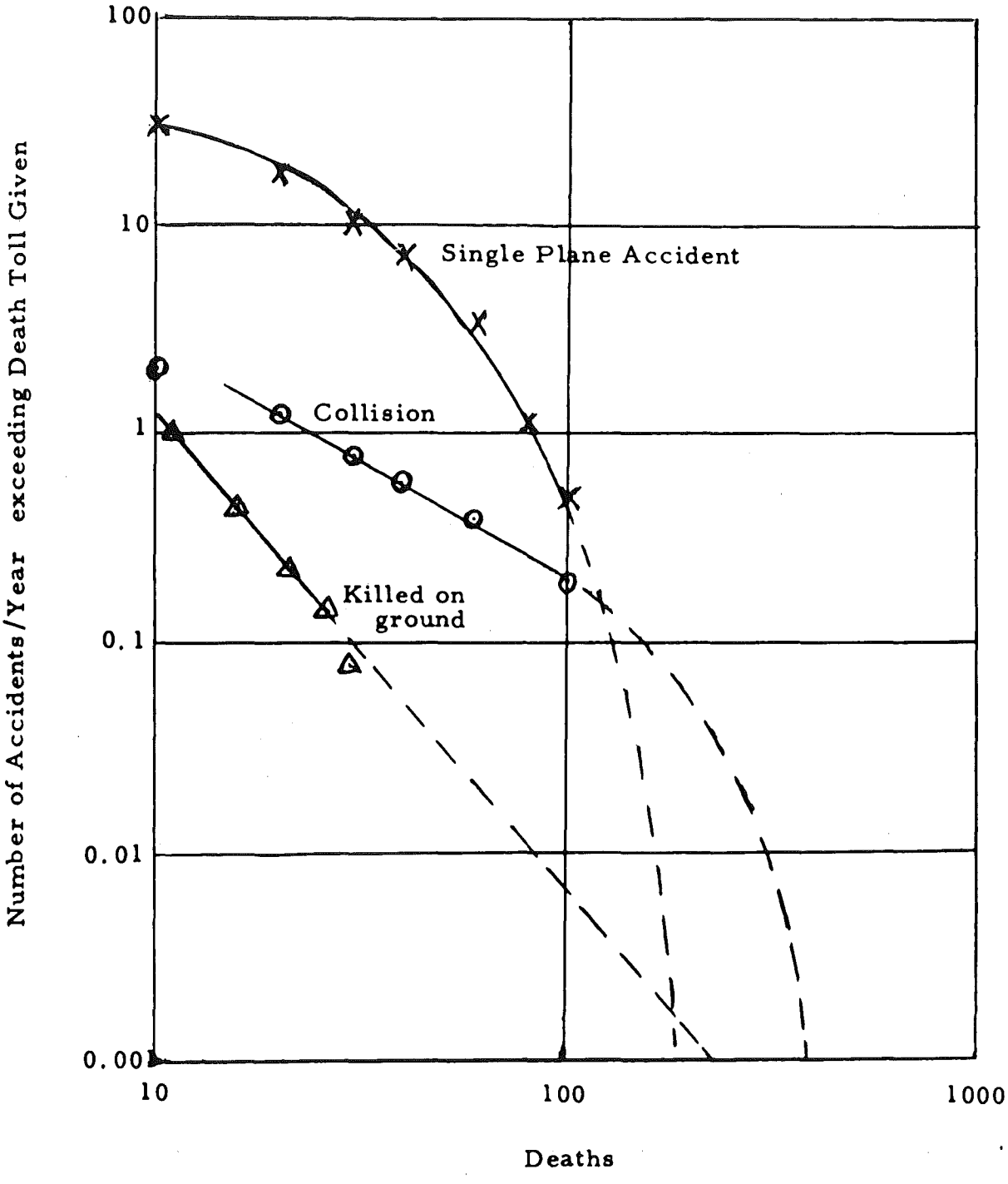


Fig. 12

FREQUENCY OF CATASTROPHIES IN
SELECTED AREAS

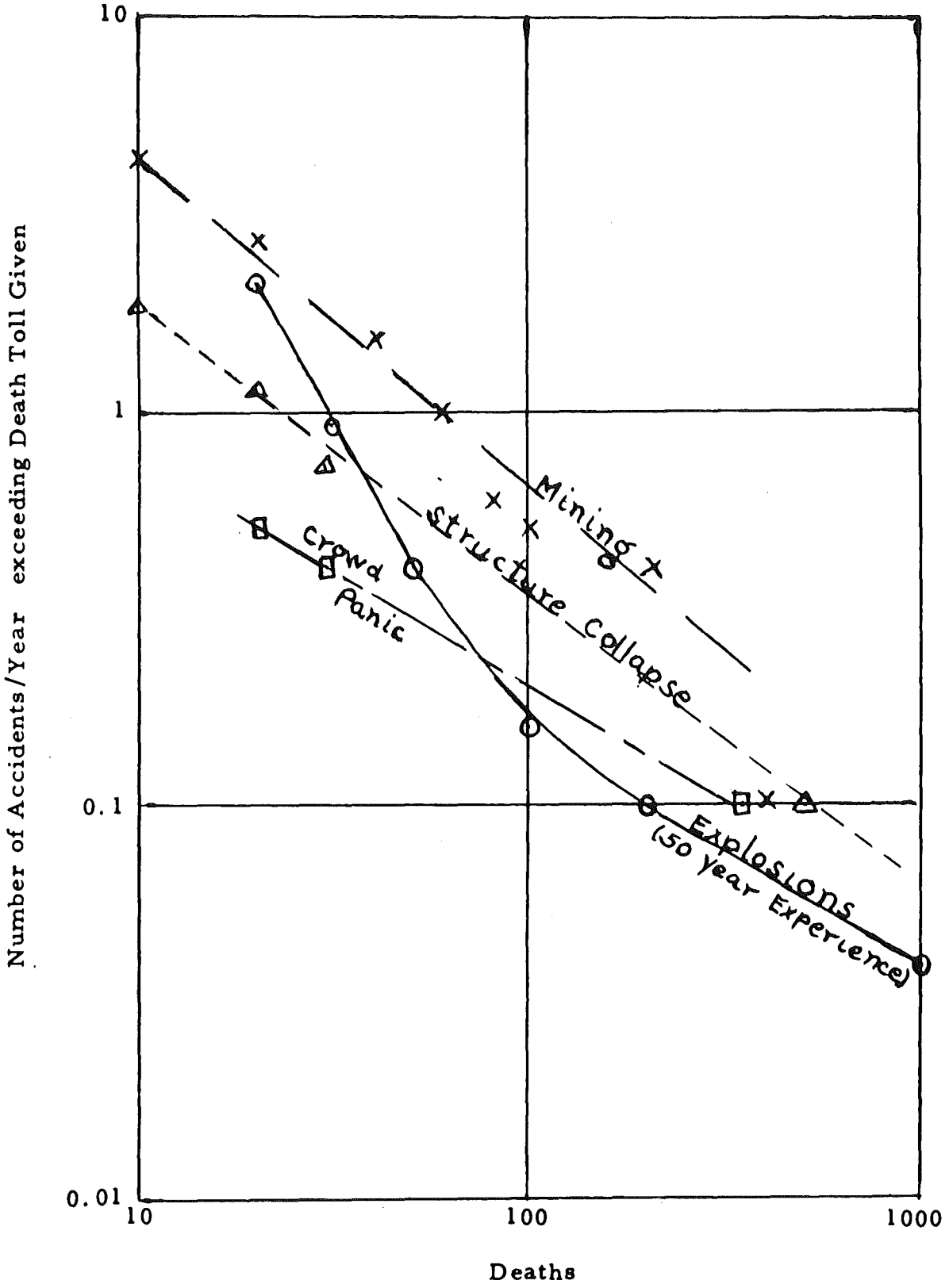


Fig. 13

Kapitel 5 : Ermittlung von Zuverlässigkeitskenngrößen

Kostenminimale Lebensdauerexperimente

D. Sellinschegg

Bemerkung

Die vorliegende Ausführung zu meinen Seminarvorträgen "Kostenminimale Lebensdauerexperimente" sowie die in den Vorträgen behandelten Parameterpunktschätzungen und Alternativtests werden in ausführlicher Form zu einem späteren Zeitpunkt veröffentlicht.

1. Einleitung

Die Zuverlässigkeit eines Elements sei wie üblich definiert als die Wahrscheinlichkeit, daß dieses Element in einem vorgegebenen Zeitintervall nicht ausfällt. Eine Zuverlässigkeitsaussage über ein System erhält man, indem man solche Systeme betreibt (Lebensdauerexperiment) und aus dem Beobachtungsmaterial eine statistische Aussage über die Zuverlässigkeit ableitet. Häufig ist ein solches Vorgehen aus ökonomischen Gründen nicht möglich. In solchen Fällen versucht man, eine Zuverlässigkeitsaussage über das System aus den Zuverlässigkeitsaussagen über die einzelnen Elemente des Systems zu erhalten (Fehlerbaumanalyse).

Im Fall von Kernkrafwerken ist man aus sicherheitstechnischen Überlegungen daran interessiert, daß eine bestimmte Mindestzuverlässigkeit für den Reaktor nachgewiesen wird. Drückt man diese Mindestzuverlässigkeit mit Systemzuverlässigkeitsbetrachtungen auf die einzelnen Elemente des Systems durch,so bleibt nachzuweisen, daß die Zuverlässigkeit der einzelnen Elemente in einem vorgegebenen Bereich liegt. Dabei ist bei der Wahl des Lebensdauerexperiments darauf zu achten, daß die Genauigkeit der statistischen Aussage ausreicht, um den geforderten Nachweis zu erbringen.

Im folgenden soll nach Lebensdauerexperimenten gesucht werden, die

1. eine maximale Information über die Zuverlässigkeit bei vorgegebener

Genauigkeit der statistischen Aussage liefern,

2. minimale zu erwartende Kosten und

3. kurze zu erwartende Experimentdauer haben.

2. Modellvorstellung

Es wird angenommen, daß sich ein Element nur in zwei Zuständen befinden kann, nämlich im Zustand "funktioniert" und im Zustand "ausgefallen".

Zu Beginn des Experiments befindet sich das Element im Zustand "funktioniert". Der Zustand "ausgefallen" wird als ein absorbierender Zustand angenommen, der Übergang in diesen Zustand soll zufällig erfolgen.

Die Zeit, die vergeht, bis das Element in den Zustand "ausgefallen" gelangt, wird als Lebensdauer des Elements bezeichnet.

Es sei τ eine Zufallsvariable, die die Lebensdauer eines Elements angibt. Dann hat τ die Verteilungsfunktion

$$F(t) = \begin{cases} 0 & : \ t \leq 0 \\ 1-e^{-\lambda t} & : \ t > 0, \ (\lambda \varepsilon (0,\infty)). \end{cases}$$

Für die Zuverlässigkeit eines Elements R(t) gilt damit nach Definition $R(t) := P(\tau > t) = e^{-\lambda t}$. Es genügt also eine Aussage über den Parameter λ, der auch als Ausfallrate bezeichnet wird, um die gewünschte Aussage über die Zuverlässigkeit eines Elements zu erhalten.

3. Lebensdauerexperimente

Man hat zur Durchführung eines Lebensdauerexperiments Vorschriften anzugeben, die den Ablauf des Experiments festlegen. Diese Vorschriften werden zusammengefaßt als Plan bezeichnet. Im folgenden werden die Pläne (n, E, r), (n, O, r) und (n, E, T) betrachtet, dabei gibt

n	die Anzahl der zu prüfenden Elemente an;
E bzw. O	gibt an, daß ausgefallene Elemente erneuert (E), bzw. nicht erneuert (O) werden und

r bzw. T gibt an, daß das Experiment nach r Ausfällen, bzw. nach der Experimentdauer T abgebrochen wird.

Es sei $d_T \in \mathbb{N}_o$ die Anzahl der beobachteten Ausfälle in der Zeit T. Dann ist das Beobachtungsergebnis aus einem Lebensdauerexperiment ein r- bzw. d_T-Tupel, nämlich

$(t_1, t_2, \ldots, t_r)$: (n, E, r), (n, O, r) und

$(t_1, t_2, \ldots, t_{d_T})$: (n, E, T),

wobei t_i (i = 1,2,...) den i-ten Ausfallzeitpunkt angibt.

4. Statistische Auswertung

Die t_i (i = 1,2,...) sind Zufallsvariable mit bekannter Wahrscheinlichkeitsverteilung. Man hat also ein statistisches Entscheidungsproblem vorliegen, bei dem der Typ der Wahrscheinlichkeitsverteilung bekannt ist, und nur der Parameter der Verteilung unbekannt ist. In diesem Fall unterscheidet man im allgemeinen zwei Typen von statistischen Entscheidungsfunktionen, nämlich

(i) Parameterschätzungen und

(ii) Tests.

Für welchen Typ von statistischen Entscheidungsfunktionen man sich entscheidet, hängt von der Problemstellung ab. Für Problemstellungen, die die Zuverlässigkeit betreffen, kommen Parameterpunkt- und Parameterbereichschätzungen als Parameterschätzungen und Alternativtests als Tests zur Anwendung. Im folgenden sollen Parameterbereichsschätzungen (Konfidenzintervallschätzungen) betrachtet werden.

Es sei $(\underline{\lambda}, \overline{\lambda})$ eine Parameterbereichschätzung für λ zum Konfidenzniveau $1-\alpha$. Dann gilt (vergl. G. Nägele, D. Sellinschegg /1/)

$$\underline{\lambda} = \begin{cases} \dfrac{\chi^2_{2r;\alpha/2}}{2\,S(t_1,\ldots,t_r)} & : (n, E, r), (n, O, r) \\ \dfrac{\chi^2_{2d_T;\,\alpha/2}}{2nT} & : (n, E, T), \end{cases}$$

$$\bar{\lambda} = \begin{cases} \dfrac{\chi^2_{2r;\,1-\alpha/2}}{2\,S(t_1,\ldots,t_r)} & : (n,E,r),\ (n,O,r) \\ \dfrac{\chi^2_{2(d_T+1);1-\alpha/2}}{2nT} & : (n,E,T), \end{cases}$$

mit

$$S(t_1,\ldots,t_r) = \begin{cases} nt_r & : (n,E,r) \\ \sum_{i=1}^{r} t_i + (n-r)t_r & : (n,O,r), \end{cases}$$

$\chi^2_{n;p}$ ist das p-Quantil der Chi-Quadrat-Verteilung mit n Freiheitsgraden.

Dabei gibt $S(t_1,\ldots,t_r)$ die summarische Betriebszeit der geprüften Elemente an.

Es gilt ferner (vergl. G. Nägele, D. Sellinschegg /1/)

$$E\left(\frac{\bar{\lambda}-\lambda}{\lambda}\right) = \begin{cases} \dfrac{\chi^2_{2r;1-\alpha/2} - \chi^2_{2r;\alpha/2}}{2(r-1)}\ ,\ r>1 & : (n,E,r),(n,O,r) \\ \dfrac{1}{2\lambda nT} \sum_{i=0}^{\infty} \left(\chi^2_{2(i+1);1-\alpha/2} - \chi^2_{2i;\alpha/2}\right) \dfrac{(\lambda nT)^i}{i!} e^{-\lambda nT} & : (n,E,T). \end{cases}$$

Intuitiv gibt $E(\frac{\bar{\lambda}-\lambda}{\lambda})$, die zu erwartende relative Länge des Konfidenzintervalls, ein Maß für die Genauigkeit der statistischen Aussage über λ an. Man bemerkt sofort, daß durch geeignete Wahl von r, bzw. λnT die Genauigkeit der statistischen Aussage für (n,E,r) und (n,O,r), bzw. (n,E,T) Pläne eingestellt werden kann. In Fig. 1 bzw. Fig. 2 ist $E(\frac{\bar{\lambda}-\lambda}{\lambda})$ als Funktion von r bzw. λnT dargestellt.

5. Kostenmodell

Bei der Wahl eines Plans für ein Lebensdauerexperiment spielen die Experimentkosten und die Experimentdauer eine entscheidende Rolle. Die Bewertung der Experimentdauer soll durch einen Kostenterm erfolgen, der den zeitabhängigen Wert einer statistischen Aussage über die Zuverlässigkeit angibt. Im folgenden wird dies durch ein Bonus-Malus-Pönale für Überschreitung der vereinbarten Experimentdauer t_o berücksichtigt.

Es sei

C_A : Anlagekosten pro Versuchseinrichtung

C_I : Bonus-Malus-Pönale pro Stunde Abweichung von der vereinbarten Experimentdauer t_o

C_O : Betriebskosten pro Betriebsstunde

C_R : Erneuerungs- bzw. Reparaturkosten pro ausgefallenes Element

C_V : Abschreibung pro geprüftes Element, das bei Experimentende noch funktionsfähig ist,

$C_A, C_I, C_O, C_R, C_V > 0$. Es wird ferner angenommen, daß

(i) in jeder Versuchseinrichtung nur ein Element zur gleichen Zeit geprüft werden kann und

(ii) C_V+C_R die Abschreibung eines bei Experimentende nicht funktionsfähigen Elements angibt.

Dann gilt in Abhängigkeit vom gewählten Plan die folgende lineare Kostenfunktion:

$$C^E(n,r) = (C_A+C_V)n + C_O\, n\, t_r + C_R\, r + C_I(t_r-t_o) \qquad :(n,E,r)$$

$$C^O(n,r) = (C_A+C_V)n + C_O\Big(\sum_{i=1}^{r} t_i+(n-r)t_r\Big)+ C_R r + C_I(t_r-t_o) \qquad :(n,O,r)$$

$$C^E(n,T) = (C_A+C_V)n + C_O\, n\, T + C_R\, d_T + C_I\,(T-t_o) \qquad :(n,E,T).$$

Es gilt dann (vergl. G. Nägele, D. Sellinschegg /1/):

$$E(C^E(n,r) = (C_A+C_V)n + C_O\, r/\lambda + C_R r + C_I \frac{r}{\lambda n} - C_I\, t_o \qquad :(n,E,r)$$

$$E(C^O(n,r)) = (C_A+C_V)n + C_O\, r/\lambda + C_R r + C_I \frac{1}{\lambda} \sum_{k=1}^{r} \frac{1}{n-k+1} - C_I t_o \qquad :(n,O,r)$$

$$E(C^E(n,T)) = (C_A+C_V)n + C_O nT + C_R \lambda nT + C_I(T-t_o) \qquad :(n,E,T).$$

Man bemerkt, daß für $r,n \in \mathbb{N}$ beliebig fest, $r>1$ gilt $E(C^E(n,r))$ $E(C^O(n,r))$ für alle $\lambda \in (0,\infty)$. D.h., ein Lebensdauerexperiment mit Erneuerung ausgefallener Elemente ergibt geringere zu erwartende Kosten als ein Lebensdauerexperiment ohne Erneuerung. Setzt man $E(\frac{\bar{\lambda}-\lambda}{\lambda})_r = E(\frac{\bar{\lambda}-\lambda}{\lambda})$: (n,E,r), (n,O,r) und $E(\frac{\bar{\lambda}-\lambda}{\lambda})_T = E(\frac{\bar{\lambda}-\lambda}{\lambda})$:(n,E,T), so bemerkt man nach Fig. 1 und Fig. 2, daß für $E(\frac{\bar{\lambda}-\lambda}{\lambda})_r = E(\frac{\bar{\lambda}-\lambda}{\lambda})_T$ gilt, $\lambda nT \leq r$. Daraus folgt $E(C^E(n,T)) \leq E(C^E(n,r))$ für $E(\frac{\bar{\lambda}-\lambda}{\lambda}) = \text{const.}$, $n \in \mathbb{N}$ beliebig fest. D.h., daß in diesem Fall ein Lebensdauerexperiment nach dem (n,E,T) Plan bezüglich der zu erwartenden Kosten mindestens so gut ist wie eines nach einem (n,E,r) Plan.

6. Kostenminimaler Plan

Es wird nun der Fall betrachtet, daß der zu ermittelnde Parameter λ in etwa bekannt ist, und $E(\frac{\bar{\lambda}-\lambda}{\lambda})$ aus der Zuverlässigkeitsforderung für das zu prüfende Element fest vorgegeben ist. In diesem Fall kann man den kostenminimalen Plan für ein Lebensdauerexperiment dadurch erhalten, daß man $E(C^*(n,.))$ unter der Nebenbedingung $r = \text{const}$ bzw. $\lambda nT = \text{const}$ minimiert. Es sei $(\tilde{n},E,\tilde{T})$ der kostenminimale (n,E,T) Plan, dann gilt (vergl. G. Nägele, D. Sellinschegg /1/)

$$\tilde{T} = \sqrt{\frac{C_A+C_V}{C_I}} \cdot \sqrt{\frac{\lambda nT}{\lambda}}, \quad \tilde{n} \in \{ n_1, n_2 \},\ n_1 \leq \sqrt{\frac{C_I}{C_A+C_V}} \cdot \sqrt{\frac{\lambda nT}{\lambda}} \leq n_2,\ n_1,n_2 \in \mathbb{N}.$$

7. Beispiel

Das Beispiel soll nur Tendenzen aufzeigen und keine Absolutwerte angeben. Es soll ein kostenminimaler (n,E,T) Plan für ein Lebensdauerexperiment einer

Na-Pumpe (KNK-Pumpe mit 500 m^3/h Durchsatz) ermittelt werden. Gegeben seien folgende Kostenparameter

C_A = 520.000,-- DM/ Versuchseinrichtung

C_I = 120,-- DM/h

C_O = 152,-- DM/Betriebsstunde

C_R = 20.000,-- DM/Reparatur

C_V = 400.000,-- DM (Pumpenlaufwerkkosten).

Es wird ferner angenommen, daß man nur am Nachweis einer Mindestzuverlässigkeit interessiert ist, also $E(\underline{\lambda}) = 0$. Man erhält

λ	$E(\overline{\lambda})$	$\approx$ n	$\approx$ T / Jahre /	$\approx$ E(C) /Mill DM /
2.10^{-5}	10^{-4}	3	2	10
10^{-5}	5.10^{-5}	4	3	18
10^{-5}	2.10^{-5}	8	7	80
2.10^{-6}	10^{-5}	8	7	80

mit $E(C) = (C_A+C_V)\ n + C_O nT + C_R \lambda nT$; d.h. ohne Berücksichtigung der Strafkosten.

Man bemerkt, daß die Genauigkeitsforderung einen entscheidenden Einfluß auf die Experimentdauer und die zu erwartenden Kosten hat.

Wie man der letzten Zeile der Tabelle entnehmen kann, ist mit einem Plan (8,E,7) der Nachweis einer mittleren Lebensdauer der Pumpe von 100.000 h nur dann möglich, wenn die tatsächliche Lebensdauer der Pumpe bei 500.000 h oder $\approx$ 57 Jahren liegt. Andererseits wird für die Na-Pumpe des SNR eine mittlere

Lebensdauer von 100.000 h gefordert. Geht man also davon aus, daß Zuverlässigkeitsforderungen auch nachgewiesen werden müssen, so wird man sich zu überlegen haben, wie hoch man mit den Forderungen gehen kann.

Literatur

/1/ Nägele G., Sellinschegg D.
"Test Cost Minimization for Reliability Assessment",
Proceedings of the Reliability and Maintainability Symposium 1972,
San Francisco, USA

/2/ Nägele,G., Sellinschegg D.
"Kostenoptimale Testauslegung unter Vorgabe einer bestimmten Genauigkeitsanforderung an die Zuverlässigkeit",
Proceedings of the First International Conference on Structural Mechanics in Reactor Technology 1971, Berlin

/3/ Nägele G., Sellinschegg D.
"Kostenoptimierung von Zuverlässigkeitstests bei vorgegebener Genauigkeitsforderung",
TÜ, Sicherheit + Zuverlässigkeit, Band 12, No. 10 (1971)

/4/ Epstein B.
"Statistical Life Tests Acceptance Procedures"
Technometrics, Vo. 2, No. 4 (1960)

/5/ Epstein B.
"Statistical Techniques in Life Testing"
(1961) available from Clearinghouse PB 171 580

/6/ Gnedenko B.W., Belyayev J.K., Solovyev A.D.
"Mathematische Methoden der Zuverlässigkeitstheorie".
Nauka 1965

/7/ Lloyd D.K., Lipow M.
"Reliability: Management, Methods, and Mathematics",
Prentice-Hall, INC., Englewood Cliffs, N.J. (1964)

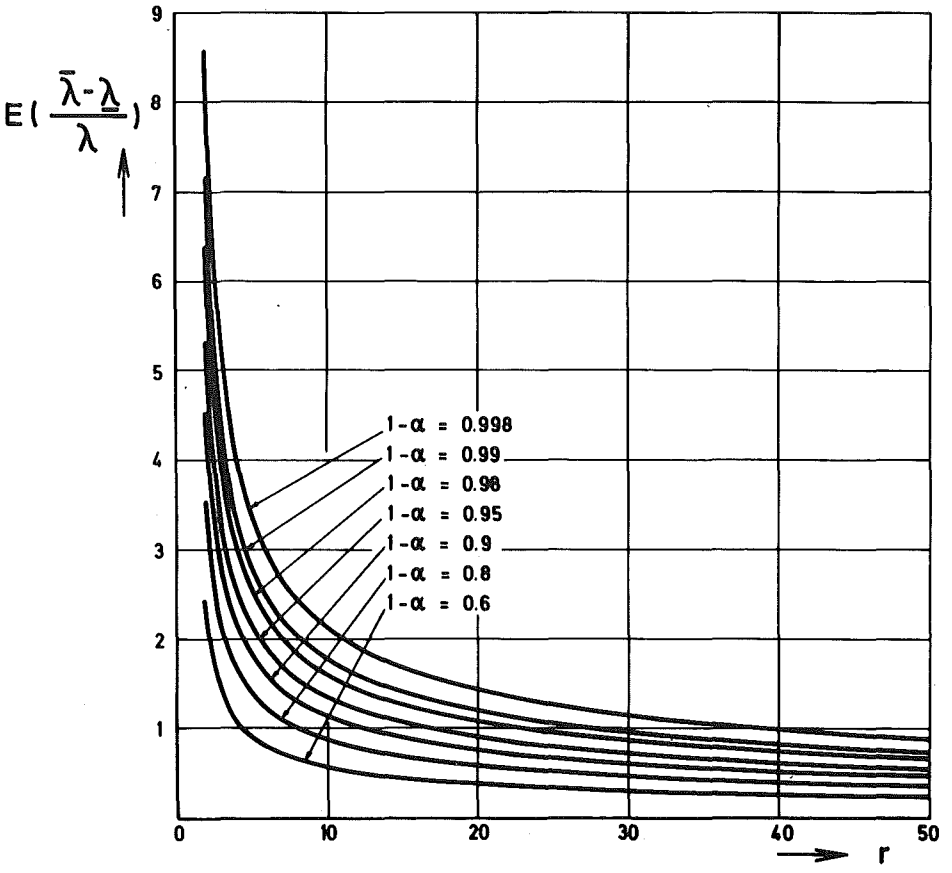

E((λ̄-λ)/λ)
9
8
7
6
5
4
3
2
1
1-α = 0.998
1-α = 0.99
1-α = 0.98
1-α = 0.95
1-α = 0.9
1-α = 0.8
1-α = 0.6
0
10
20
30
40
50
r

Fig.1

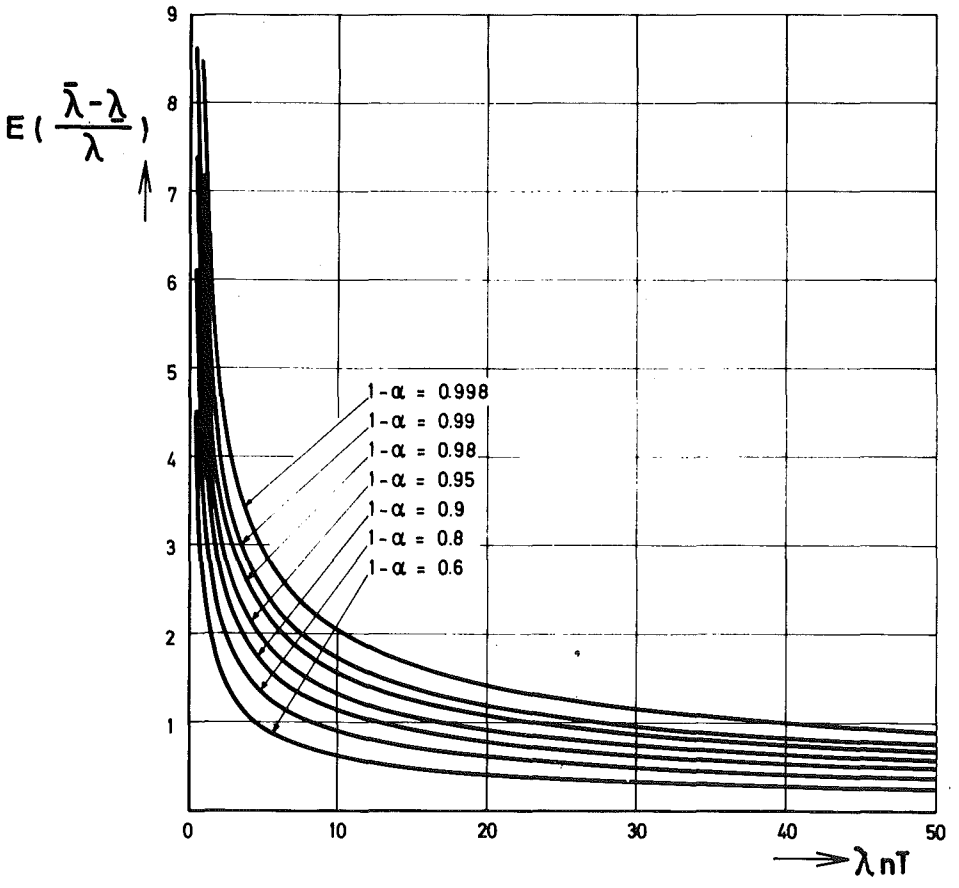

E((λ̄-λ)/λ)
9
8
7
6
5
4
3
2
1
1-α = 0.998
1-α = 0.99
1-α = 0.98
1-α = 0.95
1-α = 0.9
1-α = 0.8
1-α = 0.6
0
10
20
30
40
50
λnT

Fig. 2

Optimale Auslegung von Lebensdauertests unter Berücksichtigung sequentieller Teststrategien

G. Nägele

1. Einleitung

Lebensdauertests werden durchgeführt um freie Parameter der Modelle der Zuverlässigkeitstheorie (speziell die mittlere Lebensdauer) an das Ausfallverhalten realer Komponenten anzupassen.

Zur Beurteilung von Lebensdauertests gibt es drei verschiedene Bewertungskriterien:

(i) Bewertung nach der Information, die über die Zuverlässigkeitskenngrößen erhalten wird.

(ii) Bewertung nach der Zeit bis zu der diese Information zur Verfügung steht (also der Testdauer).

(iii) Bewertung nach den Kosten des Lebensdauertests.

Ziel der Auslegung eines Lebensdauertests ist ein optimaler Ausgleich dieser drei Bewertungskriterien. Dabei werde ich mich darauf beschränken einen optimalen Ausgleich zwischen Testdauer und Testkosten zu finden bei einer gegebenen Mindestanforderung an den Informationsgehalt. Eine solche Untersuchung vermittelt gleichzeitig einen Eindruck, welche Zuverlässigkeitsanforderungen realistisch sind in dem Sinne, daß sie sich mit sinnvollem Aufwand nachprüfen lassen.

Im Rahmen dieses Seminars hat bereits Herr Sellinschegg über die optimale Auslegung von Lebensdauertests gesprochen und dabei vier Typen von Teststrategien betrachtet. Hier soll nun untersucht werden, inwieweit sich der außerordentlich hohe Aufwand an Zeit und Geld reduzieren läßt durch den Übergang zu sequentiellen Teststrategien.

Hinsichtlich einer ausführlicheren und strengeren Behandlung des Problems möchte ich auf die Arbeiten verweisen die von Herrn Sellinschegg und mir demnächst erscheinen werden.

2. Das Modell für den Lebensdauertest

Ein Lebensdauertest besteht im Prinzip darin, daß eine Anzahl technischer Komponenten unter möglichst realistischen Bedingungen betrieben, und ihre Funktionsfähigkeit laufend überprüft wird. Entsprechend dem Zweck eines Lebensdauertests basiert das Modell auf dem in der Zuverlässigkeitstechnik allgemein üblichen Komponentenmodell. D.h. die Komponenten werden in zwei Klassen eingeteilt - funktionsfähige und nicht funktionsfähige (ausgefallene). Der Komponentenausfall, also der Übergang vom funktionsfähigen in den nicht funktionsfähigen Zustand sei nur während des Betriebs möglich, er sei irreversibel, d.h. eine Rückkehr in den funktionsfähigen Zustand kann nur durch eine Reparatur erfolgen, und er erfolge rein zufällig. In diesem Modell wird das Ausfallverhalten einer Komponente vollständig beschrieben durch die Angabe ihrer Lebensdauer, die definiert ist als die Summe aller Betriebszeiten der Komponente bis zum Ausfall. Die Gesetzmäßigkeit des Ausfallprozesses für einen Komponententyp wird dann festgelegt durch die Verteilungsfunktion F der Lebensdauer. Ich setze hier wie allgemein üblich eine exponentielle Lebensdauerverteilung voraus, also:

$$F(t) = F_{\lambda}(t) = \begin{cases} 1 - e^{-\lambda t} & \text{für } t \geq 0 \\ 0 & \text{sonst} \end{cases}$$

wobei λ ein positiver reeller Verteilungsparameter ist.

$1/\lambda$ ist gleich dem Erwartungswert der Lebensdauer.

Bei einem Lebensdauertest laufen nun die Ausfallprozesse für eine ganze Anzahl solcher Komponenten nebeneinander ab. Ich setze voraus, daß die einzelnen Komponentenausfälle voneinander stochastisch unabhängig sind. (Andernfalls sind die gesammelten Daten nicht repräsentativ für das Verhalten von Einzelkomponenten). Bei dem vorliegenden Komponentenmodell ist es nun ausreichend, den Lebensdauertest zu beschreiben durch die Angabe der Zahl der im Test eingesetzten Komponenten n(t) in Abhängigkeit von der Zeit, die Folge $(t_{1,\ldots,t_d})$ der beobachteten Ausfallzeitpunkte und die Testdauer T. Die Identität der betriebenen und ausgefallenen Komponenten spielt keine Rolle, da aus der Annahme einer exponentiellen Lebensdauerverteilung folgt, daß keine Alterung der Komponenten eintritt, also jederzeit alle funktionsfähigen Komponenten, unabhängig von ihrer Vorgeschichte, äquivalent sind.

Die Freiheit bei der Auslegung eines Lebensdauertests besteht nun in der Wahl der Funktion n(t) und der Testdauer T. Herr Sellinschegg hat die Fälle betrachtet, daß n(t=o) vorgegeben wird und, je nach dem ob ausgefallene Komponenten erneuert werden oder nicht, n(t) während des Tests konstant bleibt (E - Pläne) oder durch jeden Ausfall um eines verringert wird (O - Pläne). Die Testdauer wurde entweder fest vorgegeben (T - Pläne) oder auf den Zeitpunkt t_r des r - ten Ausfalls festgelegt (r - Pläne). Die Idee sequentieller Teststrategien besteht nun darin, die vorläufige Testinformation zur Festlegung der kostenbestimmenden Größen n(t) und T in geeigneter Weise heranzuziehen. Das bedeutet, daß n(t) zu jeder Zeit t von den Zeitpunkten $t_{1,\ldots,t_d}$ der d(t) bereits beobachteten Ausfälle abhängig gemacht werden kann. Ebenso kann die Testdauer T nach jedem Ausfall in Abhängigkeit der bereits beobachteten Ausfallzeiten neu festgelegt werden. Aus der Vielzahl der damit möglichen Teststrategien ist dann eine optimale auszuwählen.

Für das weitere Vorgehen empfiehlt es sich, eine monotone Transformation der Zeitskala vorzunehmen und den Ablauf des Lebensdauertests in dieser modifizierten Zeitskala zu beschreiben. Ich gehe daher über von der Testzeit t zu der summarischen Betriebszeit s(t) aller Komponenten bis t.

Diese ist gegeben durch:

$$s(t) = \int_0^t n(\tau)\, d\tau$$

Die Komponentenstrategie n(t) geht dann über in eine Funktion $n^*(s)$ von s und den "Zeitpunkten" der bis s beobachteten Ausfälle, diesmal aber gemessen in der modifizierten Zeitskala. Ebenso geht das Abbruchkriterium T über in das entsprechende S in der transformierten Zeitskala. Die Gesetzmäßigkeit des zeitlichen Ablaufs eines solchen Lebensdauertests läßt sich nun für die ganze Klasse der betrachteten Teststrategien in einheitlicher Weise darstellen.

Ich betrachte den zeitlichen Ablauf eines Lebensdauertests mit einer beliebigen Komponentenstrategie n(s) (>0 für alle s) der zunächst nicht abgebrochen werden soll. Verfolge ich den Lebensdauertest bis zu einer beliebigen Zahl r ($\in \mathbb{N}$) von Ausfällen, so wird die Gesetzmäßigkeit des Testablaufs (in der summarischen Betriebszeit s) beschrieben durch den Wahrscheinlichkeitsraum $(\Omega^r, \mathfrak{B}^r, P_\lambda^r)$. Dabei ist:

Ω^r die Menge aller möglichen Versuchsausgänge (Ausgangsraum), also die Menge aller geordneten Folgen von r Ausfallzeitpunkten $(s_1, \ldots, s_r)$.

$\mathfrak{B}^r$ die Menge aller Ereignisse die wir voneinander unterscheiden wollen, eine σ - Algebra auf Ω^r. Hier sei $\mathfrak{B}^r$ die σ-Algebra der Borelschen Mengen in $\mathbb{R}^r$ eingeschränkt auf Ω^r.

P_λ^r die Wahrscheinlichkeitsverteilung auf $(\Omega^r, \mathfrak{B}^r)$ die gegeben ist durch die Dichtefunktion:

$$f_\lambda^r(s_1, \ldots, s_r) = e^{-\lambda s_r}$$

Ich schränke nun die Beobachtungsdauer durch ein Abbruchkriterium $S = S(s_1, \ldots, s_{r-1})$ gegenüber dem obigen Fall ein. Dann können zwei Testverläufe aus Ω^r, die erst nach dem Versuchsabbruch voneinander abweichen nicht mehr unterschieden werden. Die Menge der unterscheidbaren Ereignisse wird reduziert, ohne daß neue Ereignisse hinzukommen. Auf Ω^r wird also durch das Abbruchkriterium S eine gröbere σ-Algebra $\tau^r(S)$ bestimmt, die ganz in $\mathfrak{B}^r$ enthalten ist. Daher ist P_λ^r auch für alle Mengen aus $\tau^r(S)$ definiert. Wir haben daher das folgende Ergebnis:

Die Gesetzmäßigkeit des Testablaufes bei einer beliebigen Teststrategie (n(s), S) wird bis zu einer beliebigen Anzahl r von Ausfällen beschrieben durch den Wahrscheinlichkeitsraum

$$(\Omega^r, \tau^r(S), P_\lambda^r).$$

Interessant ist, daß n(t) keinen Einfluß auf den Wahrscheinlichkeitsraum hat. Dies gilt jedoch nur für die Beschreibung des Testablaufes in der verzerrten Zeitskala der summarischen Betriebszeit.

3. Problemstellung bei der Auslegung eines Lebensdauertests

Sinn eines Lebensdauertests ist es, Entscheidungen bezüglich eines Komponententyps zu erleichtern. Ich gehe speziell von dem Problem einer Alternativentscheidung über Annahme oder Ablehnung des Komponententyps aus, dabei sei ein gewisses Maximalrisiko für die Entscheidung von außen vorgegeben. Diese Situation führt im allgemeinen auf das statistische Problem, eine Hypothese $H_0: \lambda \leq \lambda_0$ gegen eine Alternative $H_1: \lambda \geq \lambda_1$ $(0 < \lambda_0 < \lambda_1)$ mit vorgegebenen maximalen Fehlerwahrscheinlichkeiten 1. bzw. 2. Art α bzw. β zu testen.

Bei der Auslegung stellt sich also das Problem, zunächst solche Teststrategien zu bestimmen, die einen Test von Ho gegen H_1 mit Fehlerwahrscheinlichkeiten kleiner α bzw. β zulassen, und dann unter diesen diejenige Strategie auszuwählen, die Testkosten und Testdauer gleichzeitig minimiert.

Auf Grund der Struktur des Wahrscheinlichkeitsraums führt das erste Teilproblem zur Festlegung des Abbruchkriteriums S das zweite Teilproblem zur Festlegung der Komponentenstrategie n(s).

4. Informationsgehalt einer Teststrategie, minimale Abbruchkriterien.

Beobachten wir einen Lebensdauertest nach einer Teststrategie (n(s),S) bis maximal zum r-ten Ausfall so ist dadurch ein meßbarer Raum $(\Omega^r, \tau^r(S))$ gegeben, auf dem eine Familie von Wahrscheinlichkeitsmaßen $(P_\lambda^r)_{\lambda \in \mathbb{R}^+}$ definiert ist. Gesucht ist nun eine solche Zerlegung von Ω^r in einen Annahmebereich A und einen kritischen Bereich K mit $A + K = \Omega^r$ $A \cap K = \emptyset$ und $A, K \in \tau^r(S)$, so daß gilt:

$$\max_{\lambda \leqq \lambda_0} P_\lambda^r(K) \leqq \alpha$$

$$\max_{\lambda \geqq \lambda_1} P_\lambda^r(A) \leqq \beta$$

Es ist offensichtlich, daß dieselbe Zerlegung bei jedem anderen Abbruchkriterium, bei dem der Test erst später abgebrochen wird, ebenfalls möglich ist, insbesondere auch bei einem reinen r-Plan. Nach dem Lemma von Neyman-Pearson ist nun eine optimale Zerlegung von Ω^r im Falle eines r Plans gegeben durch:

$$A = \left\{ (s_1, \ldots, s_r) \in \Omega^r \,/\, s_r > S^* \right\}$$

$$K = \left\{ (s_1, \ldots, s_r) \in \Omega^r \,/\, s_r \leq S^* \right\}$$

wobei S^* so zu wählen ist daß beide Ungleichungen (nach Möglichkeit) erfüllt sind.

Nun ist sofort ersichtlich, daß jeder Versuchsausgang aus A von jedem Versuchsausgang aus K genau dann unterscheidbar ist, wenn das Abbruchkriterium S keinen Versuchsabbruch entweder vor S^* oder vor dem r-ten Ausfall vorsieht.

Andererseits läßt sich zeigen, daß es ein minimales $r = r_o$ gibt und zu diesem ein minimales $S^{\#} = S_o$, so daß die beiden Ungleichungen gerade noch erfüllt werden können. Daraus folgt daß ein kombinierter (r_o, S_o)-Plan, also das Abbruchkriterium:

$$S = \min (s_{r_o}, S_o)$$

ein minimales Abbruchkriterium ist das gerade noch einen Hypothesentest von H_o gegen H_1 mit den geforderten Mindestanforderungen zuläßt. Gleichzeitig ist S_o eine untere Schranke für ein Abbruchkriterium $S = S' = \text{const}$, das dieser Informationsanforderung noch genügt.

Gehen wir von der Voraussetzung aus, daß die Testkosten monoton in S und in r anwachsen, so stellt also : $S = \min (s_{r_o}, S_o)$
im gewissen Sinne ein optimales Abbruchkriterum dar.

Es stellt sich nun die Frage ob es nicht durch eine Anpassung des Abbruchzeitpunktes an den Testverlauf möglich ist wenigstens die Mittelwerte für Testdauer und Zahl der beobachteten Ausfälle wesentlich zu reduzieren, wobei allerdings in bestimmten Fällen wesentlich längere Experimente zugelassen werden müssen.

Dies wird geleistet durch den Likelihoodratio-Sequenztest von Wald /1/,/2/. Man verfolgt dabei den Verlauf des Lebensdauertests an Hand des Likelihoodratios :

$$R^d = \frac{f^d_{\lambda_1}(s_1, \ldots, s_d)}{f^d_{\lambda_0}(s_1, \ldots, s_d)}$$

von Ausfall zu Ausfall. Wenn R sehr hohe Werte annimmt ($R > a (> 1)$) betrachtet man die Alternative $H_1 : \lambda \geq \lambda_1$, für kleine Werte von R ($R < b (< 1)$) dagegen die Hypothese $\lambda \leq \lambda_o$ als richtig und bricht den Test sofort ab sobald $R > a$ bzw. $R < b$ feststeht.
Im Falle $b \leq R \leq a$ wird weitergetestet.

Graphisch kann man sich dieses Vorgehen an Hand des (d,s)-Diagramms veranschaulichen. (Bild 1)

Dabei wird die Zahl der bis zur "Zeit" s beobachteten Ausfälle d(s) aufgetragen über der summarischen Betriebszeit s. In diesem Diagramm sind die Linien R^d = const gegeben durch die Schar paralleler Geraden mit Steigung $m = \frac{\lambda_1 - \lambda_0}{\lambda_1 / \lambda_0}$. Die Anforderungen an den Informationsgehalt werden (in guter Näherung) erfüllt für:

$$a \approx \frac{1-\beta}{\alpha} \qquad \text{und} \qquad b = (\lambda_1/\lambda_0) \cdot \frac{\beta}{1-\alpha}$$

Auch der Sequenztest ist minimal in dem Sinne, daß sich bei weiterer Verkürzung der Informationsgehalt verringert.

5. Optimierung der Komponentenstrategie

Bei der Optimierung der Komponentenstrategie (bei festem Abbruchkriterium) gehe ich aus von dem bereits von Herrn Sellinschegg eingeführten Kostenmodell /3/. Ich nehme an, daß zum Betrieb der Komponenten Hilfseinrichtungen, die Testplätze, erforderlich sind. Die Zahl der zum Einsatz kommenden Test-Plätze n_T bzw. Komponenten n_K sind vor Testbeginn festzulegen. Ausgefallene Komponenten können ohne Zeitverzug durch Reservekomponenten ersetzt bzw. repariert werden.

Die reinen Testkosten setzen sich zusammen aus den Abschreibungskosten für die Testplätze: $C_A \cdot n_T$, den Abschreibungskosten für die Komponenten $C_V \cdot n_K$, den Betriebskosten $C_0 \cdot S$ sowie den zusätzlichen Kosten für ausgefallene Komponenten $C_R \cdot (d(S) - r(S))$ und den Reparaturkosten $C_R \cdot r(S)$. Dabei ist d(S) die Zahl der während der Testdauer beobachteten Ausfälle, r(S) die Zahl der insgesamt durchgeführten Reparaturen. Insgesamt ergibt sich für die reinen Testkosten:

$$K = C_A \cdot n_T + C_V \cdot n_K + C_R \cdot d(S) + C_0 \cdot S$$

Hinzu kommt ein Pönale, das eine Bewertung der Testdauer darstellt:

$$P = C_I \cdot (T(S) - t_0) \ .$$

Als Zielfunktion der Optimierung betrachte ich den Erwartungswert der Summe K + P :

$$Z = C_A \cdot n_T + C_V \cdot n_K + C_R \cdot E\lambda(d(S)) + C_0 \cdot E\lambda(S) + C_I \cdot (E\lambda(T(S)) - t_0).$$

Zu beachten ist, daß zur Bestimmung der Testdauer T(S) die Transformation der Zeitskala rückgängig gemacht werden muß. Dies erfolgt durch die Transformation:

$$t(s) = \int_0^s ds/n \quad (s).$$

Sind n_T und n_K festgelegt, so ist also die Testdauer die einzige Größe über die die Komponentenstrategie noch die Zielfunktion beeinflußt. Bei festem n_T und n_K wird Z offensichtlich minimal, wenn n(s) für alle $s \in (0, S)$ maximal wird. n(s) ist andererseits beschränkt durch:

$$n(s) \leq \max (n_T , n_K - (d(s) - r(s))).$$

Daraus folgt daß für die optimale Komponentenstrategie auf jeden Fall $n(s) = n_T = n_K = \text{const}\ (s)$ und $d(s) = r(s)$ gelten muß. Optimale Komponentenstrategie ist daher unabhängig vom Abbruchkriterium ein reiner E - Plan. Für diesen gilt $T = S/n$. Ich erhalte also die Zielfunktion:

$$Z = (C_A + C_V) \cdot n + \frac{C_I}{n} \cdot E\lambda(S) + C_R \cdot E\lambda(d(S)) + C_o \cdot E\lambda(S) - C_I \cdot t_o.$$

Diese Zielfunktion nimmt ihr Minimum an für jede ganze Zahl n_o für die gilt:

$$1/2 \left(\sqrt{1+4 \cdot \frac{C_I}{C_A+C_V} \cdot E\lambda(S)} - 1\right) \leq n_o \leq 1/2 \left(\sqrt{1+4\frac{C_I}{C_A+C_V} \cdot E\lambda(S)} + 1\right).$$

Zu Bestimmung einer optimalen Teststrategie sind daher noch für die beiden Abbruchkriterien, $S = \min (s_{r_o}, S_o)$ bzw. den Sequenzplan die Erwartungswerte für d(S) und S zu bestimmen, daraus die zugehörige optimale Komponentenstrategie n_o zu berechnen und zu vergleichen für welche der beiden Teststrategien die Zielfunktion den kleineren Wert annimmt.

6. Beispiel für eine optimale Testauslegung

Als Beispiel betrachte ich den bereits von Herrn Sellinschegg behandelten Fall der Na-Pumpen des KNK-Reaktors /3/.

Ich gehe aus von einem Test der Hypothesen:

H_o : Ausfallrate $\lambda \leq \lambda_o = 1/50\ 000\ n^{-1}$

H_1 : Ausfallrate $\lambda \geq \lambda_1 = 2\,\lambda_o$

wobei die Fehlerwahrscheinlichkeiten $\alpha = \beta = 0{,}05$ eingehalten werden soll.

Bild 1 zeigt die minimalen Abbruchkriterien, mit denen sich diese Forderungen gerade noch erfüllen lassen. Die hohen Werte von mindestens 23 Ausfällen die, bzw. einer Testdauer von 15,7 * 50 000 h während der, zu beobachten ist zeigen, daß die verlangte Testinformation außerordentlich groß ist (höher als die ähnlich laufende Forderung von Herrn Sellinschegg an die mittlere Länge des Konfidenzintervalls).

Mit den Kostendaten von Herrn Sellinschegg ergibt sich als optimale Komponentenstrategie für einen wahren λ-Wert von ungefähr λ_o im Falle des (r_o, S_o)-Plans ein n_o von 20, im Fall des Sequenzplans von nur 14. Für diese Auslegungen habe ich die Erwartungswerte der reinen Testkosten und der Testdauer berechnet und im Bild 2 bzw. 3 aufgetragen über dem wahren Wert der Ausfallrate (normiert auf $\lambda_o = 1$).

Es zeigt sich, daß, abgesehen von einem schmalen Bereich zwischen λ_o und λ_1 der Sequenztest durchweg Resultate liefert die mindestens einen Faktor 2 besser sind als die des (r_o, S_o)-Plans der wiederum besser ist als die von Herrn Sellinschegg betrachteten Pläne.

Literaturverzeichnis

/1/ A. Wald, Sequential Analysis, John Wiley and Sons, 1947.

/2/ B. Epstein und M. Sobel, "Sequential life tests in the exponential case", Ann. Math. Stat., Vol. 26, pp. 82-93, 1955.

/3/ G. Nägele, D. Sellinschegg , "Test Cost Minimization for Reliability Assessment", Proceedings of the Reliability and Maintainability Symposium 1972,San Francisco, U.S.A.

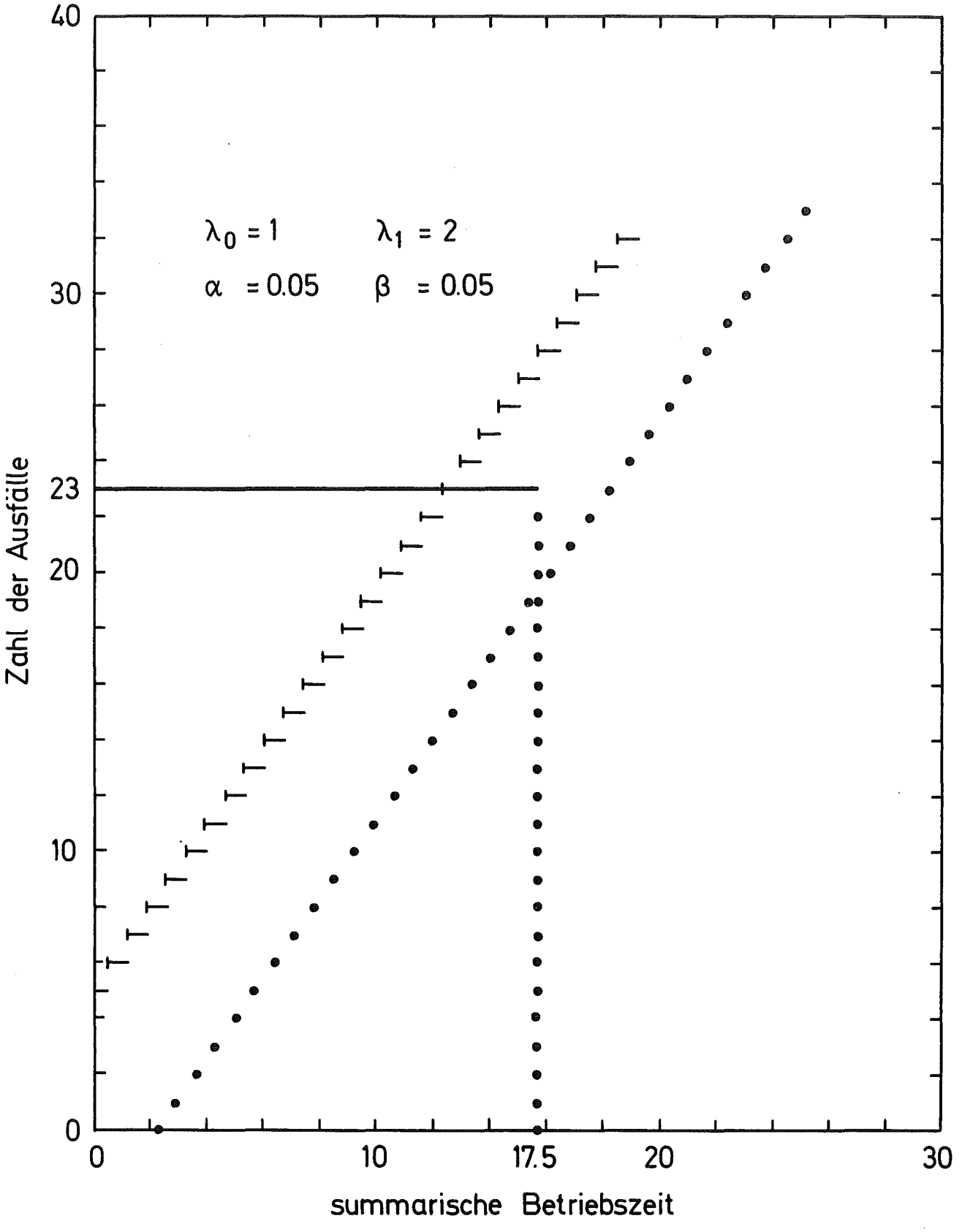


Abb.1 Minimaler (r,S) - Plan und Sequenzplan für gleiche Testinformation

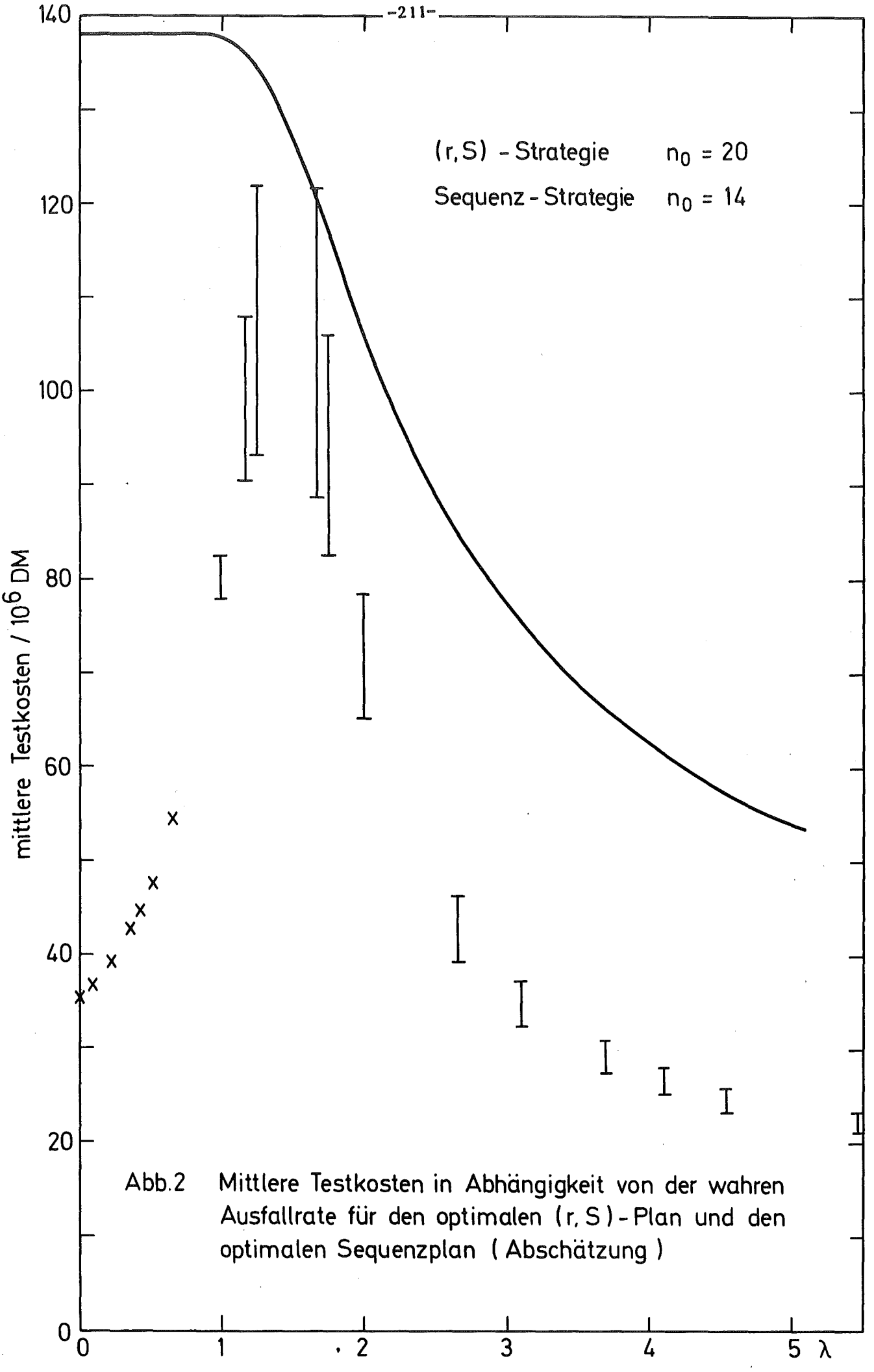


Abb.2 Mittlere Testkosten in Abhängigkeit von der wahren Ausfallrate für den optimalen (r, S) - Plan und den optimalen Sequenzplan (Abschätzung)

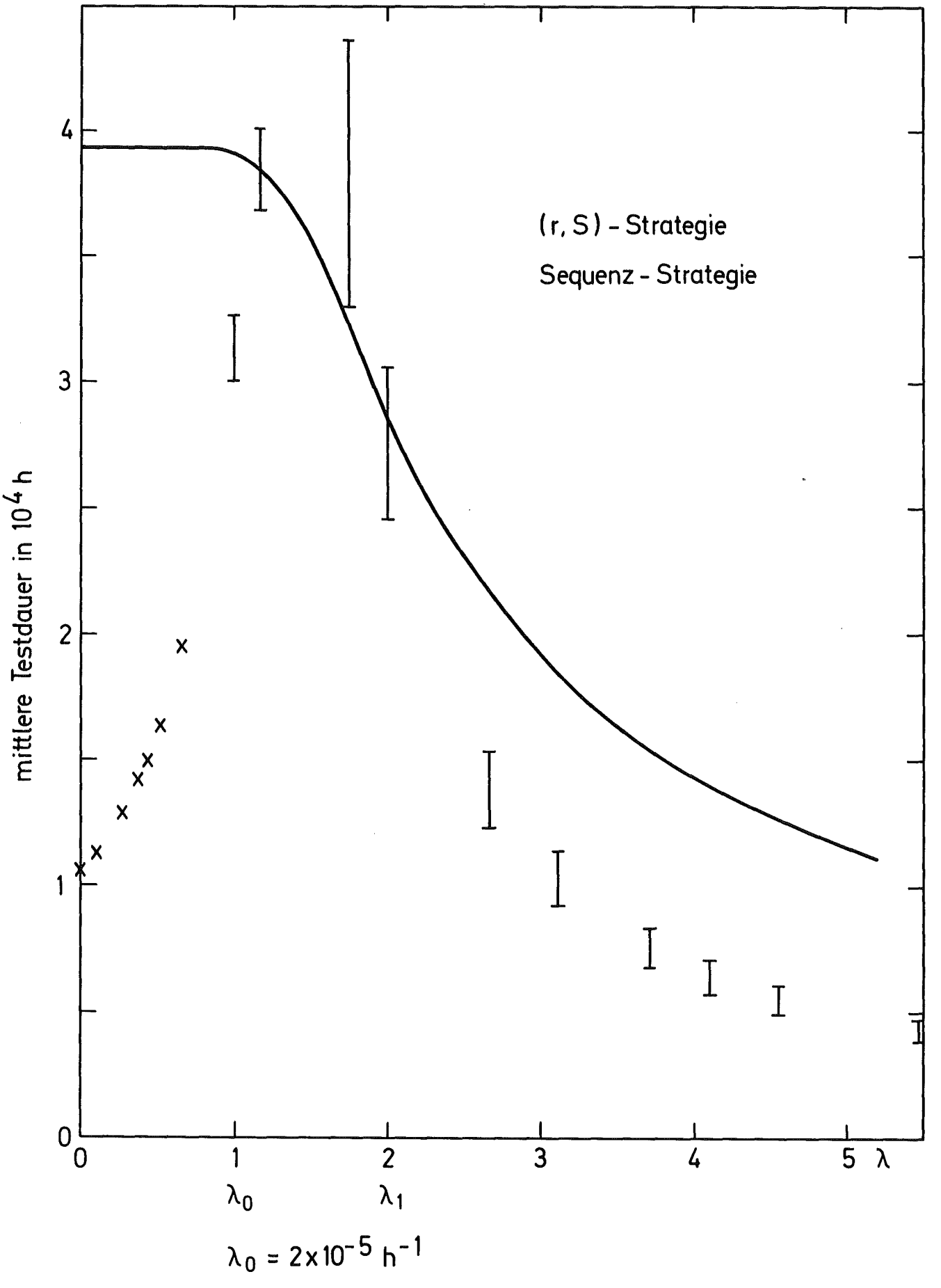


Abb. 3 Mittlere Testdauer in Abhängigkeit von der wahren Ausfallrate

Kapitel 6 : Die Methode der kontinuierlichen Vorhersage der Lebensdauer +)

L. Caldarola

+)"New Definition of Reliability, Continuous Lifetime Prediction, and Learning Processes" (Work presented at the International NATO Conference on Reliability, University of Liverpool, England, 16-27 July, 1973

(see also KFK 1847-EUR 4969 e)

Contents

1. Introduction

Modern technology continuously asks for higher and higher degrees of reliability. Clear examples are the nuclear, airplane and rocket industries, where reliability plays a vital role. No one infact would let a company build a nuclear plant, if it is not possible to demonstrate that the probability of an accident is below the threshold of acceptance. No one would fly in an airplane, if they were not sure that the probability of an accident during the trip was so low, that they would be prepared to accept this risk against the advantage of considerable less travel time than by other more traditional means, such as a train or ship.
The request of reliability is also dictated by economical considerations, which are extremely important to modern society. If one thinks for example of the enormous economical loss due to the unplanned shut down of a 1000 MW electric nuclear power plant for only a few hours, one would immediately recognize that the plant must be designed and operated in such a way that the probability of an unwanted shut down is very low.

A common practice used to improve the reliability of a plant is to build in it redundant systems, which operate only if a given number, above a minimum, of their components is able to operate.

Fig. 1 shows a schematic diagram of a redundant system made with "n" similar components, which functions if at least one component is able to operate. When a component fails, it is repaired (or substituted by a new one) and again put into operation.

Fig. 2 shows the mean time to failure (MTTF) of the system of fig. 1 as a function of the number "n" of its components. The curves of fig. 2 are characterized by the parameter "α", defined as the ratio between the mean time to failure (MTTF) of a component and its mean time to repair (MTTR).

For a given "α", the MTTF of the system increases, in general, with the number "n" of the components, but always less and less, so that, above a certain number of components, it remains practically constant. This means that the gain factor of the system MTTF produced by the last added component decreases with "n", as it is shown more clearly by the curves of fig. 3.

For instance, let us consider the case $\alpha = 200$ of fig. 3. The first redundant component ($n = 2$) increases the MTTF of the system by a factor of 101.5, the

second (n = 3) by a factor of 67 and the third (n = 4) by a factor of about 50, and so on. This shows that redundancy is rewarding only if the number of the components is low, especially if one considers that the cost of the last added component is equal (if not higher because of the more complicated installation problems) to that of the other components.

In addition there are engineering problems (like limited available space, greater complications for the connections between the various components, and for the alarm system which indicates the failure of each component), so that redundancy is usually limited to only few components (2 or 3), especially if these are large in size and expensive (like the Diesel generators for an emergency power supply system). If now one wants to further improve the MTTF of the system, one has two choises:

1. To decrease the MTTR, t_r, of each component
2. To increase the MTTF, t_f, of each component

A reduction of t_r increases α, which in turn increases the MTTF of the system as clearly shown in fig. 2. However this method also has limitations, because there are dead times which cannot be eliminated (like the time for the repairing crew to reach the point where the repair has to be carried out, and the time needed to find out the part of the component, which has actually failed), and because it may be physically impossible to further decrease the effective repair time, after the failed part of the component has been identified.

If we indicate with "t_s" the mean time to failure of the system, for large values of "α" and for $n \ll \alpha$ we have (ref. 1),

$$t_s \cong t_f \frac{\alpha^{n-1}}{n!} = \frac{1}{n!} \frac{t_f^n}{t_r^{n-1}} \qquad (1)$$

If we consider for instance the case n = 3, we get from eq. 1 that if t_r is decreased by a factor of 10, t_s increases by a factor of 100, while if t_f is increased by the same factor of 10, a gain in t_s as large as 1000 results.

This simple numerical example shows that the incentive to increase the MTTF of each component belonging to a system may be even greater than that to decrease the MTTR of the same components. In order to increase the MTTF of a component, one may decide to design a stronger component, but this method may reveal to be either too expensive, or even ineffective if the design has already reached the boundaries of the technology, which is being used. For instance, if one has to design a cylindrical vessel to contain a gas at a given pressure, it can be shown that to increase the wall thickness of the vessel becomes practically ineffective above a certain ratio between the wall thickness and the radius of the vessel. One could of course improve the situation by looking at a better material for the vessel, but this would imply the use of a new technology.

There is however a second method to improve the MTTF of a component, and this consists of predicting the time at which the component is going to fail and in carrying out the necessary repairs, before it fails.
This method is commonly called "preventative maintenance".

Subject of this paper is to show that it is possible to make this preventative maintenance much more effective, by continuously predicting during operation the remaining lifetime of the components.

This method has been called "Continuous Lifetime Prediction" method (CLP), and it is described and discussed in the following sections.

The method of CLP consists in recording during operation the environmental stresses (such as temperature, pressure etc.) applied to a device, in monitoring any useful and significant quantity (for instance vibrations, noise etc.), and in processing continuously the data obtained from these measurements and from eventual tests of the device (during its operation and during its downtime) to predict the remaining lifetime of the device.

Some examples should clarify better the above definition. If we have for instance a mechanical structure which is under creep, we may record continuously the temperature of this structure and the load applied to it.
This data may be used as input to a theoretical model, which describes the creep, to predict the remaining lifetime of the structure.

In the same way in the case of the under carriage or of the wings of an airplane, we may predict more precisely their time of failure due to fatigue if we would use the information obtained by recording the stresses applied to them and their vibrations, which are both stochastic in their nature. Another example may be that of the ball bearings of a pump. The acoustic vibrations may be monitored and, if at a certain frequency range the amplitude exceeds a preestablished level, it follows that the bearing is near to failure and is therefore replaced by a new one (ref. 5).

One may also think of testing during operation from time to time a relay belonging to a redundant system of relays, and decide on the basis of the information gained from the test whether or not to replace the relay with a new one.

In all the four above examples a continuous (or semi continuous) estimation of the remaining lifetime of the device is carried out, which serves as basis for the decision whether or not a preventative repair (or replacement) should be carried out.

The theory of "Continuous Lifetime Prediction", developed in this paper, should greatly assist one in making these preventative maintenance decisions. This is true because it provides the mathematical tool and basic insight necessary for making these decisions.

In addition, as we shall see in the following section, the analysis leads us to the conclusion that the reliability of a device depends upon the degree of knowledge that one has of its characteristics, and of the processes which take place during operation. A new definition of reliability is therefore proposed, and it is given in section 2.

Finally it must be pointed out that the CLP method allows one, during operation, to produce additional information about the device lifetime, which has the same value as that produced by laboratory tests. This is true because the operating conditions are continuously recorded, so that at the end one knows them exactly like it happens in the case of the laboratory tests, where these conditions are controlled. After operation, the device can be made to fail, and the information

gained in this way can be used to increase the knowledge of the device's characteristics and of the processes which have occurred. This gives the possibility of organizing "learning processes", as it will be shown in section 6.

Before closing this introduction we want to inform the reader that in this paper capital letters have been used to indicate the random variables and small letters to indicate a specific value or a specific realization of the same random variable. We shall indicate for example:

$S(t)$ = random variable function of time

$s(t)$ = a realization of the random variable $S(t)$

2. Fundamentals and new definition of reliability

"The failure of a device occurs because of natural laws, and not because blind fate randomly chooses a group of devices and orders them to fail.

Nevertheless the field of reliability has developed as an application of the statistics and of the theory of probability.

The characteristics of a device degrade with time because of some basic chemical, physical or metallurgical processes, which have a known or measurable dependence upon stresses such as temperature, pressure, electrical voltage etc." (Ref. 6).
For this reason one may expect to be able to calculate the exact time of failure of a specific device, if he could know exactly the state of the device, its behaviour under given operating conditions and how these conditions would develop in the future. The reliability would be in this case a discontinuous function of the time ("ideal case" in fig. 4) with the discontinuity at the time of failure. This may be called a deterministic model of the time of failure.

Since we have a limited knowledge of all the facts, we are bound to calculate a spectrum of possible times of failure, and to associate with them a probability density distribution, which is the probability of occurence of failure within an infinitesimal time interval.

In this case the reliability would be a continuous function of time ("real case" in fig. 4).

We now want to formulate a mathematical model for calculating the reliability of a device, starting from its characteristics and operating conditions.

For this reason let us first consider the concept of failure.

We shall say that a device has failed, if it no longer can fulfill the task (for which it was built and installed in the plant) with that degree of accuracy which was foreseen when the plant was designed. Failure is here being used in a rather general context which includes, as one special case, the rupture of a pressure vessel where the term is universally accepted. In general we shall say that an electric resistance has failed, if its value exceeds the limits which are not supposed to be exceeded for a correct operation of the electric circuit in which the resistance is operating.

In the same way we may say that a cylindrical tube has failed if its ovality exceeds the limits which are not supposed to be exceeded for a correct operation of the system to which the tube belongs.

This definition of failure entails the concept of the comparison between the capability (strength) of the device to fulfill its task and the minimum (or maximum) value (reference or load) which the strength can take at the failure. In the case of a pressure vessel, the task is to contain the energy released by an explosion, so that we shall say that the vessel has failed when it breaks. In this example "strength" is understood to be the normal mechanical engineering definition, and "reference" is the minimum allowed value of strength before rupture.

In the case of an electric resistance the "strength" is the value of the resistance and the "reference" is, for example, the maximum value which the resistance is allowed to take before an abnormal behaviour in the circuit of the resistance occurs.

The strength of a device will change in general with time, because the stresses due to environmental conditions (such as temperature, pressure, electric voltage etc.) may produce degradation of the device properties, which reduces the value of the strength. We shall call this change "permanent loss of strength". A change of the strength may also occurr which is "not permanent". This means that this

change is cancelled out, if the stresses again take their initial values.

For a given device, we may therefore identify the following quantities

M = reference or load
Y = initial strength evaluated at design conditions (that is with all the stresses and the reference taking specific values, which are called design values)
L = permanent loss of strength
C = non permanent change of strength

The quantities "M", "L", and "C" may be predictable or stochastic functions of time, while "Y" does not depend upon time. The device will function correctly as long as

$$Y - L + C - M > 0 \qquad (1)$$

The time of failure is the minimum real and positive value of the roots of the following equation

$$Y - L(t) + C(t) - M(t) = 0 \qquad (2)$$

The quantity Y-L in eq. 2 may be called "strength evaluated at design conditions". It is useful to introduce the ratio "N" between the "non permanent change of strength C" and "Y-L", that is

$$C = N\ (Y-L) \qquad (3)$$

In addition we define the quantity "X"

$$X = \frac{M}{1+N} \qquad (4)$$

which we call "effective reference" or "effective load".

Taking into account eqs. 3 and 4, eq. 2 becomes finally

$$Y - L - X = 0 \qquad (5)$$

Eq. 5 contains three quantities, "Y", "L" and "X".

"Y" is a characteristic of the device, which is constant with time, and it is a function of the fabrication process.

"L" is a quantity which depends upon the device's past history (from the time at which the device is put into operation (t=o) until time "t").

"X" is a quantity which depends almost entirely upon the values of the environmental stresses and the reference at time "t". The statistical properties of Y and L may of course influence X (because of N), but this may be considered as a second order effect.

Returning to eq. 5, we can now point out the following

A) If Y is known exactly (Y=y), and L and X are both predictable functions of time, eq. 5 becomes

$$y - \ell(t) - x(t) = 0 \qquad (6)$$

where $\ell(t)$ and $x(t)$ indicate predictable functions of time respectively for L and X.
The minimum real and positive value of "t" which solves eq.6, is the exact value of the time of failure "t_f".

B) If Y is not known exactly, and/or L or X are not predictable functions of time, one finds that the solution of eq. 5 is a random value "T_f" characterized by a probability density distribution, and it is not a particular value "t_f".

The most general case will be that in which Y is a random variable and both "L" and "X" are stochastic functions of time.
In general we have to solve the stochastic equation

$$Y - L(t) - X(t) = 0 \qquad (7)$$

One may solve eq. 7, by considering a large number of randomly chosen combinations of realizations y; $\ell(t)$ and x(t) of Y; L and X, and by solving the resultant deterministic equations (which are similar to eq. 6). For each deterministic equation, one could find the exact solution "t_f", to which one can associate the corresponding value of the probability density distribution obtained by calculating the frequency of occurrence of each value of "t_f". From this distribution one can easily calculate the reliability "R(t)" that is the probability that the sum of three random variables, namely Y; L and X, is larger than "0" during the whole time interval between "0" and "t".

$$R(t) = P \{ Z > 0 \quad \text{during the whole time interval until "t"} \} \tag{8}$$

where

$$Z = Y - L - X = \text{Margin of strength} \tag{9}$$

and "P {..... } " indicates probability.

We can now discuss the definition of reliability.
Barlow and Proshan (ref. 3) in their book, "Mathematical Theory of Reliability" write that "the definition of reliability given in the literature are sometimes unclear and inexact and vary among different writers". At the end they choose the following definition given by the "Radio Electronics Television Manufacturers Association" in the year 1955.

<u>"Reliability is the probability of a device performing its purpose adequately for the period of time intended under the operating conditions encountered".</u>

This definition is incomplete because not all the conditions are specified, and it does not seem adequate because it does not state clearly that the reliability depends upon the knowledge that the estimator has of the phenomena which occur during device operation. In addition the expression "operating conditions encountered" is very vague and may lead to different interpretations.
Let us consider the case in which a population of devices is tested under controlled operating conditions, that is the environmental stresses and loads

are predictable functions of time. An estimator, who is supposed to know in advance the strength distribution of the population, by solving the stochastic equation 7, would calculate the exact distribution of the time of failure measured during the experiment.

Let us now consider the case in which the operating conditions are not controlled. The two extreme subcases exist. Each member of the population is tested under the same stochastic stresses and loads (1) or the applied stresses and loads are derived from the same probability distributions but are uncorrelated (2). For a better understanding consider the following example. Electrical capacitors are operated in parallel under a stochastic voltage (stress), which is identical for all capacitors, and which is artificially produced by means of some probability distributions and a sequence of random numbers. This corresponds to subcase 1. Subcase 2, instead, corresponds to the experiment in which each capacitor is operated independently under a separate stochastic voltage. All the voltages have the same probability distributions, but are produced by different random number sequencies. The two distributions of time of failure which result from the two experiments will be in general different. However the estimator at the initial time, by solving the stochastic eq. 7, is able to calculate the distribution of only subcase 2. In fact he cannot make a distinction between the two subcases, because in subcase 1 he does not know yet which one among all the possible realizations of the stress will occurr.

This indicates that in the most general case it is more appropriate to look for a definition of reliability, which is linked to the degree of knowledge that the estimator has of the device's characteristics, its past history and expected operating conditions. Returning to the case of controlled operating conditions, one can consider the specific device as an individual, and say that its characteristics (for instance its strength) are known to him not exactly but with uncertainty. For example one can regard strength as a random variable "Y-L" characterized by a probability density distribution, which was measured during the past by means of lifetime tests carried out on devices very similar to the specific device which is being considered. This function is therefore the knowledge that the estimator has of the device strength, which is used in eq. 7 to calculate the time of failure. The only alternative to this procedure is that of testing the specific device directly. This would produce the exact

knowledge of the time of failure of the device. But this procedure would imply the destruction of the device, before it can even be used. This means that the exact knowledge of the device's characteristics prior to the operation of the device is impossible to obtain, and that we are bound to assume that the specific device in question will behave in a way similar to that of the other devices which were similarly fabricated and installed, and which previously failed. This is true as long as no technical method exists to make a distinction between the various devices belonging to a given population, without destroying each member of the population. Non destructive preoperational tests usually will only provide more confidence that the device has the same characteristics of the population which was previously operated or tested. The probability density functions of this population can then be applied to calculate the reliability of the device.

The above way of thinking brings us therefore to the conclusion that reliability must be explicitly defined in terms of the knowledge that the estimator (a person or a machine) has of the phenomena which occurr during device operation. The proposed new definition follows.

"The reliability of a device "R(t)" is the calculated probability that the device will perform the required function up to the time "t". This probability depends upon the degree of knowledge of the component's characteristics, of its past history and of the expected operating conditions".

The definition of reliability proposed in this paper seems to be general because it covers all the cases, concise because it is contained in only two short sentences, exact because it is based on a well defined mathematical model, complete because all the conditions are specified so that only one interpretation is possible, and finally clear because it eliminates the misunderstandings between statisticians and engineers, by stating that the probability enters into the picture only as a means to measure the lack of knowledge of the physical processes which are taking place.
Let us now consider the failure rate h(t)

$$h(t) = - \frac{dR/dt}{R(t)} \qquad (10)$$

which may also be defined as the following conditional probability

$$h(t) = \lim_{dt \to 0} \frac{1}{dt} P \quad \{ Z < 0 \text{ between } t \text{ and } t + dt \; / Z > 0 \text{ during the whole time until "t" } \} \qquad (11)$$

In eq. 11 the hypothesis is included that the evaluation of "h" is done at the initial time. In general the device will be replaced (or repaired), when the failure rate reaches a given upper level, above which the operation of the device is considered unsafe. Since the calculation of "h(t)" is performed at the initial time, this decision of the time of repair is taken at that time. Now it usually happens that the time, at which this upper level is reached, is much larger than the time Δt needed to carry out the necessary repair (for instance one year against few days). The repair time "Δt" is intended here to also include planning time for maintenance.
One therefore needs to take the decision only at the time "$t - \Delta t$", which is much nearer to "t".
This means that the failure rate may be evaluated at the time "$t - \Delta t$" and it will therefore be a function of both "t" and Δt.

$$h(t-\Delta t;t) \lim_{dt \to o} \frac{1}{dt} P \left\{ \begin{array}{l} Z < 0 \text{ between "t" and "t+dt"} \,\middle|\, Z > 0 \text{ during the} \\ \text{whole time from } t - \Delta t \text{ until "t" and that the} \\ \text{calculation is carried out at } t - \Delta t \end{array} \right\} \quad (12)$$

From eq. 12 we get

$$\left[h(t-\Delta t;t) \right]_{\Delta t = t} = h(0;t) \quad (13)$$

which is equal to eq. 11, because it indicates that the evaluation of the failure rate is carried out at the initial time.

The advantage of adopting eq. 12 (CLP method) is that now the estimator can use for its calculations all the additional information obtained from the operating past history until the time $t - \Delta t$. We shall see (sect. 4) that the use of this additional information allows one to increase the operating time of the device.
The adoption of eq. 12 implies the continuous recording of the environmental stresses and of the loads applied to the device, the continuous monitoring of some significant quantities (for instance vibrations, noise etc.), and eventually the carrying out of tests from time to time of the device.
The data obtained in this way must then be continuously processed to calculate at each time the probability density distribution of the remaining lifetime of the device. The failure rate h ($t-\Delta t$; t) can be calculated from this

distribution.

For this reason we have called this method "Continuous Lifetime Prediction". Note that the word "continuous" must not be understood "ad litteram". It may suffice that all these measurements and calculations are carried out at time intervals sufficiently small.

We consider again the example of the electrical capacitors which are all operated under the same stochastic voltage (subcase 1), and we suppose now that two persons, which we call respectively A and B, are requested to predict at each time the number of capacitors which will fail in the next time interval "dt". Estimator "A" is assumed to know only the statistical characteristics of the population of capacitors and the stochastic properties of the voltage. Estimator "B" is assumed to be also continuously informed of the voltage applied to the capacitors. Estimator "A" will make his prediction at the initial time and will never change it up to the time "t", because his knowledge will remain unchanged. Estimator "B", instead, will wait until "t" to make his prediction, because at that time he will know all the past history of the electrical voltage until "t" and will take advantage of this additional information in his calculation. For this reason his prediction will be more precise than that of "A". At the initial time therefore, "B" cannot say what his prediction will be, but he can surely say that his prediction, whatever it will be, will be better than that of "A". This leads us to the definition of the failure rate of a device again in terms of the knowledge that the estimator has of the phenomenona which occurr during device operation. The proposed new definition follows.

"The failure rate of a device is the limit of the ratio between the calculated conditional probability that the device with age "t" will fail in the subsequent time interval "dt" and the same "dt" for "dt" tending to zero. This limit is a function of the degree of knowledge of the device's characteristics, of its past history and of the expected operating conditions."

This definition also takes into account the different predictions about the failure rate at a given time which one gets by carrying out the estimations at different times. These estimations will, in general, be different, because the degrees of knowledge associated with each of them will also, in general, be different.

Before closing this paragraph we want to point out that we have purposely limited ourselves to the case in which only one mode of failure can take place in the device.

Some devices have more than just one mode of failure. One should then write a separate equation (such as eq. 7) for each mode of failure. These equations may be eventually correlated in some manner.

In order to avoid mathematical complications, but without any loss of generality, the case of only one mode of failure is developed in this paper.

3. The statistical properties of the initial strength, permanent loss of strength and effective reference

The initial strength "Y" of a device is a random variable, which is characterized by a probability density distribution, $\varphi(y)$, which is measured by testing similar devices produced by means of the same fabrication process. The effective load (or effective reference), X, may be considered as a stationary stochastic function of time.
The permanent loss of strength "L" will be instead a monotonically increasing stochastic function of time.
Let us now consider the rate, V, of the permanent loss of strength

$$V = \frac{dL}{dt} \tag{1}$$

This rate V will, in general, be a function of time, of some stresses, S_n, and of X;

$$V = V\ (t;\ S_1\ .....;\ S_n;\ X) \tag{2}$$

Without any loss of generality, we restrict ourselves to the case of only one stress acting on V

$$V = V\ (t;\ S) \tag{3}$$

The functional link between "V" and the independent variables "t" and "S" is measured by means of laboratory lifetime tests, where the stresses and the load are controlled, that are predictable functions of the time (in most cases constant with time).

In order to evaluate the statistical properties of V (and consequently those of L) we need to know the properties of S. The stress S (like X) may also be considered as a stationary stochastic function of the time. Fig. 5 shows a realization of S as a function of time. We may approximate such a function by means of a sequence of rectangular pulses, each pulse terminating when the next starts (fig. 5). Amplitude "S" and duration "T" of each pulse are random. The following probability density distributions are introduced for S and T;

$\psi(s_1;s)$ = probability density distribution for the transition from the state S = s_1, to the state S = s, when an elementary pulse takes place.

$\lambda(s)\, e^{-\bar{t}\lambda(s)}$ = probability density distribution for the waiting time at the state S = s.

where

$\bar{t}$ = time measured from the beginning of the pulse

$\lambda(s)$ = inverse of the average waiting time at state S = s

For the sake of simplicity, we shall limit ourselves in this paper to the case

$$\psi(s_1;s) = \psi(s) \tag{4}$$

$$\lambda(s) = \lambda = \text{const} \tag{5}$$

The more general case is treated in ref. 2.

The statistical properties of S (and of X), that is " $\psi(s)$" and "λ", can be obtained by analyzing a realization of S, and by making use of the properties of the ergodic functions. This is shown in Appendix 1.

The statistical properties of the permanent loss of strength "L" can now be evaluated from those of the rate "V".
We have from eq. 1

$$L(t) = \int_0^t V(S;t')\,dt' \tag{6}$$

We can develop V(s;t) in a Taylor's series with respect to the time "t"

$$V(S;t) = \sum_{n=o}^{\infty} A_n(S) \cdot t^n \qquad (7)$$

For the sake of simplicity we shall limit ourselves in this paper to the case n = o (linear kinetics). The more general case of eq. 2 is treated in ref. 2. We can therefore write

$$V(s;t) = A_o(S) = V(S) \qquad (8)$$

We can now calculate the probability density distribution of L. This has been done in Ref. 2. Here we have limited ourselves to calculate only the average value of "L" and its variance (Appendix 3)

$$\overline{L} = \overline{V}t \qquad (9)$$

$$\sigma_L^2 = \frac{\sigma_v^2}{\lambda^2}\left(\lambda t + e^{-\lambda t} - 1\right) \qquad (10)$$

where

$\overline{L}$ = average value of L

$\overline{V}$ = average value of V = $\int_o^{\infty} \bar{V}(s)\,\varphi(s)\,ds$ (11)

σ_L^2 = variance of L

σ_v^2 = variance of V = $\int_o^{\infty} [V(s) - \bar{V}]^2\,\varphi(s)\,ds$ (12)

Higher moments of "L" can be calculated by procedures similar to that shown in Appendix 3.

However for the sake of simplicity we have assumed in this paper the Gamma distribution as an appropriate approximation of the exact probability density distribution g(l;t) of "L" and therefore (ref. 4),

$$g(l;t) \cong \frac{1}{\beta^{\alpha+1}\,\Gamma(\alpha+1)}\; l^{\alpha} e^{-l/\beta} \tag{13}$$

The parameters α and β must be chosen in such a way, that the average value and the variance of the Gamma distribution satisfy respectively eqs. 9 and 10. We have therefore,

$$\beta(\alpha+1) = \bar{V}\cdot t \tag{14}$$

and

$$\beta^2(\alpha+1) = \frac{\sigma_v^2}{\lambda^2}\left(\lambda t + e^{-\lambda t} - 1\right) \tag{15}$$

which can be solved to obtain $\alpha(t)$ and $\beta(t)$.

Returning to eq. 10, we see that " σ_L^2 " is given by the product between a constant σ_v^2/λ^2 and a function of the time

$$f(t) = \lambda t + e^{-\lambda t} - 1 \tag{16}$$

This function is shown in fig. 6. It starts with the value "0" at time t=0, and it tends to increase first with the square of the time and later linearly for large values of time.

This suggests the following.

If one records the stress S up to the time "t $-\Delta t$" at which the evaluation of "L(t)" is carried out, the function"L' up to this time can be evaluated exactly.
This means that the variance of L at time "t $-\Delta t$" is zero.
In the case of linear kinetics the variance σ_L^2 of $\Delta L = L(t) - L(t-\Delta t)$ will be given by

$$\sigma_L^2 = \frac{\sigma_v^2}{\lambda^2} f(\Delta t) \tag{17}$$

where

$$f(\Delta t) = \lambda \Delta t + e^{-\lambda \Delta t} - 1 \tag{18}$$

This means that, if one records the stress S, one is in a position at time t $-\Delta t$ to reduce the value of σ_L^2 (eq. 17) because one uses the additional information recorded during the time interval between "0" and t $-\Delta$ t.

The same reasoning may be applied to the calculation of the higher moments, and we can conclude that the distribution of $\Delta L = L(t) - L(t-\Delta t)$ calculated at the time t $-\Delta$ t is given by

$$g(\ell; \Delta t) \cong \frac{1}{\beta^{\alpha+1} \Gamma(\alpha+1)} \ell^{\alpha} e^{-\ell/\beta} \tag{19}$$

with

$$\beta(\alpha+1) = \bar{V}\cdot\Delta t \tag{20}$$

and

$$\beta^2(\alpha+1) = \frac{\sigma_v^2}{\lambda^2}\left(\lambda\cdot\Delta t + e^{-\lambda\Delta t} - 1\right) \tag{21}$$

Eq. 19 gives the distribution of "ΔL" in the case that the rate V at time $t - \Delta t$ is unknown. If we suppose now that the stress S is known at that time ($S(t-\Delta t) = s$), the rate of loss of strength will be also known ($V(t-\Delta t) = v$), and the conditional density distribution $\varphi(l;\Delta t; v)$ defined by eq. 22, will be given by eq. 23 (see also Appendix 4)

$$\varphi(l;\Delta t;v) = P\{\Delta L = l \text{ at } t \;/\; V(t-\Delta t) = v\} \tag{22}$$

$$\varphi(l;\Delta t;v) = e^{-\lambda\cdot\Delta t}\,\delta(l-v\Delta t) + \lambda\int_0^{\Delta t} e^{-\lambda t_1}\cdot g(l-vt_1;\Delta t-t_1)\,dt_1 \tag{23}$$

where "δ" indicates the impulse function.

It is interesting to point out the particular case

$$\text{For } \lambda\cdot\Delta t \ll 1 \qquad \varphi(l;\Delta t;v) \longrightarrow \delta(l-v\cdot\Delta t) \tag{24}$$

The following equation must be satisfied

$$\int_0^\infty \varrho(\ell;\Delta t;v)\cdot q(v)\,dv = g(\ell;\Delta t) \qquad (25)$$

where

q(v) = probability density distribution of V

Eq. 25 is of course satisfied only in the case in which the exact distribution $g(\ell;\Delta t)$ is used in eq. 23. The demonstration is given in ref. 2.

In the case of the CLP method the conditional probability density distribution $\varrho(\ell;\Delta t;v)$ is used to calculate the failure rate. In the case instead "without CLP" the probability density distribution $g(\ell;t)$ must be used, because the rate of the permanent loss of strength is unknown.

4. The particular case of constant reference

In the case of constant reference (X = x = const.), eq. 5 of section 2 is reduced to

$$Z = Y - L - x = 0 \tag{1}$$

Since Y does not depend upon the time and L is a monotonically increasing function of the time, we can write for the failure rate

$$h(t-\Delta t;t) = \lim_{dt \to 0} \frac{1}{dt} P\left\{ \begin{array}{l} Z > 0 \text{ between } t \text{ and } t + dt / Z > 0 \text{ at } t \text{ with} \\ \text{the calculation being carried out at } t - \Delta t \end{array} \right\} \tag{2}$$

If Y and L are statistically independent, we have in the case of linear kinetics

$$h(t-\Delta t;t) = - \frac{\int_{y_{min}}^{y_{max}} \varphi(y) \cdot \left[\int_0^{y-(l+x)} \frac{\partial \rho(l';\Delta t;v)}{\partial \Delta t} \, dl' \right] dy}{\int_{y_{min}}^{y_{max}} \varphi(y) \left[\int_0^{y-(l+x)} \rho(l';\Delta t;v) \, dl' \right] dy} \tag{3}$$

where

y_{min} = minimum value of the random variable Y estimated at the time $t - \Delta t$

y_{max} = maximum value of Y

v = value of V estimated at the time $t - \Delta t$

l = value of L estimated at "$t - \Delta t$"

Let us look at fig. 7. At the time $t - \Delta t$, if the device has not yet failed, we must have

$$Y > y_{min} \tag{4}$$

with

$$y_{min}\ (t - \Delta t) = x + l(t - \Delta t) \qquad \text{if } y_{min} > y_{min}(o) = y_o \tag{5}$$

otherwise

$$y_{min} = y_o \tag{6}$$

where $l(t - \Delta t)$ is the known permanent loss of strength calculated at "$t - \Delta t$".

This explains why the density distribution of Y at the time $t - \Delta t$ is given by

$$\frac{\varphi(y)}{\int_{y_{min}}^{y_{max}} \varphi(y)\, dy} \tag{7}$$

We introduce now in eq. 3 for $\varrho(l; \Delta t; v)$ the expression given by eq. 23 of section 3. This has been done in the Appendix 5.

In this section we consider the expressions of only two particular cases

1st Case — Without CLP

$$\bar{h}(0;t) = \frac{\int_{y_o}^{y_{max}} \varphi(y) \left[\int_0^{y-x} \frac{\partial g(l;t)}{\partial t}\, dl \right] dy}{\int_{y_o}^{y_{max}} \varphi(y) \left[\int_0^{y-x} g(l;t)\, dl \right] dy} \tag{8}$$

2nd Case — With CLP and $\Delta t \ll \frac{1}{\lambda}$

$$h(t-\Delta t;t) = \frac{\varphi(y_{min} + v \cdot \Delta t)}{\int_{y_{min}+v\cdot\Delta t}^{y_{max}} \varphi(y)\, dy} \tag{9}$$

We want now to compare the results obtainable by applying eq. 8 with those obtainable by applying eq. 9.

Since the values which "y_{min}" and "v" will take at the time "t" are not known at the initial time, the failure rate defined by eq. 9 is stochastic. This means that the minimum time, at which this failure rate reaches a preestablished value h_1 satisfies the stochastic equation

$$V \frac{\varphi(Y_{min} + V \cdot \Delta t)}{\int_{Y_{min}}^{y_{max}} \varphi(y)\, dy} = h_1 \qquad (10)$$

We shall therefore speak of a distribution of the minimum time at which the level h_1 is reached.

If we choose $y_o = x$, eq. 6 will always apply.

Eq. 10 has been calculated in the special case $\Delta t = o$. The numerical values of the parameters are given in Appendix 6. The results are shown in fig. 8 (curve 2, with CLP). Here the time in abscisse is the expected time (probabilistic) at which the level "h" of failure rate is reached for the first time.

The case "without CLP" given by eq. 8 is also shown in fig. 8 (curve 1). In this case the time on the abscisse is the deterministic time. In fig. 8 the time is measured in absolute units.

We set now the maximum acceptable level of the failure rate at 10^{-7} per unit of time, because the operation above that level is considered to be unsafe. Referring to the curve 1 (without CLP), we say that we shall replace the device at time 0.43, because initially we calculate a failure rate which at time 0.43 will reach the level of 10^{-7} per unit of time.

Referring to the curve 2 (with CLP) we say instead that we shall probably replace the device at time 0.78, because initially we expect that we shall calculate at that time a failure rate which reaches the level of 10^{-7} per unit of time.

We conclude therefore that the time of replacement is deterministic in the case "without CLP" and probabilistic in the case "with CLP".

On the other hand we shall have instead a probabilistic loss of strength (degree of wearout) at the time of replacement in the case "without CLP", because we calculate only once and initially the expected loss of strength at the time of replacement.
In the case "with CLP" we shall have instead a deterministic degree of wear-out, because we shall calculate at each time the exact loss of strength which has already occurred.

We have seen from the curves of fig. 8 that, for a given level of the failure rate, the use of the CLP method may increase considerably the operating time of the device (from 0,43 to 0,78). This is due only to the fact that with this method one has a better knowledge of the state of the device and one can therefore more completely utilize the device's strength.

In order to better understand this point, let us look at fig. 9. At time t=0 we have a density distribution $\varphi(y)$ with an average value $\overline{Y}$ and a variance σ_y^2. If we now consider the case without CLP, the distribution of Y-L at time $t > 0$ will be brooder than $\varphi(y)$, because the variance now includes that due to L, which, as seen in section 3 (fig. 6), increases with time.
In the case "with CLP", the variance instead remains constant, because the variance due to "L" is equal to zero. In addition the information is used of the rate "V" of the permanent loss of strength, which is calculated from the stress S, which is measured.

5. The CLP method as a policy for preventative maintenance and as a means to detect correlations among failures of different devices

We have seen in section 4 that, for a maximum acceptable failure rate level, the use of the CLP method may allow the operation of the same device for a time longer than it would be allowed in the case "without CLP".

We now want to compare the different types of maintenance policies. For this reason let us refer to the table of fig. 10. In this table "Δt_m" indicates the time interval between the time at which the decision to carry out the replacement is taken, and the time at which the replacement is effectively carried out.

One may define three types of maintenance policies, namely

1. Normal Maintenance
2. Preventative Maintenance without CLP
3. Preventative Maintenance with CLP

In the case of "normal maintenance", the device is replaced when it has failed. This means that its degree of wearout is complete (because it has failed) and deterministic (because the failed state is a very determined state). The time of replacement is probabilistic, because we don't know the exact time at which the device will fail. The time interval Δt_m is equal to zero, because failure, decision and replacement all occur at the same time. The basic parameter is the estimated time of failure, because it allows one to calculate the expected number of devices which shall be replaced in a given operating time interval.

In the case of preventative maintenance without CLP, the device is replaced before failure. This means that its degree of wearout is less than complete. The time of replacement is deterministic, because it is planned in advance.

This in turn gives a probabilistic degree of device wearout, because the wearout is not known exactly at the time of replacement. The time interval Δt_m between decision and replacement is equal to the whole maintenance interval. The basic parameter is the failure rate at the time of replacement, because the time of replacement is chosen as the time at which the failure rate reaches a preestablished level.

In the case of preventative maintenance with CLP, the device is replaced before failure, but at a time which is probabilistic in its nature. The degree of wearout is less than complete, and deterministic. This in turn gives a probabilistic time of replacement. The time interval Δt_m is equal to zero, because decision and replacement occurr both at the same time, which is the time at which the degree of wearout reaches a level above which the operation of the device is considered to be unsafe at the operating conditions encountered. The basic parameter is the estimated time at which the failure rate reaches a preestablished level, because this is the probable time at which the replacement will be carried out.
It is interesting to point out that this type of maintenance is preventative, because the device is replaced before failure, but it is very similar to the normal maintenance because in both cases the time of replacement is probabilistic and the degree of wearout deterministic.

The CLP method gives one also the possibility of detecting in a complex plant the correlation between the failure (cause) of a device and the change (effect) of the stress applied to another device belonging to the plant. The cause may also be a change of the environmental conditions external to the plant.

It has been often observed that a device shows during operation a failure rate higher than that measured during lifetests carried out with the same environmental conditions as the ones the device experiences during normal operation. It may infact happen that, due to the failure (or malfunction) of another component in the plant, the device in question is exposed for some time to stresses and/or loads which are higher than those which were foreseen.
Consider, for instance, the case of an engine of a motorcar where the lubrication oil is cooled by water which in turn is cooled by means of an air fan.

If the belt (which links the main shaft to that of the fan) fails, the oil temperature (stress) will raise and the bearing of the main shaft will suffer a higher rate of wearout. If now the driver does not notice the failure of the belt and continues to drive the car, the bearing will also fail and the engine will stop. The driver will examine the engine and will easily discover the correlation between the failure of the belt and that of the bearing. However, it may also happen that the driver notices the failure of the belt before the bearing fails, and stops the engine. In this case the bearing will suffer, during the time in which the car is driven with the belt broken,

partial damage larger than it would have suffered if the belt would have not failed. The driver will replace the belt and start the engine again. It may now happen that the bearing, due to the higher partial damage already suffered, will fail before it is expected to fail. The driver will conclude that the failure rate of the bearing is higher than that obtained during the laboratory lifetests, but in general he will not be able to correlate the increased failure rate of the bearing to the failure rate of the belt, especially if the engine is very complex, and the failure of many components may effect the failure rate of the bearing.
If the engine is now provided with two recorders which record respectively the time of failure of the belt and the oil temperature (as is the CLP method), the driver, by analyzing both the records, will find out the correlation between the increase of the bearing failure rate and the failure rate of the belt.
Analysis using traditional fault trees is unsuitable for studying such correlations, because the failures of two (or more) devices are supposed either to be uncorrelated (independet) or completely correlated (dependent), that is if the first device fails the second fails too.

For this reason a new technique which can analyze this type of correlation must be developed, in which each device should be deseribed by its margin of strength (eq. 9 of section 2).

6."Integrated Learning Processes"

The adoption of the CLP method on a large scale gives the possibility of organizing learning processes where the knowledge of the manufacturer and user of a given device merge together. In these processes, which may be called "integrated learning processes", the knowledge is produced in the laboratory for lifetests and in the user's plant and is stored in the information bank, which is a computer.

In the case of replaceable devices, new (not yet used) devices will be tested only initially in order to provide sufficient knowledge to render the devices operationabl Later, since the preventative maintenance policy will be currently adopted, lifetests will be carried out preferably on used devices, which were dismissed before failure after having been used for the allowed length of time. It turns out in this case that the learning process takes the form of a cycle. The cycle begins when a new device starts operation in the user's plant, and ends when the information gained from the lifetests, carried out in the laboratory on the same device (now called "used device"), reaches the user through the "bank". Information will be produced continuously, and the speed of learning will be proportional to the flow of devices in the cycle, that is to the ratio between the number of devices present in the cycle and their residence time in the cycle.

Fig. 11 shows a schematic diagram of an integrated learning process. The manufacturer may be for example a firm which produces ball bearings and the user may be an air company (like Lufthansa) or an electricity producer (like the R.W.E.). Solid lines in the diagram indicate flows of materials, while the dotted lines indicate flows of information. The manufacturer "A" gives a sample of new devices to the laboratory for lifetime tests. The information gained from these tests together with that coming from the manufacturer is stored in the "bank", where is processed and made available to the user "B", who buys the device from A. The user B operates the device for a length of time, which is determined by the value of the reliability imposed upon him, and then replaces the device with a new one, before it fails. The used device is then given to the laboratory, while the information on the operating experience of the device is given to the bank. The laboratory will perform a lifetime test of the used device and will give the information gained from these tests to the bank. Information about devices which

eventually fail during operation in the user's plant is also given to the bank. All the information stored in the bank about a given device is available to the laboratory, to A and to B.

It is important to point out that with the system of Fig. 11 only a limited amount of new devices must be sacrificed initially in order to get an initial amount of knowledge about the characteristics of the device. Later, further new device tests are not needed. The used devices will be tested, and the information gained from these is as good as that obtained from the new one, because, due to the application of the CLP method, the full operating history of the used devices is made available from the user to the bank.

It follows (Fig. 11) that the integrated learning process takes the form of a cycle. The new devices enter the cycle at "M", where they start to be operated in the plant owened by the user. After being operated, the devices are given to the laboratory, where they are brought to failure, in order to produce information. The information is given from the bank to the user, which will use it to decide the operating time of the new devices arriving at M. A new cycle characterized by a higher level of knowledge starts, and the process can be repeated continuously and indefinitely. A secong path is possible, with which the user is by-passed. This is the path LN, where the new devices are given directly to the laboratory, which will be especially used at the beginning to obtain initial information.

In addition the "bank" will provide a means to quickly diagnose devices that need improvement, and provide information for their redesign.

Fig. 12 qualitatively shows various paths of a learning process by giving the allowed operating time of a device as a function of the time.
A path which has been considered is that indicated with OBDE. This would correspond to the case in which the operation of the devices is started after one has obtained their reliability by means of lifetests performed on new devices over the time interval OB. At the time corresponding to the point B the knowledge has been gained which would allow one to operate the device in the user's plant up to the final value of its operating time with the associated maximum allowed value of the failure rate. This would correspond in Fig. 11 to the case in which only the path LN is used. This learning process is very safe, but it may also be very expensive.

If instead, one makes use of the path LN (Fig. 11) only at the beginning to acquire an initial knowledge and then takes advantage of the cycle (Fig. 11) by making lifetests on the used devices, one would get a path in Fig. 12 of the type OFGCE. New devices will be tested (path LN in Fig. 11) until the time corresponding to the point F is reached. At this time, for a given maximum value of the failure rate, the allowed operating time of each device is lower than its final value.

The allowed operating time now increases with time (GC in Fig. 12) because of the knowledge continuously gained by means of the lifetests on the used devices (cycle in Fig. 11).

For a given maximum failure rate there is a family of learning paths of the type OFGCE, which may be obtained by properly choosing the stress levels in the laboratory for lifetests (accelerated tests). The learning path also depends upon the number of devices which are put into operation. Among all possible paths belonging to a given family, the most economical path should be chosen.

7. Conclusions

In ref. 2 the author has developed a more complete theory, which includes also the case where the reference X is a stochastic function of the time. However, for the sake of simplicity, we have limited ourselves here to a very simple case. The treatment of more general cases would not have added anything new to the concept of preventative maintenance with CLP (section 5) to the discussion on the "integrated learning processes" (section 6) and to the new definition of reliability (section 2), but the additional mathematical complexity would have distracted the reader. For this reason, if the reader is interested in the details of the general theory of reliability calculation from the properties of the device and from its operating conditions, he is referred to reference 2.

We can now close our paper by listing the advantages which derive from the use of the CLP method and of the "integrated learning processes" and the problems which arise by their adoption.

A) Advantages

1. A more precise estimate of the lifetime of devices and systems is possible. Therefore either their reliability and availability is improved, or, for a given reliability, their operating time is increased.

2. The possibility exists of detecting in a complex plant the correlation between the failure (cause) of a device and the change (effect) of the stress applied to another device belonging to the plant. The cause may also be a change of the environmental conditions external to the plant.

3. The learning process is rationalized by ensuring a preestablished maximum allowed failure rate during the whole learning process, and by providing a means to quickly diagnose devices that need improvement and the information for their redesign.

B) Problems

1. The ability to closely reproduce the device's characteristics is required, which in turn asks for high standardization of the fabrication processes.

2. Standardization of the installation methods and of the procedures for repair is also required.

3. Lifetests must be carried out, which allow the measurement of the important parameters. Interpretation of the tests must be done through correct theoretical models.

4. Diagnostic tests during device operation must be developed, because these too may improve the knowledge of the state of the device at a specific time.

5. Development of special instrumentation and special methods for the transmission of the measurements may be needed.

6. The automatic continuous recording and processing of an enourmous quantity of data is also required. Criteria must be developed to decide what should be recorded, what should be recorded and afterward discarded, and how data should be processed.

The higher the degree of reproduceability of a device, the greater the incentive to use the CLP method. Since the fabrication processes continuously improve their degree of reproduceability and since more and more new diagnostic tests are found, one should expect that the CLP method will become in the long range the most powerful tool to improve the reliability and availability of devices and systems.

The application of the "integrated learning processes" will be a revolution in the fields of design, production and operation of technical devices. All the existing human scientific and technical knowledge must be organized in the bank. But more information must be produced at high rates to make these learning processes effective.

To reach the stage, where the application of these integrated learning processes is possible, is a gigantic task, which will require a tremendous coordinated effort in all fields of scientific and technical research.

8. Acknowledgements

The author wishes to thank Professor Kastenberg and Mr. Rumble for their useful comments on this paper and for having improved the english style, and Mr. Wickenhäuser for having carried out the necessary calculations.

9. References

1. Caldarola, Weber, "General criteria to optimize the operation of a power plant with special consideration to its safety requirements, KFK 640 and EUR 3685 e, August 1967

2. Caldarola, "A general theory to calculate the reliability of a device from its characteristics, its past history and from the expected operating conditions", (in preparation)

3. Barlow, Proschan, "Mathematical theory of reliability", John Wiley and Sons

4. Shooman, "Probabilistic reliability: an engineering approach", Mc Graw Hill

5. Bjorn Weichbrodt "Mechanical signature analysis: a new tool for product assurance and early fault detection"
Conference on "Incipient failure diagnosis for assuring safety and availability of nuclear power plants", Gatlinburg-Tennessee, October 30 - November 1, 1967 - USAEC - CONF 671011

6. Stewart, "A causal redefinition of failure rate - Theorems, stress dependence, and application to devices and distributions", IEEE Transactions on reliability, Vol. R-15, No. 3, December 1966

7. Joseph O. Muench, "A complete reliability program", Proceedings Reliability and Mantainability Symposium - San Francisco, California USA 1972

10 Appendix 1

Evaluation of the statistical properties of a stationary and ergodic stochastic function of the time

Let us consider the stationary and ergodic stochastic function of the time S(t).

Fig. 5 shows a realization of "S" as a function of time. We may approximate such a function by means of a sequence of rectangular pulses, each pulse terminating when the next starts (fig. 5). Amplitude "S" and duration T of each pulse are random. The following definitions are introduced;

$\psi(s)$ = probability density distribution that the state S=s will occurr, when a pulse takes place

$\lambda e^{-\bar{t}\lambda}$ = probability density distribution for the waiting time at the state S=s

where

$\bar{t}$ = time measured from the beginning of the pulse

λ = inverse of the average waiting time at any state S = s

The average value $\bar{S}$ can be evaluated by averaging the recorded S(t) over a sufficiently long period of time

$$\int_0^\infty s\psi(s)\,ds = \lim_{t\to\infty} \frac{1}{t}\int_0^t S(t')\,dt' \qquad (1)$$

The term on the left side of eq. 2 is called the "ensemble average" while that on the right side is called the "time average".

They are equal only if the process is ergodic.

For a generic moment of order "n", we can write the equation

$$\int_0^{\infty} (s-\bar{S})^n \psi(s)\, ds = \lim_{t\to\infty} \frac{1}{t} \int_0^t (S(t')-\bar{S})^n dt' \qquad (2)$$

Again the term on the left side is called "ensemble average" and that on the right side "time average".

The time averages can be evaluated from a record of S(t). The distribution $\psi(s)$ can be evaluated by means of the eq. 2 and the series of eqs. 3. An alternative method of evaluating $\psi(s)$ from a record of S(t) may be the following. Let us consider the time intervals t_m during which $S \geqslant s$ (fig. 13).

Clearly for an ergodic process we can write the equation

$$\int_s^{\infty} \psi(s)\, ds = \lim_{t\to\infty} \frac{\sum_{m=1}^{\infty} t_m}{t} \qquad (3)$$

which allows us to evaluate the function $\psi(x)$.
Finally the constant "λ" can be calculated by equating the autocorrelation function evaluated theoretically (ensemble average) to that evaluated experimentally from a record of S(t) (time average) (see Appendix 2).

$$\left[\overline{S^2} - (\bar{S})^2\right] e^{-\lambda \Delta t} = \lim_{t\to\infty} \frac{1}{t} \int_0^t [S(t')-\bar{S}][S(t'+\Delta t)-\bar{S}]\, dt' \qquad (4)$$

11. Appendix 2

Calculation of the autocorrelation function

Let us consider a stationary stochastic function S(t), which is approximated by a sequence of uncorrelated elementary pulses characterized by an amplitude and a duration (fig. 5).

Let us indicate with $\psi(s)$ the probability density function of the amplitude S. The duration of the pulses are assumed to be exponentally distributed with an average value $1/\lambda$ with λ = const.

Let us consider now the joint probability density distribution $\chi(s_1;\ t_1 \text{ and } s_2;\ t_2)$ of the event

$$S = s_1 \quad \text{at} \quad t = t_1 \tag{1}$$

$$S = s_2 \quad \text{at} \quad t = t_2 \tag{2}$$

$$\text{with} \quad t_2 > t_1 \tag{3}$$

where

t = time

t_1 and t_2 being two particular values of the time and s_1 and s_2 being two particular values of the amplitude.

We have

$$\chi(s_1;t_1 \text{ and } s_2;t_2) = \psi(s_1)\, e^{-\lambda(t_2-t_1)}\delta(s_2-s_1) + \left[1 - e^{-\lambda(t_2-t_1)}\right]\psi(s_1)\psi(s_2) \tag{4}$$

where

$$\delta(s_2-s_1) = \infty \quad \text{for } s_2-s_1 = 0 \tag{5}$$

and

$$\delta(s_2-s_1) = 0 \quad \text{for} \quad s_2 - s_1 \neq 0 \tag{6}$$

The autocorrelation function $A(t_2-t_1)$ is given by

$$A(t_2-t_1) = E\left\{ [S(t_1) - \bar{S}\,][S(t_2)-\bar{S}\,] \right\} =$$

$$= \int_0^\infty\int_0^\infty \chi(s_1; t_1 \text{ and } s_2; t_2)\,[s_1-\bar{S}\,][s_2-\bar{S}\,]\,ds_1\,ds_2 \tag{7}$$

where "E" indicates expectation and

$$\bar{S} = \int_0^\infty s\,\psi(s)\,ds \tag{8}$$

Taking into account eq. 4, eq. 7 gives finally

$$A(t_2-t_1) = \left[\,\overline{S^2} - (\bar{S})^2\right] e^{-\lambda(t_2-t_1)} \tag{9}$$

where

$$\overline{S^2} = \int_0^\infty s^2\psi(s)\,ds \tag{10}$$

12 . Appendix 3

Calculation of the variance of the permanent loss of strength

Let us indicate with V(S) the rate of permanent loss of strength.
We have

$$L(t) = \int_0^t V(S(t'))\,dt' \tag{1}$$

where "S" is a stochastic stress applied to the device.
If σ_V^2 is the variance of V and "λ" is the average frequency of occurrence of the elementary pulses which approximate S, the auto-correlation function "A" is given by (Appendix 2)

$$A(t_2-t_1) = \sigma_V^2\, e^{-\lambda(t_2-t_1)} \tag{2}$$

with

$$t_2 > t_1 \tag{3}$$

The variance σ_L^2 is given by

$$\sigma_L^2 = E\left\{ \int_0^t \int_0^{t_2} [V(S(t_1)) - \bar{V}][V(S(t_2)) - \bar{V}]\,dt_1\,dt_2 \right\} \tag{4}$$

where

$\bar{V}$ = average value of V

Eq. 4 can be written as follows

$$\sigma_L^2 = \int_0^t \int_0^{t_2} E\left\{\left[V(S(t_1)) - \bar{V}\right]\left[V(S(t_2) - \bar{V}\right]\right\} dt_1\, dt_2 = \int_0^t \int_0^{t_2} A(t_2 - t_1)\, dt_1\, dt_2 \tag{5}$$

From eq. 5, taking into account eq. 2, we get finally

$$\sigma_L^2 = \frac{\sigma_v^2}{\lambda^2}\left(\lambda t + e^{-\lambda t} - 1\right) \tag{6}$$

The function

$$f(\lambda t) = \lambda t + e^{-\lambda t} - 1 \tag{7}$$

is shown in fig. 6.

13. Appendix 4

Calculation of the conditional probability density distribution of the permanent loss of strength

Let us indicate with $\rho(\ell; \Delta t; v)$ the conditional probability density distribution of the event

$$\Delta L = L(t) - L(t-\Delta t) = \ell \quad \text{at} \quad "t" \tag{1}$$

under the condition

$$V(t - \Delta t) = v \tag{2}$$

where

L = stochastic permanent loss of strength
V = stochastic rate of the permanent loss of strength
t = time
$t - \Delta t$ = time at which the evaluation is carried out

We have

$$\Delta L = v \cdot T + \left[L(t) - L(t - \Delta t + T) \right] \tag{3}$$

where

T = duration of the first elementary pulse (belonging to the sequence of elementary pulses which approximate V) in the time interval between $t - \Delta t$ and t.

By applying the basic theorem of the sum of the probabilities of the mutually exclusive events, we get

$$\varphi(\ell;\Delta t;v) = P\left\{\Delta L = \ell \text{ at } t \,/\, V(t-\Delta t)=v\right\} = P_1 + P_2 \qquad (3)$$

where

$$P_1 = P\left\{\Delta L = \ell = v\Delta t \text{ at } t \text{ and } T \geq \Delta t \,/\, V(t-\Delta t)=v\right\} \qquad (4)$$

$$P_2 = P\left\{\Delta L = \ell \text{ at } t \text{ and } T < \Delta t \,/\, V(t-\Delta t)=v\right\} \qquad (5)$$

Since T is supposed to be exponentially distributed with average value $1/\lambda$, we obtain easily

$$P_1 = e^{-\lambda\Delta t}\,\delta(\ell - v\Delta t) \qquad (6)$$

and

$$P_2 = \lambda\int_0^{\Delta t} e^{-\lambda t_1}\, g(\ell - v t_1 ; \Delta t - t_1)\, dt_1 \qquad (7)$$

where $g(\ell, \Delta t)$ is the probability density distribution of ΔL and "δ" indicates the impulse function.

14. Appendix 5

Calculation of the failure rate

Let us start from eq. 3 of section 4 and eq. 23 of section 3

$$h(t-\Delta t;t) = -\frac{\int_{y_{min}}^{y_{max}} \varphi(y)\left[\int_0^{y-(\ell+x)} \frac{\partial \rho(\ell';\Delta t;v)}{\partial \Delta t}\, d\ell'\right] dy}{\int_{y_{min}}^{y_{max}} \varphi(y)\left[\int_0^{y-(\ell+x)} \rho(\ell';\Delta t;v)\, d\ell'\right] dy} \qquad (1$$

$$\rho(\ell';\Delta t;v) = e^{-\lambda\Delta t}\,\delta(\ell'-v\Delta t) + \lambda\cdot\int_0^{\Delta t} e^{-\lambda t_1} g(\ell'-v t_1;\Delta t-t_1)\, dt_1 \qquad (2$$

where

y_{min} = minimum value of the random variable Y calculated at the time t - Δ t

v = value of V calculated at "t -Δ t"

δ = impulse function

1 = value of L calculated at "t- Δt"

If we put eq. 2 into 1, we obtain

$$h(t-\Delta t;t) = -\frac{v e^{-\lambda\Delta t}\varphi(y_{min}+v\Delta t) - \lambda\int_{y_{min}}^{y_{max}}\int_{0}^{\Delta t}\int_{0}^{y-(x+\ell+vt_1)}\varphi(y)\, e^{-\lambda t_1}\frac{\partial g(\ell';\Delta t-t_1)}{\partial \Delta t}\, d\ell' dt_1 dy}{e^{-\lambda\Delta t}\int_{y_{min}+v\Delta t}^{y_{max}}\varphi(y)dy + \lambda\int_{y_{min}}^{y_{max}}\int_{0}^{\Delta t}\int_{0}^{y-(x+\ell+vt_1)}\varphi(y)\, e^{-\lambda t_1} g(\ell';\Delta t-t_1)\, d\ell' dt_1 dy} \tag{3}$$

In the particular case

$$\lambda\Delta t \ll 1 \tag{4}$$

we have simply from eq. 3

$$h(t;t) = v\,\frac{\varphi(y_{min}+v\Delta t)}{\int_{y_{min}+v\Delta t}^{y_{max}}\varphi(y)dy} \tag{5}$$

In the case "without CLP", the density distribution of "L" is given by the function g (l;t), and we have for "h" the following expression

$$\overline{h}(0;t) = \frac{\int_{y_0}^{y_{max}}\varphi(y)\left[\int_0^{y-x}\frac{\partial g(\ell;t)}{\partial t}\,d\ell\right]dy}{\int_{y_0}^{y_{max}}\varphi(y)\left[\int_0^{y-x} g(\ell;t)\,d\ell\right]dy} \tag{6}$$

15. Appendix 6

Numerical example

The numerical example given in this paper is characterized by the following values of the parameters

$\varphi(y)$ = truncated normal density distribution

$$y_o = 0.1\ \overline{Y} \tag{1}$$

$$y_{max} = 2{,}2\ \overline{Y} \tag{2}$$

$$\sigma_y = 0.04\ \overline{Y} \tag{3}$$

$$\overline{Y} = 1 \tag{4}$$

$$x = y_o \tag{5}$$

The time scale has been normalized by means of a factor

$$\tau = t\,\frac{\overline{V}}{\overline{Y}-x} \tag{6}$$

where

τ = dimensionless time (absolute units)

t = real time

In addition we have

$$\lambda = 10.5\,\frac{\overline{V}}{\overline{Y}-x} \tag{7}$$

and

$$\sigma_V^2 = 0{,}1\ (\overline{V})^2 \tag{8}$$

$$\overline{V} = 0.86 \tag{9}$$

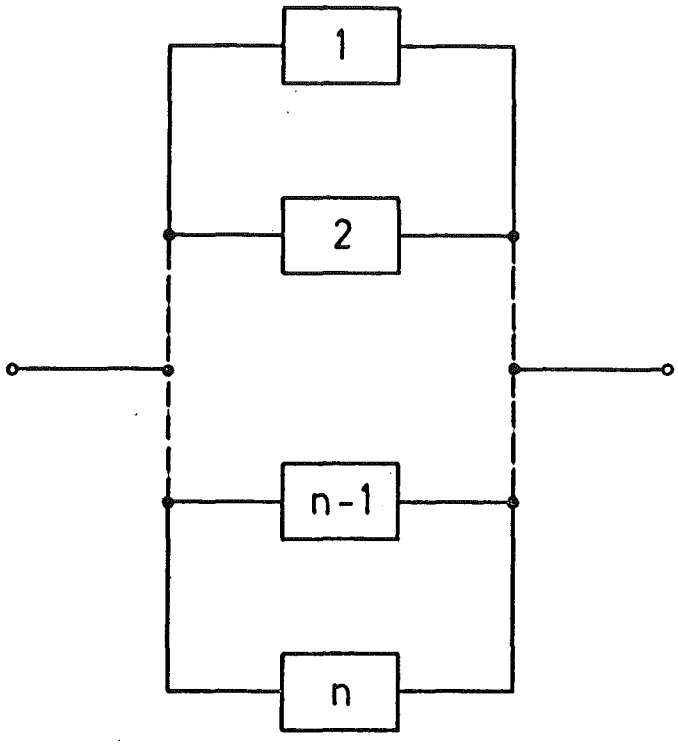


Fig.1 Schematic diagram of a redundant system made of "n" components

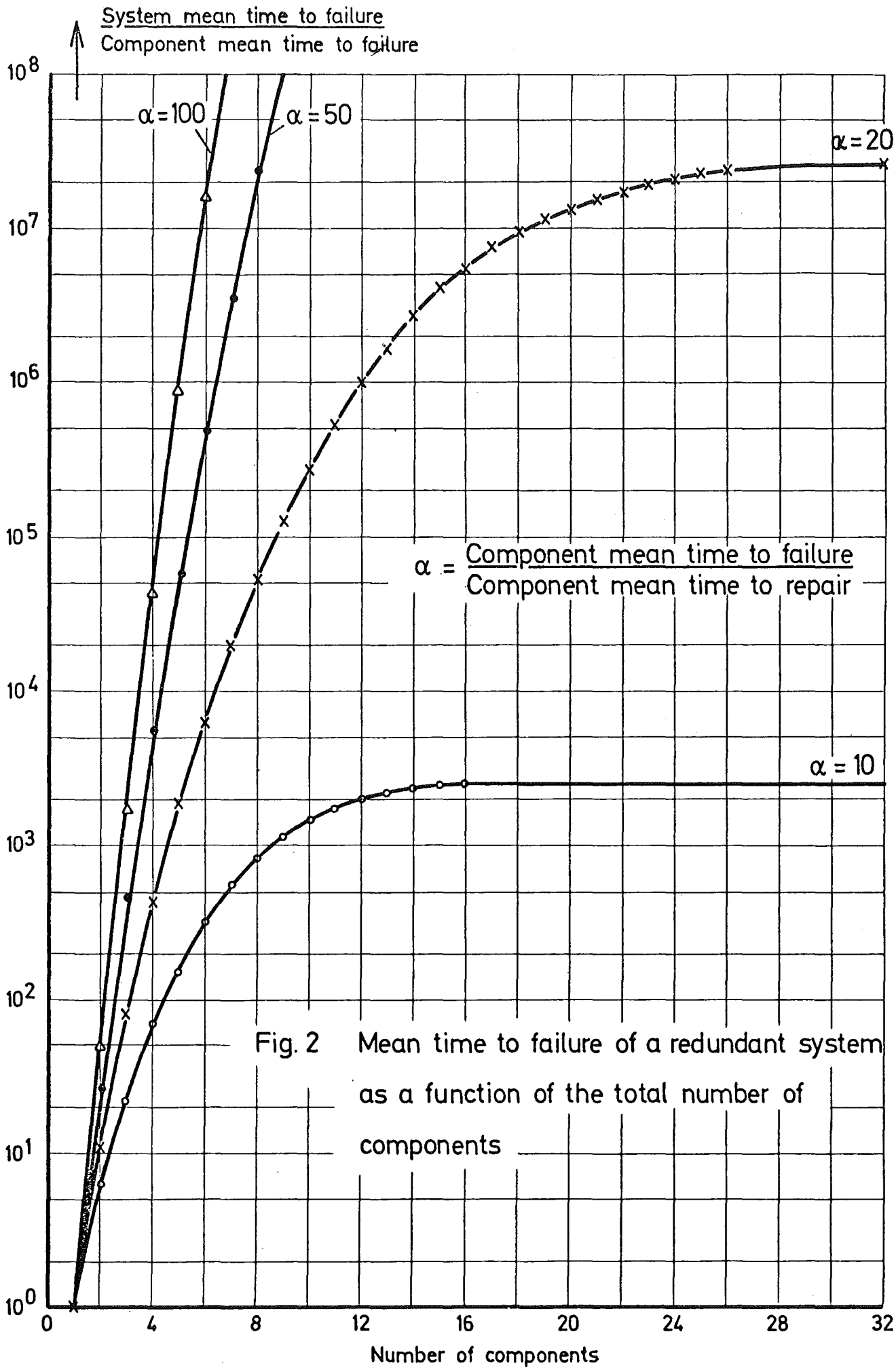


Fig. 2 Mean time to failure of a redundant system as a function of the total number of components

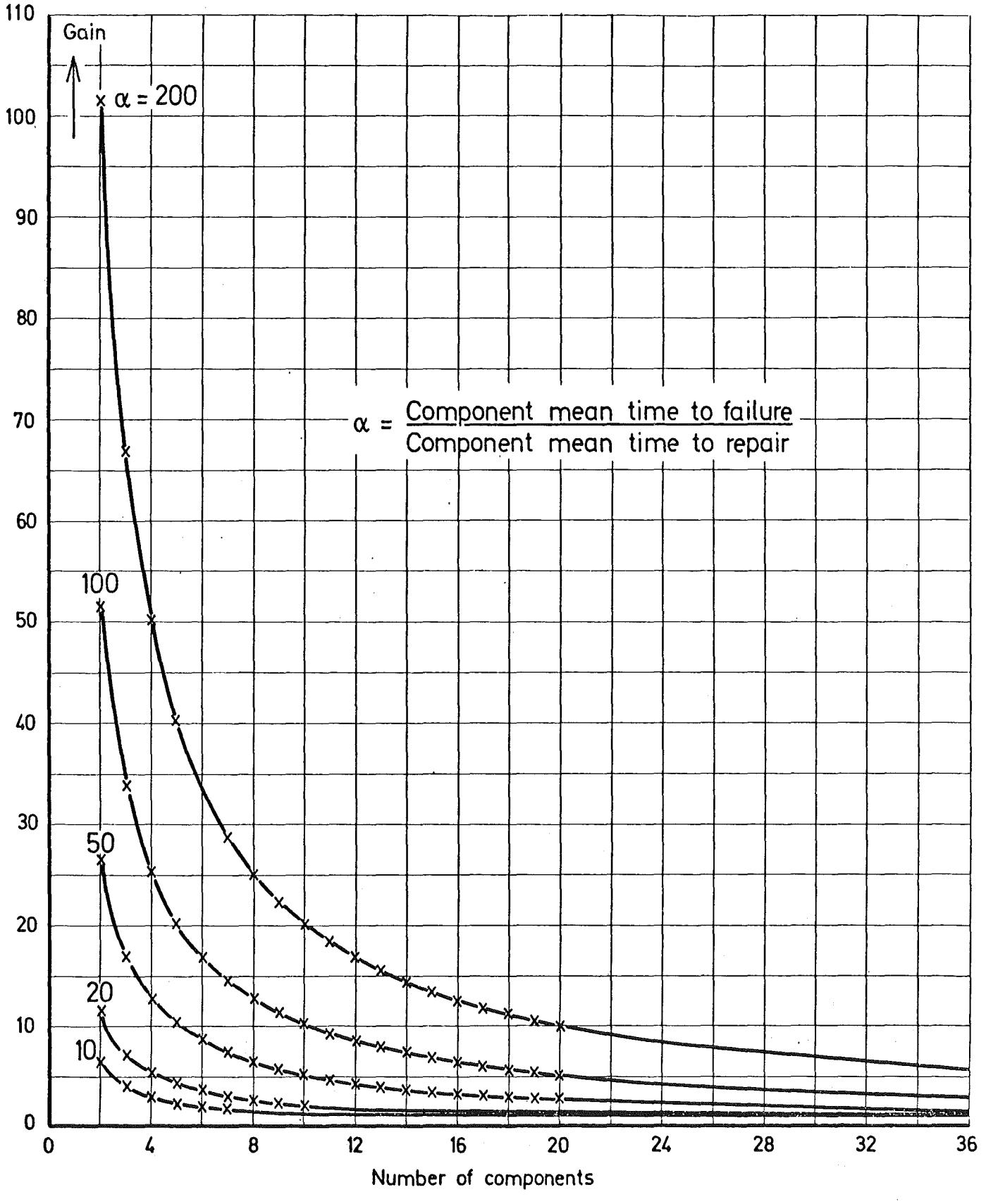


Fig. 3 System lifetime gain produced by the last added redundant component as a function of the total number of components

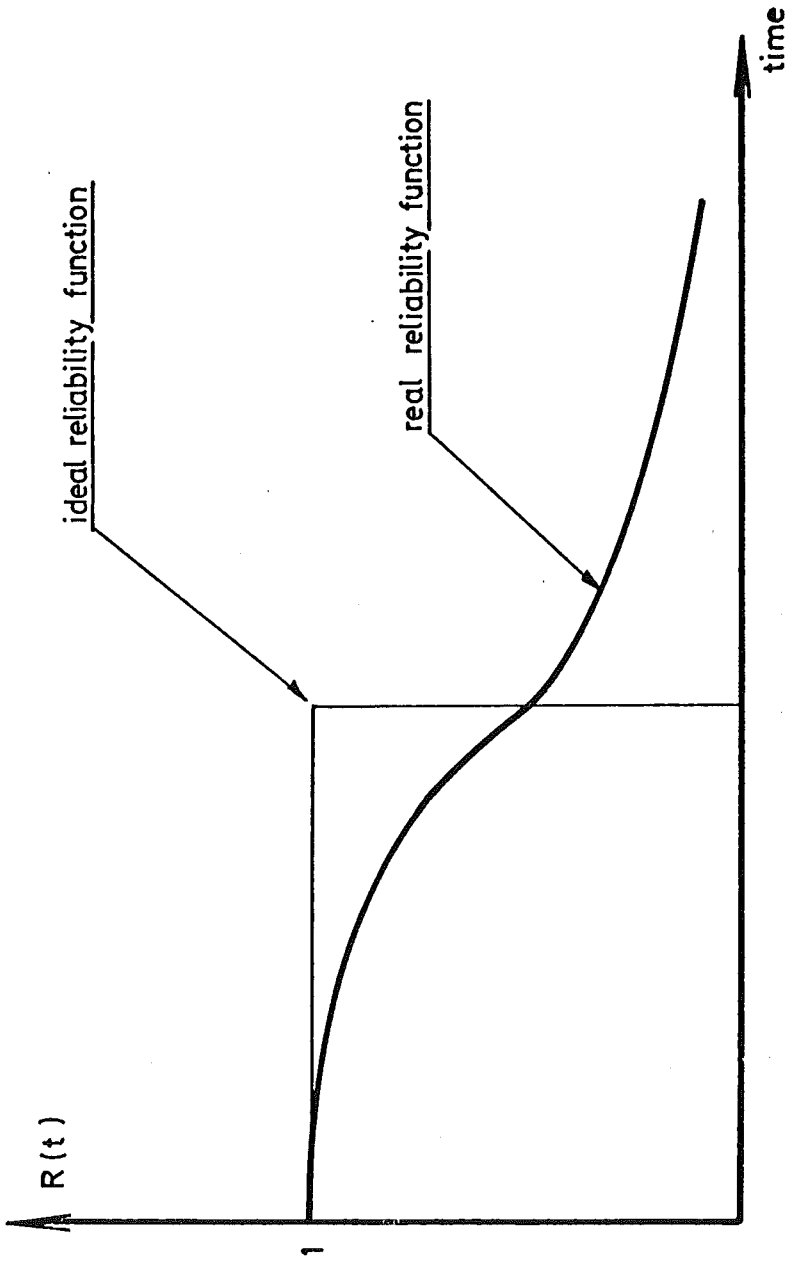


Fig. 4 Real and ideal reliability

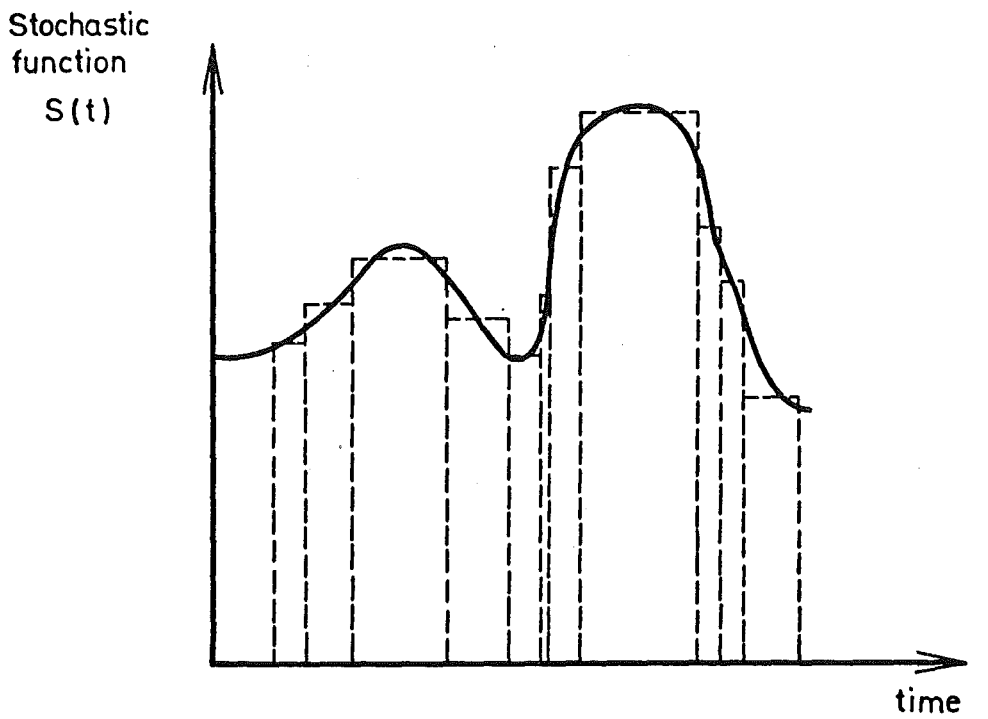


Fig.5 Approximation of a stochastic function by means of a sequence of rectangular pulses

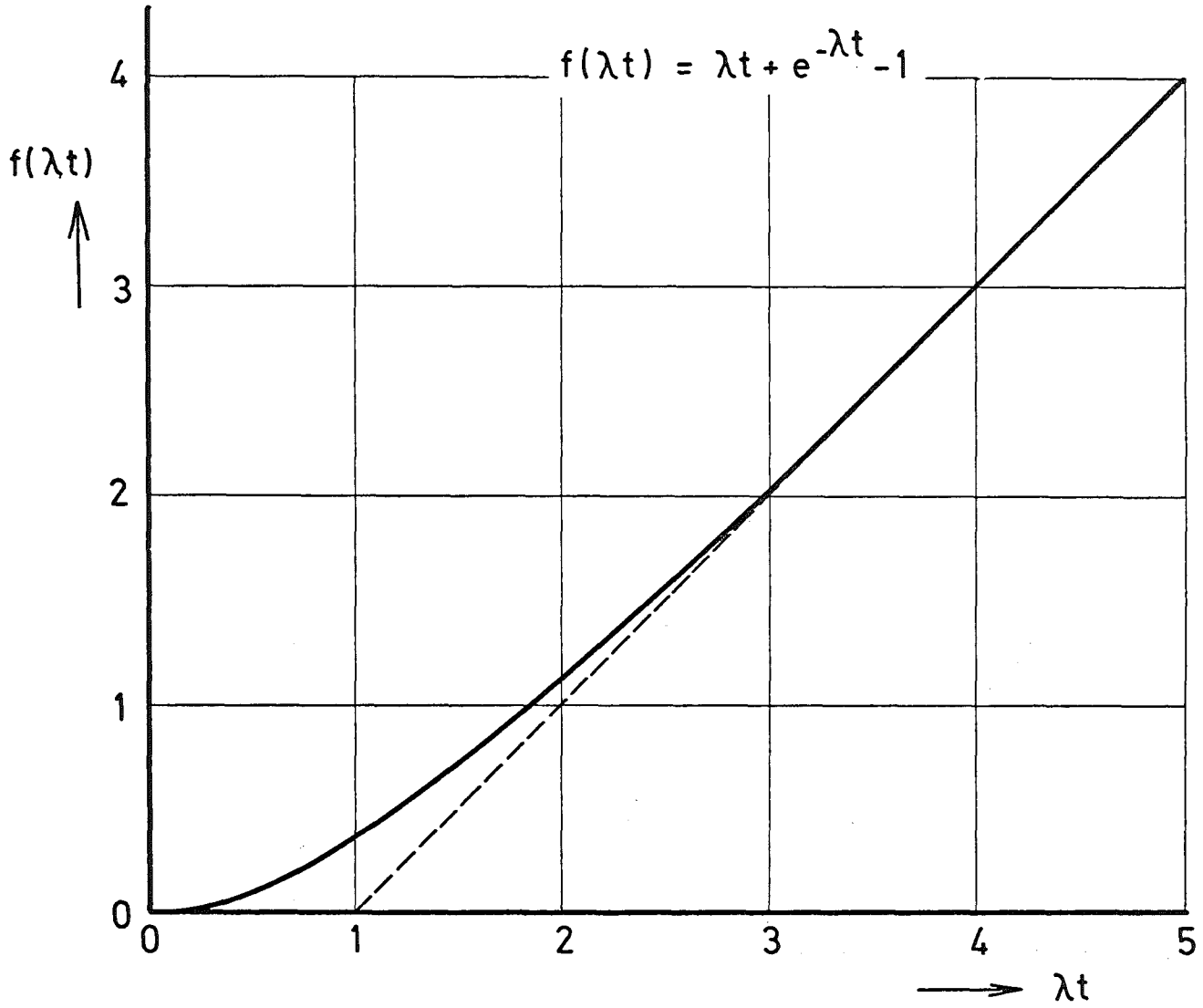


Fig. 6 Dependence of the normalized variance $f(\lambda t)$ of the permanent loss of strength upon time

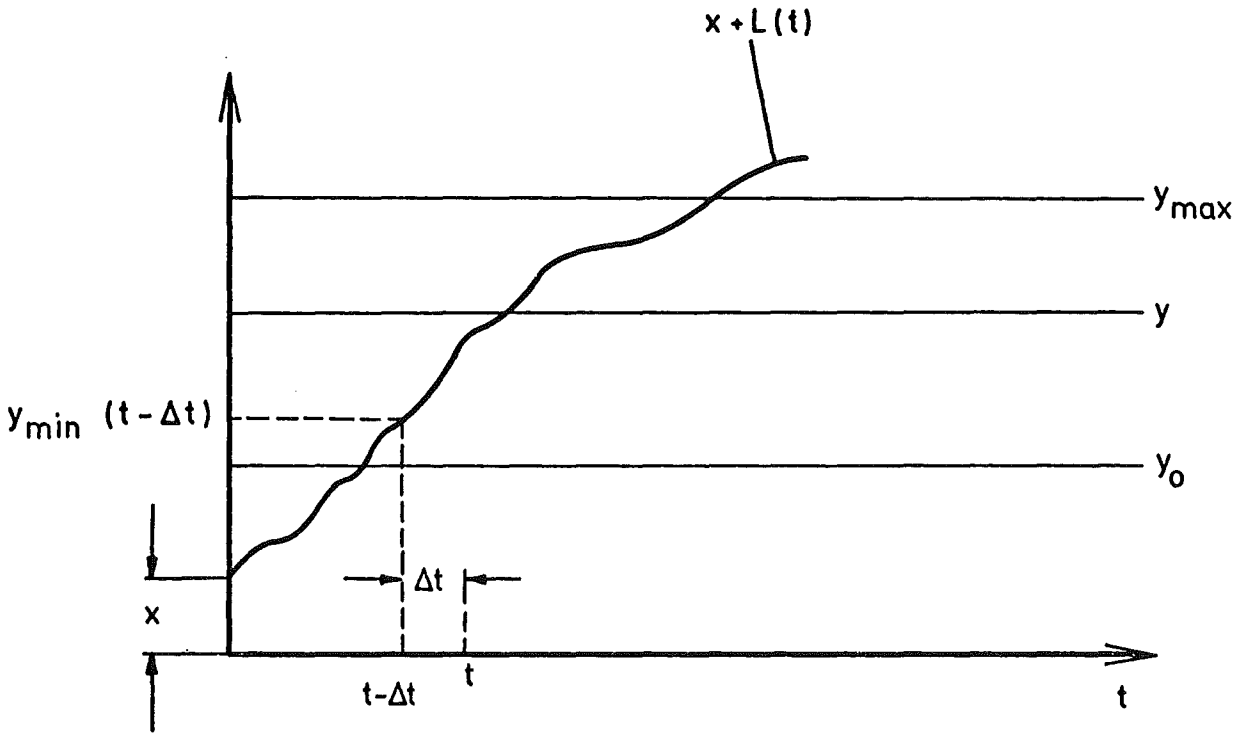


Fig.7 The loss of strength as function of time

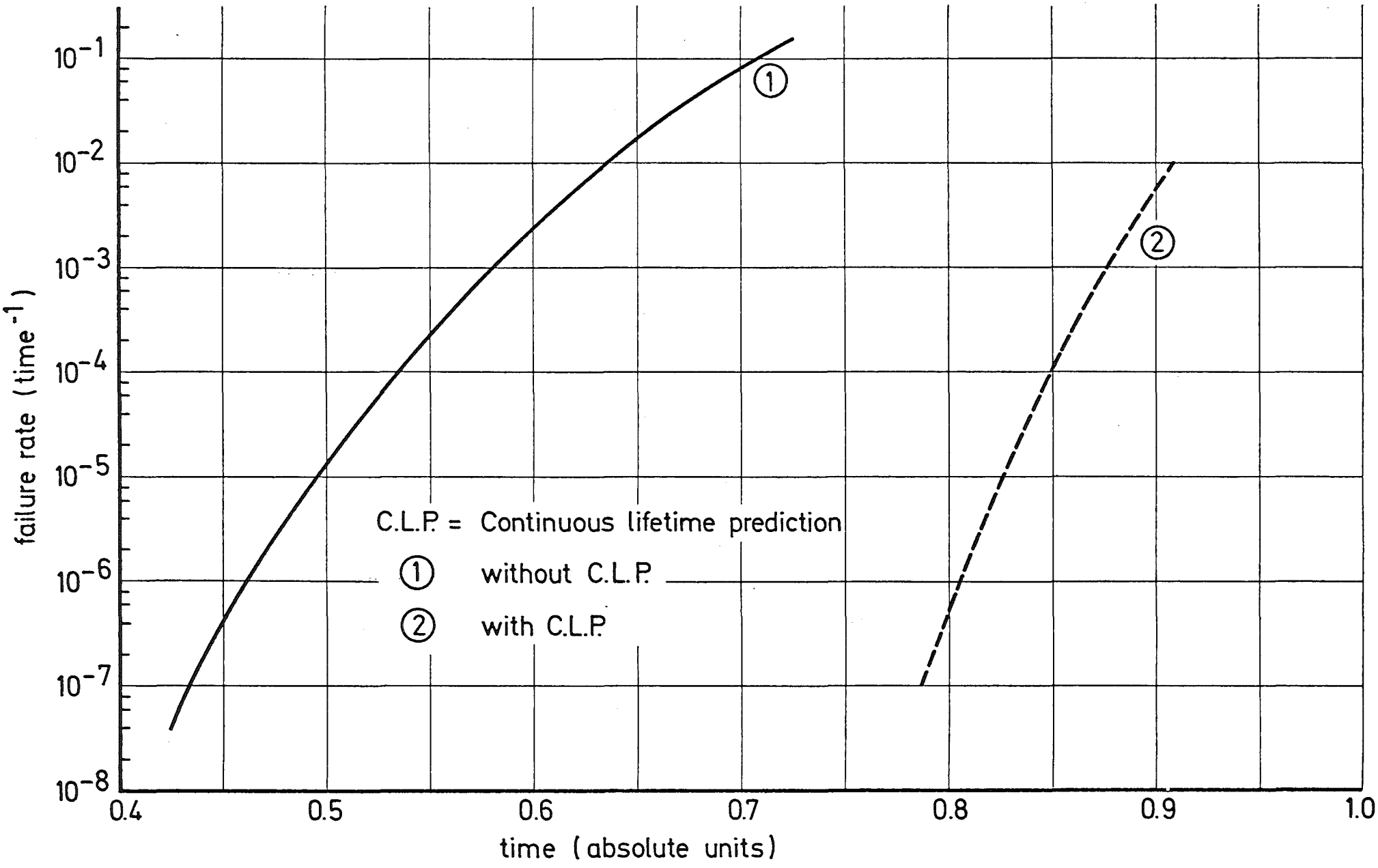


Fig. 8 Failure rates as functions of the time

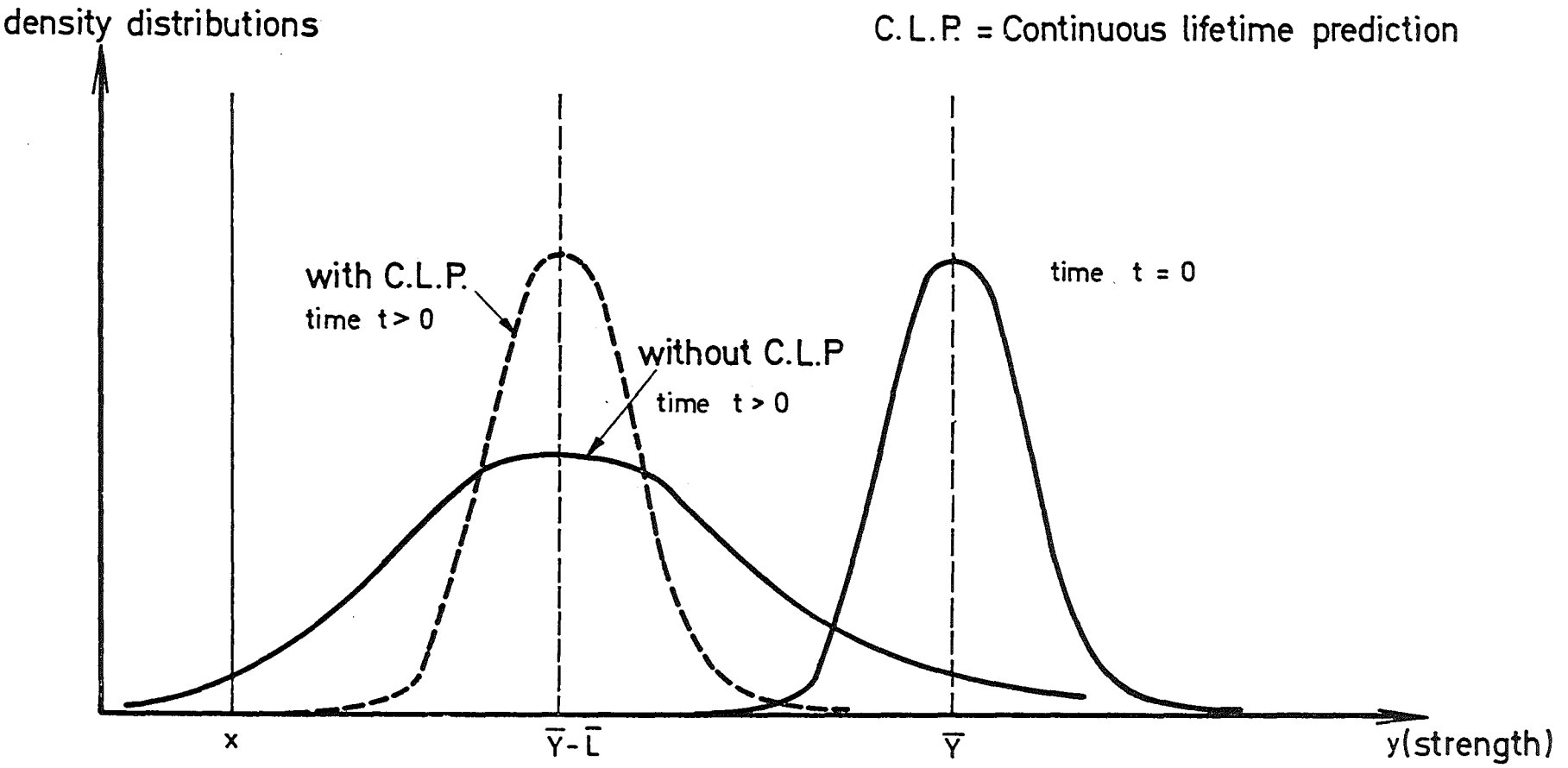


Fig. 9 Strength distributions at different times

Type of maintenance		Time of replacement	Degree of device wearout	Time interval, Δt_m, between the time at which the decision to carry out the replacement is taken and the time at which the replacement is effectively carried out	Basic parameter
1	Normal	Probabilistic	Complete and deterministic	None	E { time of failure }
2	Preventative	Deterministic	Less than complete and probabilistic	Whole maintenance time interval	failure rate at the time of replacement
3	Preventative with CLP	Probabilistic	Less than complete and deterministic	None	E { time at which a given failure rate is reached }

Fig. 10 Maintenance policies

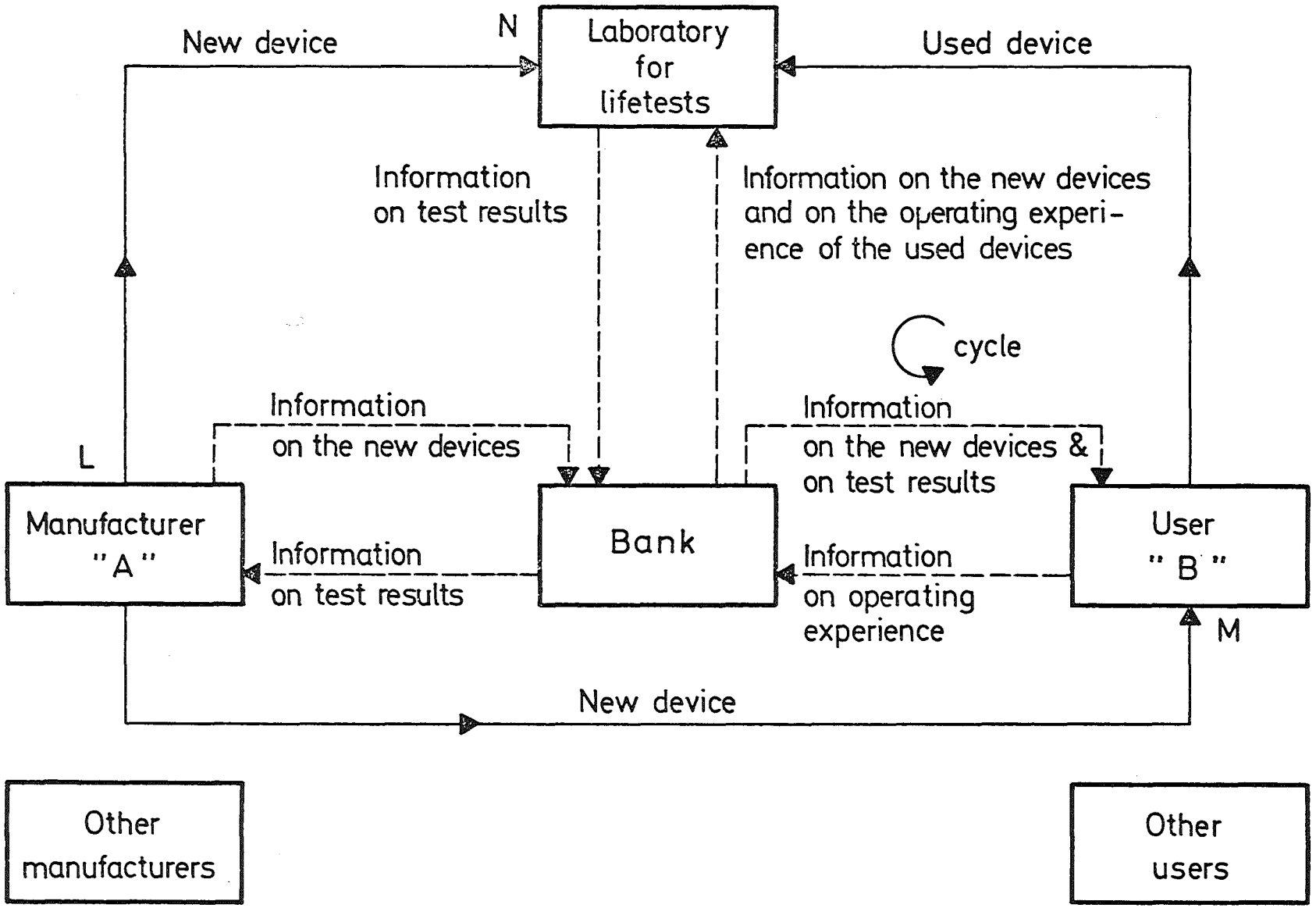


Fig. 11 Schematic diagram of an integrated learning process. Case of replaceable devices.

M. A. F. R. = Maximum allowed failure rate

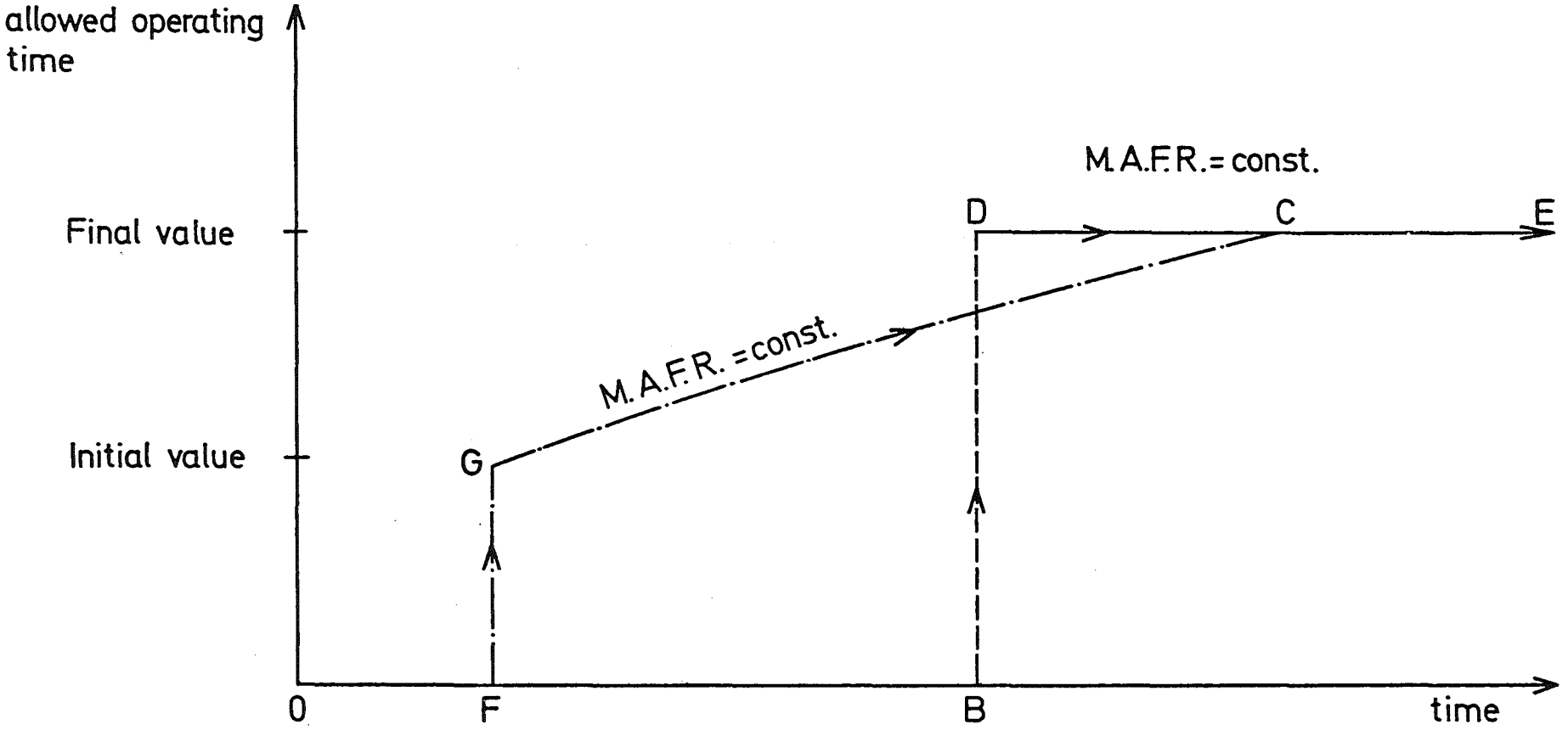


Fig. 12 Various paths of a learning process

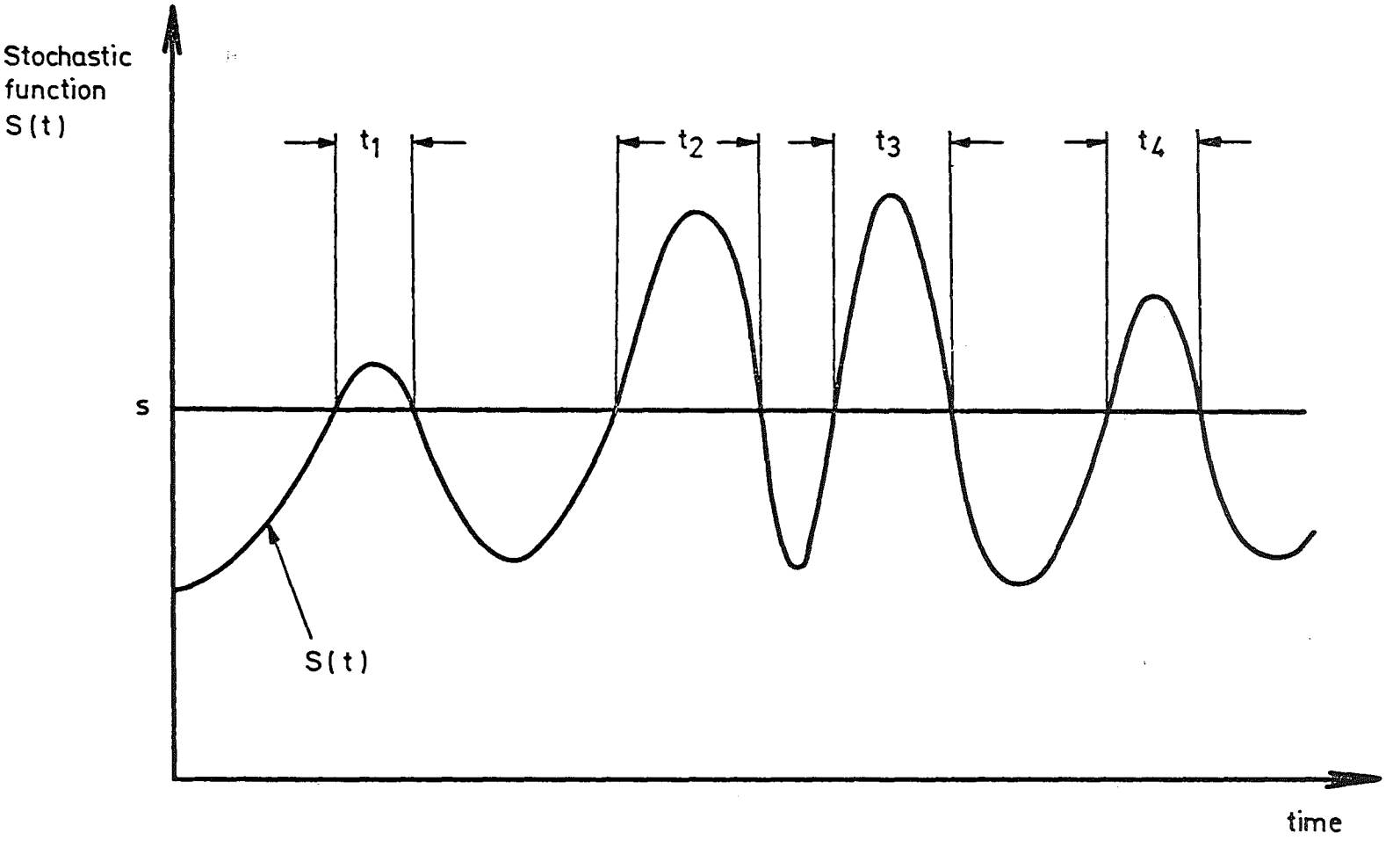


Fig. 13 Evaluation of the time intervals "t_m" during which the stochastic function S(t) exceeds the level s

Kapitel 7 : On the Maximization of Drift Reliability using Computer Aided Design (CAD)

P. W. Becker

Literaturverzeichnis zu Kapitel 7

ON THE MAXIMIZATION OF DRIFT RELIABILITY USING CAD

by
Peter W. Becker
Electronics Laboratory
Technical University of Denmark
DK-2800 Lyngby
Denmark

Abstract.

In this paper computer aided design, CAD, is used as a means for optimizing circuit or system drift reliability. A mathematical model for the drift reliability is introduced, and methods for numerical evaluation hereof are briefly reviewed. Finally the theory is used to optimized the reliability of two transistor circuits. The results and implications of the optimization are discussed.

1. Introduction

The early seventies have brought with them a new and healthy interest in reliability theory. The public concern is illustrated by the heated discussions regarding such diverse topics as the reliability of the BART-system (Friedlander 1973) and the necessity of improving reliability of consumer goods to slow down the consumption of nonrenewable mineral resources (Meadows et al. 1972, Table 4). In short the ability to predict circuit and system reliability is becoming increasingly important due to the amounting awareness of product reliability by government and the informed public. In most cases efforts are concentrated on the prediction of catastrophic failures, whereas the marginal reliability or drift reliability meaning the probability of a circuit or system failing due to gradual deterioration of its components has been shown only secondary interest. This notwithstanding the fact that an appreciable amount of field-failures are out-of-tolerance failures (General Electric 1961).

Techniques for the prediction and optimization of drift reliability using computer methods is the subject of this paper; said techniques have been discussed in far greater detail elsewhere (Becker and Jensen 1973).

2. A Mathematical Model for the Computation of Drift Reliability.

A commonly accepted definition of reliability for electronic engineering purposes is that reliability is the probability that a device will perform its required function under stated conditions and for a stated period of time.

The reliability of a system is dependent on both catastrophic and drift failures. The event "system success" (i.e. no system failure) represents the joint event of no catastrophic failure (ncf) and no drift failure (ndf). The joint probability is therefore:

$$R(t) = P(\text{ncf and ndf in } (0,t)).$$

Applying the product rule for conditional probabilities we may write:

$$R(t) = P(\text{ndf in } (0,t) \,|\, \text{ncf in } (0,t)) \cdot P(\text{ncf in } (0,t))$$

The overall reliability is here defined as the product of a conditional drift reliability and a catastrophic failure reliability.

We will assume that the catastrophic failures and the drift failurues are independent of one another. The drift reliability defined above then becomes an unconditional probability. This assumption, though often used in reliability calculations, is not necessarily a sound one. Rather on the contrary, in some types of component screening procedures, aimed at sorting out the most reliable elements, it is assumed that a component which exhibits a strong degree of degradation over a time interval will be an inherently unreliable component also with respect to catastrophic failures (Ryerson, 1966). The situation where the two types of failures are dependent may be handled by Monte Carlo methods (Becker and Warr 1963). In the following, we will assume independence and address ourselves to the problem of determining $R_d(t)$:

$$P(\text{ndf in } (0,t) \,|\, \text{ncf in } (0,t)) = P(\text{ndf in } (0,t)) = R_d(t).$$

Let an electronic device or system be made up of a number of components, whose time dependent parameters we will denote:

$$x_1(t),\ x_2(t),\ \ldots,\ x_n(t).$$

In the following these variables will be called input variables. They could be true values of resistors, transistor gains, etc. Also the device is taken to have a number of important output parameters denoted

$$y_1(t),\ y_2(t),\ \ldots,\ y_m(t).$$

The output parameters could be bandwidth, gain, input indepance, etc. In general, all the inputs must be considered random variables, whose probabili-

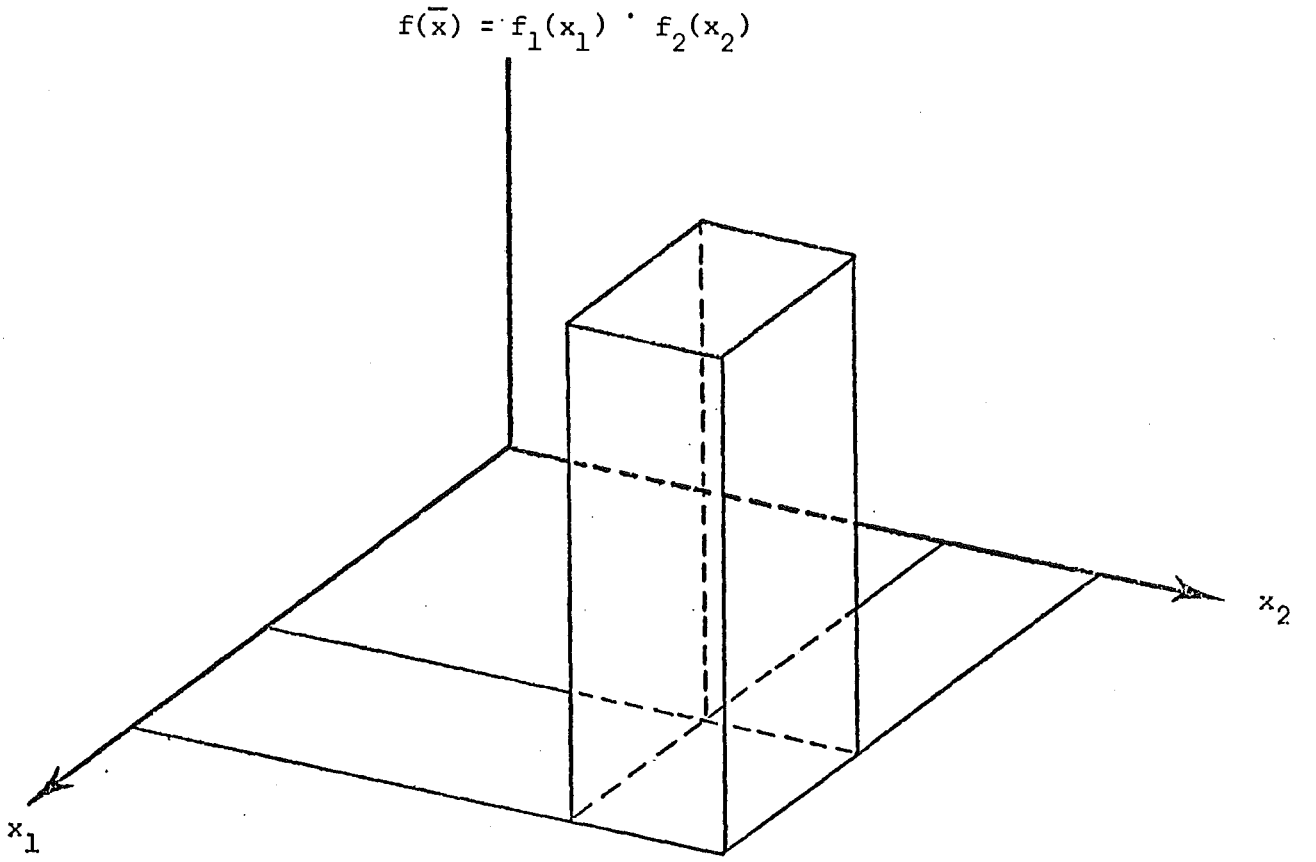


Figure 1. Joint probability density function for two independent variables having uniform density functions.

ty density functions are assumed to be known. Let the joint probability density function for all inputs be $f(\bar{x}) = f(x_1, x_2, .., x_n)$. In the case where alle input variables are independent, $f(\bar{x})$ is simply the product of the individual density functions, i.e.:

$$f(\bar{x}) = f_1(x_1)\, f_2(x_2) \ldots f_n(x_n).$$

In the case of only two inputs this may be illustrated as in Fig. 1, where uniform densities have been assumed for both variables. To find the probability of x_1 lying between two specified limits and x_2 simultaneously between two other limits, it is necessary to integrate, by way of a double integral,

the joint probability density function between the specified pair of values. This corresponds to the volume of probability mass under the joint density function over the rectangular area defined by the x-values.

When there are not 2 but n input variables, the joint density function, $f(\bar{x})$, may be illustrated by a surface in (n + 1)-space, and the joint probabilities are illustrated by volumes in this (n + 1)-dimensional space. Let $\Gamma_{\bar{x}}$ define the region of x-values under consideration; i.e. the values which are at all possible. The probability of finding $\bar{x} = (x_1, x_2, \ldots, x_n)$ in this region is then:

$$\int_{\Gamma_{\bar{x}}} f(\bar{x})\, d\bar{x} = 1 \qquad (1)$$

Let us now turn our attention to the outputs. Each of the outputs $y_1, y_2, \ldots, y_m$ is constrained to lie within specified limits, the output constraints. Consider again the case of two input variables as in Fig. 2. Here the curves for constant outputs y_1 and y_2 have been mapped on to the input variable plane. The region where all output variables have acceptable values is referred to as $\Gamma_{\bar{y}}$. The input variables have been allotted nominal values, $(x_1)_{nom}$ and $(x_2)_{nom}$, and truncated normal (Gaussian) density functions. To find the probability of device success (i.e. the device meeing the specifications) in the example from fig. 2 we must integrate the joint density function of the two input variables over the cross-hatched area shown in the figure. The boundaries of this area are made up of the output constraints and the tolerance limits of the input variables. In the general case of many input variables and many output variables the mathematical model for the computation of drift reliability becomes:

$$R_d(t) = \int_{\Gamma_{\bar{x},\bar{y}}} f(\bar{x};\, t)\, d\bar{x} \qquad (2)$$

the integration being performed over the region $\Gamma_{\bar{x},\bar{y}}$; the region $\Gamma_{\bar{x},\bar{y}}$ is the region which is common to $\Gamma_{\bar{x}}$ and $\Gamma_{\bar{y}}$. $f(\bar{x})$ is written $f(\bar{x};t)$ to show a possible dependence of the joint density function upon time.

As an aside we notice that worst-case design simply is a design procedure where the designer locates the orthotope $\Gamma_{\bar{x}}$ inside $\Gamma_{\bar{y}}$. Consequently the intersection of $\Gamma_{\bar{x}}$ and $\Gamma_{\bar{y}}$ equals $\Gamma_{\bar{x}}$. Then Eq. (2) reduces to Eq. (1) and the integral becomes unity, $R_d(t) = 1$.

From an analytic point of view the $R_d(t)$-integral from Eq. (2) is really all there is to the analysis problem. In practice, however, the computation of

$R_d(t)$ is complicated by three factors to be discussed shortly.

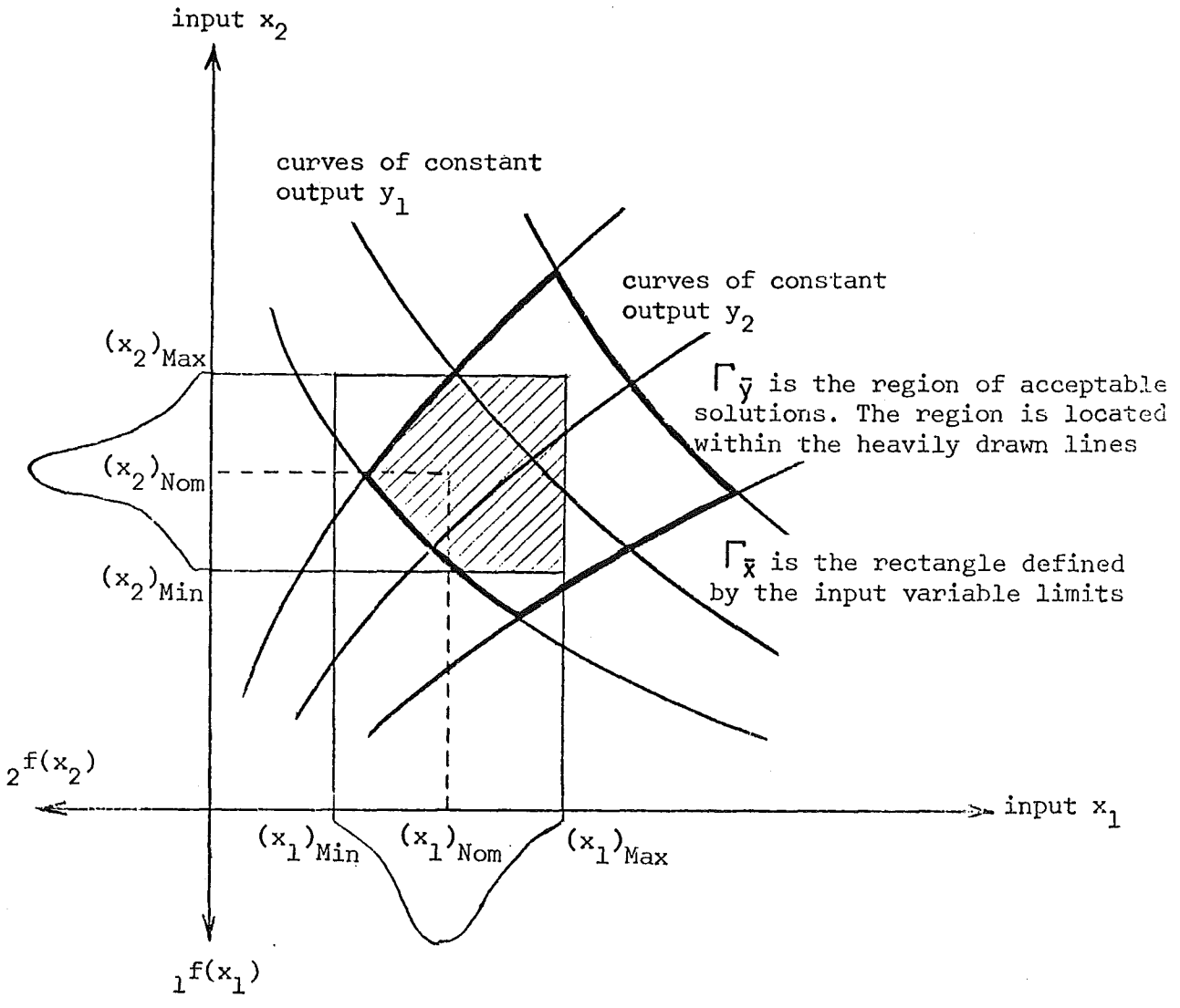


Figure 2. Illustration of the design problem for two inputs and two outputs n=m=2. The joint probability density function of the two inputs is to be integrated over the cross-hatched area shown in the figure. The result is the drift reliability, R_d.

We note, that without any loss of generality one can concentrate on the computation of the integral at a fixed time, $t = t_o$. If we compute $R_d(0)$ we have obtained what is known as the production yield. In the following we will disregard the time dependence and speak in general of the drift reliability of the device. The integral may then be written in the simplified form:

$$R_d = \int_{\Gamma_{\bar{x},\bar{y}}} f(\bar{x})\, d\bar{x}$$

The complications in computing the integral R_d, basically stem from the following circumstances.

1) The output variables $y_1, y_2, \ldots y_m$ are usually highly nonlinear functions of the input variables.

2) The true values of the n input variables will very often show some form of statistical dependence. The integral R_d calls for an expression for this hard-to-get multivariate density function $f(\bar{x})$. Here we must remember that only if the input variables are statistically independent can $f(\bar{x})$ be expressed by simple multiplication of the marginal densities $f_1(x_1), \ldots f_n(x_n)$.

3) The true values of the m output variables are nearly always statistically dependent.

The problem of computing the multivariate density function when only the marginal density functions are known has, of course, no unique solution as the statistical dependence among the n input variables will affect the result. We will not pursue this very interesting theoretical problem any further here, only mention that the answer to the following basic question can be found elsewhere: which multivariate density functions are possible with a specified set of marginals (Becker 1970)?

3. Methods for Computing the Drift Reliability

Direct integration of the multiple integral for drift reliability, $R_d(t)$, is possible only in the simplest of cases which rarely are of true practical interest. Some kind of numerical integration will usually be necessary.

Three techniques are generally useful in dealing with one or all of these situations. They are:

1) The normal approximation.

2) The method of multidimensional convolution.

3) The Monte Carlo method.

The method of normal approximation and the Monte Carlo method have been discussed extensively in the literature (Ottlinger 1967 ; Shooman 1968). The multidimensional convolution scheme (Becker and Jarkler 1973) is new and has not received the same amount of attention.

The last of the three methods, the Monte Carlo method, is perhaps the most widely used of the methods. It is also the one which was used in the optimization examples to be mentioned later. It has great intuitive appeal and the

further asset of being able to handle, without difficulty odd statistical relationships and any number of output variables, be they linear or non-linear functions of the input variables. The drawback with the Monte Carlo method is of course, that very large sample sizes and consequently much computer time may be necessary to obtain R_d estimates in which one can have real confidence.

4. The Optimization Problem

Our objective is the maximization of drift reliability as expressed by the integral R_d. The statement of the problem in mathematical terms is as follows:

(i) Given the joint probability density function

$$f(\bar{x}/_N\bar{x}) = f(x_1/_N x_1, \ldots, x_n/_N x_n)$$

for the true values of the input parameters normalized with respect to their nominal values and

(ii)a range of permissible values for the nominal values:

$$\begin{aligned} {}_N x_{1,\min} \leq {}_N x_1 &\leq {}_N x_{1,\max} \\ - \quad &- \quad - \\ - \quad &- \quad - \\ - \quad &- \quad - \\ {}_N x_{n,\min} \leq {}_N x_n &\leq {}_N x_{n,\max} \end{aligned}$$

we are to find a set of nominal input parameter values $({}_N x_1, \ldots, {}_N x_n)$ such that the drift reliability R_d is maximized. R_d is the joint probability of the true values of the m output parameters all meeting the given output specifications:

$$\begin{aligned} y_{1,\min} \leq y_1 (x_1, \ldots, x_n) &\leq y_{1,\max} \\ - \quad &- \quad - \\ - \quad &- \quad - \\ - \quad &- \quad - \\ y_{m,\min} \leq y_m (x_1, \ldots, x_n) &\leq y_{m,\max} \end{aligned}$$

To solve the optimization problem we must introduce the concept of a feasible solution. A feasible solution is defined as a set of input parameter values

for which all output specifications are met (i.e. the corresponding point is located in $\Gamma_{\overline{y}}$ in Fig. 2). The computer optimization consists of two steps:

1) We let the computer search for a feasible solution; this step may be omitted if the designer already knows of a feasible solution.

2) We let the computer optimize R_d. We here use the feasible solution as the starting point for the set of nominal values, $({}_N x_1, \ldots, {}_N x_n)$, which we change. Using the terms from Fig. 2 we move $\Gamma_{\overline{x}}$ around to obtain the cross-hatched area with the most probability mass.

To perform the first step the following must be specified: the topology of the circuit, some set of input parameter values with which the search can be started, and the output specifications. The output specifications are used to generate an index of performance, Y, which we strive to maximize during the optimization. Y could for instance take the form:

$$Y = \sum_{i=1}^{m} - a_i \left[\frac{2\left[y_i - (y_{i,min} + y_{i,max})/2\right]}{y_{i,max} - y_{i,min}} \right]^{2b_i}$$

where y_i is the value of the i'th output parameter, a_i is a positive weighting factor, and b_i is a positive integer. The value of the expression in brackets lies between -1 and 1 for any single output y_i satisfying the output specifications. Y is a non-positive function and decreases rapidly if one or more of the output constraints are violated. During the first step all the component tolerances are set to zero; consequently we need not know $f(\overline{x}/{}_N\overline{x})$ to find a feasible solution. To perform the second step we obviously must know $f(\overline{x}/{}_N\overline{x})$.

In both the first and the second step the constraints on the output parameters are incorporated in the objective function (i.e. in the index of performance (Y) or in R_d). This reduces the problem to one of unconstrained optimization (Wood 1965).

If the partial derivatives of the objective function are easily calculated, one of the well known gradient methods would undoubtedly be the best choice for the optimization problem. Unfortunately, the objective functions, with which we are dealing, are very complicated functions of the input variables, and neither the partial derivatives nor the functions themselves can be written in closed form. This leads us to applying search methods in which only the objective function itself, Y or R_d, need to be evaluated.

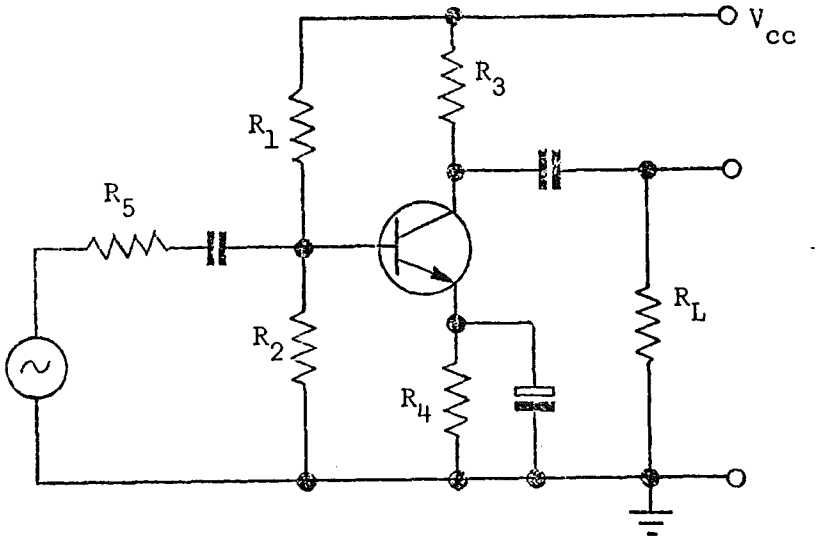


Figure 3. Low frequency amplifiers.

5. Putting the Theory to Work

The optimum design strategies outlined in this paper have been tested using transistor amplifiers as examples. The first example is a very simple one-transistor amplifier shown in Fig. 3. Six output parameters were specified for this circuit (voltage gain, input impedance, junction temperature, et al.).

Fig. 4 illustrates the use of the Pattern Search strategy (Wilde and Beightler 1967) for finding feasible solutions, when only R_1 and R_2 (in the circuit illustrated in Fig. 3) are allowed to vary. Contours for two of the output parameters are plotted on the input parameter plane, and the feasible solution region shown by the heavily drawn lines. Two search paths for finding a feasible solution by minimizing the index of performance are shown in the figure. Various other starting points were tried, all cases resulting in solutions well within the feasible region.

Having found a feasible solution the next step is to optimize R_d. The Monte Carlo method was used for the R_d calculations. The improvements in drift reliability experienced using the Pattern Search strategy are for four runs shown in Table 1.

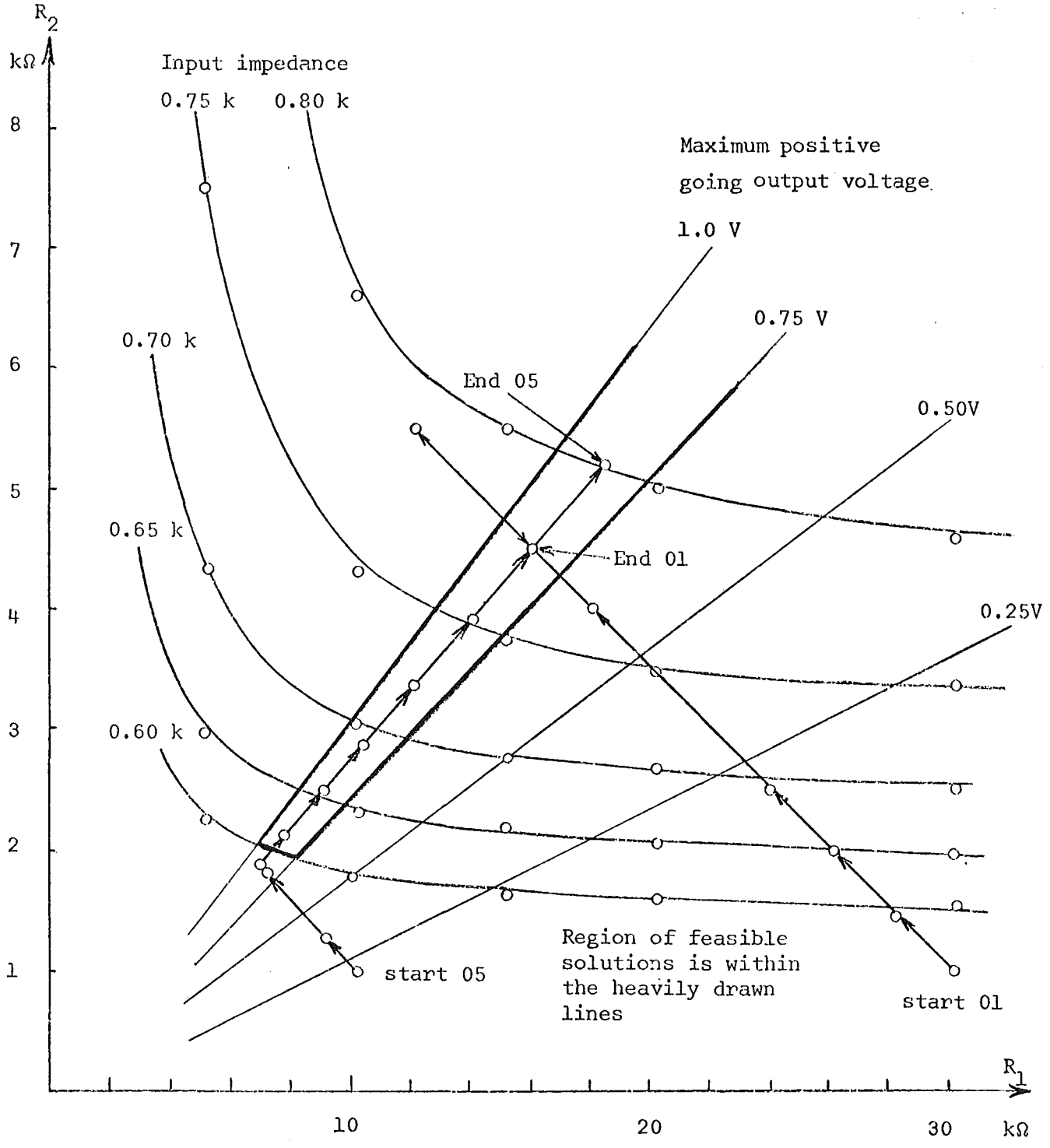


Figure 4. Illustration of the computer aided search for a feasible solution when only R_1 and R_2 are allowed to vary. Two search paths, 01 and 05, are shown.

Run no.	R_d-value at end of step no.1	R_d-value at end of step no.2
1	82.6 %	88.4 %
2	82.4 %	83.0 %
3	89.0 %	90.8 %
4	84.8 %	90.0 %

Table 1. Drift reliability improvements for the one-transistor amplifier using the Pattern Search strategy.

The second example is a wide-band three-transistor amplifier illustrated in Fig. 5. Here six resistors are allowed to vary, and nine output parameters are specified. With a single exception all runs end in feasible solutions with resistor values of one set not differing greatly from those of another. In the case where a feasible solution was not found, a new search was initiated from the end point of the first unsuccessful search using the original step lengths for the input parameters. Doing so, a feasible solution was found.

Eight optimization runs were carried out with different starting points for step no. 1. The results are given in Table 2. All runs ended with a drift reliability of approximately 90 %. An increase in yield of no less than 9.6 % is experienced in one example.

Run no.	R_d-value at end of step no.1	R_d-value at end of step no.2
1	88.2 %	90.4 %
2	83.6 %	93.2 %
3	88.8 %	90.4 %
4	88.8 %	91.6 %
5	84.2 %	90.0 %
6	85.8 %	91.0 %
7	81.4 %	90.4 %
8	84.2 %	91.0 %

Table 2. Drift reliability improvements for the three-transistor amplifier using the Pattern Search strategy.

6. Conclusions

We have strived to demonstrate that given the topology of a circuit (or system) and a set of specifications we can let the computer do two things. First we can let the computer search for and find a feasible solution assuming that feasible solutions exist, this was step no. 1. Secondly, if we can specify a joint density function, $f(\bar{x}/_N\bar{x})$, for the normalized input parameters we can let the computer search for and find a set of nominal input parameter values which maximizes the drift reliability, R_d, this constituted step no.2. The experimental results indicate that we succeeded in doing both in case of our two examples. The increase in drift reliability is appreciable, R_d-improvements exceeding 9 % are observed. We are therefore inclined to think that an automated search for the design with the largest R_d-value is not only practical - it may be advisable to perform such a search before mass production of electronic circuits and systems are undertaken. The benefits should be especially notable in fields where designer experience has trouble keeping up with a quickly changing technology, e.g. the field of integrated or hybrid circuit design.

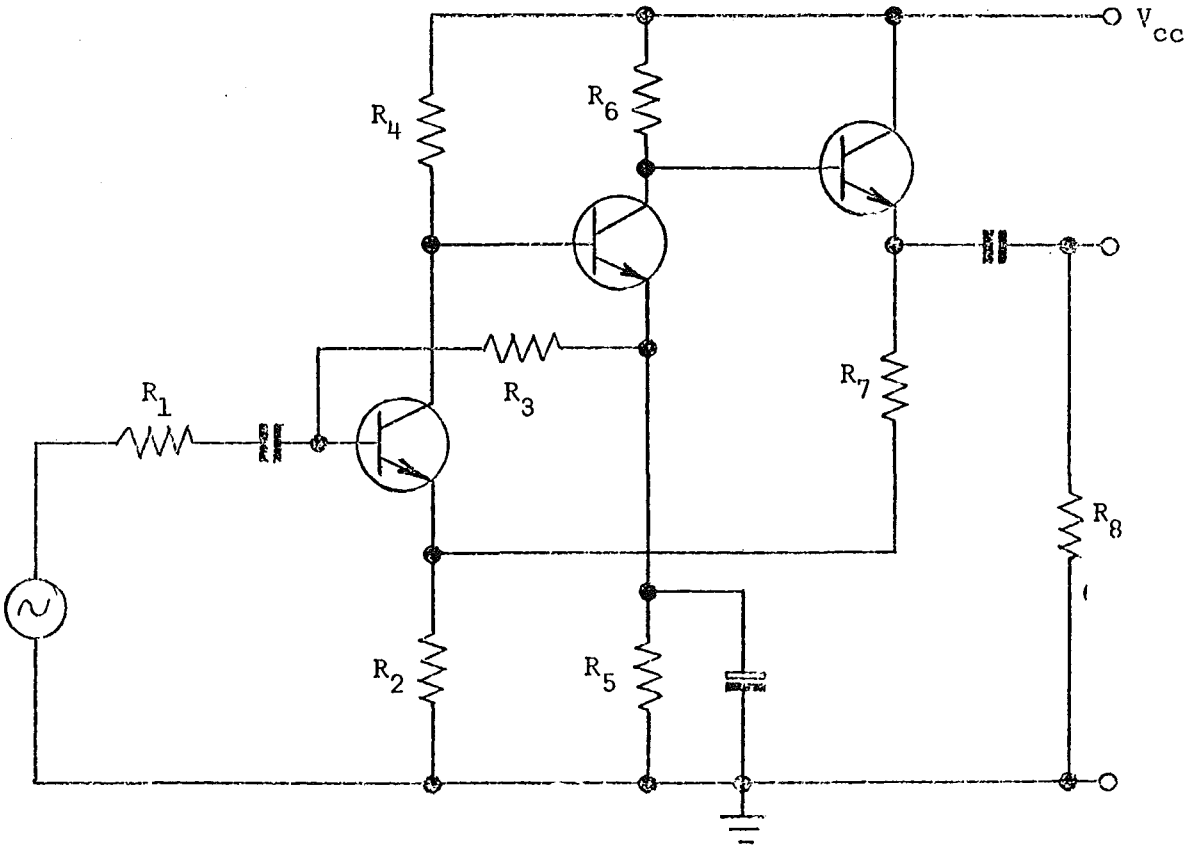


Figure 5. Wide-band amplifier.

References

Becker, P.W., 1970, "Transformations on Probability Density Functions that Retain Marginals". Paper presented at the International Symposium on Information Theory, Nordwijk, The Netherlands, June 15-19, 1970.

Becker, P.W. and Jarkler, B., 1973, "Assessing Reliability by Multi-dimensional Convolution with Quantitation". Third Symposium on Reliability in Electronics, Budapest, Hungary, 1973.

Becker, P.W. and Jensen, F., 1973, "Design of Systems and Circuits for Maximum Reliability or Maximum Production Yield". Book to be published in 1973.

Becker, P.W. and Warr, R.W., 1963, "Reliability vs. Component Tolerances in Microelectronic Circuits". Proc. IEEE, Vol. 51, pp. 1202-1214, Sept. 1963.

Friedlander, Gordon D., 1973, "Bigger Bugs in BART?". IEEE Spectrum, Vol. 10, No.3, pp. 32-37, March 1973.

General Electric, 1961, "Handbook of Reliability Analysis for System and Computer Design Engineers". General Electric PB 181080, 1961.

Meadows, D.H., Meadows, D.L., Randers, J. and Behrens III, W.W., 1972, "The Limits to Growth", New York: Signet Books, 1972.

Ottlinger, J.A., 1967, "Computer Tolerance Analysis of Electronic Circuits". Proceedings of the National Electronics Conference 1967, pp. 770-775.

Ryerson, C.M., 1966, "Spacecraft Component Reliability". Proceedings of the 1966 Annual Symposium on Reliability, San Fransisco, California, 25-27 January, 1966, pp. 173-179.

Shooman, M.L., 1968, "Probabilistic Reliability: An Engineering Approach". New York, McGraw-Hill, 1968.

Wilde, D.J. and Beightler, C.S., 1967, "Foundations of Optimization". Englewood-Cliffs, N.J.: Prentice-Hall, 1967.

Wood, C.F., 1965, "Review of Design Optimization Techniques". IEEE Trans. on Systems Science and Cybernetics, Vol. SSC-1, pp. 14-20, November 1965.

Kapitel 8 : Analysis and Diagnosis of In-Service Failures by Pattern Recognition

L. F. Pau

ANALYSIS AND DIAGNOSIS OF IN-SERVICE FAILURES BY PATTERN RECOGNITION

by

L. F. PAU

Abstract: It is first pointed out that the knowledge of the operational circumstances, and of the whole past history of an equipment, is required for a better analysis of the equipment reliability. The failure data collection system concept is then introduced; the main implementation rules hereof are then stated, as based upon experience.

The theory of a feature extraction method, called correspondence analysis, is given. It is applied to learning datas made of all stored in a reliability and maintenance data bank.

Correspondence analysis is a variant of principal component analysis, based upon a CHI-square distrubutional metric wherein patterns and observations play symmetrical roles. A simultaneous graphical representation of both patterns and observations helps in analyzing the operational behaviour of the equipment for design review and maintenance control; two examples hereof are given for an airborne equipment, and for resistor components.

Real time diagnosis and fault localization have been achieved, thanks to a real time data compression into the reduced feature space generated by correspondence analysis, and by a sequential recognition procedure. This procedure is the generalized nearest neighbour rule, applied sequentially to learning sets of increasing size; the stopping rule uses a compromise between recognition time and the misclassification probability. An example of automated real time testing is given, showing a 92 % true recognition rate for acceptable items produced by machinetools, and a mean correct diagnosis rate of 81 % for non-accepted items.

1. INTRODUCTION : THE FAILURE DATA COLLECTION SYSTEM

The purpose of any diagnosis searching procedure is to recognize a failure, or a set of failures (also called syndrome), on the basis of:

. informations about the past history of the equipment, including maintenance and operational utilization, alltogether called learning data; these learning data are stored in a reliability and maintenance data bank, with permanent updating.

. informations about the circumstances of the failure (s), visual observations of the equipment, and results of non-destructive tests, alltogether called pattern coordinates.

The "correlation" of the present symptomas described by the pattern parameters, with the learning data, yields a classification of the ill-working equipment into some few classes of possible failure causes. A final decision is made regarding the class membership of the observed equipment by a stored decision rule.

Such a diagnosis searching procedure can be formalized as a pattern recognition problem, the unknown patterns being the equipments described by pattern coordinates. Some research has been reported since 1968 on testing methods which were automated to varying degrees and which utilize pattern recognition. HANKLEY and MERRILL [5] consider the error analysis problem in an inertia platform; BECKER[1] and PAGE[8] detect up to three faults on the basis of jet engine vibrations; CORTINA[3] reports operational results on truck motors and PAU[9] on airborne electromechanical equipments.

Our discussion will be centered around the practical applications of a pattern recognition technique designed in order to contribute to the solution of following problems P1-P3:

P1: eliminate all redundant tests and observations, and select those synthetic observations yielding the best discrimination between the failure causes: this is the feature extraction or data compression problem;

P2: how to build a satisfactory list of a few relevant diagnosis assumptions, and to display the relations among these on some drawings;

P3: automation of the diagnosis or test procedure, through a minimization of the misclassification probability.

Because of the role of a priori information in the above mentioned approach, we must first state implementation rules for a failure data collection system, as based upon author's experience.

1.1. Desk survey

A survey should first be conducted of government agencies, industries, and users, for the purpose of identifying and reviewing all failure documentation related to the systems to be considered. Specific component-in-service failure records should be examined to determine component description and failure circumstance which would contribute to the failure data tabulation and analysis development efforts. The objective of this survey should be to obtain a broad cross-section of past and present component failure experience on a wide variety of system's supports and components of the system. This general survey identifies numerous types of service failures, and enables a comprehensive overview of the failure investigation and correction problem. From this general survey, specific component/system failures should be selected for further review and data gathering.

1.2 Subsystems/components considered for failure data analysis

The subsystems initially considered as candidates for service failure data should include as many of the subsystems which the

users have in their present inventory or the maintenance responsibility of. The goal of such a broad preliminary survey is to permit the selection of subsystems and component failures which offer the best potential for investigation analysis (due to operations, priority and economics).

The subsystems should be grouped into general mission categories to permit classifying failure data and comparing similar service operations even though specific mission profiles may vary within each group, or subsystem itself. Thus specific component failures and statistical tabulations can be presented without identifying specific systems.

If different subsystems have similar components and operations, they may be combined. Attemps should be made in order to get data from other users handling the same systems, which would permit comparison of different operational and maintencance characteristics. The complete range of accumulated operating hours are of interest to assess the historical nature of early life failures; however, new inventory systems with little operational experience may be disregarded.

1.3. Data sources

The failure information gathered for analysis and statistical development should be obtained from all organizations which are directly concerned with the system, either in operations, or in testing. Much of the failure information should be gained from direct contacts and requests (correspondence, telephone communications) from the data bank organization.

The greatest care, and severe measures should be taken with respect to the security of all these informations; an organization providing data should only be abilitated to have access to its own data, and to fully agregated failure figures. Within the data bank organization, the greatest care should be taken to avoid lacking discretion towards outcomers.

It was found in field experiences that detailed information on any one particular failure may be very difficult to obtain, even from these organizations that directly handled the investigation and solution of the specific failure problems. Any data gathering process and organization should therefore incorporate staff members with design/maintencance experience, allowed to make special investigations within all member organizations; this may rise psychological problems, but is absolutely necessary in order to conduct continuously improved data gatherings, and to make the data providers conscious of their individual/collective responsability; through such human contacts, these data providers may also feel more positive, than they would have done if they only had to fill-out regularily anonymous failure reports.

1.4. Data request format and procedures

The data gathering efforts should be directed towards two areas:

- general fleet failure information for statistical evaluation;
- detailed failure documentation on individual subsystems/components for analysis development.

The depth of data requested will usually be significantly different.

The data for the statistical analysis should be obtained from the major data bank, and various fixed-format reports. These sources of failure data should be used to identify the most significant and interesting component failures for subsequent data gathering in providing information for the detailed failure analysis development. The type of data for this major data bank, stored on random access tapes, should be concerned with all subsystems/components selected in 12., and over a maximum operating time period; they may be summarized in the following checklist valid for each failure:

1. System description

    1.1. Designation
    1.2. Model; user/operator code
    1.3. Number
    1.4. Operating hours, and dates of overhauls, inspections
    1.5. Nominal operational specifications
    1.6. Work-center issuing the report

2. Component/subsystem identification

    2.1. Part name and location
    2.2. Part number, work unit code
    2.3. Use
    2.4. Designation
    2.5. Part form, treatment
    2.6. Processing/treatments performed
    2.7. Types of all previous maintencance operations (preventive, corrective)

3. Failure description

    3.1. Origin of the failure and past history of the component/subsystem; when was failure discovered
    3.2. Failure mode, malfunction code
    3.3. Contributing influences due to state of the component
    3.4. Recent environmental factors
    3.5. Action taken: repair, change, and time for repair /inspection

The data formats should allow for selective and detailed sorting out of data of particular interest. Comments written and stored in natural language should also be adressed selectively, but analyzed inside the data bank organization. Aggregate reports on these analysis should be mailed regularily to all organizations contributing to the data bank.

The staff organization within the data bank organization should be such, that an analysis may be performed on request with short notice.

The data for the detailed failure analysis should be collected in the minor data bank from various files and records of engineering, maintenance, user organizations. Selection of these individual failures may be based on the identification of repeated failures during the statistical data gathering phase and identification of the more completely documented component failures of particular interest are comprehensive failure reports, investigation documents, test results, and descriptions of the circumstances surrounding the failure. For each such component, designers should outline a comprehensive checklist of the information required for a thorough analysis.

Periodically, the list of components receiving this special treatment should be revised, with accept from all organizations. The data bank organization should be allowed to go on requesting information from all data suppliers, if a majority of these feel that it is necessary. The content of the minor data bank should also be arranged for easier handling and sorting; data sheet formats, and checklists for each component monitored, should be used as a means of compiling information.

1.5. Failure data compilation

The failure data survey and screening involves processing data in often various formats and from numerous sources. In order to make the analysis as cheep as possible, one may decide:

- either to require that all participants in the program use the same reporting formats, prodedures and dates; this may require special funding, often incentive, from the data bank organization;
- or to let each participant process and compile his data as he wants it; all participants must then agree on the common format for presenting the results of these decentralized processing steps; these results must though include the basic failure reports, once rewritten into a common data record format and code.

Manuals should be written, published in large numbers, and kept up-to-date, in order to ease this retrieval, compilation and processing phase. The programs used for analysis purpose will usually include, depending upon the needs expressed by the system users and designers:

- standard statistical programs
- reliability and failure rate estimation programs with computation of confidence intervals
- selective retrieval and grouping programs
- tabulation programs of all kinds, i.e. for component-by-component analysis.

All reports having received a proper security clearance, are forwarded to the proper organizations for analysis of the failures, together with aggregated investigation results on those failures where more complete documentation was obtained.

1.6. Data limitations and problems

During the failure data survey, screening and classifying efforts for the failure analysis development phases of the program, a number of limitations and problems will usually be encountered which compromise the validity and accuracy of the results:

* Some failure data may represent failure occurences only for specific periods of time during the operational life of the system: this will bias the statistics. The monitoring should be permanent, and it should be checked that all subsystems have separate clocks if they are allowed to work at different times independently.

* The possibility also exists that fleet-wide inspection directives or technical orders might require certain parts to be inspected or replaced, and reported. This should be avoided by specifying such circumstances in the reporting code.

* There is also the possibility that a given part failure results in more than one entry into the data bank: such as one for inspection, removal, repair and part replacement. Here again appropriate coding keys should be defined and filled out so that the full maintencance process may be reconstituted on the basis of the data records registered.

* The reliability of the data entries should always be questioned since it is possible to make a coding entry error, or to enter an incorrect code if a suitable one is not immediately known.It is therefore very important to make the maintencance/coding manuals very clear and complete.

* Voluntary over-, under-reporting or inconsistent reporting is frequent for psychological reasons, or because time has not been provided by management for filling out the reports properly.

Probably the greatest limitation will be the lack of pertinent and complete data, from the standpoint of the failure meachanisms. The type of data necessary for a proper analysis will sometimes not be detailed in failure investigation since the primary importance is the fix and repair, rather than the systematic investigation of the failure mechanism. Another related problem is that, for the majority of failure histories, all data surrounding the failure (operational parameters before the failure), are not obtainable from a single location. To obtain the complete failure history on a given part, several individuals and organizations must be contacted with much of the needed information not documented but obtained through personal discussions.

Moreover, the primary data source for the various failures will differ considerably, and depend on the status of production, years in inventory, organization assigned maintencance responsibility, and contractor system obligations. Transferring engineering and maintenance responsabilities, and changes in the system's base of operation, make the fleet failure statistical evaluation difficult. Programs should be able to compile and re-assemble data independently of such aspects.

The recording of precise and valid information on the data sheets presents several problems. Any one source of information generally results in partial or sketchy information in a number of data categories. An attempt to obtain missing data via other sources or documentation raises often the problem of identifying the correct failure, part or system. Thus, it is very possible that different failures, failure locations, operational histories, failure causes or environmental influences could be entered as a single, complete failure data occurence.

Also, failure data inaccuracies are possible as the result of part replacement or changes during the lifetime, and could involve a number of different configurations, materials, part numbers, operational stresses or processing steps which appear in the documentation to represent a single component operational lifetime.

Bacause of improper coding, the type of failure may generally be limited to a single cause, and brief identification of failure origin. Usually, no description of progression through various stages of failure are described during the failure mechanism initiation and growth. Initial system states are not identified in many cases. For most component failures involving a number of occurences, only the first ones are usually examined and documented in detail with subsequent failures resulting in little or no failure documentation, as it is often assumed that the same failure mode and cause applies.

These above problems, to varying degrees, may be encountered throughout the detailed failure data gathering and screening; they generally limit the completeness and usefulness of the failure information for subsequent development of failure analysis methods utilizing models of its apparition process.

1.7. Failure data correlation

The classifying and statistical correlation of the various failure data gathered, may be grouped under two main headings:

* general failure reporting from the major data bank;

* significant failure occurences, including the tabulation of the more critical failure documentation for these failures monitored in the minor data bank.

Because of different form and nature of these two types of data, separate statistical correlation and tabulation efforts must be conducted.

The most common agregate tables, which may be reported back to the data source organizations, include:

- number of failures in the different subsystems/components, as a function of time(from reporting period to reporting period)

- number of failures in each category, and distrubution with time

- proportions of critical failures with respect to the availability of the system, or to the mission

The most significant failure areas and causes should thereafter receive the primary attention in the development of improved failure analysis methods. Feedback from the designers and maintenance staff is then awaited, and the data bank organization should verify that something is undertaken, at least for the critical failures.

All results should be presented in such a way, that it is accounted for the variations of the number of systems in service from reporting period to reporting period.

2. REDUCTION OF THE LEARNING DATA AND DESIGN REVIEW

This part is devoted to the description of the data used, and to a short development of the feature extraction algorithm to be applied.

2.1. Description of the learning datas k(I,J)

Assume that all learning datas $k(I,J) = \{(k(i,j) \geq 0,\ i \in I,\ j \in J\}$ about equipments $j \in J$ of the same type, are coded and stored in a data bank:

$$k(i,j) = \begin{cases} 1 & \text{symptoma i present} \\ 0 & \text{- i absent or missing information} \end{cases}$$

and/or

k(i,j) = measured value i concerning the equipment j, i.e. time since last overhaul TBO_j, operational circumstances,.....

In the coding, at most N different types of information c = 1,N are given about each equipment j, due to the content of the failure/ maintenance reports. Each information "c" has a fixed set of alternatives "i", corresponding for example to a fixed partition of the intervals "i" of variations of the time since last overhaul "c".

2.2. Transformations of the tableau k(I,J)

The past experiments have shown that misleading conclusions may be drawn from once compressed learning data, either because of too small learning samples, or because of carelessly filled reports. Methods to account for these phenomenons have been thoroughly tested in practice and justified theoretically (PAU [9]). Other transformations may be done, in order to study the learning datas from specific viewpoints:

a) the learning data k(I,J) are called explicit if one of the sets I, J designates equipments, and the other observations about these (as in 2.1).

b) the learning data k(I,J) are called implicit if both sets I, J are observations; such a tableau is deduced from an explicit tableau by aggregating some observations with respect to all equipments, or by classifying all equipments with respect to some observations. For example, if J has become the set of TBO intervals, we may define:

> k(i,j) = number of learning equipments having had a failure in the TBO-interval "j", and on which the symptoma "i" was present.

Design review uses generally learning data in the implicit form (2.4, 2.5), while automated diagnosis uses the explicit form (3.).

2.3. Feature extraction by the means of correspondence analysis

Assume that the tableau k(I,J) of non-negative numbers is given. The feature extraction procedure used herein, is a special form of principal component analysis, characterized by the following additional properties demonstrated in BENZECRI (2) and PAU (10):

- no a priori hypothesis is made about the nature of the elements in the sets I (failures) and J (observations or equipments), and all interactions are considered; in other words, we do not care for the labels in the sets I and J;

- all elements in both sets I and J may be displayed simultaneously in the same reduced feature space, because they play symmetrical roles in a tableau; in this reduced pattern space, the euclidean distance between any two elements of I-J, I-I, or J-J, is an overall statistical measure of the correspondence between those elements, independently of all scale effects.

It can be shown that the pricipal component analysis, factor analysis, and the present correspondence analysis are all special forms of the KARHUNEN-LOEWE expansion or Varimax priciple, for different choices of the metrics on I, J and/or of the criterion used (see KULIKOWSKY (6), WATANABE (15)). We will therefore describe correspondence analysis according to the common guidlines:

a) The non-negative learning datas k(I,J) are transformed into an estimated contingency table p(I,J):

$$p(i,j) = k(i,j) \Big/ \left(\sum_{\substack{\ell \in I \\ m \in J}} k(\ell, m) \right)$$

with estimated marginal probability density functions as in a contingency table:

$$P^I = \left\{ p(i,.) = \sum_{j \in J} p(i,j) / i \in I \right\} \qquad \text{Prob}(j \mid i) = p(i,j) \mid p(i,.)$$

$$P_J = \left\{ p(.,j) = \sum_{i \in I} p(i,j) / j \in J \right\} \qquad \text{Prob}(i \mid j) = j(i,j) \mid p(.,j)$$

b) The metric on I is the distance function d_I, while the metric on J is the distance function d_J:

$$d_I^2(i_1,i_2) = \sum_{j \in J} \left[\text{Prob}(j \mid i_1) - \text{Prob}(j \mid i_2) \right]^2 / p(.,j)$$

$$d_J^2(j_1,j_2) = \sum_{i \in I} \left[\text{Prob}(i \mid j_1) - \text{Prob}(i \mid j_2) \right]^2 / p(i.,)$$

c) The element i has the weight p(i,.), while j has the weight p(.,j). The element i has Card (J) coordinates

$$(\text{Prob}(j \mid i)) \quad j = 1, \text{Card } (J).$$

The element j has Card (I) coordinates

$$(\text{Prob}(i \mid j)) \quad i = 1, \text{Card } (I).$$

d) Let be given a constant $r \leq \text{Inf}(\text{Card}(I), \text{Card}(J))$. We want to minimize, in the sense of the d_I or d_J metric, the dependence between I,J defined as $\left|\left|P(I,J) - P^I P_J\right|\right|^2$.

It can be shown that the r-dimensional vector basis of basic features which minimizes this dependence after transforming Card (I) - or Card (J) - dimensional patterns in k(I,J) into r-dimensional feature vectors, can be constructed as follows (see PAU (9,10)).

- for I the r base vectors f_ℓ ($\ell = 1,r$) are the r first principal axes of inertia of the solid body made of the discrete Card (J) dimensional elements $i \in I$ having the weight p(i,.); this inertia is computed for the d_I distance; let $\lambda(f_\ell)$ be the inertia of axis f_ℓ ($\ell \in 1,r$) ordered by $\lambda(f_1) \geq \lambda(f_2) \geq \ldots \geq \lambda(f_r)$; the f_ℓ's are normed to the unit length with respect to d_I. And $f_\ell(\lambda_\ell)$ is the $(\ell + 1)$'st eigenvector (resp. eigenvalue) of the $S = \left[s_{j_1 j_2}\right]$ matrix:

$$\left[s_{j_1 j_2} = \sum_{i=1,\text{Card}(I)} p(i,j_1)p(i,j_2)/p(i,.)\sqrt{p(.,j_1)p(.,j_2)} \right.$$

$$\left. j_1, j_2 = 1, \text{Card}(J) \right.$$

- for J, we have equivalent definitions and relations for the r basis vectors g_ℓ ($\ell = 1,r$)

f_ℓ, g_ℓ ($\ell = 1,r$) are here row vectors, i.e. linear mappings.

e) The coordinates of the learning patterns projected into the r-dimensional fearure space, are computed as follows:

- for I, the feature $\ell = 1,r$ of learning pattern $i \in I$ on the axis f_ℓ, originated in the center of inertia of all elements in I, is given by (see Figure 1):

$$G(i,\ell) = f_\ell \cdot \left[\text{Prob}(j|i) \quad j = 1, \text{Card}(J) \text{ vector}\right] \qquad (1)$$

- for J, the feature ℓ of learning pattern $j \in J$ on the axis g_ℓ, originated in the center of inertia of all elements in J, is given by:

$$F(j,\ell) = g_\ell \cdot \left[\text{Prob}(i|j) \quad i = 1, \text{Card (I) vector}\right] \qquad (2)$$

f) I can be shown that $\lambda(f_\ell) = \lambda(g_\ell)$, ($\ell = 1,r$, and that it is sufficient to compute either the f_ℓ's or the g_ℓ's because:

$$\left[\begin{array}{l} g_\ell = \dfrac{1}{\sqrt{\lambda(f_\ell)}} \; f_\ell \left[\begin{array}{l} \text{Prob (j/i)} \\ \end{array}\right. \begin{array}{l} i = \text{column} \\ \\ j = \text{row} \end{array} \left.\begin{array}{l} \\ \\ \end{array}\right] \\ \\ G(i,\ell) = \displaystyle\sum_{j=1,\text{Card}(J)} F(j,\ell) \; \text{Prob}(i|j) / \sqrt{\lambda(f_\ell)} \qquad \ell = 1,r \end{array}\right. \qquad (3)$$

Moreover, the latter formula transforms biunivocally a d_I - orthonormal vector base into a d_J - orthonormal vector base of same dimension r and with the corresponding unit lengths. Consequently, all elements of I and J may be displayed simultaneously in this feature space $f_\ell (\ell = 1,r)$, thanks to formulas (1) (2) (3). In this space, the euclidean distance d between any two elements of I or J being proportional to d_I, we may also measure mixed d_I distances between an element of I and an element of J (see BENZECRI [2], PAU [10]).

g) The best two-dimensional (r=2) approximation of the learning data (see BENZECRI [2], PAU [10]), is obtained by displaying all elements of I and J on the (f_1, f_2) plane which contains the largest inertia, namely $(\lambda(f_1) + \lambda(f_2))$. Such a 2-dimensional approximation will be called a map, and any pair of vectors f_ℓ, f_m yields such a map of weight $\lambda(f_\ell) + \lambda(f_m)$.

2.4. Application to design review and control of maintenance

The correspondence analysis used as indicated is an answer to the problem P1:

a) All redundant observations can be identified: the distance d_I, and thus d, of any two observations i_1, i_2 in I will be small m if they are conditionally associated in the same way to all observations of J:

$$\forall j \in J \quad \text{Prob}(j|i_1) = \text{Prob}(j|i_2) \Rightarrow d_I(i_1, i_2) = 0 \Rightarrow d(i_1, i_2) \neq 0$$

Thus, if two failures i_1, i_2 are represented almost by the same point in the feature space:

- either: one of the observations i_1, i_2 is redundant, i.e. because of the coding, or because one of these observations can only be done by taking down a module connected to the other one (this is a maintainability question);

- or: the failure mode i_1 may systematically be the main cause of the failure i_2, or conversely.

b) It can be shown that, when the sample size $\sum_{I,J} k(i,j)$ becomes infinite, the asymptotic distributions of d_I, d_J, d, are CHI-square distributions with (Card (I)-1)(Card (J)-1) degrees of freedom; we do therefore obtain a natural clustering and discrimination between failures, quite equivalent to CHI-square partitions in a contingency table.

Moreover, the interpretation phase suggests a simple answer to problem P2 with applications to design review and maintenance control. We will use the natural clustering obtained in the data compression process, and the meaning of the metrics d_I, d_J, d; the goal will be to express in the physical terms used for the definitions of the i's and the j's, the associations corresponding to the geometrical proximities observed on the maps of decreasing weights.

a) In the first phase, we will interpret the natural clusters obtained; if any two points are:

- d-very close, those points will be very strongly associated with respect to the d_I, d_J similarity measures: one point is very probably the cause of the other one, or conversely:

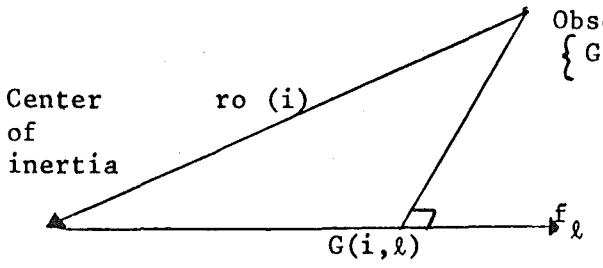
- d-close, these points will often have a similar behaviour with respect to d_I, d_J and there exists a causality relation between them at a medium level;

- d-distant, those points will often have different behaviour, and the causality association is weak in the sense of d_I, d_J.

Once an association has been detected, i.e. between certain failures and maintenance operations, the maintenance department will have to give technical reasons herefore, or demonstrate why it is meaningless.

b) In the second phase, which is the confirmation of the first one, the d-distances measured on the map, and CHI-square tables are used to compute the probabilities that two vectors p(J/i) or p(I/j) are identical.

c) In the third phase, we want to select those observations or failure having effectively an influence upon the extracted features. This is done by a study of the contribution to the r features, as illustrated below in the case of I:



$\lambda(f\ell)$= inertia with respect to the direction f_ℓ .

$$p(i,j) = p(i,.)p(.,j)\left(1+\sum_{\ell} F(j,\ell)G(i,\ell)\sqrt{\lambda(f\ell)}\right)$$

$$\lambda(f_\ell) = \sum_{i\in I} p(i,.)G(i,\ell)^2$$

$p(i,.)ro(i)^2$ = absolute contribution of i

$p(i,.)G(i,\ell)^2$ = absolute contribution of i to $\lambda(f_\ell)$

$G(i,\ell)^2$ = absolute contribution of feature ℓ to i

$G(i,\ell)^2/ro(i)^2$ = relative contribution of feature ℓ to i

Figure 0 : Study of the contributions in the extracted feature space for I.

If the absolute contribution of the observation $i \in I$ is large , it contributes significantly to $\left|\left| p(I,J) - P\ P_J \right|\right|$, which means that an observation i, located far away from the center of the map, and having a small weight p(i,.), does not have much meaning. The relative contribution of the feature ℓ to $i \in I$, indicates whether this feature explains correctly the location of this observation.

The main goal of this interpretation procedure is to draw attention upon causality relations among failures, maintenance, modifications, operating conditions and times; it has been applied to both electronic and mechanical airborne equipments in order to:

- detect systematic coding errors;

- criticize maintenance operations and their real time schedule;

- detect subsystem or operating conditions which may be responsible for failures because of uncareful design, fabrication, maintenance, eventually in some special time intervals.

These preoccupations, as related to specifications and test organizations, are discussed by YOUNG[16]. Our view is that the learning phase must be conducted in parallel with the analysis of expert' special reports, in order to compare them both.

2.5. Example 1: airborne equipment

We will interpret some associations between observations and/or time intervals in the Fig. 1 relative to a radiocompass RNA 26 C. Our main concern will here be to criticize the coding of the learning data of the implicit type 1 explained in Fig. 3.

All observations of class c=1 (physical failure cause) are, except 1DV, 1TR, lined up on the first axis f_1 in the following order: 1TE, 1EM, 1EL, 1ME. The latter classification, obtained through a natural discrimination, is feasible from the technical point of view, namely:

- electromechanical lies halfways between electrotechnical and passive component failures;
- electrotechnical and mechanical failures are strongly dissociated.

In the same way, the failures of active components are clearly discriminated: these components have quite specific failure causes, mostly between 50 h and 100 h. The other failures are very strongly dissociated from 1TR; which means that there is no ambiguity from the point of view of those people who classify failures as being of the 1TR type. We will almost never find among "other failures" some 1TR failures.

The failures 1TE, 1EM, 1EL are approximately equidistant of 1DV: there is an indifferent tendency to classify the n med failures as miscellaneous in case of ambiguity. The failures 4 CO, 4CC are also fairly frequently classified as "miscellaneous", or the opposite. There seems therefore to be an ambiguity about all these failures, expecially 1EL. The measure taken was to modify the maintenance handbook in order to avoid this kind of coding ambiguity, and a success was noted.

Many other failure diagnoses may be formulated, and are left as an exerciese to the reader. It should for example be noted that 1EL, and 1EM, are the failures to be investigated most thoroughly by the designers in order to improve the life-time up to around 400-800 h.

2.6. Example 2: common and high-stability resistors

An implicit learning data set is being used in order to investigate the actual drift failures J, as related to other characteristics of the resistors announced by the manufactures. Correspondence analysis yields the map of highest inertia given in Fig. 3 while the data sets are reported in GOARIN [4].

Note that the axis f_1 is ranking the drifts so that the other observations may be classified with respect to the drift reliabilities. This is why the socalled "high-stability resistors" FHS and "common resistors" FUC are located diametrally in the f_1-direction, and have high absolute contributions to f_1. We do also remark that metal film resistors behave better than metal oxide resistors, and even better than carbon film resistors.

The negative drifts DMO are well explained by f_2 and by the manufacturer F of carbon film resistors having this property. The connection mode, welded or set, has a significant effect. Though, F is not the only manufacturer to produce carbon film resistors, and the technology alone cannot explain his criticable position. In the same way, the manufacturer E has an enviable position on f_1 and f_2, even if he produces both carbon and metal film resistors with very different drift properties; it is therefore proved that the manufacturer has a big influence upon this kind of reliability, and that this influence is not due to the technology used.

3. REAL TIME DIAGNOSIS BY PATTERN RECOGNITION

Real time diagnosis has been achieved, yielding a simultaneous solution to the problems P2 and P3. The pattern recognition technique which has been used, includes first the learning stage, next the real time feature extraction, and lastly the recognition procedure wherein the r features characterizing the observed failures are compared to the learning datas.

3.1. Learning stage

The learning patterns are defined as being the explicit tableau $k(I,J) = \{k(i,j) \geq 0,\ i \in I \quad j \in J\}$ defined in 2.1. They are obtained by gathering all informations $i \in I$, and moreover TBOj and others, about a large number of equipments $j \in J$, for which the failure cause $d(j)$ has been determined by the quality control or maintenance personnel. We assume that the total number of different failure causes $d \in D$ is small with respect to the total number of equipments observed. Assume that the probability distribution $\{P(d) \mid d \in D,\ P(d) > 0\ \sum_D P(d) = 1\}$ of the failure causes has been estimated within the learning datas or by other means.

The learning features, which will be used during the recognition phase, are the images of the learning patterns in a reduced feature space having a fixed dimension r. The feature extraction procedure used is the correspondence analysis of paragraph 2.3 applied to the tableau k(I,J).

3.2. Real time feature extraction for a failed equipment

Assume that troubleshooting has just been observed on an equipment $\bar{j}$ of the type investigated in 2.1, and that it has been possible to gather all informations $\{k(i,\bar{j}),\ i \in I\}$ about $\bar{j}$. We may consider $\bar{j}$ as a supplementary learning pattern belonging to an unknown class $d(\bar{j})$; but, since the correspondence analysis of k(I,J) is made without taking into account the knowledge of $d(j)$, $j \in J$, we may locate $\bar{j}$ in the feature space thanks to the formula [2] :

$$\begin{cases} F(\bar{j}, \ell) = g_\ell \cdot [\text{Prob}(i|\bar{j}) \quad i = 1, \text{Card } (I)] \quad \ell = 1,r \qquad [4] \\ \text{Prob}(i|\bar{j}) = k(i,\bar{j}) / \left(\sum_I k(i,\bar{j}) \right) \end{cases}$$

where $F(\bar{j}, \ell)$ is the coordinate of the equipment $\bar{j}$ on the ℓ-th feature axis g_ℓ ; it is assumed that the numerical values of $\{k(i,\bar{j}),\ i \in I\}$ do not perturbate the earlier calculation of the vectors g_ℓ ($\ell = 1,r$). Here again, the failed equipment may be displayed on maps as those discussed in 2.4, and we look for associations, either with the learning equipments $j \in J$ for which $d(j) \in D$ is known, or with the observations $i \in I$.

These associations may help in formulating some precise experimental hypothesis about the mechanism of the failure detected in 3.3 on the equipment $\bar{j}$.

3.3. Recognition procedure

We will consider one single recognition procedure, applied sequentially, and yielding at each step a classification of the observed equipment pattern $\bar{j}$ into the most probable failure class $d(\bar{j}) \in D$. The nearest neighbour rule has been generalized as follows (see LOFTSGAARDEN [7], PAU [8], and Fig. 4) :

$$\bar{j} \in \text{class } d(\bar{j}) \iff \frac{n_{d(\bar{j})} \quad P_{d(\bar{j})}}{\left[N_{d(\bar{j})} + 1\right] V_{d(\bar{j})}} = \max_{d \in D} \frac{n_d \quad P_d}{\left[N_d + 1\right] V_d}$$

- d = class of failure causes selected in D.
- N_d = number of "reference patterns" in class d, as defined below.
- P_d = estimated probability of occurence of random failure cause d in the set D, as introduced in 3.1.
- n_d = integer paramter, determined for each class d.
- V_d = minimal volume of a neighbourhood of the newly observed equipment $\bar{j}$, so that (n_d-1) reference patterns of the class $d \in D$ are interior to this neighbourhood, while one single reference pattern is on the boundary hereof; the neighbourhood have statistically independent shapes as those of TUKEY's [14] tolerance regions.

The named "reference patterns" are N_d points, i.e. learning equipments, projected into the feature space, and representing a single class of failure causes $d \in D$; for each cause $d \in D$ they are:

a) the center of gravity of all the learning equipments j belonging to the class d because $d(j) = d$: then $n_d = N_d = 1$;

b) the extremities of r dipoles approximating the cloud of all projected learning equipments j belonging to the class d: then $N_d = 2r, n_d \neq r$;

c) all teh projekted learning equipments j belonging to the class d: their number is again called N_d, and n_d is determined in order to minimize the probability of misclassification; n_d is of the size 3 to 20.

Our nearest neighbour rule is then used sequentially as follows (see PAU[12] : given an observed failed equipment $\bar{j}$ for which we need a diagnosis, we do apply this rule successively from a) to c) to different types of "reference patterns" so that the ratio (global recognition time for $\bar{j}$, estimated probability of good classification) is minimized. The computation time at each step, and the approximation of the probability of good classification, will probably both increase with the N_d's. Therefore, if a quick procedure such as 3.3 a) yields a high recognition rate thanks to a good experimental discrimination of j, it will be useless to continue to step b).

The final diagnosis is made by computing the product of the probabilities of misclassification yielded by each step we have been through, and for all classes in D, when taking into account the apriori recognition rates. The best classification decision ($d(\bar{j})$ minimizes this global misclassification probability within the set D of alternatives, even if conflicts may appear between successive steps. The two or three best alternatives, including $d(\bar{j})$, may also be obtained. We will only put down and repair those few subsystems which are the failure causes of highest probability.

Though, it is clear that this procedure would be misleading if the actual failure had not been included in the catalog D; if the result $d(\bar{j})$ happens frequently to be absurd, one has to examine thoroughly the learning data and the set D of alternative failures.

3.4. Example of automated testing

We have considred a stationary fabrication process of complex electro-mechanical systems with very stringent specifications and small dimensional tolerances. The 82 observations on each equipment $j \in J$ in the process were the measurements made by the quality control department at the input of the process, and the operational characteristics of the machine tools when used on each specific system (settings, cumulated time of operations, time

since servicing, type of tool, air flow, temperature, oil flow, rotation speeds, workers operating the machines,...). The 21 classes of failures included the special class d_o of all equipments for sale fulfilling all quality control requirements.

a) During the learning phase, data were collected on Card (J) = 2000 items (20 days of production), among which 800 non-acceptable items were identified at the final quality control and received a diagnosis each (chosen among the 21 classes of failures). These learning datas were processed on a general purpose IBM 370-65 computer (12 min CPU). The computation of the $f_\ell(\ell = 1,r)$ ran into some numerical diagonalization problems. Through the review process described in 2.4, it became possible to pinpoint those systematic aspects of the production process having indirectly the strongest contributions to the named failures, in this case the oil flows.

b) During the testing phase, a true recognition rate of 92 % was achieved for the items classified into the class d_o by the final quality control, still working. The mean true diagnosis rate for the 20 types of actual failures was 81 % when r=10; mean unitary diagnosis computing time: 0,46 s.

c) During the operational phase under final implementation, all 82 observations will be monitored in real time for each equipment in the production line; most non-destructive tests and the final quality control will be suppressed. Some few specialists will play a supervisor role for the automatic diagnosis system, including the small on-line data-logging and computing unit. Considerable economical benefits may be obtained, as evaluated on the basis of the testing phase b). These specialists will perform design reviews, modify and enlarge the learning data bank.

The case of a non-stationary fabrication process, has been investigated by POKROWSKY [13] along with accelerated testing. The mean result is that the number of observations by item, here 82, must be increased as the process stabilizes.

The author has at a certain moment been uncertain on the wisdom of using reduced features whithout reference to the learned diagnosis d(j) $j \in J$, when the features are to be used for diagnosis. Therefore a canonical correlations analysis and discriminant analysis were used, but performed very badly; the reason is that the "natural" clusters obtained by the non-parametric correspondence analysis do not usually fit well with the classifications determined by the coding (see again 2.5).

4. CONCLUSION

The conclusion is that pattern recognition techniques can help providing the designers and the maintenance specialists with a set of assumptions, and in making repairs more efficient through a rationalization of the inductive and sequential diagnosis formulation processes.

The results will be all the more realistic than the individual equipments will be numerous to be monitored during their whole life or during the production process. But even more important is the quality requirement for these datas. It is indeed a very actual problem to define properly the reliability or maintenance paramters to be monitored, to control the data-logging process, and to make the data files compatible. These are very lengthy, costly and even risky steps, and the manufacturer should beforehand be aware of it. Since data banks with technical informations are set up and the gathering initiated in an increasing number of institutions, especially for military or aerospace applications, this compatibility requirement must have the very first priority.

Lastly, the profits which may be expected from the outlined automatic diagnosis system are important, because it is basically designed for complex systems of high cost, characterized by multiple failure patterns, and important interactions between the external environment, the maintenance and the production control. Statistical pattern recognition like hereabove is probably the only approach to diagnosis in mechanical and non-purely electronic equipments.

While automated diagnosis is being implemented on operational systems connected to small embarkable computing units, the research is being carried forward about:

- diagnosis on the basis of the variations in time of certain paramters, i.e. fluctuations in rotation speeds;

- sequential learning and diagnosis (see POKROWSKY [13], PAU [11]).

REFERENCES

(1) BECKER, P.W. Recognition of patterns, Copenhagen, Denmark, Polyteknisk Forlag, 1968.

(2) BENZECRI, J.P. Statistical analysis as a tool to make patterns emerge from data. Proc. 1968 Honolulu Cong. on pattern recognition, Academic Press, 1969.

(3) CORTINA, E., ENGEL, H.L., and SCOTT, W.K. Pattern recognition techniques applied to diagnostics. SAE rep. 7000407, Midyear meeting, Detroit, Michigan, 18-22/5/1970.

(4) GOARIN, R. Application de l'analyse des correspondances à l'étude de la fiabilité des composants électroniques, Congrès national de fiabilité, Perros-Guirec, September 1972.

(5) HANKLEY, W.J., and MERRILL, H.M. A pattern recognition technique for system error analysis, IEEE Trans. on reliability, Vol. R-20, No. 3, August 1971.

(6) KULIKOWSKY, C.A. Pattern recognition approach to medical diagnosis, IEEE Trans. Systems Science & Cybernetics, Vol. SSC-6, No. 3, July 1970.

(7) LOFTSGAARDEN, D.O. and QUESENBURY, C.P. A non-parametric estimate of a multi-variate density function. Ann. Math. Statist., 36, 1965, 1049-1151.

(8) PAGE, J. Recognition of patterns in jet engine vibration signals, IEEE Publ. No. 16 c 51, 102-105.

(9) PAU, L.F. Diagnostic statistique; synthèse des informations relatives á la fiabilité et à la maintencance d'un matériel aéronautique, L'Aéronautique et l'Astronautique, No. 34, 1972-2.

(10) PAU, L.F. Méthodes statistiques de réduction et de reconnaissance des formes, dr. thesis, Paris University, 1972.

(11) PAU, L.F. Sequential pattern recognition methods applied to technical diagnosis and maintenance, IMSOR, Technical University of Denmark, 1972.

(12) PAU, L.F. Statistical reduction and recognition of speech patterns, in : Machine perception of patterns and pictures, book, published by the Institute of Physics, London, as Conference series No. 13, 1972.

(13) POKROWSKY, F.N. On reliability prediction by pattern classification, Proc. 1972 Annual reliability and maintainability symposium, San Francisco, Annals of Assurance sciences, IEEE Catalog 72CH0577 - 7R, 367-375.

(14) TUKEY, J.W. Non-parametric estimation, II: statistical equivalent blocks and tolerance regions, Ann. Math. Statist., 18, 1947, 529-539.

(15) WATANABE, S., and LAMPERT, P.F. Evaluation and selection of variables in pattern recognition, in: Computer and information sciences, Vol. 2, N.Y., Academic Press, 1967, 91-122.

(16) YOUNG, H.W. Specifying the interface between design and test organizations, Inst. of electronic and radio engs., Conf. on automatic test systems, Proc. April 1970.

(17) PAU, L.F. Applications of pattern recognition to the diagnosis of equipment failures, in : Kognitive Systeme und Verfahren, Lecture Notes no 83, Springer Verlag Heidelberg & N.Y., april 1973.

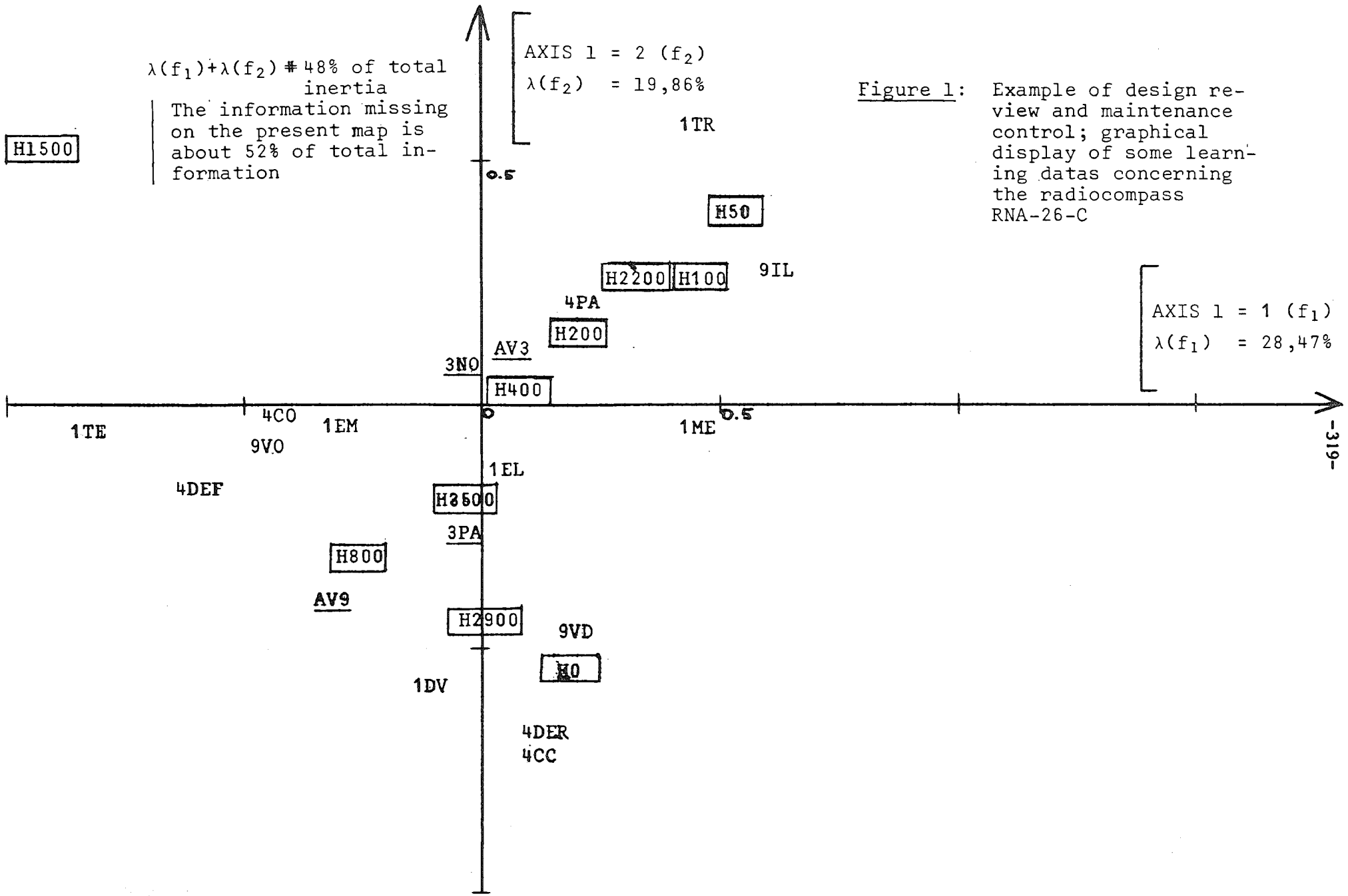
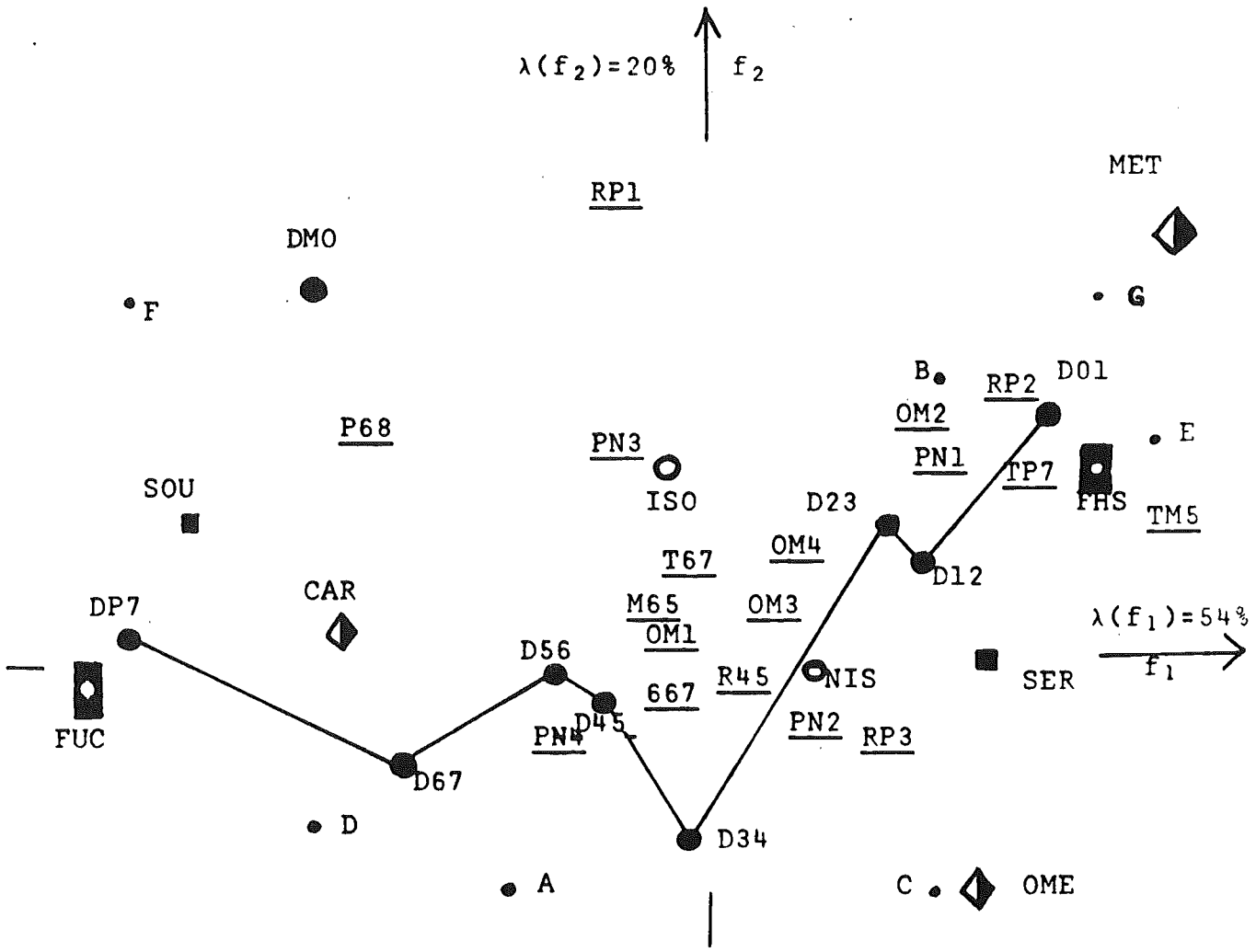


Figure 1: Example of design review and maintenance control; graphical display of some learning datas concerning the radiocompass RNA-26-C

Figure 2

Class c∈C of informations	Alternative i∈c	Interpretation
AV (type of aircraft)	AV3	Caravelle
	AV9	Fokker Friendship
H (TBO-intervals)	Hj*	Hj* is the TBO-interval j*∈J*; i.e. H400 means that there is an interval j* beginning at 400 hours; the next interval begins at 800 hours
1 (failed component)	1 EL	failures of non-active electronic components, i.e. resistors, ...
	1 TR	failures of active electronic components, i.e. transistors, ...
	1 EM	failures of electromagnetic components, i.e. relays, ...
	1 ME	failures of mechanical parts
	1 TE	failures of the electrical supply system
	1 DV	miscellaneous failures of non-identified nature
3 (nature of operation)	3 PA	justified maintenance operations, because of failures of components.
	3 NO	other maintenance operations: check, unjustified, trimming, ...
4 (diagnosis)	4 DEF	component out of service
	4 DER	badly trimmed component
	4 CO	bad electrical contact
	4 CC	short-circuit
9 (external implications)	9 VO	necessary maintenance of the VOR
	9 VD	badly trimmed VOR system
	9 IL	necessary maintenance of the ILS system



DMO : negative mean drift of electrical resistance at 1000 hours
D01,D12,D23,D34,D45,D56,D67,DP7 : Dmn indicates a positive mean drift of n to m percent at 1000 hours
FHS,FUC : high-stability and common resistors , respectively
CAR,MET,OME : carbon film, metal film , metal oxyd resistors,resp.
ISO,NIS : isolated, non-isolated resistors , resp.
SOU,SER : welded,set connections , resp.
A until G : symbols for the manufacturers of resistors
M65,667,P68 : resistors manufactured before 1965,1966 or 1967 , 1968 or later
PN1,PN2,PN3,PN4 : nominal effects as limited by 250,500 and 1000mW
OM1,OM2,OM3,OM4 : nominal resistance limited by 35Ω ,100kΩ ,300kΩ
TM5,T67,TP7 : test temperatures limited by 50° C , 75° C
RP1,RP2,RP3,R45 : ratio of actual to nominal effect , limited by 25 %, 50 %, 75 %.

Figure 3 : Design review of common and high-stability resistors .

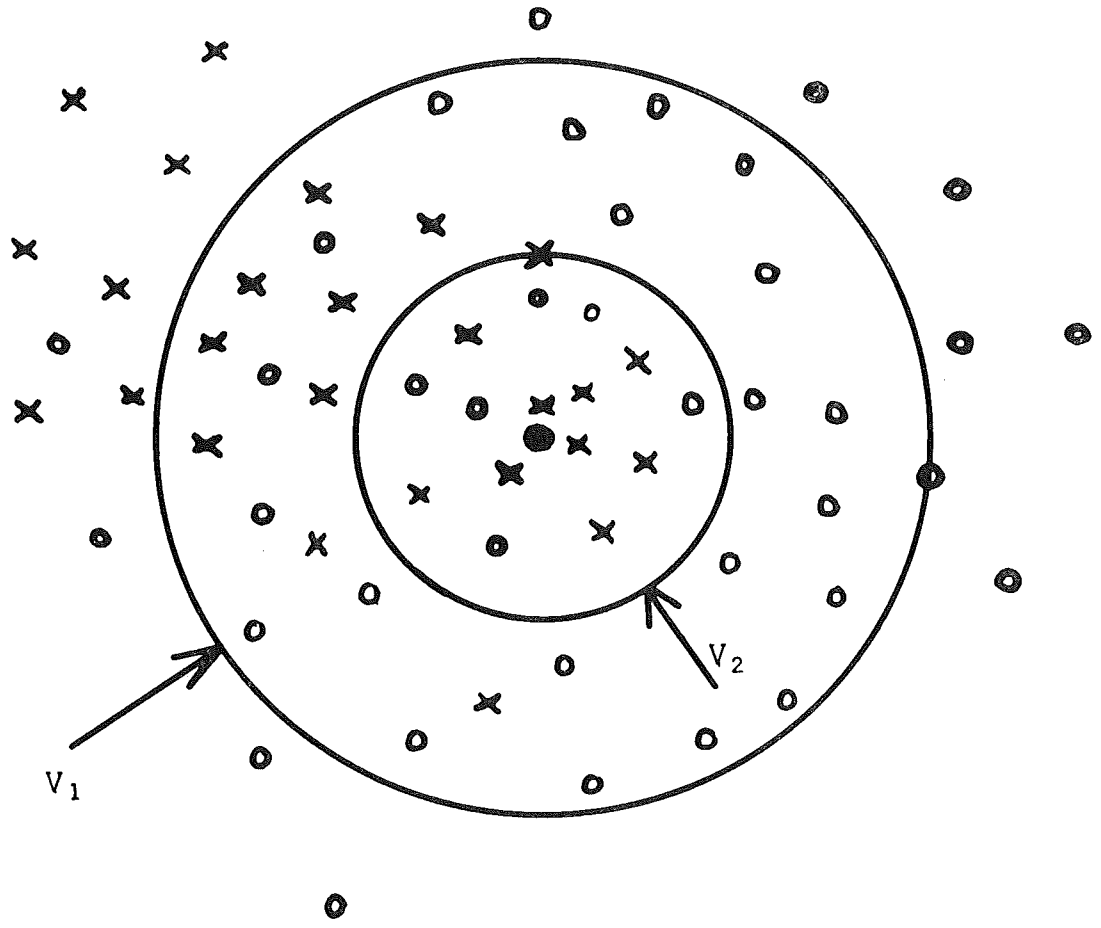


Figure 4 Generalization of the nearest neighbour rule

	Class d=1 (symbol 0)	Class d=2 (symbol x)
n_d	28	9
P_d	α	$(1-\alpha)$
N_d	38	25
V_d	2,500	0,529
$\frac{n_d P_d}{(N_d+1)V_d}$	0,287 α	0,654 $(1-\alpha)$

The unknown pattern belongs to:

- class d=1 if $\alpha > 0,692$
- class d=2 if $\alpha < 0,692$