KERNFORSCHUNGSZENTRUM

KARLSRUHE

März 1975 KFK 2100

Projekt Nukleare Sicherheit
Institut für Angewandte Systemtechnik und Reaktorphysik

STATUSBERICHT

Methoden zur quantitativen Analyse von Kernenergie-Risiken

R. Papp, L. Caldarola, F. Helm
P. Jansen, P. McGrath, G. Weber

GESELLSCHAFT
FÜR
KERNFORSCHUNG M.B.H.

KARLSRUHE

GESELLSCHAFT FÜR KERNFORSCHUNG M. B. H.

KARLSRUHE

K E R N F O R S C H U N G S Z E N T R U M
K A R L S R U H E

Januar 1975 KFK 2100

Projekt Nukleare Sicherheit

Institut für Angewandte Systemtechnik
und Reaktorphysik

S T A T U S B E R I C H T

Methoden zur quantitativen Analyse von Kernenergie-Risiken

R. Papp, L. Caldarola, F. Helm,
P. Jansen, P. McGrath, G. Weber

Gesellschaft für Kernforschung m.b.H., Karlsruhe

Diese Studie wurde im Auftrag des
Projektes Nukleare Sicherheit erstellt.
Die Autoren möchten Herrn Dr. M. Fischer
und Herrn Dr. J.P. Hosemann für nützliche
Diskussionen danken.

Inhaltsverzeichnis

VORWORT

Im vorliegenden Bericht werden vor allem die Störfall-Risiken von Kernenergieanlagen behandelt. Auf Normalbetriebs-Risiken wurde nicht eingegangen; allerdings kann die Grenze zwischen Normalbetrieb und Störfall oft nicht eindeutig festgelegt werden, der Übergang zwischen diesen beiden Bereichen ist fließend.

Die Risiken, die durch Entwendung radioaktiven Materials, durch Sabotage und beim Transport radioaktiven Materials entstehen, wurden in diesem Bericht nicht behandelt.

Die Gliederung wurde so gewählt, daß der Teil A ("Übersicht") die Problematik der Analyse von Kernenergierisiken zusammenfaßt. Eine detailliertere Behandlung von wichtigen Teilaspekten erfolgt im Teil B ("Spezielle Analysen"). Die zitierte Literatur ist jeweils am Schluß des betreffenden Kapitels zusammengestellt. Eine Übersicht über das gesamte beachtete Schrifttum findet sich, nach Autoren in alphabetischer Reihenfolge geordnet, im Teil C.

A. Ü B E R S I C H T

I. EINLEITUNG UND ZUSAMMENFASSUNG

Die Einführung der Kernenergie findet zu einem Zeitpunkt statt, der durch zunehmende Einwirkung des Menschen auf den Lebensraum gekennzeichnet ist. Gleichzeitig wird in verstärktem Ausmaß die Notwendigkeit erkannt, quantitative Methoden zu entwickeln, mit deren Hilfe das Ausmaß dieser Einwirkung abgeschätzt werden kann.

Obwohl die Verwendung der Kernenergie (KE) auch Vorteile im Hinblick auf Wirtschaftlichkeit und Umweltbeeinflussung gegenüber konkurrierenden Energieformen mit sich bringt, kommt es zu Widerständen großen Ausmaßes gegen den Einsatz der KE. Opponenten weisen auf das große Ausmaß des damit verbundenen Risikos hin.

Um die Möglichkeit zu schaffen, zu quantitativen Aussagen zu kommen, versucht man daher gerade auf dem Gebiet der KE mehr und mehr Kosten/Nutzen/Risiko-Analysen einzusetzen. Jedoch ist der Blickwinkel, unter dem diese Untersuchungen durchgeführt werden, heute noch sehr schmal, denn es handelt sich dabei im wesentlichen nur um Sicherheitsstudien. Diese sollten aber nur ein - wenn auch sehr wesentlicher - Teil einer Gesamtstudie sein, die alle Phasen des Brennstoffzyklus, aber auch Untersuchungen über die Haltung der Öffentlichkeit gegenüber Risiken zum Inhalt hat /1/.

Ein spezielles Problem im Rahmen der oben genannten Analysen stellt die Standortfrage von Kernkraftwerken dar. Bei der Auswahl von Standorten sind es vor allem sicherheitstechnische und wirtschaftliche Aspekte, die bei der Entscheidungsfindung eine wesentliche Rolle spielen. So besteht z.B. die wirtschaftliche Notwendigkeit, nahe an Zentren des Energiebedarfs - gleichbedeutend Bevölkerungszentren - zu bauen. Dem entgegengesetzt ist die Bestrebung, aus Gründen einer Verminderung des mit der Verwendung von Kernenergie verbundenen Risikos, Standorte in dünn besiedelten Gebieten auszuwählen. Daraus ergibt sich die Forderung, quantitative Sicherheitsnormen aufzustellen, so daß das Reaktorrisiko (R) als Planungsgrundlage in den Entscheidungsprozeß bei der Standortwahl mit einbezogen werden kann. Im Rahmen eines Risikokonzeptes müssen daher beispielsweise folgende Punkte behandelt werden:

a) Quantifizierung von R, wobei Abhängigkeiten wie etwa von der Umgebungsbevölkerung des Reaktors, dem Reaktortyp und klimatischen Faktoren in Rechnung gestellt werden müssen.

b) Quantitifizierung der Einflußgrößen der gesellschaftlichen Akzeptierung des Risikos ("Risk Acceptance" RA).

   Ansätze dazu werden durch Schaffung eines Bezugsrahmens, gebildet aus gesellschaftlich bekannten (und tolerierten) Risiken, geliefert, wie dies vor allem Starr /2, 3/ betrieben hatte.

   Dazu soll kritisch Stellung genommen werden, vor allem im Hinblick auf die Tatsache, daß der Vergleich von Erwartungswerten (Erwartungswert von Toten etwa) ungeeignet und eine Lösung dieses Problems mit Hilfe der Utility-Theorie /4/ möglich erscheint.

Bevor spezielle Methoden der Risikoberechnung betrachtet werden, sollen einige Aspekte der heutigen Sicherheitsphilosophie skizziert und Gemeinsamkeiten des deterministischen und probabilistischen Standpunktes unterstrichen werden:

Nach der heute praktizierten Sicherheitskonzeption wird eine Verringerung des Risikos dadurch erzielt, daß Sicherheitsfachleute einen größten anzunehmenden Unfall (GAU) als Auslegungsunfall definieren und das Kernkraftwerk zur Beherrschung dieses Unfalls ausgelegt wird. Auf diese Weise glaubt man auch eine Barriere gegen jeden weniger schweren Unfall geschaffen zu haben. Dieses Konzept wird in der Literatur üblicherweise als "deterministisch" bezeichnet (z.B. /5/); es gilt wohl als sehr konservativ, weist jedoch drei wesentliche Nachteile auf:

- Der Prozeß der Identifikation eines größten anzunehmenden Unfalls könnte ohne Ende sein, da man immer wieder Unfälle annehmen kann, deren Auswirkungen größer sind, als die des eben definierten.

- Die Bemühungen konzentrieren sich auf die Verringerung der Eintrittswahrscheinlichkeit schwerer, aber unwahrscheinlicher Unfälle, weniger schwerwiegenden, jedoch wahrscheinlicheren Störfällen wird nicht so großes Augenmerk geschenkt, obwohl nicht vollkommen ausgeschlossen werden

kann, daß einige von diesen - durch Propagationseffekte etwa - mit weitreichenden Konsequenzen verbunden sein könnten. Außerdem könnten Unfälle mit geringfügigen Auswirkungen auf Grund ihrer relativ großen Häufigkeit langfristig größere Konsequenzen haben als der eine größte anzunehmende Unfall mit seiner sehr kleinen Eintrittswahrscheinlichkeit.

- Ob der Konservatismus des GAU-Konzepts hinreicht, kann jedoch in Frage gestellt werden. Das zur Beherrschung des Auslegungsunfalls bestimmte Sicherheitssystem wird äußerst selten (bzw. nie) angefordert, so daß über dessen Wirksamkeit keine volle Klarheit herrscht und sich mangelnde Funktionsfähigkeit erst bei Anforderung herausstellen könnte. Außerdem können die zur Beherrschung großer Unfälle installierten Sicherheitssysteme selbst wieder Ursache von Unfällen sein.

Die Nachteile des deterministischen Konzepts sind wohl zum Teil darin begründet, daß bei der Unfallanalyse die Frage nach der Wahrscheinlichkeit des Eintretens aufeinanderfolgender Ereignisse nicht gestellt wird. Ist jedoch mindestens eines dieser Ereignisse unwahrscheinlich, so ist der Unfall selbst auch unwahrscheinlich.

Die Tatsache, daß der Kernenergie in Zukunft ein immer größerer Anteil der Gesamtenergie zukommen wird und daher die Frage des Risikos zusehends an Wichtigkeit gewinnt, verdeutlicht die Notwendigkeit der Einführung einer weiterentwickelten Sicherheitskonzeption. In steigendem Maße wird versucht, das mit der Kernenergie verbundene Risiko zu quantifizieren. Dazu genügt es aber nicht, nur die Konsequenzen eines Unfalles abzuschätzen, sondern es ergibt sich auch die Notwendigkeit der Bestimmung der Eintrittswahrscheinlichkeit dieses Unfalls. Diese Konzeption wird als "probabilistisch" bezeichnet.

Probabilistische Methoden kamen zuerst in der elektronischen Industrie zur Zeit des 2. Weltkrieges zum Einsatz. Bei der Massenfabrikation von elektronischen Bauelementen treten trotz enger Toleranzen und Qualitätskontrolle immer wieder Versagen von Bauelementen auf, ohne daß eine Ursache angegeben werden kann. Wollte man das Funktionieren etwa eines elektronischen Systems deterministisch sicherstellten, wäre es notwendig, alle Anfangs- und Randbedingungen für alle Kausalzusammenhänge zu kennen. Für

Menschen ist das in einem absoluten Sinne nicht vollziehbar. Man kann jedoch die Informationslücke hinsichtlich der im deterministischen Sinne vollständigen Kenntnis der Anfangs- und Randbedingungen durch Einsatz statistischer Methoden überbrücken, wodurch man zum Konzept der Ausfallwahrscheinlichkeiten kommt /6/. Das Auftreten möglicher Ausfälle kann demnach nicht deduktiv durch Naturgesetze beschrieben werden, sondern durch eine auf Beobachtung ähnlicher Ereignisse beruhenden induktiven Methode. Diese Beschreibung enthält als wesentliche Größe die Ausfallswahrscheinlichkeit. Auf Betriebserfahrung und Laboratoriumstests aufbauend, werden mittlere Lebensdauer und Zuverlässigkeit von Komponenten mittels statistischer Methoden errechnet. Gewisse Ausfälle können eben nach dem Stand des derzeit gültigen Wissens nicht kausal auf eine bestimmte Ursache zurückgeführt werden (was natürlich nicht bedeutet, daß dafür keine bestimmten Ursachen maßgebend wären). Trotzdem ist es offensichtlich, daß die etwa für elektronische Bauteile gültige Betrachtungsweise nicht voll auf Kernenergieanlagen übertragbar ist. Dort können nämlich Versagenshäufigkeiten der Größenordnung 10^{-6} - 10^{-11} pro Reaktorjahr auftreten. Dies würde bedeuten, daß im Mittel etwa 10^{6} - 10^{11} Reaktorjahre verstreichen müßten, bis dieses Versagen eintritt. Das umfassende Sicherheitsexperiment kann hier, auch wegen seiner großen "Reichweite" /7/, nicht durchgeführt werden. +) Daraus wird ersichtlich, daß diese Versagenswahrscheinlichkeiten experimentell nicht ermittelt werden können, sondern theoretisch abgeleitet werden müssen. Das erfolgt in einer Fehler- bzw. Ereignisbaumanalyse. Alle möglichen Ursachen oder Konsequenzen eines bestimmten Ereignisses werden zunächst mit Hilfe eines Ereignisbaumes in Diagrammform dargestellt und nach logischen Gesichtspunkten untersucht. Anschließend erfolgt die systematische Bestimmung der Fehlerwahrscheinlichkeiten eines komplexen Systems aus den Fehlerwahrscheinlichkeiten seiner Einzelteile. Allein die letztgenannten Wahrscheinlichkeiten werden experimentell gewonnen.

Es muß betont werden, daß die auf diese Art erhaltenen Unfallwahrscheinlichkeiten keine absolute Aussage liefern, sondern nur innerhalb der Grenzen desjenigen Wissens Gültigkeit haben, worüber der die Analyse ausfüh-

---

+) Die Frage nach dem Funktionieren moderner technologischer Systeme, wie etwa von 1000 MWe-Kraftwerken, stellt sich anders, als wenn es beispielsweise nur um das Funktionieren eines Motors geht, eben weil die funktionale Reichweite dieser Systeme beträchtlich ist. Mit der Reichweite der Funktionalität geht jedoch auch die Reichweite des Risikos einher.

rende Sicherheitsexperte bzgl. eines bestimmten Ereignisses verfügt /8/. Mathematische Modelle können hier nicht die Lücken schließen, die durch mangelnde Erfahrung und Erkenntnis entstanden sind.

Ein sehr altes und einleuchtendes Beispiel dafür liefert der Windscale-Reaktor in Großbritannien. Zur Zeit als der Reaktor gebaut wurde, waren die Sicherheitsingenieure im Rahmen ihres Kenntnisstandes von seiner Sicherheit überzeugt. Jedoch wußten sie nichts vom sogenannten "Wignereffekt" in Graphit, durch den ein schwerer Unfall ausgelöst wurde, der das ganze Core zerstörte.

Probabilistische Methoden sind daher kein Ersatz für mangelnde Kenntnis der physikalischen Phänomene! Dieses aus mangelnder Erkenntnis von Systemfehlern erwachsende Restrisiko läßt sich probabilistisch nicht fassen (man ist jedoch bemüht, durch konservative Auslegung kritischer Komponenten diesen Bereich abzudecken). Risikoberechnungen müssen im Rahmen eines Lernprozesses gesehen werden: die Berechnung des Risikos ein und desselben Reaktors kann, wenn sie zu verschiedenen Zeiten durchgeführt wird, auf Grund veränderter Erfahrung und Einsicht zu verschiedenen Ergebnissen führen. Das errechnete Risiko ist eben eine dynamische, keine statische Größe! Fehler- und Ereignisbäume sind ein Werkzeug, um den Lernprozeß in logischer, vollständiger und systematischer Form zu durchlaufen. In der Raum- und Luftfahrtindustrie ist es bereits geübte Praxis, Fehlerbäume in Computern gespeichert zu haben. Wann immer ein neues Phänomen auftritt, wird der Fehlerbaum sofort im Sinne der neuen Erkenntnis geändert; zusätzlich gestattet es die FB-Analyse, Bereiche zu erkennen, in denen verstärkte Forschungsarbeit nötig ist, womit wiederum die Entwicklungstendenz des Lernprozesses gesteuert wird.

Einige Vertreter der deterministischen Reaktorsicherheitsphilosophie bzw. der probabilistischen meinen, daß keine Verbindung zwischen den beiden Richtungen bestünde. Das ist ein Irrtum. Das deterministische Konzept einerseits und das probabilistische andererseits stellen zwei Phasen in diesem Lernprozeß dar, in dem die eine auf die andere folgt und sie sich gegenseitig ergänzen. Am Beginn einer neuen Technologie, wenn der Grad an Erfahrung und Erkenntnis gering ist, legt der Sicherheitsfachmann entspre-

chend diesem niedrigen Kenntnisstand einen größten anzunehmenden Unfall fest und plant entsprechende Sicherheitsmaßnahmen. Mit wachsender Betriebserfahrung erhöht sich der Kenntnisstand und auch das Vertrauen in die neue Technologie. In dieser zweiten Phase gehen die Experten daran, ihr Sicherheitskonzept zu überdenken und versuchen, zu einem vollständigeren und ausgewogeneren Gesamtbild zu kommen. Dies ist der Augenblick der Einführung der probabilistischen Konzeption.

Das bedeutet jedoch nicht, daß probabilistische Methoden selbst einen so hohen Entwicklungsstand haben, daß sie heute schon in die Genehmigungsverfahren von KKW Eingang finden könnten. Sie werden heute erst in beschränktem Umfang akzeptiert und etwa zur Identifikation von Schwachstellen in Systemen oder Festlegung von Wartungsstrategien herangezogen. Die Gültigkeit dieser Methoden muß in mancher Hinsicht noch demonstriert werden.

Um den Wert der Aussage von Risikoanalysen zu erhöhen, muß es z.B. auf den folgenden vier Gebieten zu einer Verbesserung des Kenntnisstandes kommen:

1. Die Korrelation von Fehlern von verschiedenen Komponenten und/oder Systemen könnte noch nicht erkannt sein: Common-Mode-Fehler (siehe Kapitel IX).

2. Ausfallarten und Ausfallraten von Komponenten sind häufig nicht hinreichend bekannt. Diese Frage wird detailliert in Kapitel II.A und VII behandelt.

3. Die Erfahrung zeigt, daß Unfallsituationen durch menschliches Fehlverhalten herbeigeführt oder verschärft werden können (siehe Kapitel X).

4. Es besteht die Notwendigkeit, alle möglichen Pfade eines Unfallablaufs zu beschreiben, so daß alle möglichen Konsequenzen berechnet werden können. In diesem Zusammenhang scheint es zwei schwierige Probleme zu geben:

   a) Identifikation der realistischen Propagationseffekte, auf Grund derer ursprünglich geringfügige Störfälle zu gefährlichen Unfällen ausarten.

b) Kenntnis der physikalischen Abläufe in einem Reaktor bei Änderung der ursprünglichen Geometrie.

Diese beiden Probleme sind allgemeine Sicherheitsprobleme, die natürlich auch im Rahmen des deterministischen Sicherheitskonzepts von Bedeutung sind. Sie werden daher in diesem Bericht nicht näher erläutert.

Das Problem der Feststellung von Schäden durch Kernenergie ist unmittelbar mit der Definition des Risikos verbunden. Risiko kann als die Gesamtheit aller möglichen Schadensarten gewichtet mit der Wahrscheinlichkeit ihres Eintretens definiert werden. Diese Definition reicht jedoch für Vergleichszwecke nicht aus; dazu müßten zwei Probleme gelöst werden:

- Für jede Schadensart muß ein Mittelwert errechnet werden, der nicht nur von der Verteilung der Eintrittswahrscheinlichkeit abhängt, sondern auch von der Bedeutung, die einem bestimmten Schadensniveau von der Gesellschaft beigemessen wird.

- Unterschiedliche Schadensarten können nur durch Einführung mathematischer Hilfsmittel in Hinblick auf ihre Wirkung auf die Gesellschaft verglichen werden.

Die beiden Probleme sprechen den Problemkreis "Public Acceptance" an (Kapitel IV); sie werden außerdem im Kapitel XIII behandelt.

Die Risiken des Brennstoffzyklus sind Gegenstand der Kapitel III und XII.

Im Kapitel V werden Empfehlungen für zukünftige Arbeiten gegeben, wodurch eine Verbesserung der Anwendbarkeit der Methoden und Verfahren der quantitativen Risikoberechnung erreicht werden soll.

METHODS FOR THE QUANTITATIVE ANALYSIS OF THE RISKS ASSOCIATED WITH NUCLEAR ENERGY

I. INTRODUCTION AND SUMMARY

The introduction of nuclear energy is taking place at a time that is characterized by the increasing influence of man on his environment. This realization promoted the incentive and necessity of developing quantitative methods which allow an estimation of the magnitude and dimension of this influence.

During the last few years, large scale opposition against nuclear energy is arising even though the utilization of nuclear energy promises economical and environmental advantages compared to other forms of energy production. Nuclear critics are pointing to the risk associated with nuclear energy.

In order to meet this challenge, quantitative assessments such as cost/benefit/risk-analyses are being introduced to a growing extent into the field of nuclear energy. The perspectives however, under which most of these analyses are performed today must necessarily yield an incomplete picture. Most of these analyses, for example, are merely safety studies of individual components such as the reactor and relatively little considerations have been paid to the total risk associated with the entire nuclear fuel cycle, or the public attitude toward risk /1/.

The problem of reactor siting constitutes another important part in these analyses. Economic and safety considerations are the most important criteria which influence the decision process on site selection. Economic reasons call for the construction of nuclear power plants near population centers whereas safety aspects require remote sites. This necessitates the establishment of defined quantitative safety standards so that the associated risk of nuclear power can be utilized as a siting criterion. The following problems should therefore be considered within the framework of a risk concept:

a) Quantification of the risk, where several parameters such as population density, type of reactor, meteorological conditions etc. have to be taken into account.

b) Quantification of the parameters which influence the attitude of the public towards risk.

The most notable attempt in the field of risk acceptance has been made by Starr /2,3/, whose methodology involves a comparison of expected values of risks and benefits for various voluntary activities versus involuntary ones. This concept of comparing expected values is rather questionable. Instead, the handling of the problem seems to be possible with the utilization of utility theory /4/.

At this point, some aspects of the existing reactor safety philosophy should be discussed. An attempt will be made to emphasize the common features of the "deterministic" and "probabilistic" approach.

According to the safety concept of today the safety engineer identifies the maximum credible accident, MCA, (design basis accident), assumes that the accident occurs, and than minimizes the associated risk by designing the containment system in such a way that it can cope with this accident. By doing this, he feels to have provided a protection barrier against any sort of accident, because the other credible accidents are less severe than the maximum credible accident. This approach is usually referred in the literature as the "deterministic approach to safety" /5/. The deterministic approach, which may be considered very conservative, has however three primary disadvantages:

- The process of identification of the maximum credible accident may be without an end, because one can always hypothesise accidents which are worse than the one which has already been chosen.

- The attention is focussed on the problem of eliminating or reducing the consequences of very severe but improbable accidents. Less attention and effort are instead invested in the problem of preventing less important but more probable accidents of occurring. However, these minor accidents may in fact, due to propagation effects, lead to large and dangerous accidents. In addition neglecting smaller consequence accidents with larger probabilities may, in fact, have a larger total average consequence than the one worst credible accident with its small probability.

- The conservatism of this MCA-approach may be deceiving. The system coping with the severe accident is required to work very seldom (or never) because the accident is very improbable, so that it may be unavailable, when required, for example, because of an undetected failure.

  In addition a built-in safety equipment to cope or to prevent a large and improbable accident may itself cause an accident.

These disadvantages are all due to the fact that the deterministic approach to safety is one-sided, because it places a heavy importance on the severity of the accident but does not consider the probabilities of occurrence of the events leading to the accident. If only one of these events is improbable, then the accident too is improbable. As nuclear energy takes over, the increased risk to society due to the large number of nuclear reactors requires a more logical and complete approach to safety. In particular safety experts are trying to quantify the risk associated with the use of nuclear energy. If one tries to quantify this risk, it is obvious that one must consider not only the severity of each possible accident, but also the associated probability of occurrence. This second approach is usually called "probabilistic approach to safety".

Probabilistic methods were used first in the electronic industry as early as World War II. Due to the complexity of the phenomena taking

place in the electronic components, people apply pure statistical methods to evaluate the component lifetime from data coming from previous operating experience as well as from laboratory tests.

It is obvious that the approach used for the electronic components is not entirely applicable to nuclear power stations.

In fact the probabilities are, in this case, of the order 10^{-6} - 10^{-11}/reactor-year. This would mean that one should accumulate an operating experience of 10^{6} - 10^{11} reactor-years of all equal nuclear power stations before one can reasonably expect a power station to fail. This simply means that these probabilities cannot be obtained experimentally, but must be calculated theoretically. One must apply probabilistic methods combined with deterministic methods. This is done in the fault tree and event analysis. Here all possible causes or consequences of a particular occurrence are depicted in a diagramatic form; the events are traced through a logic diagram until all causes or consequences are identified. The probability of occurrence of an accident can now be calculated from the occurrence probabilities of the basic components faults. These probabilities only are obtained experimentally.

It must be pointed out that the occurrence probability of an accident obtained in this way has by no means an absolute value. It has a value only within the limits of the degree of knowledge that the calculator has of the phenomena which occur under normal as well as abnormal plant conditions /8/.

A very enlighting and often cited example is that of the Windscale reactor in Great Britain. When this reactor was built the safety engineers were convinced that it was very safe, and this was surely true according to the level of knowledge that they had at that time. However they were not yet aware of the so called "Wigner effect" in the graphite, which caused a severe accident destroying the entire reactor core.

Probabilistic methods are not a substitute for the lack of knowledge of physical phenomena! There is no way to calculate the residual risk due to this lack of knowledge! Risk evaluations must be considered in the context of a learning process. Risk evaluations of the same reactor carried out at different times may yield different results because the degrees of knowledge were different. Evaluated risk is a dynamic and not a static quantity! Fault- and event trees are the tools for learning progressively in a logical, complete and formalized manner. In the airplane industries it is already common practice to have fault trees stored in the computer. Each time a new phenomenon occurs, the fault tree is immediately modified according to the new knowledge acquired. In addition, the use of fault and event tree analysis allows one to correctly identify areas in which more research is needed, thus directing the development of the learning process.

Some people like to talk of probabilistic approach to safety as unrelated to the deterministic one. This is, however, not true. The deterministic and probabilistic approaches characterize two phases of the learning process. One follows the other, they complement each other.

At the beginning of a new technology, when the level of knowledge is very low, the safety engineer identifies what he thinks is the worst credible accident and tries to build what he thinks is the best protection against it. As time passes, the degree of knowledge increases, and people become more confident about the performance of the new system. In this second phase people are in the position to modify their approach to safety, and try therefore to have a more complete and balanced picture of the safety problems associated with the new technology. This is the time in which the so called probabilistic approach takes over.

This does not mean, however, that probabilistic methods are already so developed and so highly credible, that they can be immediately introduced in the licensing procedure of nuclear power stations.

Probabilistic methods are today accepted only for limited tasks such as the identification of weak points is a system, comparison among different maintenance policies etc.

Knowledge must be improved in the four following areas which are believed to be of crucial importance for accepting risk analysis as normal engineering practice.

1. Correlation among failures of various components and/or systems may be inadvertently neglected in the fault and event trees (common mode failure). This point is discussed in chapter IX.

2. Failure modes and failure rates of basic components may not be sufficiently known. In addition, data on component repair times must also be available. The state of the art in this area is discussed in chapter II.A and VII.

3. Experience has shown that accidents may be initiated or made worse by human failures. Modelling human behaviour is a very difficult task (see chapter X).

4. Once an accident has started, one should be able to correctly predict all possible realistic paths through which the accident may develop, so that all possible consequences can be evaluated. In this context two problems seem difficult to solve, namely (a) identification of the realistic propagation effects which may cause initially minor accidents to degenerate into larger and more dangerous accidents, and (b) knowledge of the realistic physical phenomena which may occur in a nuclear reactor when its initial geometrical configuration has been changed. These two problems are very general safety problems which are common also to the "deterministic approach to safety". Since they are therefore not peculiar to the "probabilistic approach", they have not been discussed in detail in this report.

The problem of identifying the damages produced by nuclear energy is intimately related to the quantitative definition of risk.

Risk can be defined as the sum of all possible damage types weighted with their associated cumulative probability distributions of occurrence. Risk defined in this manner is not very suitable for comparison purposes. In order to be able to synthetically express the risk by means of a single parameter, two problems must be solved:

- For each damage type an average value must be calculated which accounts not only for the occurence probability distribution but also for the degree and importance of the damage to human society.

- The total average value (the risk) must be calculated by weighting each average damage type with a corresponding second importance function which represents the importance and acceptability of the particular damage type to human society.

Here it must be pointed out that the above mentioned problems are directly connected to the problem of "risk acceptance", which will be also discussed in section IV and XIII.

The risk associated with the entire nuclear fuel cycle is discussed in section III and XII.

Finally, recommendations for further research work are given in section V which are thought to be needed in order to render these methods in the near future more generally applicable and accepted than they are today.

Literaturverzeichnis:

/1/ Bedaux-Mathematica: "Risk Analysis of Nuclear Power Plants - A Definition of Some Unresolved Issues" (Dez. 1973), priv. comm.

/2/ Starr, C., "Social Benefit vs. Technological Risk: What Is Our Society Willing to Pay for Safety?" Science 165, (1969).

/3/ Starr, C., "Benefit-Cost Studies in Socio-Technical Systems", paper presented at Coloquium on Benefit-Risk Relationship for Decision-Making, Wash, D.C. (April 1971).

/4/ McGrath, P., Papp, R., (GfK), Maxim, D., Cook, F. (Mathematica Inc.), "A New Concept in Risk Analysis of Nuclear Facilities" Nuclear News, 17 (Nov. 1974)

/5/ Merz, L., "Philosophie des Reaktorschutzes. Determinist. und probabilist. Thesen zur Reaktorsicherheit", Atomwirtschaft (März 1970).

/6/ Häfele, W., Seminar über Zuverlässigkeitskontrolle, Kernforschungszentrum Karlsruhe, (1972).

/7/ Häfele, W., "Die Kernenergie in der technischen Welt der Zukunft", Nuclear Inter-Jura 1973, Karlsruhe.

/8/ Caldarola, L., "New Definition of Reliability, Continuous Lifetime Prediction, and Learning Processes", KFK 1847, Kernforschungszentrum Karlsruhe.

II. METHODEN UND VERFAHREN DER RISIKOBERECHNUNG

A. BESTIMMUNG DER VERSAGENSWAHRSCHEINLICHKEIT VON SYSTEMEN

In diesem Kapitel sollen Methoden der Zuverlässigkeitsanalyse von Systemen beschrieben werden. Diese Methoden können zur Abschätzung von Risiken beitragen. Dabei erscheint es notwendig, zu fragen:

- Welche Methoden gibt es?
- Was sind die spezifischen Beiträge dieser Methoden?

Die folgende Einteilung ist von grundlegender Bedeutung:

a) Ausgangspunkt und Ziel der Analyse.
   - Von einer Ursache ausgehend (z.B. Komponentenausfall) werden alle möglichen Folgen bestimmt.
   - Von einem definierten "Unerwünschten Ereignis" ausgehend (z.B. Systemausfall mit erheblichem Schaden) werden alle möglichen Ursachen gesucht.

   b) Qualitative und quantitative Analyse.

Die hier getroffene Einteilung der Methoden wird in nachfolgender Tabelle weiter ausgeführt:

Art / Ausgangspunkt	Qualitative Analyse	Quantitative Analyse
Definierte Ursache	- Ausfallart- und Fehlereffektanalyse (FMEA /26/) - consequence diagram /26/	Störfalldiagramm /1/
Definiertes Unerwünschtes Ereignis	- Fehlerbaum (nichtprobabilistische Analyse /2/) - Netzwerk mit Reihen- und Parallelschaltung /13/ - cause diagram /26/	- Fehlerbaum (probabilistische Analyse /13/)

Es ist darüberhinaus möglich, für einen definierten Ausfall (critical event /26/) eines sicherheitsrelevanten Untersystems

a) seine möglichen Folgen und

b) seine möglichen Ursachen zu bestimmen

(cause - consequence diagram, Nielsen /26, 33, 34, 35/).
Siehe dazu Abschnitt 3 dieses Kapitels.

Dazu sind in allen Fällen noch weitere Überlegungen notwendig, die zur Fehlerfreiheit und Effizienz der Analyse beitragen können (z.B. Behandlung statistischer Abhängigkeiten, Art der Auswertung (Kap. VI.iii)).

1. Bestimmung möglicher Rolgen einer definierten Ursache

1.1 Qualitative Analyse

Stichworte, unter denen diese Analyseart zu finden ist, sind: induktive Analyse /8/, Verhaltensanalyse /9/, Ausfallart- und Fehlereffektanalyse /8/, Failure Mode and Effects Analysis (FMEA) /30, 31/, consequence diagram /26/, deterministische Analyse /32/.

Die Ausfallart- und Fehlereffektanalyse

ist eine Formalisierung der häufig vorkommenden ingenieursmäßigen Überlegungen zur Frage nach den Folgen eines Komponentenausfalles. Es ist dabei besonders wichtig, auf die Formalisierung hinzuweisen. Zur Formaliserung können verschiedene Mittel verwendet werden:

- Formblattanalyse /8/ (siehe Kap. VI.i)
- Graphische Darstellung (consequence diagram /26/)
- Ausführung mit Computer /20/.

Die Formblattanalyse wird z.B. im IRS (Köln) ausgeführt /8/. Die graphische Analyse wurde an verschiedenen Stellen angewendet, jedoch am weitesten von Nielsen /26/ entwickelt. Die Ausführung mit Computer geht auf Colombo und Volta /20/ sowie auf Taylor /25, 27, 28/ zurück.

Es wird empfohlen /8/, die Analyse im Laufe der Entwurfs- und Entwicklungsphase mehrmals durchzuführen. Die Betrachungsebene verschiebt sich dabei entsprechend der fortschreitenden Detaillierung des Systementwurfs. Vor Beginn der Analyse müssen folgende Informationen vorliegen:

- die dem Entwurf zugrundeliegenden Systemspezifikationen,
- Funktionsbeschreibung, Funktionsblockdiagramme und Zeichnungen des zu analysierendem Systems
- Beschreibung der Einsatzbedingungen, wie Einsatzprofil, Umgebungsbedingungen und angrenzende Systeme.

Diese Informationen bilden auch eine Grundlage der anderen hier beschriebenen Analysen.

Die Ausfallart- und Fehlereffektanalysen stellen häufig einen festen Bestandteil der Entwicklung und Konstruktion von Systemen dar. Dies gilt z.B. für folgende Bereiche:

- Luft- und Raumfahrt, Waffensysteme /3, 4, 5/
- Reaktorsicherheit (z.B. USAEC /6,30/, UKAEA /7/, IRS /8/).

Die Ergebnisse dieser Analyse sind Aussagen über die möglichen Wirkungen ohne Verwendung von Ausfallwahrscheinlichkeiten ("nichtprobabilistisch"). Anmerkung: Für Fragen der langfristigen Abfall- Endlagerung (waste management) sind qualitative Analysen von größter Bedeutung /37/.

Die hier beschriebenen Methoden können auch auf andere Bereiche angewendet werden, wie z.B. Fehler bei Bedienung von Geräten, Versagen von Betriebspersonal und Fehlinformation /8/.

1.2. Quantitative Analyse

Stichworte unter denen diese Analyseart zu finden ist, sind: induktive Analyse /8/, Störfallanalyse /16/, consequence diagram mit probabilistischer Auswertung /26/, Ereignisbaum, event sequential diagram /26/.

Die Störfallanalyse eines Systems verläuft in derselben Richtung wie 1.1

(Ursache—Wirkung).

Von der Ursache eines Störfalles wird angenommen, daß sie mit einer bestimmten Wahrscheinlichkeit auftritt. Während des Ablaufs eines Störfalls können weitere Ereignisse auftreten, denen ebenfalls eine Wahrscheinlichkeit zugeordnet wird. Der Ablauf eines Störfalls ist ein dynamischer Vorgang der durch seine Logik gesteuert wird, d.h. es ist für den Ablauf der Störfallkette z.B. die Koinzidenz zweier Ereignisse notwendig. Es gibt jedoch auch Steuerung durch physikalische Kriterien (z.B. Erreichen der Siedetemperatur von Natrium) und durch Zeitverzögerung im Ablauf.
Die Formalisierung der Störfallabläufe geschieht meist mit graphischen Mitteln (Störfalldiagramm /1/), consequence diagram (Nielsen /26/).
Ist es möglich den Störfallauswirkungen

a) Schadenshöhen (z.B. als Strahlungsdosis),

b) Eintrittswahrscheinlichkeiten (für die als Auswirkungen gefundenen Ereignisse) zuzuordnen

so kann diese Methode zur Risikoabschätzung verwendet werden /15, 29/.

Auswertung:

Das Störfalldiagramm kann mit den Mitteln der Wahrscheinlichkeitsrechnung ausgewertet werden.

- Häufig wird das Störfalldiagramm manuell ausgewertet. Dies ist bei kleineren Diagrammen ohne weiteres möglich /18/.
- Komplexe Störfälle, sowie einfachere Störfälle, auf die eine Sensitivity - Analyse angewendet wird, könnten mit Rechenprogrammen ausgewertet werden. Dazu wurden Programme entwickelt, welche die möglichen Abläufe eines Störfalls automatisch suchen und eine Berechnung der Wahrscheinlichkeiten der verschiedenen Auswirkungen durchführen. Einschränkungen sind dabei durch die im Programm definierten logischen Elemente gegeben (Richter, Memmert /19/).

2. Bestimmung möglicher Ursachen eines definierten unerwünschten Ereignisses

2.1 Qualtitative Analyse

Stichworte, unter denen diese Analyseart zu finden ist, sind: deduktive Analyse /8/, cause diagram /26/, deterministische Analyse, nichtprobabilistische Analyse, qualitative Fehlerbaumanalyse (DIN 25 424 /2/).

Fehlerbaumanalyse

Die hier beschriebenen Grundbegriffe der Fehlerbaumanalyse gelten auch für die quantitative Analyse (2.2).
Der Fehlerbaum ist ein logisches Diagramm zur Darstellung von Ereignisfolgen, die zu einem definierten unerwünschten Ereignis führen können. Die formalisierte Suche nach möglichen Ursachen führt noch nicht zu einer Risikoabschätzung. Es ist jedoch möglich, durch eine qualitative Analyse Schwachstellen zu finden (z.B. Einzel- und Doppelfehler die zu einem Systemausfall führen können). Damit sind wichtige Hinweise zur Sicherung einer Anlage zu erhalten.

Ziele der Analyse sind im einzelnen:

a) die systematische Identifizierung aller möglichen Ursachen, die zu einem vorgegebenen unerwünschten Ereignis führen können,
b) die Erstellung einer klaren und nachvollziehbaren Dokumentation der Analyse,
c) die Ermittlung von Beurteilungskriteren zur Systemauslegung (DIN 25 424 /2/).

Wir können uns für die Fehlerbaumanalyse auf Vorschläge des Fachnormenausschusses Kerntechnik (FNKe 3.3) stützen, in die Erfahrungen aus Arbeiten verschiedener Gruppen zur Fehlerbaumanalyse /10, 11, 12, 22/ eingegangen sind.

Schritte der Fehlerbaumanalyse:

Die Aufgabe besteht darin, ein Modell für ein System aufzustellen, welches

die obengenannten Ziele der Analyse zu erreichen gestattet. Dazu haben sich folgende Analysenschritte bewährt (DIN 25 424 /2/):

1. Detaillierte Beschreibung mit Hilfe einer Systemanalyse des normal funktionierenden Systems, Festlegung des betrachteten Zeitintervalls
2. Definition des Unerwünschten Ereignisses
3. Definition von Ausfallkriterien
4. Untersuchung der Ausfallarten
5. Aufstellung des Fehlerbaums (siehe Kap. VI.ii).

Analyse eines Blockdiagramms (Netzwerk mit Reihen- und Parallelschaltung)

Die Ziele der Analyse sind dieselben wie bei der Fehlerbaumanalyse, u.z. die Untersuchung eines Systems und seine Beurteilung bezüglich Schwachstellen /13/.
Die Schritte der Analyse sind grundsätzlich dieselben. Man kann einen Fehlerbaum in ein ihm äquivalentes Blockdiagramm übersetzen und umgekehrt. So entspricht z.B. das logische "UND" (X_1 und X_2 fällt aus) des Fehlerbaums einer "Parallelschaltung" aus den Komponenten X_1, X_2 in einem Blockdiagramm. Das Blockdiagramm und der Fehlerbaum sind zwei Darstellungsarten eines Systems, welche die formalisierte Suche nach möglichen Ausfallursachen erleichtern. Die Auswertung von Fehlerbaum bzw. Blockdiagramm erfolgt grundsätzlich mit denselben Methoden /13/. Eine getrennte Darstellung der Methoden ist darum nicht erforderlich.
Anmerkung: Es ist auf die Wichtigkeit qualitativer Analysen für Fragen der Abfall - Endlagerung mit den dabei möglichen Risiken langfristiger Art hinzuweisen /37/.

2.2 Quantitative Analyse

Stichworte, unter denen diese Analyseart zu finden ist, sind: deduktive Analyse /8/, cause diagram /26/, Fehlerbaum mit probabilistischer Auswertung /2, 21/), Blockdiagramm mit probabilistischer Auswertung /17, 32/.

Fehlerbaumanalyse

Es ist das Ziel, eine Systembeurteilung mit Hilfe probabilistischer Zu-

verlässigkeitskenngrößen durchzuführen. Dazu ist zunächst in allen Einzelschritten die in 2.1 beschriebene qualitative Analyse auszuführen.
Als weitere Schritte kommen hinzu:

1. Zusammenstellung der Ausfallraten, Ausfallzeiten, Eintrittswahrscheinlichkeiten
2. Auswertung des Fehlerbaums
3. Bewertung der Ergebnisse.

Auswertung eines Fehlerbaums:
Das Hauptziel der Auswertung ist die Berechnung der Ausfallwahrscheinlichkeit eines Systems. Diese kann, wenn die Schadenshöhe quantifizierbar ist, zu einer Risikoabschätzung dienen /6, 29/.
Zur systematischen Auswertung eines Fehlerbaums stehen analytische Methoden und Simulationsmethoden zur Verfügung /23, 24, 36, 38, 39/ (siehe auch Anhang 1.3).

Analytische Methoden:
Sie ermöglichen es, die durch den Fehlerbaum gegebene Struktur soweit umzuformen, daß eine Auswertung mittels Wahrscheinlichkeitsrechnung möglich wird.

a) Zunächst kann die logische Richtigkeit eines Fehlerbaums getestet werden, wobei Tautologien, Widersprüche etc. ermittelt werden /20, 14/.

b) Darauf werden alle Critical Paths des Fehlerbaums gesucht. Dies sind diejenigen Kombinationen von Komponenten-Ausfällen, welche unmittelbar einen Systemausfall erzeugen.

c) Durch Kombination dieser Critical Paths kann die Systemausfallwahrscheinlichkeit berechnet werden /20, 24, 28/.

d) Die Auswirkung von Datenfehlern nicht-systematischer Art auf die Systemausfallwahrscheinlichkeit kann mittels analytischer Verfahren abgeschätzt werden /12/.

Simulationsmethoden:

Die schon weit entwickelten Simulationsverfahren bestehen darin, mit Hil-

fe von Zufallszahlen das zeitliche Verhalten der Fehlerbaumeingänge zu simulieren. Dieses Verfahren ist besonders geeignet, Betriebs- und Ausfallverhalten eines Systems in seinem zeitlichen Ablauf zu erfassen. Zum Nachweis niedriger Wahrscheinlichkeiten erfordern die direkten Simulationsmethoden jedoch einen hohen Rechenzeitaufwand. Zur Überwindung dieser Schwierigkeit werden varianzreduzierende Verfahren eingesetzt /36/.

Neben analytischen Verfahren und Simulationsverfahren (siehe Kap. VI.iii) werden auch Programme benutzt /10, 22/, die beide Verfahren systematisch kombinieren. Sie finden z.B. im Falle von Systemen mit hochzuverlässigen Komponenten und komplexen Bedienungsstrategien Verwendung.

3. Bestimmung möglicher Folgen und möglicher Ursachen für einen definierten Ausfall

Stichworte, unter denen diese Analyseart zu finden ist, sind: Cause-Consequence-Diagram (Nielsen /26/) und Allgemeine Gefahren-Analyse (AGA /8/).

Das "Cause-Consequence Diagram" ist eine Methode zur Analyse von Fehlerabläufen in komplexen Systemen (Nielsen /26, 33, 34, 35/). Bei Untersystemen, die nach einer Vorläufigen Gefahren-Analyse (VGA /8, 26/) als sicherheitsrelevant erscheinen, werden die möglichen Ursachen, die zum Ausfall dieser Untersysteme beitragen, untersucht.

a) In einem Fehlerbaum (cause diagram /26/) werden die möglichen Ursachen, die zum Ausfall dieses Untersystems beitragen, untersucht.

b) In einer Störfallanalyse (/1/, consequence diagram /26/) werden die möglichen Folgen untersucht.

Abb. II.1 zeigt in stark vereinfachter Form die Verknüpfung von cause diagram und consequence diagram durch den Ausfall eines Untersystems (critical event).

Es ist auch möglich, diese Analyse mit Formblättern auszuführen /8/. Dies ist grundsätzlich nicht von der in Kapitel VI.i beschriebenen Analyse verschieden.

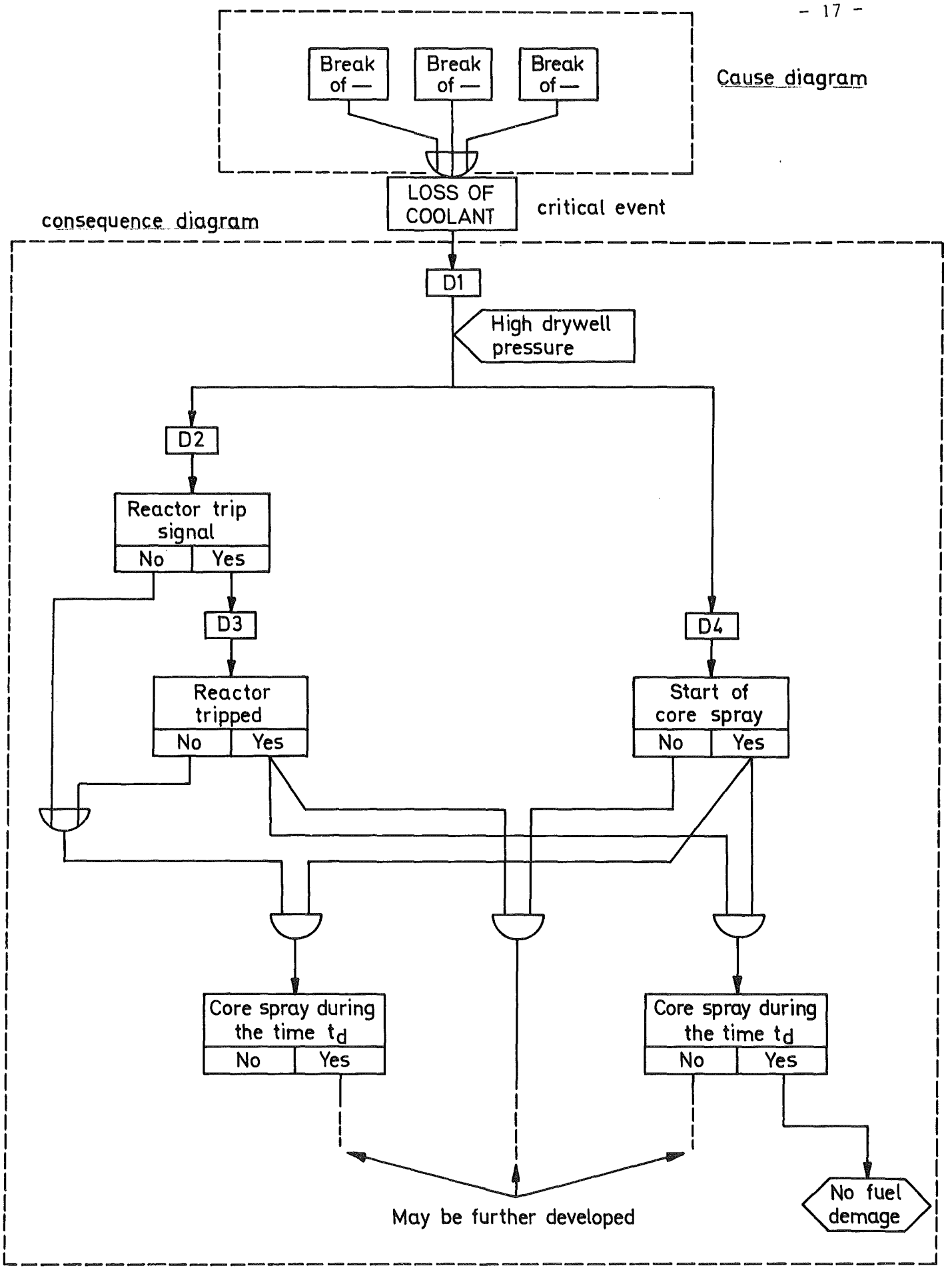

Abb. II.1 Example concerning loss of coolant

vereinfacht nach / 35 /

Das cause-consequence diagram kann neben der qualitativen Analyse (Feststellung möglicher Ursachen und Wirkungen, Untersuchung auf Einzel- bzw. Doppelfehler) auch für die quantitative Analyse (Feststellung der Ausfallwahrscheinlichkeiten) verwendet werden.

Zur Leistungsfähigkeit der Zuverlässigkeitsanalyse

Die Zuverlässigkeitsanalyse stellt ein systematisches Werkzeug zur Erfassung von Versagenswahrscheinlichkeiten von Systemen dar. Ihre wichtigsten Arbeitsmethoden wurden am Anfang dieses Kapitels in ihren Grundzügen dargestellt.

Allgemein wird der Stand der quantitativen Sicherheitsbeurteilung unter Zuhilfenahme der Zuverlässigkeitsanalyse wie folgt beurteilt /40/:

1. Die Zuverlässigkeitsanalyse ermöglicht eine quantitative Beurteilung der für die Sicherheit und den Betrieb einer Anlage wichtigen Systeme.

2. Die Zuverlässigkeitsanalyse erlaubt eine systematische Beurteilung verschiedener Einflüsse einzelner Komponenten und Teilsysteme auf das Ausfallverhalten eines Gesamtsystems, sie ermöglicht damit die Ermittlung von Systemschwachstellen und die Festlegung von Zuverlässigkeitsanforderungen an einzelne Untersysteme oder Komponenten. Die Zuverlässigkeitsanalyse ermöglicht auch "Overdesign" in den Systemen festzustellen.

3. Die Zuverlässigkeitsanalyse kann zur Untersuchung verschiedener Betriebs-, Reparatur- und Wartungsstrategien eingesetzt werden.

4. Die Zuverlässigkeitsanalyse kann als Entscheidungshilfe zur Beurteilung alternativer Auslegungskonzepte herangezogen werden.

Ein besonderes Charakteristikum der probabilistischen Betrachtungsweise unter Anwendung der Zuverlässigkeitsanalyse ist es, daß auch hypothetische Unfälle (die den Größten Anzunehmenden Unfall der deterministischen Betrachtungsweise übersteigen) mit erfaßt werden. Somit entfällt hier die unvermeidlich etwas willkürliche Grenzziehung zwischen "anzunehmend" und

"nicht anzunehmend", die der deterministischen Sicherheitskonzeption eigen ist.

Trotzdem haben probabilistische Methoden in die Genehmigungsverfahren heute noch keinen - oder nur beschränkten (etwa in der Form der Festlegung von Reparaturzeiten oder von Aussagen über Notstromsysteme) - Eingang gefunden, und es werden die auf diese Art ermittelten Risikowerte beispielsweise von der Reaktorsicherheitskommission (RSK) nicht akzeptiert /41/.

Die (noch) vorliegende Skepsis gegenüber der Zuverlässigkeitsanalyse ist in den folgenden Punkten begründet, die die Grenzen dieser Methodik beschreiben und die den in der Unterteilung 1. bis 4. angeführten Anwendungsbereich der Zuverlässigkeitsanalyse einengen. Die beschriebenen Methoden verlangen an verschiedenen Stellen besondere Aufmerksamkeit:

1. Richtige Wahl des Ausgangspunktes der Analyse

1.1 Wahl der Ursache:
Die Wahl der Ursachen soll eine sicherheitsrelevante Analyse ermöglichen. Wählen wir eine Ursache, die nicht sicherheitsrelevant ist, so kommen wir zu formal richtigen Aussagen, die jedoch bezüglich des Risikos unvollständig sind.

1.2 Wahl des unerwünschten Ereignisses:
Es ist notwendig, einen Fehlerbaum /2/ von einem durch seine Schadenshöhe ausgezeichneten Ereignis aufzubauen. Es hat keinen Sinn, nach möglichen Ursachen von nichtrelevanten Ereignissen zu suchen.

1.3 Wahl des "critical event":
Die Wahl des critical event ist eine Entscheidung, um festzustellen, wo ein cause- bzw. consequence-diagram entwickelt werden soll. Dabei gelten die Bemerkungen von 1.1 und 1.2 /26/.

2. Unsicherheiten bzgl. der Ausfallraten: Ausfallraten von Komponenten gehen als Eingangsdaten in die Berechnung der Ausfallwahrscheinlichkeiten von Systemen in die Fehlerbaumanalyse ein. Mangelnde Erfahrung

(z.B. Wahrscheinlichkeiten für den Bruch von Reaktordruckgefäßen /42, 43,44/) und/oder Unsicherheiten bei der Übertragung von Fehlerwahrscheinlichkeiten auf ähnliche Komponenten unter unterschiedlichen Betriebsbedingungen führen zu Unsicherheiten in den Ausfallraten (bzgl. "Daten" siehe auch Kapitel VII und VIII).

Zur Beurteilung bzw. Verbesserung der Daten ergeben sich verschiedene Möglichkeiten:

- Der Einfluß von Daten, die mit Ungenauigkeiten behaftet sind (Vermutung einer systematischen Abweichung, Stichprobe mit hoher Standardabweichung (nichtsystematische Abweichung)) kann mittels Sensitivity-Analyse sowie Momentenmethode abgeschätzt werden.

  Sensitivity-Analysen können den Einfluß von Änderungen der Komponentenausfallraten auf das Endergebnis einer Fehlerbaumanalyse abschätzen und damit kritische Niveaus in Fehlerbäumen feststellen. Diese kritischen Niveaus stellen Grenzen dar zwischen Anlageteilen, deren Ausfalleigenschaften die Eintrittswahrscheinlichkeit eines unerwünschten Ereignisses maßgeblich beeinflussen, und solchen, bei denen Fehleinschätzungen zu keiner wichtigen Veränderung des Endergebnisses führen. Aus diesen Analysen ergeben sich Hinweise auf eine Ausrichtung der Entwicklung bzw. experimentellen Untersuchung.

- Um die Situation bezüglich der Ausfallraten zu verbesseren, werden heute weltweit Bemühungen zur Datengewinnung unternommen. Als Beispiel sei der RWE-Modellfall /45/ genannt, bei dem detaillierte Daten über das Ausfallverhalten von ca. 13.000 Bauteilen gewonnen werden sollen. International bekannt sind Datenbanken wie SRS (System Reliability Service, England) und FARADA (Failure Rate Data, USA).

3. Unsicherheit bei der Annahme der zeitlichen Verteilungsfunktion:
   Oftmals ist die Annahme einer exponentiellen Verteilung der Zuverlässigkeit nicht voll gerechtfertigt, da in manchen Bereichen der Reaktorsicherheit die Zufallsausfälle mit konstanter Ausfallrate das Problem nur unvollständig beschreiben (Möglichkeit der Annahme von Weibullverteilungen, Normalverteilungen usw.). Jedoch steckt in der Annahme einer Exponentialverteilung ein gewisser Grad an Konservatismus.

4. Unerkannte Systemversagensarten: Bei der Analyse von Unfallabläufen können im System noch versteckte Versagensarten existieren. Selbst bei genauer Kenntnis der Fehlerraten von Komponenten kommt es daher bei der Hochrechnung der Systemausfallrate mit Hilfe eines Fehlerbaumes u.U. zu erheblichen Fehlern.

5. "Sekundärversager" (Versagen der Komponenten durch Überschreiten ihrer Auslegungsgrenzen) /46/ und Common-mode-Fehler: Diese Ausfallarten sind durch die Zuverlässigkeitsanalyse besonders schwer zu erfassen. Ihre Nichterkennung ist kein nur der Fehlerbaumanalyse eigener Mangel, sondern ist bei allen in Frage kommenden Analysenarten ein wichtiges Problem. Der Begriff des Common-mode-Fehlers ist so weitreichend, daß hier unterschiedliches Vorgehen erforderlich ist:

   - Es gibt Fehler, die in keinem Diagramm auf den Ausfall von Komponenten zurückgeführt werden können (z.B. Erdbeben).

   - Es gibt jedoch Fehler, die in einem Diagramm ohne Schwierigkeit unterzubringen sind (z.B. Ausfall von Komponenten, deren Lebensdauer durch den Ausfall anderer Komponenten verkürzt wurde (s. Definition 3, Kapitel IX)).

   Hier sollen keine allgemeinen Regeln angegeben werden. Eine Untersuchung von Ausfallkriterien und Ausfallarten wird jedoch eine Entscheidung über das Vorgehen im Einzelfall erleichtern.

6. Ein sehr schwieriges Problem für die Zuverlässigkeitsanalyse ist die Frage des menschlichen Einflusses. Auch hier wird versucht, qualitative Methoden anzuwenden /8/ (nähere Angaben über das menschliche Verhalten s. Kapitel X).

Im allgemeinen muß festgestellt werden, daß heute die Zuverlässigkeitsanalyse aus den oben genannten Gründen eine absolute Aussage über die Zuverlässigkeit von Systemen nur in Einzelfällen erlaubt, in der Mehrzahl der Fälle jedoch nur relative Aussagen (z.B. Vergleiche von Systemen unterschiedlicher Redundanz) möglich sind.

Deshalb wird die Zuverlässigkeitstechnik bis jetzt in erster Linie nur zur Erkennung von Schwachstellen und Festlegung von Betriebsstrategien (Inspektion, Wartung) eingesetzt.

B. METHODEN ZUR BESTIMMUNG DES UNFALLRISIKOS VON KERNKRAFTWERKEN

Zur Bestimmung des Risikos, das durch den Betrieb einer technischen Anlage hervorgerufen wird, sind zwei wesentliche Schritte erforderlich.

1. Die Ermittlung von Eintrittswahrscheinlichkeit und Schadensgröße für die einzelnen als möglich erkannten Schadensereignisse.

2. Überlegungen zur vollständigen Erfassung aller Schadensereignisse, die wesentliche Risikobeiträge liefern und Zusammenfassung dieser Beiträge zum Gesamtrisiko.

Der Fragenkomplex des ersten Schritts umfaßt einerseits die Zuverlässigkeitsanalyse und andererseits Überlegungen zu Ausbreitungsfaktoren, Inkorporationsmechanismen und Mortalität bei externer und interner Bestrahlung.

Um den zweiten Schritt, d.h. die Erlangung der Vollständigkeit und die Erstellung eines Gesamtrisikos, durchzuführen, sind eine Reihe verschiedener Ansätze denkbar:

a) Das Aufstellen eines Fehlerbaums, als dessen unerwünschtes Ereignis das Hauptrisiko der Kernenergie definiert wird, nämlich etwa: Schädigung von Personen durch radioaktive Strahlung.

b) Das Aufstellen einer Liste aller potentiell gefährlichen Ereignisse oder Ereigniskombinationen.

c) Eine Kombination dieser beiden Wege wäre es, die Vollständigkeit auf einer Zwischenebene, etwa auf der Ebene der Systeme anzustreben und im Sinne des cause/consequence-Diagramms in einer Richtung die möglichen Ursachen, in der anderen die potentiellen Wirkungen aufzusuchen.

Da die konsequente Durchführung eines jeden dieser Verfahren außerordentlich komplex ist und ein zwingender Nachweis der Vollständigkeit letztlich doch nicht erbracht werden kann, wurden vereinfachende Verfahren vorgeschlagen, die es erlauben sollen, aus den Ergebnissen für einzelne detail-

liert untersuchte Störfallmöglichkeiten Schlüsse auf das Gesamtrisiko abzuleiten. Während Risiko allgemein als die Menge aller möglichen Schäden, gewichtet mit ihren Eintrittswahrscheinlichkeiten definiert ist, wird im folgenden unter Risiko nur das Mortalitätsrisiko pro Individuum und Zeiteinheit verstanden. Besonders bekannt geworden ist das Verfahren von Otway /47, 48/. Aus den Untersuchungsergebnissen für die wichtigsten Störfallmechanismen leitet er eine Gesetzmäßigkeit für die Abhängigkeit zwischen der Eintrittswahrscheinlichkeit eines Ereignisses und der damit verbundenen Abgabe von Radioaktivität an die Biosphäre ab. Otway trifft die Annahme, daß die Unfallfolgen (Spaltprodukt-Emissionen) als stetige Funktion der Unfallwahrscheinlichkeiten darstellbar wären, wodurch man zu einer oberen Grenze des Risikos kommen würde. Der Berechnung des Gesamtrisikos wird diese Unfallwahrscheinlichkeits- Unfallschwere-Kurve zugrunde gelegt. Weiters werden Ausbreitungsfaktoren, das Mortalitätsrisiko pro rem und Bevölkerungsverteilungen in Rechnung gestellt /49, 50, 51/.

Die Bestimmung von Punkten im Unfallwahrscheinlichkeits- Unfallkonsequenz-Diagramm beruht auf der Zuverlässigkeitsanalyse. Die erwähnten "Schwachstellen" dieser Analyse gehen in die Bestimmung der Unfallwahrscheinlichkeit ein. Die Lage der Punkte ist somit mit der ganzen Unsicherheit dieser Methode behaftet.

Die Behauptung, eine stetige Funktion durch die erwähnten Punkte würde eine konservative Berechnung des Risikos ermöglichen, läßt sich nicht beweisen; diese Frage ist wohl nicht beantwortbar. Wohl meinen einige Autoren /52/, daß es nur eine diskrete Unfallschar gibt, oder daß ein Analogieschluß von in anderen Sparten gelegenen Unfallhäufigkeits-Unfallschwere-Zusammenhängen vielleicht zulässig wäre /53/.

Weiters ist die Integration der oben genannten Kurve über die Wahrscheinlichkeit zur Errechnung des Gesamtrisikos mathematisch inkorrekt. Man kann also sicher nicht davon ausgehen, daß das Endresultat, wie angegeben, eine konservative Abschätzung des Gesamtrisikos darstellt. Eine ausführlichere Darstellung und Begründung dieser Kritik an der Methode von Otway ist in Kapitel XI gegeben.

Eine gewisse Verwandtschaft mit dem Vorgehen von Otway hat das Grenzlinien-

kriterium von Farmer /15/. Farmer schlug als Risikostandard für Kernkraftwerke eine "Grenzlinie" in einem Diagramm vor, das die unfallbedingte Freisetzung von Radioaktivität (in Einheiten von Ci J-131) in Abhängigkeit von deren Häufigkeit darstellt. Dabei wird angenommen, daß die Jodisotope, vor allem J-131, eine größere Bedrohung für die Gesundheit darstellen, als alle anderen störfallbedingt freigesetzten Spaltprodukte. Es handelt sich dabei allerdings zunächst nicht um einen Vorschlag zur Risikoberechnung, sondern um die Erarbeitung einer Bedingung, der jeder denkbare Unfallablauf genügen muß, um nicht zu einem unannehmbaren Risiko zu führen. Diese Bedingung besagt, daß in einem Diagramm, in dem (ähnlich wie bei Otway) Unfallhäufigkeit gegen Aktivitätsfreisetzung aufgetragen ist, alle Unfälle unterhalb einer bestimmten Grenzlinie liegen müßten.

Die Festlegung dieser Grenzlinie erfolgt nach folgenden Gesichtspunkten /54/:

a) Eine unfallbedingte Freisetzung von größenordnungsmäßig 10^3Ci J-131 stellt eine Bedrohung dar, die bezüglich ihres Ausmaßes abschätzbar ist. /55/. Wohl wird keine Behörde oder kein Reaktorbetreiber das Auftreten des genannten Ereignisses einmal während der Lebensdauer eines Reaktors (30 - 40 Jahre) zulassen können andererseits wird es in diesem Jahrhundert weltweit zu einer Betriebserfahrung von größenordnungmäßig 10^3 Betriebsjahren kommen, so daß die Frage nun lautet: Ist das Risiko dieses Unfalls in dieser Zeitspanne akzeptabel? Farmer meint, daß die Wahl zwischen 0,1 und 10 Ereignissen dieser Art liegen sollte, so daß die Wahl des Startpunktes bei 10^3 Reaktorjahren liegen müßte (Abb. II.2).

b) Es ist offensichtlich, daß die meisten Menschen das Auftreten einer großen Freisetzung überproportional stärker bewerten, als einer geringfügigen. Diese Tatsache kann in der Grenzlinie durch Wahl einer Neigung, deren Betrag größer 1 ist, berücksichtigt werden. Die gewählte Neigung beträgt hier -1,5, was gleichbedeutend mit einer Reduktion um 3 Größenordnungen der Freisetzungshäufigkeit, bei einer Erhöhung der Unfallschwere um 2 Größenordnungen ist.

Diese Überlegungen zur Festlegung der Grenzlinie berücksichtigen demnach

zusammengefaßt folgende Aspekte:

- Die Linie kann als Sicherheitskriterium gelten, indem sie eine obere Grenze zulässiger Wahrscheinlichkeiten für Störfallkonsequenzen festlegt.

- Möglichkeit einer Abschätzung der Gesamtzahl der Störfallopfer in der Bevölkerung, als auch des individuellen Risikos.

- Die Festlegung der Grenzlinie gibt die Möglichkeit, die Haltung der Öffentlichkeit mit zu berücksichtigen.

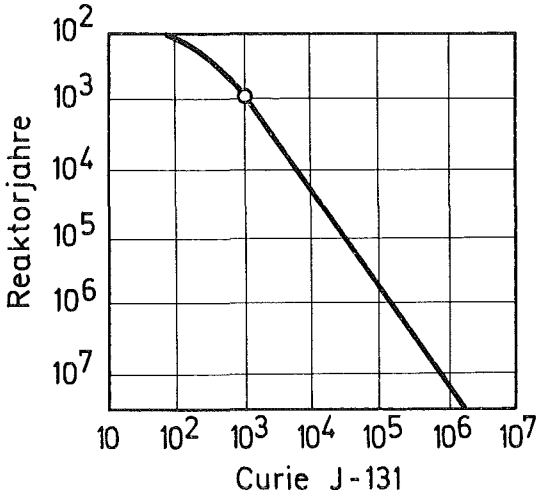

Abb. II.2 Farmer - Grenzlinie

Für den Freisetzungsbereich unter 10^3 Ci wird ein Kurvenstück mit sich ändernder Steigung derart festgelegt, daß die Häufigkeit geringer Emission möglichst klein bleibt.

Die Abschätzung des Gesamtrisikos erfolgt dann etwa folgendermaßen: Auslegung und Standort der Anlage sollen so gewählt werden, daß alle untersuchten Unfälle auf oder unter der Grenzlinie liegen. Dann werden nur einige wenige Unfälle dicht genug an der Grenzlinie liegen, um wesentlich zum Gesamtrisiko beizutragen. Dieses könnte dann etwa eine Größenordnung höher als der Beitrag eines Einzelunfalls auf der Grenzlinie angenommen werden /47, 52, 56, 57/.

Beattie /55/ berechnete für einen hypothetischen Standort mit angenommener Bevölkerungsdichte von 5000 Personen pro km^2 (Verdichtungsraum) und Unterteilung der Bevölkerung in Altersgruppen, Jodausbreitung nach Pasquill /58/ und einem Schilddrüsenkrebsrisiko von 15 Fällen pro 10^6 man-rem /59/ bei einer unfallbedingten Emission von 10^4 Ci Jod-131 eine Dosisbelastung für die in einem Umkreis von 10 Meilen um den Reaktor lebenden 4 Mio. Menschen von $2{,}2 \times 10^6$ man-rem. Dies würde 33 (15 x 2,2) Fälle von Schilddrüsenkrebs verursachen. Die oben definierte Grenzlinie ließe eine Emission von 10^4 Ci höchstens mit einer Häufigkeit von 1 mal in $1{,}5 \times 10^4$ Reaktorjahren zu, woraus sich eine mittlere Zahl von 0,002 Fällen pro Reaktorjahr und 4×10^6 Menschen ergibt. Aus dieser sehr qualitativen und nicht unbedingt konservativen Betrachtungsweise wird klar, daß auch diese Methode keine befriedigende Art der quantitativen Risikobestimmung darstellt.

Risikostandards durch Festlegung einer Grenzlinie zu schaffen, müßte wohl das Endziel der Bestrebungen sein, das mit dem Betrieb von KKW verbundene Risiko zu quantifizieren. Die hier gehandhabte Vorgangsweise bei der Definition der Kurve berücksichtigt in gewisser Hinsicht die nicht mittelwertorientierte Haltung des Menschen in der Akzeptierung von Risiken - d.h. eine Tolerierung von 10^3 Ci J-131 mit einer Häufigkeit des Auftretens von 10^{-3}/Jahr, dagegen 10^4 Ci nur einmal in $1{,}5 \times 10^4$ Jahren (Neigung - 1,5) - jedoch ist hier die Problematik der Risiko-Acceptance nur sehr oberflächlich behandelt. Somit scheint die Wahl des Anfangspunktes und auch der Kurvenneigung ziemlich willkürlich zu sein.

Um zu einer echten Einschätzung des Gesamtrisikos zu kommen, ist es daher doch notwendig, die Anlagen in ihrer ganzen Komplexität und mit allen möglichen Störungen durch internes Versagen sowie durch äußere Einwirkungen (Erdbeben, Flugzeugabsturz, Sabotage, Krieg) so eingehend wie irgend möglich zu untersuchen.

Als Beispiel für die in der Praxis geübte Standortbeurteilung seien hier die Verhältnisse in den USA erwähnt: Standortbeurteilungen werden dort nach den im "Code of Federal Regulations" (CFR) festgelegten Vorschriften durchgeführt /65/. Das Gebiet um einen Standort wird demnach in drei Zonen aufgeteilt:

- Die "Exclusion-Area" umgibt den Reaktor unmittelbar und ist unbewohnt. Die Ausdehnung dieses Gebietes ist so festgelegt, daß Personen, die sich dort während eines hypothetischen Unfalls (bzw. bis zu zwei Stunden danach) aufhielten, einen Strahlenschaden erleiden würden. Dabei werden 300 rem Schilddrüsendosis und 25 rem Ganzkörperdosis als Maß für eine Schädigung angenommen /66, 67/.

- Eine "Low-Population-Zone" schließt an das unbewohnte Gebiet an, wobei die Bevölkerungsdichte so begrenzt ist, daß bei einem Unfall notwendige Schutzmaßnahmen durchgeführt werden können /66/.

- Als "Population-Center-Distance" wird die Entfernung vom Reaktor bis zu einem dicht besiedelten Gebiet bezeichnet, wobei bei einem hypothetischen Unfall die Bevölkerungsdosis in diesem Gebiet einen bestimmten Wert nicht überschreitet. Hierzu werden in der Literatur Entfernungen vom Reaktor bis zum nächstgelegenen Siedlungsgebiet mit mindestens 25 000 Bewohnern als Radius dieser Zone /66/ und Bevölkerungsdosen von $2 \cdot 10^6$ man-rem /67/ angegeben.

Die Rasmussen-Studie: Eine sehr wichtige Studie über die Risiken von Leichtwasserreaktoren wurde in den USA im Auftrag der USAEC unter der Leitung von N. Rasmussen am MIT durchgeführt. Wissenschaftler verschiedenster Organisationen arbeiteten an diesem 2 Mio. $-Projekt mit. Der Endbericht lag im September 1974 in Entwurfsform vor (WASH-1400).

Die Rasmussen-Studie wird als die wichtigste Arbeit auf dem Gebiet der Reaktorunfallrisiken nach dem Brookhaven-Bericht WASH-740 /60, 61/ angesehen. WASH-740 war eine "worst-case"-Analyse, deren pessimistische Annahmen für drei untersuchte Störfalltypen von KKW-Unfällen im schlimmsten Fall 3.400 Tote, 43.000 Verletzte und Sachschaden zwischen 0,5 Mio. und 7 Mrd. Dollar ergaben.

Anlaß für die Erstellung dieses Berichts war die 1955 in den USA diskutierte Frage der Schadenshöhe bei schweren Reaktorstörfällen und der Abdeckung der Risiken über den durch Versicherungen gedeckten Betrag von 60 Mio $ hinaus (Price-Anderson-Act).

Einige vorläufige Ergebnisse des Rasmussen-Berichts waren im Laufe des Jahres 1974 bekannt geworden /62, 63, 64/. Demnach käme es nur durch Freisetzung beträchtlicher Mengen an Radioaktivität - vor allem infolge von Coreschmelzunfällen - zu einer Gefährdung der Öffentlichkeit. Selbst beim Betrieb von 100 Kernkraftwerken wäre die Eintrittswahrscheinlichkeit für einen Reaktorunfall mit 100 Toten sehr viel geringer als für einen Flugzeugunfall mit größenordnungsmäßig gleichen Konsequenzen /68/.

Rasmussen bediente sich in seiner Studie der Fehler- und Ereignisbaumanalyse. Ausfallraten für Komponenten wurden von Datenbanken wie FARADA und SRS zur Verfügung gestellt. Als Genauigkeit der Ergebnisse wurde ein Faktor 10 genannt, was auf Fehler in den Ausfallraten, menschliche Fehler und Common-Mode-Fehler zurückgeführt wird. Der Effekt einer Evakuierung der Bevölkerung wurde bei dieser Studie ebenfalls in Betracht gezogen. Der Rasmussen-Bericht liegt nun in Entwurfsform vor und ist Gegenstand intensiven Studiums.

Literaturverzeichnis

/1/ Störfallablaufanalyse DIN 25 419, Blatt 1 (November 1973)
(früher: Graphische Darstellung von Störfallabläufen)

/2/ Fehlerbaumanalyse - Erläuterungen und Anwendungen, DIN 25 424
(Beide Fachnormenausschuß Kerntechnik, FNKe 3.3)

/3/ Jordan, W.E., Failure Modes, Effects and Criticality Analysis,
Proc. 1972 Ann. Symp. on Reliability and Maintainability, p. 30-37

/4/ Jaschke, I., Methods for Determining and Improving the Reliability
of Electrical Supply Systems, 1968 CREST-Meeting on Electrical
Supply Systems (EUR 4517 e)

/5/ Weapon System Safety Analysis Requirements, Deptmt. of the
Air Force, Space and Missile Systems Organization, Air Force
Systems Command, 1968

/6/ USAEC, Reactor Safety Study, An Assessment of Accident Risks in
US Commercial Nucl. Power Plants, WASH-1400 (Draft), Sept. 1974

/7/ Bowen, J.H., Techniques of Consequence Assessment, Nucl. Eng.
and Design, Vol. 13 (1970), 236

/8/ Balfanz, H.P., Sicherheitsanalyse-Plan (Anwendung verschiedener
Sicherheits- und Zuverlässigkeitsanalysen zum richtigen Zeitpunkt
und zu speziellen Problemen) IRS-W-2 (April 1972)

/9/ Balfanz, H.P., "Zustandsanalysen" (Normenvorlage), in Vorberei-
tung (FNKe 3.3, Nov. 73)

/10/ Heuser, F.W., Rosenhauser, W., Projektbezogene Anwendung von
Zuverlässigkeitsmethoden, 1. u. 2. Teil in KFK 1811, Einführung
in Methoden und Probleme der Zuverlässigkeit, G. Weber (Januar
1974)

/11/ Hörtner, H., Bastl, W., Reliability Analysis of a PWR-Emergency
Core Cooling System, CREST-Meeting on Complex Systems and
Nuclear Plants, München (Mai 1971)

/12/ Murchland, J.D., Weber, G.G., A Moment Method for the Calculation of a Confidence Interval for the Failure Probability of a System, Proc. 1972 Ann. Symp. on Reliability and Maintainability, San Francisco, 1972, p. 565-577

/13/ Staff on the Safeguards Division, AHSB, UKAEA, Quantitative Safety Analysis, Nuc. Eng. and Design 13 (1970) 183 - 244

/14/ Weber, G.G., State of Reliability Effort in Europe (review for the Special Issue of IEEE Trans. on Reliability, Vol. R-23, August 1974)

/15/ Farmer, F.R., Siting Criteria - A New Approach, Symp. on Containment and Siting of Nucl. Power Plants, Wien (1967)

/16/ Knecht, O., Keil, H., Graphische Analyse von Reaktorstörfällen Atom und Strom, Folge 7/8, Juli/August 1968

/17/ Bourne, A.J., Grenn, A.E., Techniques of Quantitative Reliability Analysis, Nucl. Eng. And Design, 13, (1970) 1911 ff.

/18/ Mündliche Mitteilung bei der Beratung über Störfallablauf-analyse beim FNKe 3.3

/19/ Richter, G., Memmert, G., Berechnung von Zuverlässigkeitsdaten komplexer Systeme mit analytischen Methoden, Institut für Kerntechnik der TU Berlin, Oktober 1973, Bericht TUBIK 28

/20/ Colombo, A.G., Volta, G., Multistep Reliability Analysis and Optimization of Complex Systems, paper presented at the CNSI-Specialist Meeting on: The Development and Application of Reliability Techniques to Nuclear Plants, (Liverpool, 8-10 April 1974)

/21/ Fussell, J.B., A Formal Methodology for Fault Tree Constructions, Nuclear Science and Engineering 52, p. 421-432 (1973)

/22/ Blombach, J., Rosenhauer, W., Zeibig, H., Reliability Techniques Covering the Operational Conditions of Reactor Systems (Liverpool, 1974)

/23/ Garrick, B.J., Principles of Unified Systems Safety Analysis, Nucl. Eng. And Design, Vol. 13, (1970), No. 2 und /10/

/24/ Vesely, A Time Dependent Methodology for Fault Tree Evaluation Nucl. Eng. and Design, Vol. 13 (1970), No. 2

/25/ Taylor, J.R., A Semiautomatic Method for Qualitative Failure Mode Analysis, paper presented at the CSNI-Specialist Meeting on: The Development and Application of Reliability Techniques to Nuclear Plants (Liverpool, 8-10 April 1974)

/26/ Nielsen, D.S., The Cause Consequence Method as a Basis for Quantitative Accident Analysis, Report Risö-M-1374 (1971)

/27/ Taylor, J.R., A Formalization of Failure Mode Analysis, Report Risö-M-1654 (1973)

/28/ Fussell, J.B., Special Techniques for Fault Tree Analysis Aerojet Nuclear Company, National Reactor Testing Station, Idaho Falls, March 1974

/29/ Paddleford, D.F., Analysis of Public Safety Risks Associated with Uncontained Fission Product Release from a 1000 MWe Nuclear Power Plant, paper presented at the CSNI-Specialist Meeting (Liverpool, 1974)

/30/ IEEE Standards Committee, IEEE Trial-Use Guide: General Principles for Reliability Analysis of Nuclear Power Generating Station Protection Systems, IEEE Std. 352 (1972)

/31/ Garner, N.R., Huetinck, J.A., Equipment Aging Analysis, An Extension to Reliability, Symp. Reliability of Operation in the Process Industries, San Juan (Mai 1970)

/32/ Powers, G.J., Tompkins, F.C., Fault Tree Synthesis for Chemical Processes, AIChE Journal Vol. 20, p. 376-387 (März 1974)

/33/ Nielsen, D.S., Practical Experience with Quantitative Reliability Methods as Decision Help (paper presented at the SRS-annual Meeting 1973)

/34/ Nielsen, D.S., Platz, O., Runge, B., Probabilistic Evaluation of a Redundant Protection System Based on a Cause-Consequence Diagram, Danish Atomic Energy Commission (to be published)

/35/ Nordic Working Group on Reactor Safety, Cause-Consequence Diagrams, A Graphic Method for Description and Analysis of Failure Sequences in Complex Process Systems, NARS Publication 2 (December 1972)

/36/ Dressler, E., Programme zur Berechnung der Zuverlässigkeit von Reaktorsystemen, MRR 93 (November 1971), LRA, TU München

/37/ McGrath, P.E., Radioactive Waste Management: Potentials and Hazards from a Risk Point of View, KFK-Bericht 1992, Kernforschungszentrum Karlsruhe

/38/ Koen, B.V., Carnino, A., Reliability Calculations with a List Processing Technique, IEEE-Trans. on Reliability R-23, p. 43-50 (April 1974)

/39/ Fussell, J.B., Powers, G.J., Bennetts, R.G., Fault Trees - A State of the Art Discussion, IEEE-Trans. on Reliability R-23, p. 51-55 (April 1974)

/40/ Heuser, F.W., Kafka, P.,"Möglichkeiten und Grenzen der quantitativen Sicherheitsbeurteilung", KTG-Seminar, Berlin (März 1974)

/41/ Smidt, D., "Das Lebensrisiko verringern", Die Zeit (8.6.1973)

/42/ Kellermann, O., "Unfallanalyse in der Kerntechnik", IRS-TÜ 13 (1972)

/43/ Phillips, C.A., Warwick, R.G., "A Survey of Defects in Pressure Vessels Built to High Standards of Construction and its Relevance to Nucl. Primary Circuit Envelopes" AHSB(S) R 162 (1968)

/44/ O'Neil, R., Jordan, G., "Safety and Reliability Requirements for Periodic Inspection of Pressure Vessels in the Nucl. Industry" I Mech. E. London (1970)

/45/ Kellermann, O., "Unfallanalyse in der Kerntechnik", IRS-TÜ 13 (1972)

/46/ Balfanz, H.P., "Methoden zur Systemanalyse", Fortbildungsseminar der KTG "Statist. Methoden zur Beurteilung von Auslegung, Sicherheit und Verfügbarkeit von KKW" (Berlin, März 1974)

/47/ Otway, H., Erdmann, R., "Reactor Siting and Design from a Risk Viewpoint", Nucl. Eng. Des. 13 (Aug. 1970)

/48/ Otway, H., et. al., "A Risk-Analysis of the Omega West Reactor, LA-4449, Los Alamos, (July 1970)

/49/ Otway, H., "The Application of Risk Allocation to Reactor Siting and Design", LA-4316, Los Alamos Scient. Laboratory (June 1969)

/50/ Erdmann, R., Kastenberg, W., Meleis, M., "The Development of Siting Criteria for Nucl. Power Plants", Project Clean Air, UCLA (Aug. 1970)

/51/ WASH-1250 "The Safety of Nucl. Power Reactor (LWR's) and Related Facilities", USAEC, Wash, D.C. (July 1973)

/52/ Meleis, M., Erdmann, R., "The Development of Reactor Siting, Criteria Based upon Risk Probability", Nucl. Safety, Vol. 13, 1 (Jan.-Febr. 1972)

/53/ Tattersall, J., et. al., "A Discussion of Nucl. Plant Safety with Reference to Hazards Experienced by the Community", Genfer Konferenz (1971), A Conf. 49 P 671

/54/ Bell, G.D., "Safety Criteria" Nucl. Eng. Des. 13 (1970)

/55/ Beattie, J.R., "Risks to the Population and the Individual from Iodine Release", Symp. Containm. Siting of Nucl. Pow. Pl. (1967)

/56/ Farmer, F., R. "Reactor Safety and Siting: A Proposed Risk Criterion", Nucl. Safety 8 (6) (Nov.-Dec. 1967)

/57/ Doron, Z., Albers, H., "An Extension of the Quantitative Probability Approach", Nucl. Eng. Des. 9, (März 1969)

/58/ Pasquill, F., "The Meteorological Magazine, Vol. 90, 1063 (Febr. 1961)

/59/ ICRP Com. No. 1 "Evaluation of Risks from Radiation", ICRP-Publ.8 Pergamon Press (1966)

/60/ "Consequences of Major Accidents in Large Nucl. Power Plants", Report WASH-740 USAEC, Wash. D.C. (1957)

/61/ "Der Brookhaven-Bericht, WASH-740", IRS-TÜ 2 (1973)

/62/ Bedaux-Mathematica "Results of Interviews with Proponents and Opponents of Nuclear Power in the United States (Dec. 1973) (priv. comm.)

/63/ Rasmussen, N., "The Approach of the United States Atomic Energy Commission Study to the Public Risks of Power Reactors", The Nuclear Controversy in the USA II, Mai 1974, Luzern

/64/ "Controversy Unabated; Safety Report Anticipated", Nucl. News (Mid. Febr. 1974)

/65/ Piper, H., "Siting Practice and Its Relation to Population", Nucl. Safety Vol. 14, No. 6 (Nov.-Dec. 1973)

/66/ Richardson, J., "Comparison of U.K. and U.S. Requirements for Safety and Siting of Nuclear Power Plants", Nucl. Engin. International (Nov. 1973)

/67/ Uchida, H., "Safety, Environment and Licensing Problems of Nucl. Power Plants in Japan", Nucl. Engin. International (Juli 1973)

/68/ "Nuclear Safety: Calculating the Odds of Disaster" Science 185 (Sept. 1974)

III. DAS RISIKO DES NUKLEAREN BRENNSTOFFZYKLUS

Beinahe ausnahmslos haben sich bisher Risikountersuchungen auf das Gebiet des Reaktors beschränkt. Dies stellt eine nur sehr unvollständige Beschreibung des Risikos durch Kernenergie dar. Die einzelnen Schritte des Brennstoffzyklus werden in Fig. III.1 dargestellt, wobei die Verbindung zwischen einigen Bereichen durch Transporte hergestellt wird. Das wahre Risiko durch Kernenergie ist die Summe der Risiken der einzelnen Aktivitäten wie etwa Uranbergbau, Anreicherung, Kraftwerksbetrieb, Brennstoffwiederaufarbeitung, Abfallhandhabung und Endlagerung.

In diesem Teil des Berichts soll das Risiko des Brennstoffzyklus betrachtet werden, ohne auf Uranbergbau und Anreicherung einzugehen, weil diese Teilbereiche für die BRD praktisch ohne Bedeutung sind. Der Reaktor selbst war Gegenstand der Betrachtung vorhergegangener Kapitel. Dabei sollen in diesem Kapitel nur einige wesentliche Merkmale der Art des Risikos des Brennstoffzyklus, vor allem der Endlagerung von Abfall, erläutert werden. Eine eingehendere Behandlung der Größenordnung des Risikos in den einzelnen Stufen des Brennstoffzyklus erfolgt in Kapitel XII.

Mit dem nuklearen Brennstoffzyklus sind zwei Arten (Elemente) von Risiko verbunden. Die erste Art beinhaltet das Risiko, das bei Betreiben der Anlagen des Brennstoffzyklus entsteht (in diesem Sinne wird das Abfallendlager nach Verschluß nicht als "in Betrieb" verstanden). Dieses Risiko für Leben und Gesundheit ist einerseits eine Folge möglicher Unfälle beim Betrieb der Anlagen und andererseits der Freisetzung von Radioaktivität bei Normalbetrieb. Auch die unmittelbare oder verzögerte Freisetzung radioaktiven Abfalls aus allen Betriebsphasen vor der Endlagerung wird dem Risiko der ersten Art zugeordnet.

Die zweite Art des Risikos ist durch die Gesamtheit des entstehenden radioaktiven Abfalls bedingt; diese kann auch durch Abschalten der Anlagen des Brennstoffzyklus nicht wieder zum Verschwinden gebracht werden.

Während also der Zeitverlauf von Risiken erster Art im wesentlichen dem

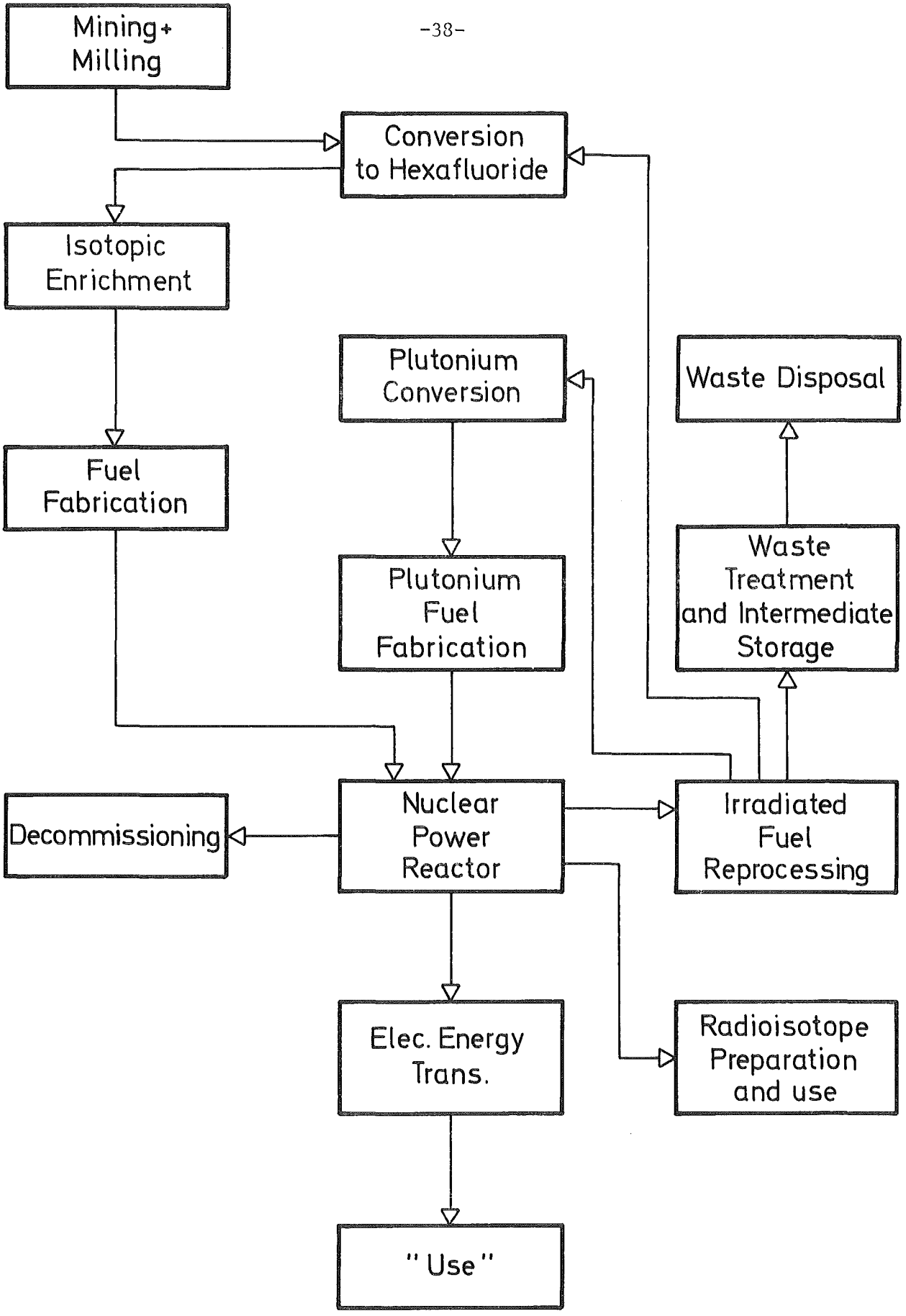

Fig. III.1 URANIUM / PLUTONIUM NUCLEAR FUEL CYCLE

Zeitverlauf des Einsatzes der Kernenergie entspricht, haben Risiken der zweiten Art eine Zeitcharakteristik, die sich weit in die Zukunft erstreckt. Sie stellen eine mehr oder weniger permanente Bedrohung dar, wenn es nicht gelingt, den Abfall sicher aus unserem Lebensraum zu entfernen. Zur Zeit gibt es keine vollkommene Methode der Abfall- und damit auch der Risikobeseitigung. Die Methoden der "Entsorgung" sind jedoch Gegenstand intensiver Untersuchungen.

Ein wichtiger Punkt ist hier die Tatsache, daß wir nur einen Teil des Gesamtrisikos der nuklearen Energieerzeugung auf uns nehmen, während der Rest zukünftigen Generationen aufgebürdet wird, die nicht direkt Nutzen aus der erzeugten Energie ziehen können. Die Probleme, die sich dadurch ergeben, daß der Langzeit-Anteil bei der Ableitung des Gesamtrisikos des Brennstoffzyklus berücksichtigt werden muß, werden im folgende diskutiert.

Die beiden Elemente des Risikos, wie sie hier bezeichnet werden, sind schematisch in Fig. III.2 dargestellt, wobei in der Darstellung kein Wert auf Maßstabstreue gelegt wurde. Es gibt keine scharfe Trennlinie zwischen den beiden Arten von Risiko, da durch die Freisetzung von langlebigen Isotopen beim Normalbetrieb der Anlage, wie z.B. J 129, eine Konzentration in Organismen erfolgen kann und somit ein Risiko mit ausgeprägter Langzeit-Komponente auftritt.

Wie in Abb. III.2 verdeutlicht, nimmt das Risiko des radioaktiven Abfalls durch den Zerfall der Isotope nach Stillegung des Brennstoffzyklus langsam ab. Die Zeit, die bis Erreichen eines effektiven "Nullpunkts" verstreicht, ist jedoch außerordentlich lang. Es ist jedoch auch denkbar, daß wegen einer Reihe von Gründen der Verlauf des Risikos mit der Zeit nicht fallend ist, sondern einen Anstieg erfährt. Eine offensichtliche Ursache könnte etwa eine Verringerung der technologischen Fähigkeiten unserer Zivilisation sein. Prognostische Untersuchungen /1/ zeigen deutlich die Möglichkeit, daß es zukünftigen Generationen an materiellen Möglichkeiten mangeln könnte, denkbare Störfälle in Abfall-Lagerstätten zu meistern. Ein zweiter Grund für einen Anstieg wäre ein unbeabsichtigtes Öffnen von Endlagern und als weitere Ursache könnte die Zerstörung der Lager durch heute nicht vorhersehbare Umstände verbunden mit einer nicht möglichen Behebung des Schadens genannt werden.

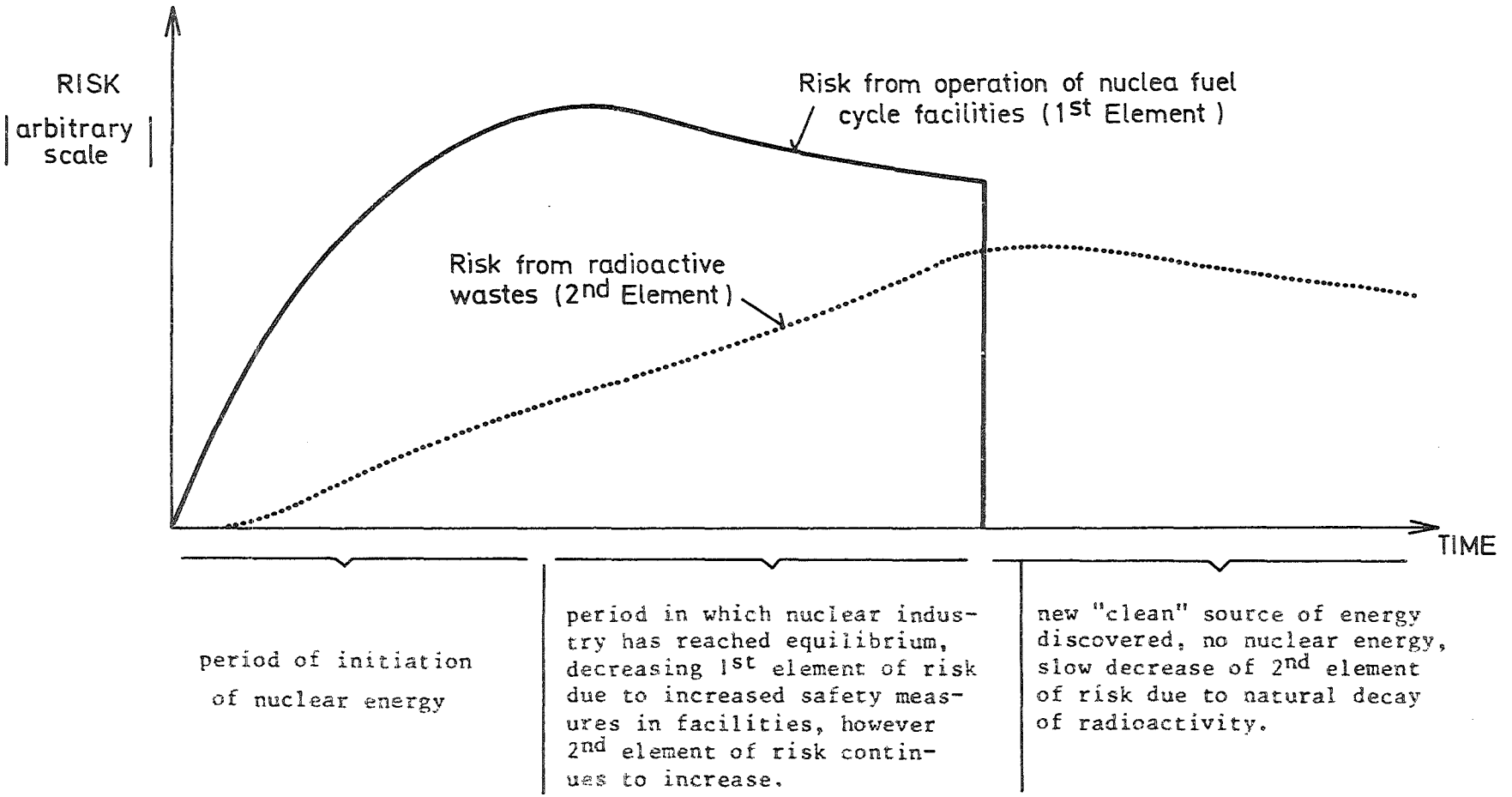

Fig. III.2 Elements of Risk Associated with the Nuclear Fuel Cycle

Ein weiterer wichtiger Punkt in dieser Betrachtung ist die Definition eines "effektiven Nullpunkts" für das zweite Element des Risikos. Theoretisch birgt der Abfall unendlich lang ein Risiko in sich, bis das letzte radioaktive Atom zerfallen ist. Praktisch kann dieser Nullpunkt aber so festgelegt werden, daß ein Zeitpunkt gesucht wird, ab dem das Risiko vernachlässigbar ist. Dieser Zeitpunkt könnte durch Vergleich von Risiken gefunden werden, z.B. wäre dieser Zeitpunkt dann erreicht, wenn unbeabsichtigtes Öffnen eines Abfall-Lagers kein größeres Risiko zur Folge hätte, als das in Uran- oder Thoriumbergwerken angetroffene.

Einen weiteren Gesichtspunkt, was gleichzeitig eine Ergänzung des oben Gesagten darstellt, liefert die sogenannte "social rate of discount". Im Prinzip handelt es sich dabei darum, daß ein Schaden, der sofort eintritt, intuitiv höher bewertet wird. als ein Schaden, der erst nach Ablauf einer bestimmten Zeit erwartet wird. Entsprechend einer subjektiven Einschätzung werden einem Menschenleben heute mehrere Menschenleben in Zukunft wertmäßig gleichgesetzt. Die Größe, die diese Veränderung der Bewertung beschreibt, wird als "social rate of discount" bezeichnet.

Bei Kenntnis dieser Größe könnte der heutige "Wert" zukünftiger Risiken beurteilt werden. Damit befände man sich in der Lage, eine obere Grenze des zukünftigen Risikos durch radioaktive Abfälle, die von der heute lebenden Bevölkerung als verantwortbar akzeptiert wird, näherungsweise zu ermitteln.

In Fig. III.3 ist der für die Entstehung radioaktiven Abfalls wesentliche Teil des Brennstoffzyklus schematisch dargestellt.

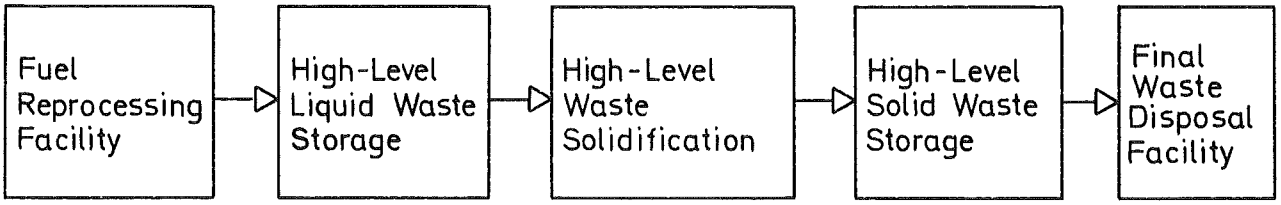

Fig. III.3 FUEL REPROCESSING AND WASTE TREATMENT IN THE FUEL CYCLE

In Kapitel XII erfolgt eine ausführliche Beschreibung der Unfallrisiken in den einzelnen Teilbereichen des Brennstoffzyklus.

IV. DAS PROBLEM DER "PUBLIC ACCEPTANCE" VON KERNENERGIERISIKEN

Die Einführung der KE[+)] bedeutet die Einführung einer Technologie, die zweifelsohne Risiken mit sich bringt. Auch andere Technologien unserer Industriegesellschaft bergen Risiken. Häufig war der Nutzen solcher Technologien unmittelbar für die von den Risiken Betroffenen empfindbar. Die Einführung solcher Technologien wurde unkritisch hingenommen. Die Verfügbarkeit von Energie ist jedoch zu einer Selbstverständlichkeit geworden, die das subjektive Empfinden eines Nutzens der Einführung der KE im Hinblick auf Energieversorgung schmälert. Zudem glaubt man, andere Alternativen zur langfristigen Sicherung der Energieversorgung zu haben. Die allgemein gehaltenen Beteuerungen der "Kernenergie-Promotoren", sie sei zwingend notwendig, werden in die Ebene von interessebezogener Reklame eingestuft. Als Folge davon ist die Risiko-Nutzen Einschätzung der Bevölkerung zumeist negativ. Insbesondere zeigt die Aktivität der Bürgeriniativen gegen die KE, daß die "Public Acceptance" der KE noch kein ausreichendes Niveau erreicht hat.

Grundlegende Untersuchungen auf diesem Gebiet wurden von Ch. Starr et. al. durchgeführt /1, 2, 3/. Dabei wird das Risiko der Kernenergie in den Bezugsrahmen derjenigen Risiken gestellt, denen der Mensch heute ausgesetzt ist (Autoverkehr, Luftfahrt). Das Schwergewicht dieser Betrachtungen liegt dabei auf der Unterscheidung zwischen freiwilligen und unfreiwilligen Risiken; als Ergebnis seiner Untersuchungen führt Starr an, daß im Fall der Freiwilligkeit ein um drei Größenordnungen höhreres Risiko akzeptiert wird, als bei Unfreiwilligkeit.

Eine Stellungnahme zu dieser Art der Darstellung des Acceptance-Problems, verbunden mit der Beschreibung anderer Verfahrensweisen, erfolgt in Kapitel XIII ("A New Concept in Risk Analysis of Nuclear Facilities").

Hier soll jedoch gezeigt werden, daß es sich bei der Public Acceptance der Kernenergie in erster Linie um ein Kommunikationsproblem handelt. Erst in zweiter Linie sind darin andere Probleme, z.B. technische, enthalten. Das Kommunikationsproblem zeigt sich in zwei Richtungen, einmal von den KE-Fachleuten in Richtung Öffentlichkeit, zum anderen von der Öffentlichkeit in Richtung KE-Fachleute. Dasselbe Kommunikationsproblem zeigt sich auch

---

[+)] Kernenergie

zwischen den KE-Promotoren und den "Betroffenen".

1. Das Kommunikationsproblem in Richtung Öffentlichkeit bzw. Betroffene kann seinerseits in drei Schwerpunkte gegliedert werden. Erstens in das Problem der Vermittlung der wissenschaftlichen und technischen Einzelheiten, um die Beurteilung der Solidität eines Vorhabens möglich zu machen; zweitens in das Problem der Durchsichtigkeit der Entscheidungs- und Überwachungsprozesse, um das Vertrauen in die verantwortungsbewußte Durchführung der Vorhaben zu stärken; drittens in das Problem der Verdeutlichung des Nutzens der Vorhaben und der Darstellung von Alternativen, damit die Notwendigkeit und Priorität der Nutzung der KE von einem großen Teil der Bevölkerung befürwortet und getragen wird.

1.1 Die Schwierigkeit der Vermittlung der wissenschaftlichen und technischen Einzelheiten und in der Folge davon die Probleme der Identifikation der Betroffenen mit einem Vorhaben führt zu dem Konzept des "technischen Staates", in dem aufgrund der zunehmenden Komplexität der technischen Sachverhalte, die jeweils auch soziale Maßnahmen zur Folge haben, die wieder nur "technisch" angegangen werden können, der Demokratie zunehmend der Boden entzogen wird und "Sachgesetzlichkeit" in den Vordergrund rückt. Ein Heer von verschiedenartigen Spezialisten hält das "System" in Gang /4/. Sehr bald wurde erkannt, daß nicht zu erwarten ist, daß sich der Bürger dieser Sachgesetzlichkeit beugt. Je mehr aber die hautnahen Anspruchsniveaus des Bürgers erfüllt sind, desto sensibler wird er gegenüber den allgemeineren Umständen der Gesellschaft, in der er lebt. Die Schwierigkeit, als Normalbürger zu verstehen, was Wissenschaft und Technik produzieren, führt in zunehmend in eine mißtrauische Position; dies umso mehr, wenn mutmaßlich Gefahren im Verzug sind, die man versucht wegzudiskutieren. Es entsteht eine Loyalitätskrise /5/. Die Vielzahl der bereits bundesweit zusammengeschlossenen Bürgerinitiativen - viele gegen KE - geben davon ein Zeugnis.

Die hier anzusprechende Ursache ist u.a. das mangelnde Bemühen von Wissenschaft und Technik, ihre Ziele, ihre Methoden, ihre Ergebnisse und deren Folgen offen und verständlich, sowie frei von Spezialisten-Fachjargon, darzustellen: den Betroffenen die Sachverhalte zu vermit-

teln. Da häufig wissenschaftliche Arbeit und Öffentlichkeitsarbeit in einer Person nicht möglich ist, sollte mehr als bisher arbeitsteilig beides in Forschung und Entwicklung und bei der Implementation neuer Technologien vorgesehen werden.

1.2 Nun wird auch bei bereitwilliger Information die Aufnahmefähigkeit des Nicht-Spezialisten begrenzt und es für eine Person schwer sein, die Entscheidungen auf allen Ebenen bis es zur Einführung einer bestimmten Technologie kommt, voll mitvollziehen zu können. Allein aber, wenn der Betroffene das Gefühl hat, daß er den Entscheidungsgang mitvollziehen könnte, verhindert dies eine Loyalitätskrise. Dazu gehört aber, daß die Entscheidungs- und auch die Überwachungsprozesse beim KE-Einsatz durchsichtig und so strukturiert sind, daß man davon ausgehen kann, daß Verantwortung gegenüber der Gesellschaft geübt wird /6/. Dies ist nicht sichergestellt, wenn sich im wesentlichen nur KE-Fachleute mit ähnlichem gedanklichen Hintergrund gegenseitig kontrollieren, wie dies zwischen den meisten kerntechnischen Anlagen beantragenden und genehmigenden Stellen der Fall ist. Dasselbe gilt für die Fachgutachter, auf die die Behörden angewiesen sind /7/. Notwendig erscheint die Offenlegung aller, auch kleinerer Störfälle, sowie eine ausgewogende Kompetenz- und Kontrollverteilung beim Betrieb kerntechnischer Anlagen.

Wenn das öffentliche Mißtrauen in die KE beseitigt werden soll, so ist eine notwendige Bedingung dafür die Transparenz und demzufolge wohl auch Verbesserung der Genehmigungsprozesse und der Überwachung von Entwicklung und Betrieb kerntechnischer Anlagen. Es muß sichtbar sein, daß hierbei von unabhängigen Personengruppen um das Tragbare gerungen wird.

1.3 Daß KE möglicherweise eines von den hautnahen Anspruchsniveaus zu erhalten vermag und dieses ohne sie in Frage gestellt sein könnte, ist weder allgemein bewußt gemacht, noch ausreichend analysiert. Für den Normalbürger ist Energie noch kein ausreichender Motivator. Auch erscheint der Öffentlichkeit Energie noch in jeder gewünschten Form verfügbar zu sein. Warum also Risiken mit Kernkraftwerken eingehen? Hier sind ja doch nur ökonomische Interessen im Spiel oder wird der Spieltrieb von Technikern befriedigt!

Um die "Public Acceptance" für KE zu erhöhen, wäre es dringend erforderlich, mit demselben Ernst, mit dem die Entwicklung der KE betrieben wurde, wenigstens zu prüfen, welche anderen Energieerzeugungsmöglichkeiten in Frage kämen, um zu verdeutlichen und glaubhaft nachzuweisen, welche Probleme ohne KE entstünden und den Nutzen der KE in mit ihren Kosten und Risiken vergleichbarer Form darzustellen. Allein der Ausweis, daß in diesem Sinne laufend Bemühungen und Prioritätenüberlegungen angestellt werden, würde die Öffentlichkeit beruhigen. Es ist jedoch heute festzustellen, daß diesbezügliche Aussagen meist zweckopportunistisch zu schnell und mit zu wenig Hintergrund getan werden. Eine kritische Öffentlichkeit merkt dies und zieht ihre Konsequenzen.

2. Es wurde behauptet, daß sich das Kommunikationsproblem auch von den Betroffenen her in Richtung KE-Promotoren zeigt. Hierzu liegt als These zugrunde, daß Wissenschaft und Technik zwar Folgen technologischer Entwicklungen grundsätzlich weitgehend aufzuzeigen, ja diese sogar empirisch in die Erfahrungsumwelt einzuordnen vermag, daß sie aber keine Antwort auf die Frage, ob man diese Folgen akzeptiert, bieten kann. Mit dem Einsatz der KE sind Risiken für die Bevölkerung unvermeidlich. Jedoch auch anderweitig setzt sich die Bevölkerung den verschiedensten Risiken aus. Wissenschaft und Technik kann die Risiken durch steigenden Aufwand verringern, aber nicht zu Null machen. Ab wann ein Risiko ausreichend niedrig ist, darf nicht dem Urteil des Fachexperten überlassen bleiben, sondern ist in einem demokratischen Staat Sache der Gesellschaft und der unmittelbar Betroffenen. Wie man im einzelnen als Betroffener in dieser Frage mitzuentscheiden vermag, ist eine andere, eine politische Frage.

   Bei der KE wird dieser Punkt besonders deutlich. Hier ist es zur Zeit nicht möglich, das Risiko quantitativ anzugeben und in die allgemeine Risikobereitschaft einzuordnen. Es liegt in der Natur der Sache, daß eine empirische Erfahrung über das Risiko der KE nicht vorliegt. Das führt natürlich dazu, daß sich KE-Fachleute bemühen, alle möglichen Unfälle zu erdenken und mangels Erfahrung weit ins Hypothetische greifen. Ein Test, ob diese hypothetischen Unfälle durch ebenfalls erdachte Gegenmaßnahmen abgefangen werden können, ist nur teilweise möglich.

Führt man eine Vielzahl von Experimenten an kleinen Teilsystemen durch, so ist eine Modell-Theorie über das Zusammenwirken dieser Teilsysteme nötig; baut man Prototypen möglichst großer Teilsysteme und testet sie, so liegt in zunehmendem Maße die Demonstration der Funktionsfähigkeit des Prototyps vor, aber die Übertragbarkeit dieser Erfahrung auf gleiche Typen wird geringer. Damit bleibt ein Rest von Ungewißheit. Mit anderen Worten, Unbedachtes läßt sich auch nicht bezüglich seiner Folgen und Eintretenswahrscheinlichkeit bedenken.

Daher ist es nützlich, die verschiedenen Risiken ein Stück weit zu ordnen (siehe auch Kapitel I):

a) In der deterministischen Betrachtungsweise der Reaktorsicherheit geht man davon aus, daß man potentielle Schadensmechanismen erkennt und durch entsprechende Konstruktionen ('Re-Design') verhindert. Damit verbleibt letzten Endes kein zu quantifizierendes Risiko.

b) In der probabilistischen Betrachtungsweise geht man davon aus, daß ein vollständiges Vermeiden von Störfällen durch entsprechende Konstruktionen nicht sinnvoll bzw. nicht möglich ist. Auch die zum 'Abfangen' von potentiellen Störfällen bei Einzelkomponenten vorgesehenen technischen Einrichtungen können mit einer bestimmten Wahrscheinlichkeit ausfallen. Die wahrscheinlichkeitstheoretische Durchrechnung dieser Störfälle ermöglicht es, für wohldefinierte Unfallabläufe Wahrscheinlichkeiten für das Eintreten bestimmbarer Schadensfälle anzugeben. Man kann dann von einem 'kalkulierbaren Risiko' sprechen. In diesen Bereich gehört auch der Auslegungsunfall bzw. der GAU und in zunehmendem Maße darüber hinausgehende Unfälle.

c) Über b) hinaus sind Unfälle denkbar, die als so unwahrscheinlich angesehen werden, daß eine wahrscheinlichkeitstheoretische Durchrechnung ihrer Abläufe unnötig bzw. teilweise unmöglich erscheint. In diesen Fällen spricht man von hypothetischen Unfällen bzw. von hypothetischem Risiko, das bereits nicht mehr quantifiziert ist.

In zunehmenden Maße wird jedoch versucht, auch für diese "hypothetischen" Unfälle die Risiken quantitativ zu fassen, womit c) und b) weitgehend verschmilzt.

d) Besonders im Anschluß an a), jedoch auch für b) und c) zutreffend, gibt es die Überlegung, daß man Unfallabläufe evtl. übersehen hat. Außer durch Ausweis des Grades der Bemühungen im Sinne von a) bis c), gibt es keine formale Absicherung gegenüber der Frage, ob man an alles gedacht habe. Wahrscheinlichkeiten für mögliche übersehene Störfälle sind nicht angebbar. Wir bezeichnen das hiermit verbundene Risiko mit 'Restrisiko'.

Im Sinne von a) vorzugehen, ist eine notwendige Voraussetzung, um bei der Entwicklung von KKW systematische Fehler zu eliminieren. Auf b) laufen die heutigen Anstrengugen hinaus, wie sie an verschiedenen Stellen unternommen werden. Dabei ergibt sich im Verein mit den Kenntnissen aus a) auch die Chance, die in c) angesprochenen Unfälle wirklich als sehr unwahrscheinlich zu dokumentieren. Es ist allerdings zu bemerken, daß insbesondere die Datenbasis und die Erfahrungen mit KE-Teilsystemen für die konsequente Durchführung von b) und c) noch nicht hinreicht (siehe Kapitel II.A und VII).

Ein Teil der öffentlichen Bedenken gegen KE rührt aus dem Unwissen über die Anstrengungen gemäß a) und aus der Ahnung, daß b) und c) noch nicht ausreichend behandelt werden kann. Vermutlich ist aber auch ein gewichtiger Faktor für die Bedenken gegenüber der Kernenergie, daß es das Restrisiko im Sinne von d) gibt. Insbesondere hier wird die Frage nach den Bedingungen einer 'Public Acceptance' von KE bedeutsam. Hier liegt die eigentliche Nahtstelle zwischen den Aussagemöglichkeiten der Wissenschaft und der Werteinschätzung der Bevölkerung (bzw. Politik). Ob ein Restrisiko akzeptierbar ist, kann nicht allein von der wissenschaftlichen Seite beantwortet werden. Das Verhalten der KE-Fachleute wird die Frage, ob KE trotzdem akzeptiert wird, jedoch maßgeblich beeinflussen. Dabei spielen mehr als sonst Urteile eine Rolle, bei denen der Betroffene wieder an Bedeutung gewinnt. Hierzu sollen folgende Aspekte kurz ausgeführt werden:

2.1 In soziologischen Studien, die empirisch in engem Kontakt mit dem Bürger ausgeführt werden sollten, müßte ermittelt werden, welche Parameter auf das Niveau der Akzeptierbarkeit von Risiken Einfluß nehmen und wie die Bedeutung der Parameter gegeneinander abhängig vom erwarteten Risikoausmaß liegt. Solche Analysen könnten aufzeigen, weshalb der Bürger gegen KE sensibel ist, und wo deshalb Maßnahmen zur Verbesserung des KE-Einsatzes am nötigsten sind.

Es würde sich auch zeigen lassen, in wieweit die Nicht-Akzeptierung der KE ein Kommunikationsproblem ist. Anstelle der Quantifizierung von Risiken könnte die Analyse der Auswirkungen möglicher Störfälle im "Wenn-Dann"-Sinne treten. Es ist von daher nötig, zunächst einmal im Sinne der deterministischen Betrachtungsweise im gesamten Brennstoffzyklus, von der Erzgewinnung über das Kernkraftwerk bis zur Abfalllagerung Gründe für mögliche Störfälle zu ermitteln. Es ist aber vor allem nötig, jeweils, ohne evtl. Gründe oder gar Wahrscheinlichkeiten für das Eintreten bestimmter Störfälle zu kennen, das potentielle Ausmaß verschiedener Störfälle, wie Niederschmelzen des Cores mit zweiter Kritikalität oder Wassereinbruch in Abfallagerstätten und ihr Auswaschen, aber auch die vielen kleinen Möglichkeiten für Umweltbelastungen darzustellen. Wir wollen in Erweiterung der Aufzählung von Risikobegriffen hier als e) den Begriff 'konditionales Risiko' einführen, ein nicht mit Wahrscheinlichkeiten belegtes Risiko, das nur durch 'Wenn-Dann'-Darstellungen, d.h. der Darstellung von denkbaren Unfällen und ihrer Folgen charakterisiert ist (siehe z.B. Kapitel "Brennstoffzyklus"). Ein Großteil der heutigen Anstrengungen, besonders auf dem Gebiet der Kernkraftwerke, fällt in diese Kategorie der Risikoanalysen. Kann das Gefühl glaubhaft vermittelt werden, daß alles Erdenkliche mit Akribie analysiert wurde, so würde dies wohl sehr stark zur Akzeptierbarkeit der KE beitragen. Unter Umständen sind anhand solcher "Wenn-Dann"-Analysen sogar Anspruchsniveaus für einzelne, Risiken beeinflussende Parameter empirisch ermittelbar und somit die Frage der Akzeptierbarkeit zum Teil wieder quantifizierbar, ohne daß absolute Risikozahlen ermittelbar sind.

2.2 Im vorangehenden Abschnitt 2.1 wurden sozusagen indirekte Methoden der Informationsvermittlung von der betroffenen Öffentlichkeit zu

den KE-Fachleuten angesprochen. Zusätzlich ist die direkte Artikulation des Betroffenen bedeutsam. Wenn die unter Abschnitt 1 geforderten Verhaltensweisen praktiziert werden, kann dies in Form eines Gesprächs ablaufen, für das die in 2.1 angesprochenen Untersuchungen und "Wenn-Dann"-Analysen Strukturhilfen geben können. Man kann heute noch nicht davon sprechen, daß zwischen der betroffenen Öffentlichkeit und den KE-Fachleuten ein Gespräch möglich geworden sei, das die Bedingungen für die Akzeptierbarkeit von KE zu ermitteln gestattet hätte. Solange man auf Seiten der KE-Promotoren es nicht für nötig hält, dies möglich zu machen, wird sich die Konfrontation zuspitzen. Insbesondere müßte als eine Voraussetzung die Einsicht stehen, daß die Frage nach dem Risiko der KE aus methodischen Gründen nur angemessen behandelt werden kann, wenn sie um die Frage nach den Bedingungen für die Akzeptierbarkeit der KE durch die Öffentlichkeit erweitert wird. Dazu muß man sich in Offenheit mit der Öffentlichkeit ebenso befassen, wie mit Akribie mit den möglichen Folgen und Nebenfolgen des KE-Einsatzes, seines Nutzens und seiner Alternativen.

Literaturverzeichnis:

/1/ Starr, C., "Social Benefits vs. Technological Risk: What Is Our Society Willing to Pay for Safety?" Science 165, (1969)

/2/ Starr, C., "Benefit-Cost Studies in Socio-Technical Systems", Colloqu. on Benefit-Risk Relationships for Decision Makers, Wash. (April 1971).

/3/ Otway, H., "Risk vs. Benefit: Solution or Dream", Los Alamos, LA-4860, (Nov. 1971)

/4/ Schelsky, H., Der Mensch in der wissenschaftlichen Zivilisation, in: Auf der Suche nach Wirklichkeit, Verlag Dietrichs, (1961), S. 439

/5/ Offe, C., Das politische Dilemma der Technokratie, in: Texte zur Technokratiediskussion, Europäische Verlagsanstalt, (1970), S. 156

/6/ Die hierbei angesprochenen Probleme von Partizipationsmöglichkeiten werden äußerst kritisch behandelt z.B. in
Schelsky, H., Mehr Demokratie oder mehr Freiheit, FAZ v. 20.1.1973, S. 7
Einen Ausweg aus dem Loyalitätsdilemma, ohne notwendig in die Gefahren zu breiter Partizipation zu kommen, zeigt unseres Erachtens:
Berkemann, J., Technokratie und verfassungsrechtliche Prinzipien, in: Technokratie als Ideologie, Verlag Kohlhammer, (1973), S. 193

/7/ vgl. hierzu den 'Wiedenfelser Entwurf', Neugestaltung des Genehmigungsverfahren im Umweltschutz. Evang. Akademie Baden (Febr. 1973)

V. SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

Die Autoren sind auf der Basis des erörterten Wissensstandes zu der Ansicht gekommen, daß unter den gegenwärtigen Voraussetzungen eine zuverlässige quantitative Abschätzung der Risiken durch die Nutzung der Kernenergie noch nicht befriedigend möglich ist. Im wesentlichen haben sich folgende Schwachstellen herauskristallisiert:

a) Die Eintrittswahrscheinlichkeit störfallauslösender Ereignisse sowie die Zuverlässigkeit der störfallhemmenden Funktion sicherheitstechnischer Einrichtungen kann wegen mangelnder Daten der Komponenten und nur unvollständiger Erfassung aller Funktionszusammenhänge im allgemeinen noch nicht hinreichend genau ermittelt werden.

b) Der physikalische Ablauf des Unfallgeschehens in der Anlage sowie die physikalsichen Folgeereignisse in ihrer Umgebung vollziehen sich in außerordentlich komplexen Systemen. Methoden zur modellmäßigen Erfassung dieser Vorgänge befinden sich heute in der Entwicklung, haben jedoch noch nicht den Stand erreicht, der zu einer Errechnung von Risikowerten vorauszusetzen wäre.

c) Über die Schadensauswirkungen eines Unfalls, d.h. über die biologischen Konsequenzen äußerer Bestrahlung und der Inkorporation radioaktiven Materials sind allgemein akzeptierte quantitative Angaben nur in beschränktem Umfang verfügbar. Schließlich befinden sich auch die Methoden zur Bewertung dieser Folgen und zum quantitativen Vergleich mit anders gearteten Risiken erst in der Entwicklung.

Wegen des großen Umfangs und der Komplexität des Problemkreises dürfte es im Moment nicht möglich sein, eine Liste von Aktivitäten aufzustellen, deren Durchführung mit Sicherheit zu einer zuverlässigen quantitativen Ermittlung der Risiken und der Möglichkeit einer definierten Herabsetzung führen würde. Es soll jedoch eine Reihe von Forschungsarbeiten vorgeschlagen werden, die die wichtigsten Lücken abdecken und daher zu einer wesentlichen Verbesserung des gegenwärtigen Standes führen würden.

(Dabei beziehen sich die Punkte 1 - 5 im wesentlichen auf den Komplex der

unfallauslösenden Ereignisse und Komponenteneigenschaften, Punkt 6 und 7 auf Unfallablauf und physikalische Folgen, Punkt 8 und 9 auf die spezifische Problematik von Transport und Endlagerung und Punkt 10 auf die Bewertung von Schadensauswirkungen.)

1. Erstellung eines zentralen Informationssystems für Zuverlässigkeitsdaten

Das System sollte folgende Eigenschaften haben:

- Spezialisierung auf Daten für sicherheitstechnisch wichtige Komponenten von Kernenergieanlagen. Solche Daten werden systematisch gesammelt und können in größerem Umfang und Detail als bei den herkömmlichen Datenbanken bereitgestellt werden.

- Erfahrungsdaten werden durch Vergleich mit theoretischen Modellen ausgewertet.

- Die zentrale Bank korrespondiert soweit wie möglich frei mit Laboratorien, Komponentenherstellern sowie Herstellern und Betreibern kerntechnischer Anlagen. Schwierigkeiten könnten noch durch kommerzielle Restriktionen bei der Datenweitergabe auftreten.

- Die Methoden für Datensammlung und Verarbeitung sowie die Terminologie für den Informationsaustausch werden standardisiert.

- Das System soll von einer unabhängigen und unparteiischen nationalen oder internationalen Organisation betrieben werden.

Ein Vorschlag für ein solches zentrales Informationssystem befindet sich in Kapitel VIII sowie in /3/.

2. Entwicklung von statistischen Methoden zur Datenauswertung

Hierunter fallen besonders zwei Problemkreise:

2.1 Die Ermittlung der Ausfallrate einer Komponente aus experimentellen Daten.

2.2 Die Auswertung der "Belastbarkeitsreserve" einer Komponente.

Zu Punkt 2.1: Stützt man sich bei der Auswertung von Testläufen, insbesondere auch bei Zeitraffertests lediglich auf die beobachteten Lebensdauern, so erhält man wegen der begrenzten experimentellen Möglichkeiten oft nur ein Ergebnis von unzureichender Aussagekraft (man arbeitet hier mit "freier Statistik").

Die Aussagekraft des Experimentes wird wesentlich verbessert, wenn man die ausschlaggebenden Vorgänge, die sich während des Betriebs in der Komponete abspielen, analytisch erfaßt. Die so gewonnene "a priori" Kenntnis wird in der Auswertung des Experimentes einbezogen.

Ist die "a priori" Kenntnis qualitativ (z.B. Ausfallrate monoton steigend) so stellt sich ein Auswerteproblem mit "nicht-parametrischer Statistik".

Ergibt die analytische Behandlung, daß die Ausfallrate eine bestimmte Funktion der Zeit ist, für die nur wenige (etwa 1 bis 3) Parameter durch das Experiment zu bestimmen sind, so handelt es sich um eine "parametrische Statistik". Hohe "a priori"-Kenntnis erlaubt es, auch unter schwierigen experimentellen Bedingungen aussagekräftige Ergebnisse über Ausfallraten und Lebensdauern zu erreichen. Letzlich ermöglicht dies auch eine rationale Anwendung der vorsorglichen Wartung.

Die mathematischen Methoden zur Auswertung der verschiedenen Typen von Statistik müssen noch weiter entwickelt werden.

Zu Punkt 2.2: Eine korrekte mathematische Behandlung des Ausfallverhaltens von Komponenten, die unter statistisch wechselnder Belastung stehen, muß entwickelt werden (siehe auch Ref. 7). Falls das Zeitverhalten der Belastung vorhersagbar ist, genügen die üblichen Methoden der Ausfallratenberechnung. Bei statistisch wechselnder Belastung muß jedoch auf der Basis einer "Belastbarkeitsreserve", die eine stochastische Funktion der Zeit ist, gearbeitet werden.*) In diesem Fall ergibt sich die Ausfallwahrscheinlichkeit für ein Zeitintervall Δt als die Wahrscheinlichkeit, daß während Δt, die Belastbarkeitsreserve ≤ 0 wird. Dieser Art der Analyse ist besonders wesentlich für eine korrekte und allgemeine Be-

*) Die Verteilung der Belastbarkeitsreserve soll auch die Effekte unentdeckter Materialfehler berücksichtigen.

handlung der Common Mode Failures, siehe Kapitel IX, und für die Anwendung des Konzepts der Continuous Lifetime Prediction, siehe /7/.

3. Rechnergestützte Aufstellung von Fehlerbäumen

Die Aufstellung von Fehlerbäumen mit Hilfe der Datenverarbeitung erweist sich als notwendig, da wegen der Komplexität der Anlagen mit konventionellen Methoden nicht alle potentiellen Ereignisketten aufgefunden werden können. In das Computer-Programm muß Information über das Flußdiagramm der Anlage, über Konstruktionsmerkmale und über die räumliche Gestaltung gleichermaßen eingehen. Dies ist besonders für die Erfassung von Common-Mode-Failures wichtig.

Grundsätzlich ist gezeigt worden, daß die Aufstellung solcher Fehlerbäume möglich ist /1, 2/. Die methodische Entwicklung muß sich jetzt auf das Erreichen vertretbarer Rechenzeiten, sowie eventuell auf die Berücksichtigung der Auswirkungen von Reparaturmaßnahmen auf den Fehlerbäumen selbst konzentrieren.

Rechnergestützt erstellte Fehlerbäume können so angelegt sein, daß sie jeweils den momentanen Zustand der Anlage berücksichtigen. Sie können dann Information über das optimale Vorgehen bei Betrieb, Wartung und Reparatur der Anlage geben und so zur Kostenminimierung bei Aufrechterhaltung der geforderten Zuverlässigkeit beitragen.

4. Common Mode Failures

Eine exakte und verbindliche Definition des Begriffs sowie eine Kategorisierung der Common-Mode-Failures (CMF) muß erarbeitet werden.

Durch Sammeln und Aufgliederung aller international verfügbaren Information über das Auftreten von CMF muß die Erfahrung aller abgelaufenen Reaktorbetriebsjahre so weit wie möglich ausgewertet werden. Darüberhinaus sollte eine Anstrengung unternommen werden, um noch unbekannte Quellen für CMF zu identifizieren.

Durch Empfindlichkeitsstudien sollte ermittelt werden, in welchen Anlage-

bereichen die Möglichkeit des Auftretens von CMF besonders intensiv untersucht werden muß.

Da mit jeder Betriebsstörung besondere Belastungen für Komponenten einhergehen, ist die Entwicklung einer Theorie der Ausfallraten unter dem Gesichtspunkt der Belastbarkeitsreserven für die Erfassung der CMF besonders wichtig.

5. Arbeiten über das menschliche Verhalten

Es besteht die Tendenz, die Funktionen menschlicher Operateure weitgehend durch Automatisierung zu ersetzen. Wegen seiner hohen Flexibilität und Entscheidungsfähigkeit auch in komplexen, unvorhergesehenen Situationen, werden dem Menschen jedoch auch weiterhin gewisse Aufgabenbereiche in der Kerntechnik vorbehalten bleiben.

Es müssen Verfahren entwickelt und angewendet werden, um die optimale Arbeitsteilung zwischen Mensch und Automatik zu erreichen.

Es ist sicherzustellen, daß die (im allgemeinen einfachen) menschlichen Verrichtungen beim Normalbetrieb, insbesondere aber auch alle potentiellen Handlungen bei Störfällen, in die Zuverlässigkeitsanalyse möglichst weitgehend integriert werden.

6. Modelle von Unfallabläufen

Die Arbeiten zur modellmäßigen Beschreibung von Unfallabläufen in Reaktoren sind weiter voranzutreiben.

Da Unfälle, die zur Freisetzung größerer Aktivitätsmengen führen, fast stets mit Propagationserscheinungen und auch mit geometrischen Veränderungen des Kerns verbunden sind, ist der Entwicklung probabilistischer Modelle für diese Vorgänge besondere Bedeutung zuzumessen.

7. Abgabe von Radionukliden und ihr Verhalten in der Ökosphäre

Theoretische Modelle für die Emission von Radionukliden müssen weiter ent-

wickelt werden. Sie müssen auf experimentellen Daten basieren. Wegen des Mangels an experimentellen Daten müssen noch konservative Werte angenommen werden. Bis heute gibt es nur sehr wenige Experimente auf diesem Gebiet, meistens unter unrealistischen Bedingungen.

Es ist daher wünschenswert, Experimente für viele Radionuklide unter so weit wie möglich realistischen Bedingungen durchzuführen.

Zum Problem der Ausbreitung von Radionukliden in der Umwelt sind weitere eingehende Untersuchungen notwendig. Als Beispiel sei die wichtige Frage genannt, ob Plutonium im Erdboden verbleibt oder durch Absorption in Pflanzen in die biologische Kette eingebracht wird. Für diese Fragen sind auf der Grundlage experimenteller Arbeiten zeitabhängige probabilistische Modelle zu entwickeln.

8. Transport von nuklearen Materialien

Auf diesem Gebiet werden sowohl Daten als auch theoretische Modelle gebraucht. Insbesondere sollten folgende Probleme untersucht werden:

- Ermittlung von Unfallwahrscheinlichkeiten für alle Transportarten. Vergleiche der Werte für Transporte, die in das öffentliche Verkehrswesen integriert sind, und solche, die speziell durchgeführt und überwacht werden.

- Erfassung und theoretische Untermauerung aller erreichbaren Daten über Containerfestigkeit und Aktivitätsabgabe bei Unfällen.

- Möglichkeiten und Konsequenzen von Sabotage sollten hier besonders sorgfältig untersucht werden.

Eine wichtige Frage in diesem Zusammenhang ist die der räumlichen Verteilung der Anlagen des Brennstoffzyklus. Sollte das Konzept der "Nuclear Parks" verwirklich werden, so kommt dem Transport als Teil des Kernenergie-Gesamtrisikos unter Umständen nur untergeordnete Bedeutung zu.

9. Auswertung der Risiken durch nuklearen Abfall

Unsere Generation wird unseren Nachkommen nuklearen Abfall hinterlassen.

Wir haben daher das Problem, uns zwischen den möglichen Alternativen für Abfallbehandlung und Endlagerung zu entscheiden. Das verursachte Risiko muß über eine sehr lange Zeitskala (viele hundert Jahre) betrachtet werden. Da für solche Zeiträume keine exakten Daten zur Verfügung stehen, sind keine quantitativen Aussagen im absoluten Sinn, wohl aber vergleichende Überlegungen möglich.

10. Bewertung von Schadensauswirkungen

Um Risiken im technologischen Bereich vergleichen zu können, ist es notwendig, folgende Fälle auf gleiche Bezugsgrößen zu normieren:

- Mehrere kleine und wenige große Schäden

- Personen- und Sachschäden

- Heutige und zukünftige Schäden

Dies geschieht mit Hilfe der Utility Theorie (Kap. XIII und /5, 6/), deren Ziel es ist, für bestimmte Lebensbereiche und Personengruppen subjektive Werte quantitativ festzustellen.

Es stellt sich die Frage, welche Gruppe oder Gruppen anzusprechen sind und wie widersprechende Wertungen zu wichten sind.

Daraus ergibt sich die Aufgabe, die Utility Theorie weiter auszubauen und auf die heutigen Probleme der Kernenergie anzuwenden.

Literaturverzeichnis: Siehe Kapitel VIII.

B. SPEZIELLE ANALYSEN

VI. DURCHFÜHRUNG DER ZUVERLÄSSIGKEITSANALYSE

(i) FORMBLATTANALYSE

Die Formalisierung der Ausfallart- und Fehlereffektanalyse (Failure Mode and Effects Analysis, FMEA) kann mit Formblättern durchgeführt werden (Balfanz /8/).

Das Vorgehen wird an einem Ventil gezeigt. Aus seinen Funktionen lassen sich die Ausfallarten ableiten.

Tabelle 1

Funktion	Ausfallart
schließen	fällt offen aus, schließt nur teilweise
öffnen	fällt geschlossen aus, öffnet nur teilweise
geschlossen	öffnet vollständig öffnet teilweise (Leckage)
offen	schließt vollständig (Blockage)

Die Analyse wird mit Formblättern durchgeführt, wobei für jede Komponente ein oder mehrere Formblätter verwendet werden. Das Formblatt ist in folgender Weise aufgebaut (dabei geben wir einen Vorschlag des IRS /8/ wieder):

- Im Kopf des Formblattes wird der Name der Anlage, des Systems und der betrachteten Komponente aufgeführt. Ferner sind die besonderen Einsatzbedingungen und verwendete Unterlagen anzugeben.

- Referenznummer für die Fehlerkennzeichnung.
  Das Benummerungssystem sollte die Kennzeichnung des Bauteils der jeweiligen Fehlerart enthalten.

- Funktion einer Komponente in einem bestimmten Betriebszustand des Systems (vgl. Tabelle 1).
  In dieser Spalte müssen alle Funktionen in allen möglichen Betriebszuständen angegeben werden.

- Ausfallart (vgl. z.B. Tabelle 1)

- Fehlererkennung sowie Komponenten-Zustände, die Fehlererkennung beeinflussen. Es ist z.B. zu unterscheiden zwischen Betriebs- und Stand-by-Komponenten, zwischen kontinuierlich betriebenen und Schaltkomponenten, zwischen Möglichkeiten zur Fehlererkennung durch Anzeige oder durch Wiederholungsprüfungen.

- Fehlerkompensation
  Es sind die Einrichtungen (z.B. redundante Komponenten) oder Maßnahmen (z.B. Umschaltung, Reparatur) anzugeben, die für die betreffende Ausfallart der Komponente vorgegesehen sind (vgl. auch Kapitel "Common Mode Failures").

- Ausfallauswirkungen
  Die Auswirkungen der entsprechenden Ausfallart auf die Funktion der Komponente und das übergeordnete System sind anzugeben.
  Die Klassifizierung durch Zuverlässigkeitskenngrößen braucht nicht in jedem Fall vorhanden zu sein.

- Ausfallrate $\lambda[h^{-1}]$, Ausfallzeit bzw. Reparaturdauer $\tau[h]$ der Komponente in der betreffenden Ausfallart. Diese Daten können zur Bewertung der Ausfallauswirkungen verwendet werden. Ferner kann in dieser Zeile auch eine Fehlerklassifikation im Hinblick auf Sicherheit oder Zuverlässigkeit vorgenommen werden.

(ii) AUFBAU EINES FEHLERBAUMS

Es ist zweckmäßig, die Aufstellung des Fehlerbaums nach einem bestimmten Schema auszuführen. Es kann z.B. folgendermaßen ausgeführt werden (nach DIN 25424 /2/):

a) Das unerwünschte Ereignis wird in ein Kommentarrechteck eingetragen.

b) Ist das unerwünschte Ereignis bereits ein Komponentenausfall, so folgt Schritt e). Anderenfalls Feststellung der Ausfälle, die das unerwünschte Ereignis nach sich ziehen.

c) Diese Ausfälle werden in Kommentarrechtecke eingetragen und mit einer ODER-Verknüpfung zusammengefaßt.

d) Ist der Ausfall ein Komponentenausfall, folgt Schritt e), anderenfalls folgt Schritt f).

e) Der Ausfall ist ein Komponentenausfall. Es folgt eine ODER-Verknüpfung. Die Eingänge der ODER-Verknüpfung sind mit Primärausfall, Sekundärausfall und Kommandofehler der Komponente belegt.

Der Primärausfall kann durch einen Fehlerbaum nicht weiter analysiert werden. Der Sekundärausfall und der Kommandofehler beziehen sich auf Ausfälle von Teilsystemen, die nicht in jedem Fall vorhanden sein müssen. Sind diese vorhanden, folgt Schritt f).

Ist der Fehlerbaumzweig abgearbeitet, wendet man sich dem nächsten Systemausfall von Schritt c) zu. Es folgt Schritt d).

Ist kein Ausfall mehr zu entwickeln, stoppt die Prozedur. Es folgt Schritt g).

f) Der Ausfall ist ein Systemausfall. Die im Kommentarrechteck angeführte Beschreibung des Ausfalles ist als unerwünschtes Ereignis des darunter zu entwickelnden Fehlerbaumes aufzufassen:

Es sind die direkten Ursachen dieses Ausfalles zu bestimmen. Je nach Art der Ursachen folgt eine bestimmte Verknüpfungsart. Danach folgt Schritt d).

g) Stop.

Zur Terminologie des Schemas:

- " Primärausfall" ist ein Ausfall unter normalen Betriebsbedingungen (z.B. durch einen Fehler im Entwurf, durch Alterung eines für die Komponente verwendeten Materials u.s.w.).
- "Sekundärausfall" ist ein Ausfall durch unbeabsichtigten Einfluß räumlich oder funktionsmäßig getrennter Komponenten.
- "Kommandofehler" ist ein Ausfall durch Fehlbedienung.

Die Aufstellung eines Fehlerbaums kann durch ein Rechnerprogramm erfolgen.

1. Es gibt ein Rechnerprogramm (G. Volta, Joint Res. Center, Euratom, Ispra), welches eine Automatisierung des Übergangs von AFAE (FMEA) zur Konstruktion eines Fehlerbaums ermöglicht /20/. Eine Prüfung dieses Verfahrens ist zu empfehlen.

2. J.B. Fussel (Aerojet Nuclear Company) /21/ berichtet über ein "Synthetic Tree Model", welches ein formelles Vorgehen zum Aufbau des Fehlerbaums angibt. Dies ist eine Methode, die für elektrische Netzwerke entwickelt wurde, jedoch auch "open ended" ist, um eine Ausdehnung auf andere Systeme zu erlauben. Eine solche Anwendung fand bei den Untersuchungen der Gruppe von Rasmussen (MIT) statt /28/. Es wäre darum empfehlenswert, diese Methodologie auch für unsere Untersuchungen zu testen und evtl. aufzunehmen.

3. G.J. Powers (MIT) /32/ stellt eine Prozedur dar, welche automatisch Fehlerbäume aufbaut. Dabei wird Information benötigt über
   - das System (als Flußdiagramm)
   - physikalische und chemische Materialeigenschaften im System und in der Umgebung, sowie über
   - Modelle welche das Komponentenverhalten beschreiben.

(iii) AUSWERTUNG DES FEHLERBAUMS

Analytische Auswertung (Abb. VI.1)

Das System sei durch einen Fehlerbaum repräsentiert, der aus Komponenten und

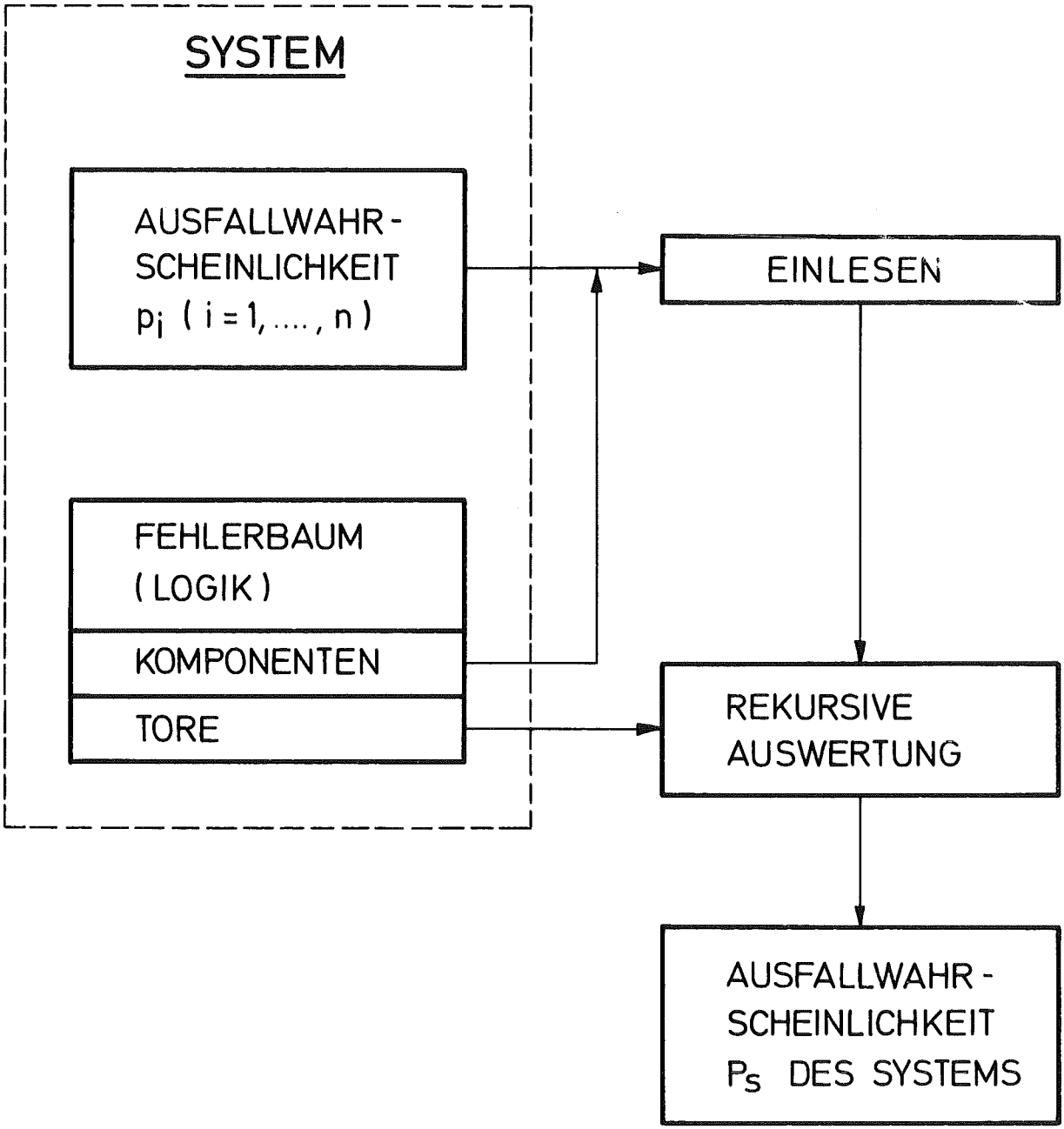

Abb.VI.1 ANALYTISCHE AUSWERTUNG

Toren besteht. Allen Komponenten sei eine Ausfallwahrscheinlichkeit zugeordnet. Dieses System wird grundsätzlich nach dem in Abb. VI.1 gezeigten Flußdiagramm ausgewertet.

a) Nichtreparierbare Komponenten
   Die "Rekursive Auswertung" sucht alle kleinsten Pfade (Ausfallarten des Systems, Critical Paths, (Colombo, Volta /20/))und berechnet dann die Ausfallwahrscheinlichkeit.

b) Reparierbare Komponenten /36/
   Die "Rekursive Auswertung" sucht alle kleinsten Pfade und berechnet rekursiv die erwartete Anzahl der Ausfälle des Systems. Daraus kann die Ausfallwahrscheinlichkeit abgeschätzt werden (Murchland, Weber /12/). Die Nichtverfügbarkeit zu einem gegebenen Zeitpunkt t kann dagegen exakt berechnet werden. Sie ist, im Gegensatz zur Ausfallwahrscheinlichkeit bzw. erwarteten Anzahl der Ausfälle, nicht direkt für eine Risikoabschätzung verwendbar.

Simulationsmethode zur Auswertung (Abb. VI.2)

Das System sei durch einen Fehlerbaum repräsentiert, der aus Komponenten und Toren besteht. Allen Komponenten sei eine mittlere Lebensdauer zugeordnet. Dieses System wird grundsätzlich nach dem in Abb. VI.2 gezeigten Flußdiagramm ausgewertet.

a) Nichtreparierbare Komponenten
   Bei jedem Simulationsspiel werden die Komponenten abgefragt, ob sie ausgefallen sind. Aus dem Fehlerbaum ergibt sich, ob eine Anzahl von ausgefallenen Komponenten zum Systemausfall führt. Die relative Häufigkeit der Systemausfälle ist ein Schätzwert für die Systemausfallwahrscheinlichkeit /12/.

b) Reparierbare Komponenten /36/
   Bei Reparatur werden die zeitlichen Koinzidenzen von Komponentenausfällen

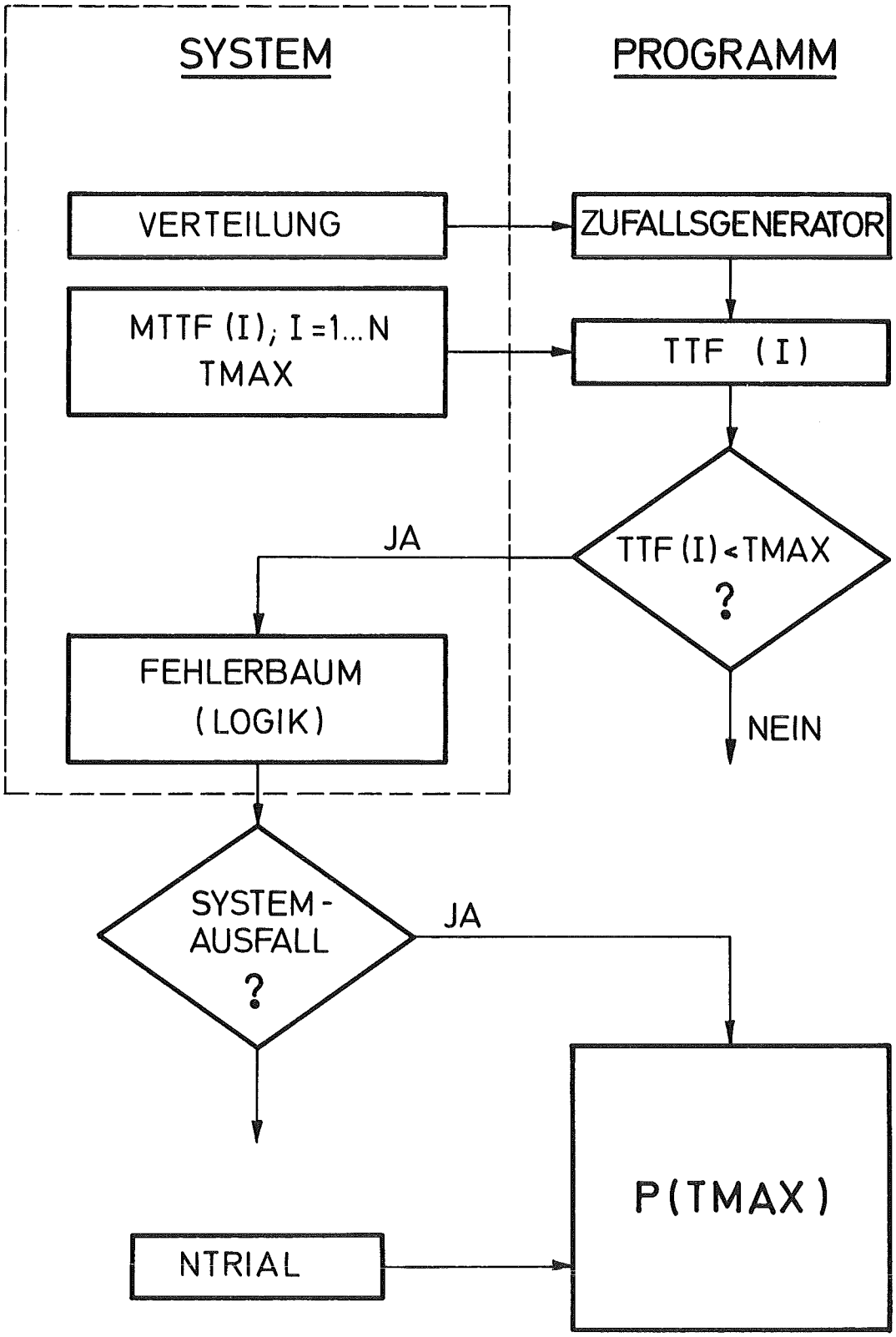

Abb. VI.2 SIMULATION

gesucht. Aus dem Fehlerbaum ergibt sich, ob diese Koinzidenzen zum Systemausfall führen.

c) Es ist auch möglich,

- Maintenance (Wartung) /21, 22/
- Standby /21, 22/ und
- Ausfälle auf Anforderung einzubeziehen (Rosenhauer /22/).

d) Einige Typen von statistischer Abhängigkeit können ebenfalls berücksichtigt werden (Heuser, Weber /12/).

Literaturverzeichnis:

Siehe Kapitel II.

VII. RELIABILITY DATA AND DATA BANKS

Numerical values assigned to the failure rates of basic component failures in a fault tree may be incorrect. This may be a very important source of error in fault tree analysis.

A component may have several failure modes. With reference to a specific failure mode, the failure rate "h" is in general a function of the time, and usually looks like the "bathub curve" of Fig. VII.1.

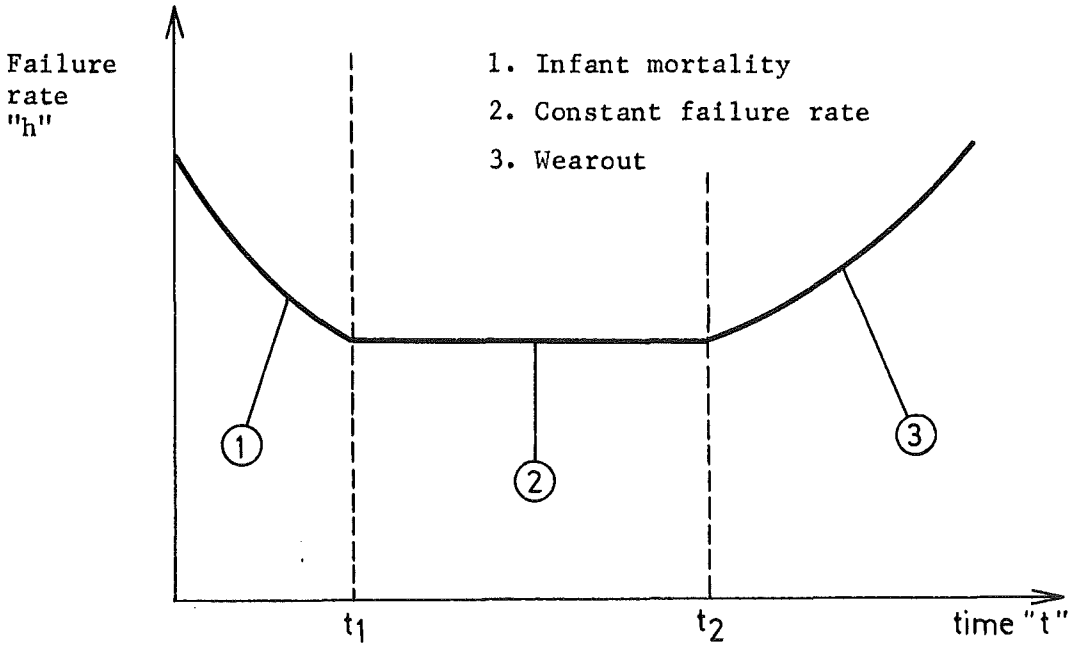

Fig. VII.1: Component failure rate as a function of time

Part 1 of the curve in Fig. VII.1 describes the infant mortality. The duration of this phase is relatively short. This phase is usually not incorporated in the fault tree analysis, because components are subjected to a burn-in period prior to installation.

Part 2 is the phase of "constant failure rate". Here the worsening of the device characteristics (due to the degradation processes taking place during operation) have not yet become significant, and failures are mainly due to the random changes of the enviromental stresses and/or of the loads applied to the device.

During phase 3 (wearout) components become increasingly weaker, so that the failure rate increases with time.

It must be noted that the curve of Fig. 1 depends upon the environmental conditions. In today's fault tree analysis an average failure rate "$\bar{h}$" is used, which is calculated as follows

$$\bar{h} = \frac{1}{\text{meantime to failure}} = \frac{1}{\int_0^\infty e^{-\int_0^t h(t')dt'} dt} \qquad (1)$$

It can be easily demonstrated that the above assumption is conservative, provided that the infant mortality phase has been previously eliminated by means of a burn-in period prior to installation. The reason for applying eq. 1 is due to the fact that many data **are needed, in order to precisely evaluate** the failure rate "h" for low values of "t", and usually only few data are available.
The failure rate may be obtained experimentally just by means of lifetests as for example in the case of electronic components. In the case of large and costly units (for instance "pressure vessels") this procedure is of course impossible, and failure rates must be evaluated theoretically starting from experimental data obtained from tests carried out on specimens made of the same material as the large unit and on small scale test models. The effect of periodic testing and inspection during operation must be included in the models.

Bayesian methods to combine " a priori" theoretical knowledge with that coming from the operating experience may be of thelp in the evaluation of failure rate of large units /1/. Data about the operating history of the devices and about lifetests results are being collected and stored in "data banks", where they can also be processed to produce failure rates. There are many "reliability data banks" in the world /2/. Here it is worthwhile to mention two banks which are probably at the moment the most important. They are the "FARADA" bank in the USA /3, 4/ and the S.R.S. bank in the UK /5, 6/.

However only the SRS data bank collects data of components used in nuclear industry. Recently a new large data bank is being organized in the USA by the Southwest Research Institute in San Antonio Texas. This bank is specialized in data of components used in nuclear industry. Failure rates evaluation is based on lifetests results and/or on data coming from previous operating experience. Often these data are few in number, or refer to operating conditions different from those of the considered case, or even do not exist at all. However, failure data is available for most components. The major exception is the pressure vessel. There is no hard data from which to infer the probability of pressure vessel failure. It is believed /7/ that the failure rate of a pressure vessel is of the order of 10^{-6}/year. Kellermann /8/ extrapolates failure data for nuclear pressure vessels from similar vessels of the chemical industry and of the "Hochdrucktrommeln von Wasserrohrkesseln" which are in operation in West Germany and which are under control of the T.Ü.V. A comprehensive report on the integrity of reactor vessels for light-water power reactors has been issued in England /9/ and very recently in the USA /10/.

In most cases where objective failure rate data are available, constant failure rates are assumed. In a few instances, sufficient data are available to construct a "bathub" curve" of the type shown in Fig.VII.1. Data collected in today's banks may therefore already allow risk evaluations.

Today's banks are still very primitive. From the collected data it is often very difficult to separate the various failure modes. Data belonging to any type of device used in any industrial branch are being collected and stored in these banks. However for each device only relatively few data are being collected, so that predictions are still inaccurate. In order to improve the situation, more data should be collected by using more reliable methods of collection, and these data should be analysed in a more sophysticated way. Future banks should be perhaps more specialized. Each bank should deal with a lower number of device types, and therefore be able to collect more data about each type. In addition data should be analysed by using correct theoretical models (Refs /11/,/12/ and /13/.In Ref./14/ the author shows that the behaviour of a device functioning in a given environment can be described by a quantity "Z" called "margin of strength". The time of failure is the minimum real and positive root of the stochastic equation

$$Z(t) = 0 \qquad (2)$$

Z (t) is a function of the stresses and loads applied to the device. The reliability R (t) is defined as follows

$$R(t) = \text{Prob}\ \{\ Z \geq 0 \text{ during the whole time interval until "t"}\ \} \qquad (3)$$

where "Prob" means probability.

Analysis of data should not be just limited to the evaluation of the failure rate. One should go further, and should try to evaluate the margin of strength by making use of properly chosen theoretical models, which describe the physics of the failure. In other words statistical methods should be combined with deterministic methods, to acquire the maximum possible knowledge about device failures.

The advantages of this methodology are the following

1. It is easier to extrapolate results from the know behaviour of a device under given operating conditions to predict the still unknown behaviour of the same device under different operating conditions. This is very useful especially in the analysis of accelerated tests.

2. The tails of the probability density distributions can be more precisely evaluated. A very good example is given by Volta in Ref./15/.Experimental data were fitted with arbitrary distributions. They seemed all good, but they gave very different results at the tails, and the tails are important for reliability calculations. Distributions based on physical models of failure allow us to evaluate the tails, when only few data are available.

3. Failure rates of devices subject to preventative maintenance can be more precisely evaluated. A more sophisticated (and therefore more reliable) type of preventative maintenance (as shown by the author in Ref./14/) can be also used.

In addition correct theoretical models are necessarily needed in all case in which an extensive testing of similar components is impossible or too expensive (for instance: pressure vessels).

In order to acquire high levels of knowledge about device failures, improvements are needed in the areas of collecting and handling the data. Information must be handled with a formal and universal language; it must be precise, complete and the access to it must be easy. The knowledge of the manufacturer and that of the user must merge together through an integrated learning process. This process requires the complete exchange of information between the manufacturer of a given device and the user. A suggestion in this direction is made in Chapter VIII and /16/.

References

/1/ Cornell "Bayesian Statistical Decision Theory and Reliability-Based Design" International Conference on Structural Safety and Reliability, Washington D.C., (April 1969), Pergamon Press 1972

/2/ Seminar on Reliability Data Banks (Stockholm, Oct. 73) FTLA-Report, A 16: 41, (Nov. 1973)

/3/ Richards and Dahl "The New Approache to Reliability Data Exchange" NATO Conference on Reliability Testing and Reliability Evaluation, The Hague, (Sept. 1972)

/4/ Richards "Technology Transfer through GIDEP" Annual Reliability and Maintainability Symposium of the IEEE, Los Angeles, (January 1974)

/5/ Ablitt "An Introduction of the Syrel Reliability Data Bank" SRS/GR/14

/6/ Fothergill "The Analysis and Presentation of Derived Reliability Data from a Computerized Data Store" Seminar on Reliability Data Banks, Stockholm, (October 1973), FTLA-Report, A 16: 41, (Nov. 1973)

/7/ "Results of Interviews with Proponents and Opponents of Nuclear Power in the USA" Report of the Company "Bedaux-Mathematica" (December 1973),(priv. comm.)

/8/ Kellermann "Unfallanalyse in der Kerntechnik" TU Bd. 13 (1972) Nr. 11, S. 330/335

/9/ O'Neil, Jordan "Safety and Reliability Requirements for Periodic Inspections of Pressure Vessels in the Nuclear Industry" I Mech E (1970)

/10/ "Report on the Integrity of Reactor Vessels for Light-Water-Power Reactors". WASH-1285, (January 1974)

/11/ Freudenthal "Intorductory Remarks to the International Conference on Structural Safety and Reliability". Washington, D.C., (April 1969) - Pergamon Press 1972

/12/ Gnedenko, Belajajew, Solowjew - Mathematische Methoden der Zuverlässigkeitstheorie II", Akademie Verlag, Berlin 1968 (Kap. 5)

/13/ Wilson "Estimating Pipe Reliability by the Distribution of Time to Damage Method" GEAP 10452, (March 1972)

/14/ Caldarola, L. "New Definition of Reliability, Continuous Lifetime Prediction and Learning Process", NATO-Confer. Liverpool, (July 1973), KFK 1847

/15/ Volta et.al. "Cumulative Damage Stochastic Models and Distribution of Strength of Steels and Graphite", NATO-Conference on Reliability Data Banks - Stockholm, (October 1973), FTLA-Report, A 16: 41, (Nov. 1973)

/16/ Caldarola, "Considerations for a European Centralized Reliability Data Bank System", International Seminar on Reliability Data Banks-Stockholm, October 1973, FTLA-Report, A 16: 41, (Nov. 1973)

VIII. CONSIDERATIONS FOR A CENTRALIZED RELIABILITY DATA BANK SYSTEM (C.R.D.B.S)

A centralized reliability data bank system (Ref. 3) would have the great advantage of easing the exchange of information because of the full standardization of definitions, terminologies and of the methods of collecting, handling and processing the data. In addition, circulation of false information would certainly be reduced, if not completely eliminated.

Fig.VIII.1 shows a tentative schematic block diagram for a "Centralized Reliability Data Bank System (C.R.D.B.S.)" (Ref. 3). Manufactures, users, banks and laboratories are all indicated by means of boxes. They will be called simply "units". A manufacturer may be a firm which produces valves or pumps or electric motors, and a user may be an airline company or an electricity producer, which uses these components. The information accumulated during the past about a given component is stored in the data banks. Components can be analyzed and tested in the laboratories. Tests can also be lifetests. Banks, manufacturers, laboratories and users can be connected in any possible wanted combination through the "Coordination and Synthesis Center" (C.S.C.). A typical connection (in the case of replaceables devices) is that shown in Fig.VIII.2, which allows for a fully integrated learning process. Solid lines in Fig.VIII.2 indicate flow of materials, while the dotted lines indicate flow of information. The C.S.C. has not been shown in Fig.VIII.2. Let us now examine how the diagram of Fig. VIII.2 functions.

The manufacturer "A" gives a sample of new devices (for example "valves") to the laboratory where lifetests are carried out. The information gained from these tests, together with that coming from

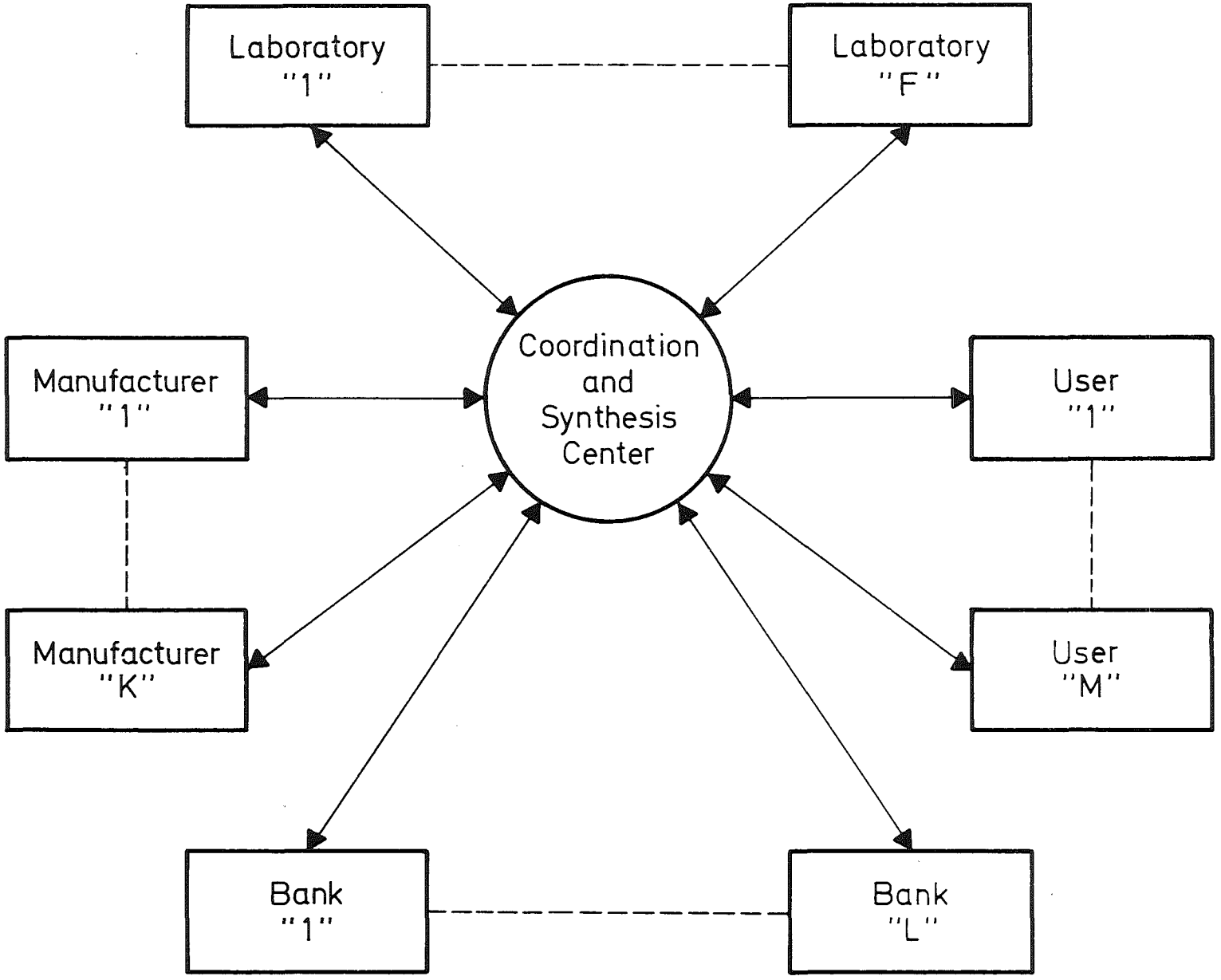

Fig. VIII.1 Schematic Block Diagram for a "Centralized Reliability Data Bank System" (C.R.D.B.S)

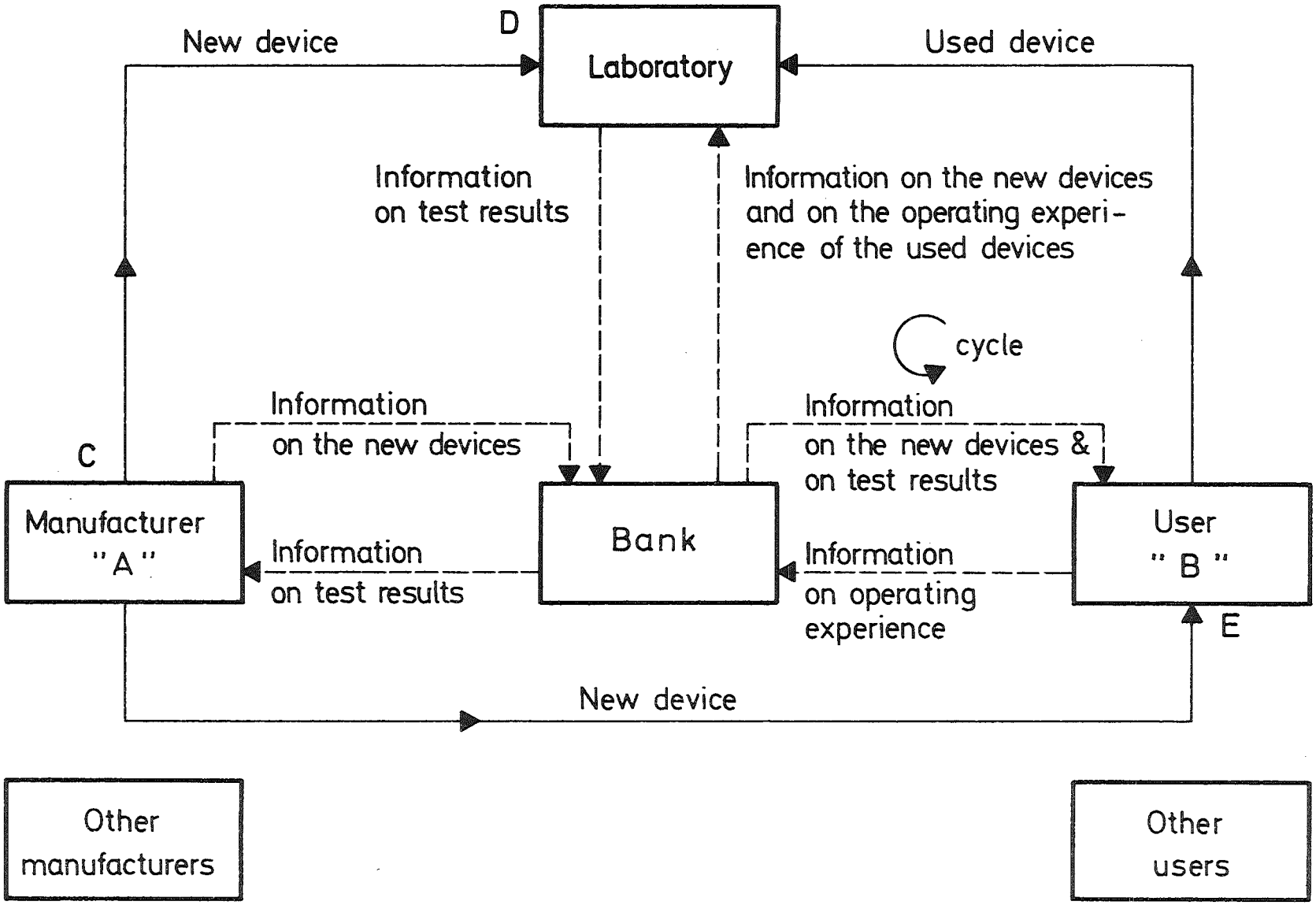

Fig. VIII.2 Schematic Diagram of an Integrated Learning Process.
The Case of replaceable Devices

the manufacturer, is stored in the "Bank" where it 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 determined by the desired level of reliability and then replaces the device with a new one (preventative maintenance). 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 lifetest on 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. Failed devices may also be given to the laboratory to better analyze causes of failure. The information stored in the bank is available to the laboratory, to A and to B.

With the scheme of Fig. VIII.2 only a limited number of new devices must be sacrificed initially in order to get an initial amount of knowledge about the characteristics of the device. Later, further testing of new devices is not needed, since used devices will be tested instead. The integrated learning process of Fig. VIII.2 has the form of a cycle. The cycle begins when the new devices enter the cycle at "E", where they start to be operated by the user, and it ends when the information gained from the lifetests, carried out in the laboratory on the same devices (now called "used devices"), reaches the user through the bank. Based on the information in the bank, the user will revise the operating time of other new devices arriving at "E". This starts a new cycle, characterized by a higher level of knowledge. This process can be repeated continuously and indefinitely.

A second path is possible, in which the user is by-passed, (path CD) and where the new devices are given directly to the laboratory. This path will be used especially at the beginning to obtain initial information. If we neglect the initial period in which only the new devices are tested, the rate of increase of knowledge will be a function of the flow N/T of the devices in the cycle, where "N" is the

number of devices which are present in the cycle at a given time, and "T" is the amount of time a device resides in the cycle, including the operating time. Since lifetests will be accelerated, the longer the operating time, the longer T. At the beginning, the degree of knowledge is low and therefore the incentive to know more about the device is very high. On the other hand, since the properties of the device are not well known and since the user is bound to operate the device with a preestablished degree of reliability, he will tend to operate the device for a shorter time. This produces a high rate of increase of knowledge. The level of knowledge will increase and this in turn will produce a longer operating time. The higher the level of knowledge, the longer the operating time, and therefore the lower the rate of increase of knowledge. When the knowledge has reached a very high level, the operating time will be long and the rate of increase of knowledge will be low. The incentive to know more about the device's properties is decreased, because a high level of knowledge has already been reached. The above discussion gives an idea of the dynamics of the process, when the degree of reliability imposed on the user is the only criterion which is used to decide the length of the operating time.

But one can also think of other strategies. For example it may be economically more convenient to artificially reduce the operating time at the beginning in order to reach a given level of knowledge faster. An extreme case is the path CD (Fig. VIII.2), where the operating time is zero. The loss due to a shorter operating time at the beginning must be counterbalanced by increased operation over a longer period of time.

Fig. VIII.3 shows various paths of a learning process by giving the allowed operating time of a device as a function of the time. A path 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

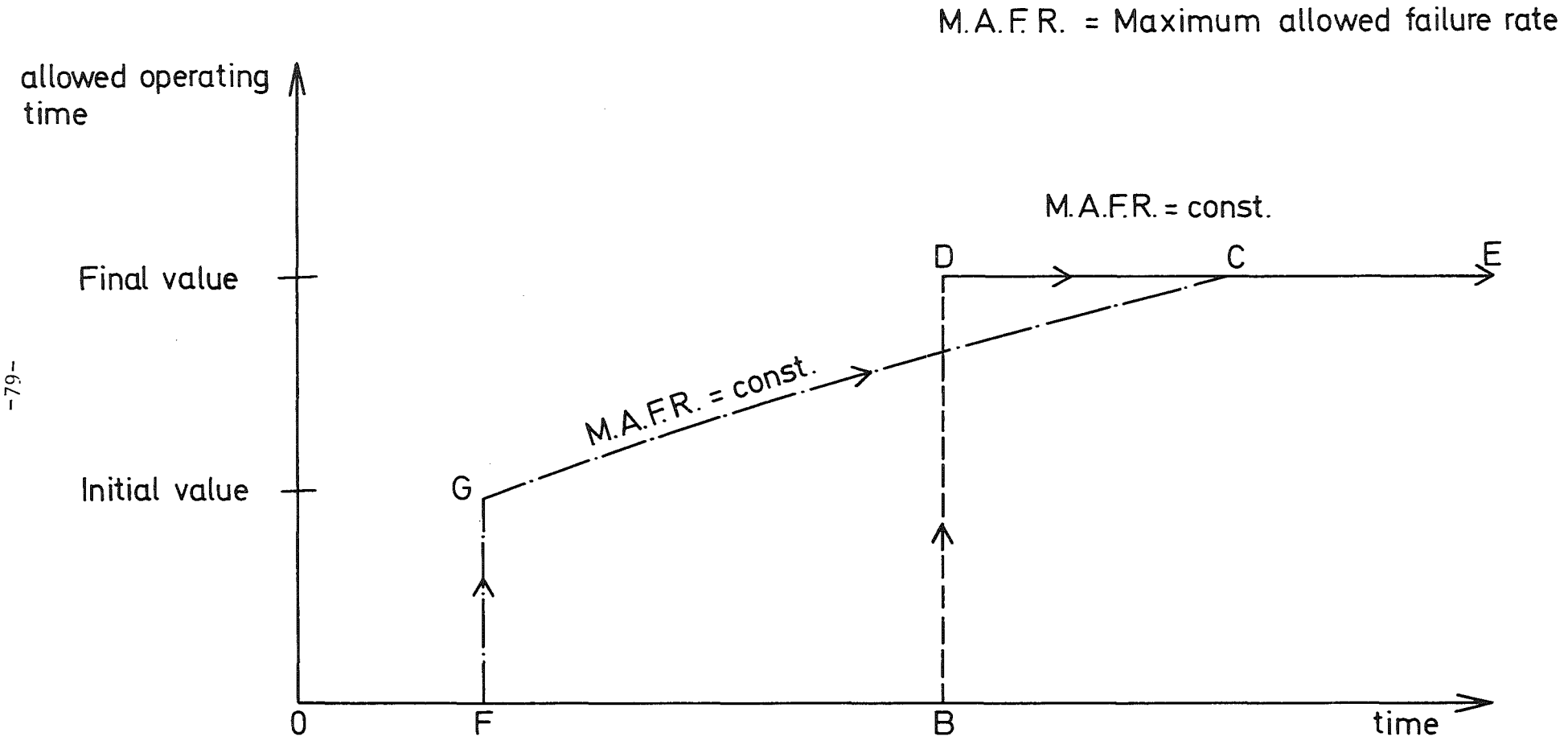

Fig. VIII.3 Various Paths of a Learning Process

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, which may dictated to the user by safety regulations or by economical considerations. This would correspond in Fig.VIII.2 to the case in which only the path CD is used. This learning process is very safe, but it may also be very expensive. If instead, one makes use of the path CD (Fig.VIII.2) only at the beginning to acquire an initial knowledge and then takes advantage of the cycle by making lifetests on the used devices, one would get a path in Fig.VIII.2 of the type OFGCE. New devices will be tested (path CD in Fig.VIII.2) 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.VIII.3) because of the knowledge continuously gained by means of the lifetests on the used devices (cycle in Fig.VIII.2).

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. The "integrated learning process" of Fig.VIII.2 provides also a means to quickly diagnose devices that need improvement, and provides useful information for their redesign.

The decision wether or not a new type of device can be introduced in the market will be made easier. Knowledge about its properties will be lower than that of other types of devices which have been

on the market for a long time. Only if the properties of the new type of device are decisively better and if its costs is decisively lower, will it be possible to overcome the initial disadvantage of the lower level of knowledge.

The schematic diagram of Fig.VIII.2 does not represent by any means the only possible type of connection among the various units of the C.R.D.B.S., but only one of the its most appealing features. Situations may also arise in which laboratory tests on used devices are not feasible, or economically not convenient, or in which devices are allowed to fail during operation. Another function of the C.S.C. is that of promoting the exchange of information among the various units of Fig.VIII.1, so that, for example, sets of data stored in two or more banks can be processed in order to produce new results, which synthesize the information contained in the old sets.

"Integrated learning processes" can also be organized in which may manufacturers, users, banks and laboratories are involved.

Information must be handled with a formal and universal language; it must be precise, complete, and the access to it must be easy and free (as much as possible).

Free access to the information is of course the ideal objective to be achieved. There are however serious difficulties in pursuing this goal. A manufacturer is reluctant to release information about its own products to its competitors, because of the commercial value of it. On the other hand it is evident that all manufacturers of a given device would benefit from the exchange of information, because this would accelerate the learning process and would certainly reduce its costs. A compromise must be found. People must learn how to attribute a value to a given information, in order to be able to sell and buy it quickly through a centralized reliability data bank system. Modern technology provides means which can allow a fast and effective exchange of infor-

mation. This is economically possible also because in the field of computers, the cost per bit is expected to fall by a factor 1000 in the next decade (Ref. 4). The main delays come now from the calculation of the commercial value of the information, on which the two contracting parties must agree, before they can exchange this information.

An independent and impartial national or international organization should have some kind of control on the information flowing in the network of Fig.VIII.1,so that there can be a sufficient guarantee for everybody that the information is produced, handled, and processed in an impartial manner.

This guarantee is necessary for the "public acceptance" of the risks associated with the use of advanced technological systems. The input data to risk analysis comes from the banks, and public opinion would become very suspicious if the control of the information is completely left in the hands of profit making private enterprises.

References

/1/ Fussel
Synthetic Tree Model - A Formal Methodology for Fault Tree Construction
Aerojet Nuclear Company, National Reactor Testing Station, Idaho Falls, ANCR 1098, (March 1973)

/2/ Powers and Tompkins
Fault Tree Synthesis for Chemical Processes
AI ChE Journal Vol. 20, p. 376-387, (March 1974)

/3/ Caldarola, L.
Considerations for a European Centralized Reliability Data Bank System
KFK-1928, (October 1973)

/4/ Perlis, A.
Computers
1973, Britannica Yearbook of Science and the Future

/5/ Turban, Efraim and Metersky
Utility Theory Applied to Multivariable Systems Effectiveness Evaluation
Management Science 17, p. 818-828 (1971)

/6/ Mc Grath, Papp, Maxim and Cook
A New Concept in Risk Analysis of Nuclear Facilities
(in preparation)

/7/ Caldarola, L.
New Definition of Reliability, Continuous Lifetime Prediction and Learning Processes
KFK-1847, (July 1973)

IX. COMMON - MODE - FAILURES

Contents

Foreword

This paper is mainly based on the author's work (Ref. 49), on the Gangloff and Loftus work (WCAP 7706-Ref. 46) and on the Ph. thesis of Dr. Wiliams at the University of Tennessee (Ref. 44). Some parts of the above mentioned publications have been reproduced in this paper in their original form or with some small changes.

1. Definitions and statement of the problem

Quantitative probability analysis of reactor systems relies upon the assumptions that basic component faults are independent. Basic component faults are input faults to a fault tree and (according to Ref. 47) are indicated in a fault tree diagram by means of a circle.

Much work has been done using this hypothesis to demonstrate that today's reactors are quite safe and quite reliable. Fault tree studies are used as a part of this analysis to depict in diagramatic form all possible outcomes or consequences of a particular occurrence; the events are traced through a logic diagram until all outcomes are identified. However the hypothesis that basic component failures are independent does not always apply. Cases may arise in which basic component failures are not independent. This type of failure is usually called "common mode failure".

The definition of "common mode failure" is a very intriguing matter. No clear and universally accepted definition seems to exist in the literature. People usually refer to"common mode failure" as that type of failure which cannot be cured just by means of redundancy alone (Definition 1). In Ref. 9 common mode failure is introduced as follows. "The failure of all members of a group in a single environment is a recognized possibility in industry where officers of a corporation are discouraged from riding as a group in a single aeroplane. Similarly, attorneys often advise their clients to provide in their wills for the possibility of both husband and wife being killed in a single accident; this, in legal circles, is known as the "common disaster". It would be expected that, when any group is made up of identical elements, all in the group would respond similarly to an externally applied stimulus; and, if the failure resulted, this would be a common mode failure. When identical elements are used in a protection system, they are subject to simultaneous failure as a result of a single event. Garrick, Gekler, and Pomrehn (Ref. 48) have pointed out the susceptibiltiy of separate but identical circuits all containing the same built-in design error."

In Ref. 44 the following definition is given. "Common mode failure, briefly, is the failure of all redundant components of a system or failure of the entire system because of a single event". (Definition 2)

In the author's opinion this definition is at the same time too restrictive and not precise. It is too restrictive because it refers only to the redundant components of a system, and not precise because it may lead to the erroneous conclusion that common mode failures are necessarily simultaneous. The following definition is suggested by the author. "Common mode failures are component failures which are not independent". (Definition 3)

This means that the simple rule of multiplication of probabilities (used for the basic failures in a fault tree) is not valid in the case of common mode failures. Another definition (equivalent to No. 3) may be the following. "Common mode failures are component failures due to causes or processes which are correlated". (Definition 4)

A particular case of common mode failure is that in which the cause or the process is the same. Components which fail due to causes or processes which are correlated may fail either simultaneously or in a more or less rapid succession.

"Common mode failure will be considered instantaneous when it occurs in a time interval smaller than that required for discovering it and taking the necessary measures to cope with it." It must be pointed out that dependence of failures (when recognized) in most of the cases can be taken into account in the fault tree diagrams. It is usually a matter of complexity and of drawing the tree in an appropriate manner. However the basic component faults are explicitly supposed to be independent, so that either they are really independent or their dependence is neglected. Common mode failure can be defined by making use of the mathematical theory developed by the author in Ref. 49.

In Ref. 49 it is shown that a stochastic equation can be associated to a device functioning in a given environment

$$Z(t) = Y - L(t) - X(t) = 0 \qquad (1)$$

where

$Z(t)$ = margin of strength

Y = initial strength (independent upon time)

$L(t)$ = permanent loss of strenght (due to the degradation process taking place in the device and dependent upon the environmental stresses)

$X(t)$ = effective load (or effective reference)

t = time

The time of failure is the minimum real and positive root of eq. 1.

The reliability "R(t)" is defined as follows

$$R(t) = \text{Prob}\ \{\ Z \geq 0 \text{ during the whole time interval up to "t"}\ \} \qquad (2)$$

Let us now consider two devices characterized by two margins of strength: $Z_1(t)$ and $Z_2(t)$. If the two stochastic variables $Z_1(t)$ and $Z_2(t)$ are independent, the probability $R_{1;2}(t)$ that both are not yet failed at time "t" is simply given by

$$R_{1;2}(t) = \text{Prob}\ \{Z_1 \geq 0 \text{ and } Z_2 \geq 0 \text{ during the whole time interval up to "t"}\}$$

$$= R_1(t) \cdot R_2(t) \qquad (3)$$

where $R_1(t)$ and $R_2(t)$ are defined by eq. 2 respectively with $Z_1(t)$ and $Z_2(t)$.

If instead $Z_1(t)$ and $Z_2(t)$ are not independent, we shall have (common mode failure)

$$R_{1;2}(t) \neq R_1(t) \cdot R_2(t) \qquad (4)$$

The above considerations allow us to give a definition of common mode failure in terms of margin of strength.

"Common mode failures are component failures chaacterized by margins of strength which are correlated". This definition (Definition 5) is equivalent to 3 and 4. From the above discussion it may be concluded that "common mode failures" are the same as dependent failures. If this is the case, one would not see the reason why one should use two different expressions to indicate the same thing. This may lead to confusion. If instead "common mode failure" is only a subclass of dependent failures, then one should define exactly this subclass. Somebody has suggested to the author to add the attribute "basic" to the word "failures" in the definitions 3; 4 and 5. In this case "common mode failure" would have not an absolute meaning because it would refer to a particular diagramatic form of the fault tree describing the case taken into consideration. Other people have suggested to the author to refer in the above definitions 3, 4 and 5 to"dependent failures which have been neglected in the fault tree purposely or because they have not yet been recognized as such". Here again "common mode failure" would not have an absolute meaning, and in addition it does not seem logical to define what is still unknown.

In attempting to make general statements concerning the "state of the art" of common mode failure, many problems arise: an universally accepted and exact definition does not exist yet; analytic procedures have not advanced very far; very little data is available because of the few years of power reactor experience available to the public; data concerning actual failures are buried in the literature or not in the public literature at all; the various organizations involved in reactor design, regulation and operation cannot agree on suitable criteria and standards; some of the information is believed to be proprietary in nature and therefore not available for public discussion; and some organizations state that their opinion is that such failures are incredible.

Detailed criteria and standards governing common mode failure are seen therefore to be in a state of dispute and change.

Since quantitative analysis is not possible, at least at present, common mode failure cannot be dismissed on this basis either. One possible way to approach this, since analytic procedures are not available, would be to accumulate data on actual failures and to categorize them as it will be shown in the next section.

Moore and Hanauer have suggested such an approach on a worldwide basis so that many more reactor years of operation would be available (Ref. 11). The administrative details of such a plan are difficult to visualize but such a system already exists to some extent in the U.S.A. because of the requirement that significant events happening at reactors be reported to the AEC.

2. Categorization of common mode failures

Common mode failures can be classified by referring to the causes and to the means of prevention.

2.1 Common-mode causative factors

Four major categories of causative factors can be identified by making use of the work developed in Refs.44 and 46.

A. Deficiency
B. Human
C. Environment
D. Unknown

A. Cause A (Deficiency) includes both functional and design deficiencies. Since valuable information is lost when functional and design hardware deficiencies are combined, one must try to keep them separate. However, in many cases it is impossible to distinguish between the two, so they must necessarily be combined into one category.

A.1 Functional deficiency occurs when a system works as designed but the functional design was inadequate for the task or purpose at hand; this could be caused for example by the inability of the designer to accurately predict the behavior of some variable, or by the erroneous prediction of the ability or usefulness of some protective action, or by the use of inappropriate instrumentation.

A.2 Design deficiency includes failures in which the installed equipment does not meet the functional requirements; this could be caused for example by unrecognized dependence upon a common element, a common deficiency in all redundant components or interdependence among redundant components or subsystems.

B. Cause B (Human) includes all common mode failures that can be identified as being caused by human error other than design; operator error, mistakes in installation and maintenance, faulty administrative procedures etc.

C. Cause C (Environment) includes both external normal environment and external catastrophe.

C.1 External normal environment takes into account environmental factors such as dust, dirt, temperature, humidity, vibration etc.

C.2 External catastrophe includes catastrophic causes such as fire, earthquake, tornado, flood etc.

D. Cause D (Unknown) can be added for the cases in which no apparent cause can be found.

2.2 Common-mode failure preventive measures

Simple redundancy does not provide significant defense against the common-mode failure unless coupled with other techniques. To prevent the occurence of such failure, it is necessary to employ other measures such as those classified in the following main five categories of section 2.2 which have been taken from Ref. 46.

A. Diversity
B. Administrative controls
C. Safe failure modes
D. Physical separation
E. Proven design and standardization

A. Diversity There are two types: functional diversity and equipment diversity.

A.1 Functional diversity consists in utilizing different plant variables to produce the same result. An example may be that of a safety system which scrams the reactor on the base of measurements of neutron flux and temperature. The adoption of functional diversity usually involves the use of different types of instrumentation (equipment diversity) which may be located in different places (physical separation) and which usually undergo different maintenance procedures (operational administrative controls). In conclusion "functional diversity" is the most effective method to combat common-mode failure, because it is usually accompanied by other measures such as equipment diversity, physical separation and operational administrative controls.

A.2 Equipment diversity

Equipment diversity, the use of multiple equipments differing in design and or manufacture to perform identical redundant functions, may afford some protection against the design dificiency or maintenance error types of common-mode failure. There is little experience available with the use of this technique to show that it is useful in reducing the occurence of common-mode failures. Some of the reasons why there have been no significant commercial applications of this technique include spare parts inventory problems, training complications, and multiple test procedures. Except where it arises as a logical consequence of the application of functional diversity, it is not clear that equipment diversity significantly reduces the likelihood of common-mode failure.

B. Administrative controls There are two types of controls: design administrative controls and operational administrative controls.

B.1 Design administrative controls

Administrative control during design, construction, and installation can be effective in reducing the probability of most classes of common-mode failure. Qualification testing, when combined with a sound quality control program, is useful against most of the environmental factors. Control of drawings and instructions can reduce the chances of maintenance errors.

Design review by independent engineers has been useful in locating and correcting design deficiencies and functional dificiencies. Such review takes place both as a formal engineering procedure internally and informally in the course of plant safety analyses, utility and architect engineer reviews, and licensing review. This type of preventive measure includes all the analyses done to verify that systems will respond adequately to various transient conditions, as well as the use of applicable standards and general design criteria in the design process.

B.2 Operational administrative controls

Administrative controls during the operation and maintenance of the plant are extremely important in preventing common-mode failures. These measures are probably the most important after the proper use of functional diversity. In the case of the operation and maintenance errors, they provide the only real assurance available.

Adminstrative controls start in nuclear plants with security systems to ensure that only authorized personnel have access to plant equipment. These authorized personnel are operational and maintenance people who are selected on the basis of experience and proven competence. Records are kepts on all maintenance actions, including routine operational tests.

Periodic testing of equipment is one of the most potent defenses against common mode failure. It is effective in eliminating many varieties of common-mode failure where a number of items fail from the same cause (and perhaps in the same manner) but not at the same time. If inspections can be made periodically or the system can be observed continuously, chances of such fault accumulation are greatly reduced.

Records of abnormal operating situations are kept and analyzed.

The collection of operating experience and implementation of the lessons to be learned from this experience can be very useful against common mode failure.Experience to date has shown that most common-mode failures are discovered in their incipient stages by alert operators or by routine periodic testing. Common deficiencies are thus found before they become common-mode failures. Careful study of such problems can reduce the chances that the same problem will be repeated many times in various degrees in several plants of similar design.

In short "operational administrative controls" are an interlocking system of checks and balances which operates for the purpose of preventing the type of conditions which can lead to common-mode failure.

C. Safe failure modes

It is often possible for a designer to recognize a common-mode failure cause and to develop the system design in such a way that the common-mode failure is in the direction of safety. This principle is utilized in the design of the Reactor Protection System to defeat perhaps the most likely of all common-mode causes, loss of power. All relays and circuit breakers in the trip logic and actuation circuits are used so as to perform their safety function on loss of power. By virtue of this design philosophy, many other potential common-mode failures are also eliminated. Obviously, a system cannot be made "fail-safe" in every regard, but wise use of safe failure modes can provide high resistance to unsafe common-mode failure without unduly affecting operational performance of the plant.

D. Physical separation

Physical separation, in conjunction with redundant channels, is a useful preventive measure for some types of common-mode failure. When combined with periodic operational testing, it offers a measure of defense except against the functional deficiency and those situations where the causative factor is both sudden in its onset and widespread in its effects.

Physical separation can be effective against some of the environmental factors by requiring a larger buildup of failures before defeating the system function. It also reduces the effects of very localized environmental problems such as heat and contamination in the vicinity of a piece of machinery or moisture in the air near an air conditioning or cooling unit.

Physical separation is at least one more in the system of checks and balances which minimizes failures of this sort.

Physical separation can be an important feature in trying to combat common-mode failure from external catastrophe. Localized fires are of less impact where redundant critical items are physically separate. Falling objects and flying missiles must be either larger or more numerous as a result of good separation. In short, physical separation is a design feature which can

increase the resistance of a system to many types of common-mode failure.

E. Proven design and standardization

Common-mode failures of the functional deficiency type may be introduced by the use of new or untried components in the design. This situation can be avoided where possible by use of standard components which are well understood from service in other applications. Where this is not possible, type test data or reasonable engineering extrapolation based on test data must be used to verify design adequacy of all components.

Standardization of design is another aid in suppression of common-mode failure. With standard design it should be necessary to learn lessons only once. Design deficiencies or functional deficiencies uncovered in one plant can be corrected before potential common-mode failure becomes actual failure. Standardization is a very powerful resource for both the designer and the reviewer as it brings to the attention of responsible and knowledgeable personnel any changes in system or equipment design and adds continuously to the depth of construction and operational experience.

Table 1 summarizes the possibilities of common-mode failure defense with the categories of causes related to the possible preventive measures.

TABLE 1 : COMMON-MODE FAILURE PREVENTIVE MEASURES

(from Ref. 46)

Causative Factors	Possible Preventive Measures
C.1 External Normal Environment	A.1 Functional Diversity B.1 Design Administrative Controls B.2 Operational Administrative Controls C. Safe Failure Modes E. Proven Design and Standardization A.2 Equipment Diversity
A.2 Design Deficiency	A.1 Functional Diversity D. Physical Separation B.1 Design Administrative Controls B.2 Operational Administrative Controls C. Safe Failure Modes
B. Human	A.1 Functional Diversity B.2 Operational Administrative Controls A.2 Equipment Diversity
C.2 External Catastrophe	A.1 Functional Diversity D. Physical Separation B.1 Design Administrative Controls C. Safe Failure Modes A.2 Equipment Diversity
A.1 Functional Deficiency	A.1 Functional Diversity B.1 Design Adminstrative Controls B.2 Operational Administrative Controls A.2 Equipment Diversity

3. Some numerical results and conclusions

The author of Ref. 44 has collected some data of the BWR and PWR reactors operating in the USA. The analysis was confined to the years 1969 and 1970, which implies a total operating time of 9.6 reactor years for the PWR type and 12.1 reactor years for the BWR type.

The author of Ref. 44 gets the following results

PWR	1.7	common mode failures/year
BWR	2.2	" " " "

If we now consider the total number of failures during the years 69 and 70, we see that common mode failures represent 17 % of the failures in the case of PWR and 25 % in the case of BWR. In average (PWR and BWR together) common mode failures were 21 % of the total number of failures in the years 69 and 70.

The main conclusions reached by the author of Ref. 44 are the following.

1. Common mode failure is a factor with which to be reckoned in power reactor.

2. Slightly over half of the common mode failures were caused by human error.

Otway (Ref. 45) accounts for common mode failures in his model by assuming that the probability of failure of a system, due to the failure or malfunction of another system, is equal to the probability of failure of the system as from internal failure of the system. This is an arbitrary assumption, which he claims to be conservative.

Mathematical methods to deal with "common-mode failures" are not yet available, so that, for the time being, work in this areas is limited to categorize the collected data, to take the necessary measures to prevent common mode failures to happen again when they are discovered, and to make sensitivity analysis of the type described in Ref. 45.

As far as future work is concerned, the author thinks the following:

1. People must agree on an universally accepted and exact definition of "common mode failure".

2. Categorization methods of "common mode failures" should be refined and applied (possibly) on a worldwide basis (as suggested in Ref. 11).

3. Sensitivity analysis of the type carried out by Otway (Ref. 45) may still remain the only practical quantitative method for a long time.

4. General mathematical methods are possible if one refers to the "margin of strength" of an operating device (as defined in section 1) instead than to the reliability of the device. However, the practical application of these methods may present serious computing difficulties.

4. References

1. E. Siddall, "Reliable Reactor Protection," Nucleonics 15 (6), June, 1957

2. E.P. Epler, "HTRE-3 Excursion," Nuclear Safety 1(2), December, 1959

3. E.P. Epler, "Dangers in Safety Systems," IRE Transactions on Nuclear Science, NS-8(4), October, 1961.

4. S.J. Ditto, "Redundancy and Coincidence in Reactor Safety Systems," Nuclear Safety 2 (4), June, 1961

5. E. Siddall, "Reliability of Reactor Control Systems," Nuclear Safety 4(4), June, 1963

6. S.J. Ditto, "Effect of Operating Experience on Safety-System Design," Nuclear Safety 6(2), Winter 1964-1965.

7. E.P. Epler, "Safety-System Reliability vs. Performance," Nuclear Safety 6(4), Summer, 1965

8. S.H. Hanauer, C.S. Walker, Design Principles of Reactor Protection Instrument Systems, USAEC Report ORNL-NSIC-51, September, 1968

9. E.P. Epler, "Common Mode Failure Considerations in the Design of Systems for Protection and Control," Nuclear Safety 10(1), January-February, 1969.

10. USAEC, Division of Reactor Licensing, Operating Experiences, Reactor Safety Bulletins.

11. V.A. Moore, Jr., S.H. Hanauer, "Status of Power Reactor Control and Instrumentation in the United States," First Meeting of the International Atomic Energy Angecy Working Group on Nuclear Power Plant Control, March 15-19, 1971.

12. R.L. Scott, Safety-Related Occurrences in Nuclear Facilities as Reported in 1969, USAEC Report ORNL-NSIC-87, August, 1971

13. R.L. Scott and W.R. Casto, Safety-Related Occurrences in Nuclear Facilities as Reported in 1969, USAEC Reprot ORNL-NSIC-87, August, 1971.

14. E.L. Crow, R.S. Gardner, "Confidence Intervals for the Expectation of a Poisson Variable," Biometrika, 46, 1959.

15. C.W. Zabel, Advisory Committee on Reactor Safeguards, to G.T. Seaborg, AEC, Docket 50-272, June 21, 1968. Available at USAEC Public Document Room.

16. T.W.T. Burnett, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors. Westinghouse Electric Corporation, April, 1969. (WCAP-7306).

17. L.G. Frederick, An Analysis of Functional Common-Mode Failures in GE BWR Protection and Control Instrumentation, General Electric Company, July, 1970 (NEDO-10189)

18. Systematic Failure Study of Reactor Protection Systems. Babcock and Wilcox Company, September, 1970. (BAW-10019).

19. W.C. Coppersmith, C.L. Kling, A.T. Shosler, B.M. Tashjian, Reactor Protection System Diversity, Combustion Engineering, Inc., February, 1971. (CENPD-11).

20. S.H. Hanauer, Advisory Committee on Reactor Safeguards, to G.T. Seaborg, AEC, Docket 50-321, May 15, 1969, Available at USAEC Public Document Room.

21. L.A. Michelotti, Analysis of Anticipated Transients without Scrams, General Electric Company, March, 1971. (NEDO-10349).

22. R. Salvatori, Manager, Licensing Engineering, Westinghouse Electric Corporation, to P.A. Morris, Director of Reactor Licensing, May 21, 1971. (E-L-215).

23. W.C. Gangloff, An Evaluation of Anticipated Operational Transients in Westinghouse Pressurized Water Reactors, Westinghouse Electric Corporation, May, 1971. (WCAP-7486).

24. Federal Register, 36(35), February 20, 1971.

25. Federal Register, 32(132), July 11, 1967

26. "Supplementary Criteria and Requirements for RDT Reactor Plant Protection Systems," Division of Reactor Development and Technology, United States Atomic Energy Commission, December, 1969. (RDT C 16-1T).

27. Commercial Nuclear Power Plants, Southern Nuclear Engineering, Inc. October, 1971.

28. "Criteria for Protection Systems for Nuclear Power Generating Stations," The Institute of Electrical and Electronics Engineers, Inc., 1971. (IEEE Standard 279).

29. S.H. Bush, Advisory Committee on Reactor Safeguards, to G.T. Seaborg, AEC, Dockets 50-352 and 50-353, August 10, 1971. Available at USAEC Public Document Room.

30. I.M. Jacobs, "Safety-System Design Technology," Nuclear Safety 6(3), Spring, 1965.

31. G.C. Laurence. "Reactor Safety in Canada," Nucleonics, 18(10), October, 1960.

32. F.R. Farmer, Letter to the Editor, Nuclear Safety 10(4), July-August, 1969

33. L. Cave, "Safety Evaluation Probability Method for GCR's," Nuclear Engineering 13 (149), October, 1968

34. Pacific Gas and Electric Company, Humbolt Bay Unit No. 3 Operations Report, Docket 50-133. February 19, 1969. Available at USAEC Public Document Room.

35. Allis-Chalmers, Linearity of Nuclear Instruments and Proposed Revised Control Mode, LAC-4130, Docket 115-4, August 1, 1969. Available at USAEC Public Document Room.

36. Dairyland Power Cooperative, to Division of Reactor Licensing (AEC), LACBWR Reactor Water-Level Instrumentation, Docket 115-5, April 7, 1970. Available at USAEC Public Document Room.

37. Pacific Gas and Electric Company to Division of Reactor Licensing (AEC), Forced Shutdown at Humbolt Bay Unit 3 and Level Indication Leak, Docket 50-133, October 2, 1970. Available at USAEC Public Document Room.

38. Consolidated Edison Company of New York, to Division of Compliance (AEC), Flux Flow Computer Causes Automatic Reactor Trips When Spurious Signals Occur, Docket 50-3 Indian Point 1, September 3, 1969. Available at USAEC Public Document Room.

39. G.R. Gallagher, "Failure of N Reactor Primary Scram System," Nuclear Safety 12(6), November-December, 1971.

40. General Electric Company, to Director of Reactor Licensing (AEC), Safety-System Relays, Docket 50-263 Monticello, July 29, 1970. Available at USAEC Public Document Room.

41. E.P. Epler, "The ORR Emergency Cooling Failure," Nuclear Safety 11(4), July-August, 1970.

42. "Guide to the Application of the Single Failure Criteria to Nuclear Power Generating Station Protection Systems (Draft Seven), IEEE Joint Committee on Nuclear Power Standards, April 19, 1971.

43. R.L. Scott, Jr., "A Review of Safety Related Occurrences in Nulcear Power Reactors From 1967-1970," USAEC report ORNL-TM-3435, May 26, 1971.

44. Wiliams "Common made failures in US commercial power reactors", Thesis, University of Tennessee, June 1972.

45. Otway and others "A risk estimated for an urban-sited reactor" Nuclear Technology, vol. 12, October 1971.

46. Gangloff and Loftus "An evaluation of solid state logic reactor protection in anticipated transients", Westinghouse Electric Corporation - WCAP 7706, July 1971

47. Fussel "Synthetic tree model. A formal methodology for fault tree construction", Aerojet Nuclear Company - ANCR 1098, March 1973

48. Garrick, Gegker and Pomrehn "Some aspects of protective systems in nuclear power plants", IEEE Trans. Nucl. Sci. NS-12 (16): 22-30 (December 1965)

49. Caldarola "New definition of reliability, continuous lifetime prediction and learning processes", Nato Conference on Reliability, Liverpool July 1973 and KFK 1847.

50. Gangloff "Probability Investigations into Anticipated Transients Without TRIP" ASME Winter Annual Meeting, Detroit, Michigan, USA, November 1973

51. Jacobs "The common made failure study discipline" IEEE Trans. on Nuclear Science, 17 (1) pages 594 - 598, February 1970

X. DAS MENSCHLICHE VERHALTEN IM RAHMEN DER RISIKOANALYSE VON KERNENERGIEANLAGEN

Tätigkeitsbereiche

Bei der Risikoanalyse von Kernenergieanlagen muß der Einfluß menschlichen Verhaltens in folgenden Bereichen betrachtet werden:

Beim Bau der Anlage:	Bei der Erstellung der Anlageteile und der Überprüfung ihrer Funktionsfähigkeit.
Beim Betrieb der Anlage:	Bei der Inbetriebnahme, im Normalbetrieb, beim Störfall

Die Arbeiten in diesen Bereichen haben folgende Charakteristiken gemeinsam:

Sie werden (mit Ausnahme mancher Störfallsituationen) nach genauen, vorher festgelegten Vorschriften durchgeführt. Die Einhaltung der Vorschriften wird im Rahmen des Möglichen überprüft, eine 100%ige Kontrolle ist jedoch nicht möglich. Fehlhandlungen erhöhen das Risiko und können unter Umständen nachträglich nicht mehr oder nur unter hohem Kostenaufwand revidiert werden.

Quantitative Risikoerfassung

Ausländische Arbeiten

Vorschläge für eine quantitative Erfassung des durch menschliches Verhalten induzierten Risikos in Kernenergieanlagen wurden in England von Ablitt und in den USA von SWAIN gemacht / 10, 11 /. Ablitt beschreibt die typische Problematik für Nullenergieanlagen, Testreaktoren und für Bestrahlungs- und Leistungsreaktoren. Er gibt Beispiele von Ereignisbäumen in die die menschliche Komponente mit ungefähren Zahlen für Fehlerwahrscheinlichkeiten eingebaut ist. Weiterhin schlägt er ein Testprogramm vor, durch das die Häufigkeitsverteilung bestimmter menschlicher Reaktionen und der Reaktionsgeschwindigkeiten beim Auftreten verschiedener Signale statistisch ermittelt werden kann.

Swain geht bei seinen Untersuchungen von anderen Arbeitsbereichen, hauptsächlich der Herstellung elektronischer Geräte und militärischen Aktivitäten aus. Er gibt statistisch belegte Fehlerraten für Produktionsschritte in der Elektronik an und weist darauf hin, daß eine Reduktion der Fehlerraten weniger durch erhöhte Motivierung der Beteiligten, sondern weit effektiver durch eine verbesserte Anpassung der Aufgabe und der Arbeitsplatzumgebung an menschliche Fähigkeiten erreicht werden kann. Als wesentliche Faktoren, die menschliche Handlungen beeinflussen, gibt er an:

Instruktionen (Bauanleitungen, Betriebsvorschriften, Weisungen etc.)
Art der Aufgabe
Arbeitssituation (Betriebsorganisation, Zuverlässigkeit der Hardware)
Psychologischer Stress (Arbeitsgeschwindigkeit, lange ereingislose Perioden, persönliches Risiko)
Körperlicher Stress (Müdigkeit, schlechte Luft, Mangel an Bewegung)
Persönliche Faktoren (Training, Geschicklichkeit, Intelligenz, Motivierung)

Er schlägt schließlich die Anlage einer Datenbank vor, in der all diese Faktoren und ihre Auswirkungen auf menschliche Fehlerraten möglichst quantitativ vorliegen sollen.

Auch in / 2 / bis / 4 / werden Methoden vorgeschlagen, mit denen Fehler- und Erfolgswahrscheinlichkeiten für zukünftige menschliche Tätigkeiten abgeschätzt werden können. In / 5 / wird eine Zusammenstellung der zahlreichen Beiträge der Sandia Laboratories zu diesem Gebiet gegeben.

Es sollte noch darauf hingewiesen werden, daß es sich bei den zitierten Arbeiten um Berichte aus nicht-nuklearen Arbeitsgebieten, um theoretische Studien oder um Vorschläge für praktische Maßnahmen in der Kernenergie handelt. Aus den vorliegenden Berichten geht jedoch nicht hervor, in wieweit solche Überlegungen Eingang in die Genehmigungsverfahren oder in die Bau- und Betriebspraxis gefunden haben.

Situation in Deutschland:

Eine echte quantitative Erfassung des Risikobeitrags menschlichen Verhaltens bei Kernenergieanlagen ist auch hier heute noch nicht gegeben - sie wird jedoch angestrebt. In einer neueren Veröffentlichung aus dem IRS / 1 / wird hierzu angegeben, daß Fehler in Folge Unkenntnis oder in Folge Fehleinschätzung menschlichen Verhaltens zur Zeit durch nahezu vollautomatische Auslegung des Schutzsystems, durch Redundanz sowie durch administrative Regelungen abgedeckt werden,

daß jedoch die Auslegungsgrundlagen hier noch keineswegs eine so feste Fügung haben, wie dies bei anderen Fehlern der Fall ist.
In einer anderen Arbeit des IRS wurden Vorschläge ausgearbeitet, wie menschliche Fehlerarten systematisch in eine umfassende Sicherheitsanalyse eingearbeitet werden können. Größtenteils auf Erfahrungen bei Boeing aufbauend, beschreibt H. Balfanz / 6 / Detailanalysen, die in die allgemeine Fehlerbaumanalyse einzubauen wären:

1. Bedienungs-Gefahren-Analyse
   Sie geht von der Aufgabenbeschreibung und der allgemeinen Arbeitssituation aus, sucht alle Gefährdungspotentiale zu erkennen und führt schließlich zu Sicherheitsforderungen für die betreffende Aufgabe.

2. Menschliche Fehlerart- und Effekt-Analyse, die die Folgen von Unterlassung unkorrekter Ausführung oder Ausführung zur falschen Zeit einer Aufgabe im Detail analysiert.

3. Informationsfehlerart- und Effekt-Analyse
   Sie untersucht die Auswirkungen falscher, unklarer oder dem Operateur nicht sofort zugänglicher Information (Betriebsanweisung, etc.)

In der Reaktortechnik werden (nach / 6 /)solche Analysearten im Einzelfall angewendet, doch ist ihr systematischer Einbau in einen vollständigen Analyseplan bisher noch nicht erfolgt.

Detailliertere Vorschläge zu einer konsequenteren Sicherheitsbegutachtung in Bezug auf den handelnden Menschen werden in einem internen Bericht des IRS erarbeitet. Man geht hier davon aus, daß eine Kernenergieanlage von der Konzept-Studie bis zur fertigen Anlage in Betrieb eine Anzahl von Konkretisierungsstufen durchläuft, wobei bei jeder dieser Stufen (z. B. von der Detailspezifikation zur Bauvorschrift) zu prüfen ist, ob der Sicherheitsinhalt der vorhergehenden Stufe erhalten bleibt. Besonders problematisch ist dies bei den letzten Konkretisierungsstufen, nämlich von der Bauvorschrift zur fertigen Anlage und von der Betriebsvorschrift zum tatsächlichen Betrieb, da hier eine 100 %-ige Kontrolle der Einhaltung aller Detailvorschriften nicht durchführbar ist.

Unter diesen Gesichtspunkten wird ein Forschungsprogramm vorgeschlagen, das sich besonders auf folgende Punkte konzentriert:
Sicherheitstechnische Optimalisierung der Funktionsteilung Mensch-Maschine,

des Bau- und Überwachungssystems, und der personellen Organisation.

Eine abschließende Behandlung dieser Probleme ist aus der heute verfügbaren Literatur noch nicht ersichtlich. Eine quantitative Risikoanalyse und ein Ansatz zur Minimierung des Risikos unter Einbeziehung menschlicher Verhaltensweisen ist daher in vollem Umfang noch nicht möglich. Wegen der weitgehend automatisierten Sicherheitstechnik kann man zwar davon ausgehen, daß ein Reaktoroperateur im allgemeinen nicht (so wie dies beim Flugzeugführer möglich ist) durch falsche Bedienung unmittelbar eine Katastrophe verursachen kann. Dennoch kann menschliches Fehlverhalten, besonders in Kombination mit technischen Ausfällen äußerst schwerwiegende Folgen haben - die größeren der bekanntgewordenen Reaktorstörfälle zeigen dies deutlich. Es erscheint deshalb notwendig, dieses Gebiet in die Sicherheitsanalyse voll zu integrieren, so wie dies auch in den zitierten Berichten des IRS vorgeschlagen wurde. Besonders eingehend sollten einige spezifische Problemkreise, mit denen sich der folgende Abschnitt befaßt, bearbeitet werden.

Tätigkeiten unter besonderer Belastung

Die wichtigsten Fälle besonderer Belastung des Personals liegen vor bei Arbeiten unter starkem Zeitdruck, beim Sonderbetrieb (z. B. während der Inbetriebnahme) und in ungewöhnlichen Störfallsituationen. Es kommt auch vor, daß mehrere dieser Bedingungen gleichzeitig auftreten. Der Effekt solcher Belastungen wird im Fall des KKW Würgassen besonders deutlich. In / 7 / wird der extreme Zeitdruck klar dargestellt, unter dem sicherheitstechnisch äußerst wichtige Arbeiten wie Zusammenbau, Einbau und Überprüfung des Druckgefäßes, sowie Anschluß des Primärkühlkreises durchgeführt wurden. Wichtige Schäden an der Anlage traten in der Inbetriebnahmephase auf und in mindestens einem Fall wurden die Auswirkungen durch eine Entscheidung des Betriebspersonals verschärft / 8 /.

Daß menschliches Handeln unter den genannten Bedingungen mit einer Erhöhung des Risikos verbunden ist, wird auch von verschiedenen sicherheitstechnisch erfahrenen Autoren dargelegt: So führt H. Stute (IRS) in / 1 / aus, daß der Sonderbetrieb wegen des Terminzwangs als die kritischste Phase im Hinblick auf die Wahrscheinlichkeit des Eintritts von Störfällen und Frühausfällen erscheint, ohne daß zusätzliche Maßnahmen dies berücksichtigen würden.

J. Rasmussen berichtet in / 9 / über eine Untersuchung einer Anzahl schwererer Störfälle, die ergab, daß die Mehrzahl dieser Störfälle durch menschliche Fehlhandlungen unter anormalen Betriebsbedingungen verursacht wurden. Auch er

führt ausdrücklich Zeitdruck, anormale Betriebszustände sowie nicht vorhersehbares und nicht vorschriebbares Operateurverhalten während des Störfalls als Problempunkte in der Systemzuverlässigkeit an.

Es ergibt sich der Schluß, daß menschliches Verhalten, obwohl im Normalbetrieb durch das technische Schutzsystem in seinen Auswirkungen weitgehend kontrolliert, unter besonderen Bedingungen doch zu einem wichtigen Risikofaktor werden kann.

Eine Aufgabe der weiterführenden Risikoanalse müßte es daher sein, diesen Faktor zu quantifizieren und schließlich Vorschläge zu seiner Eliminierung zu machen.

Bibliographie

/1/ H. Stute: Auslegung von Reaktorschutzsystemen
TÜ 14 Nr. 2 (1973) 86

/2/ A.D. Swain: Shortcuts in Human Reliability Analysis
SLA-73-5530, Proc. of the NATO Advances Study Institute
on Genoric Techniques in Systems Reliability Assessment,
University of Liverpool, July 1973

/3/ Th.L. Regulinski: Human Performance Reliability Modelling
in the Time Continuous Domain, Proc. wie /2/

/4/ D.R. Towill: Recent Developments in the Prediction of Human Operator Performance, Proc. wie /2/

/5/ Description of Human Factors Reports by Sandia Laboratories, Proc. wie /2/

/6/ H.P. Balfanz: Anwendung verschiedener Sicherheits- und Zuverlässigkeitsanalysen zum richtigen Zeitpunkt und zu speziellen Problemen

/7/ Ablauf von Planung, Bau und Inbetriebnahme des KKW Atomwirtschaft 17 Nr. 2 (1972), 98

/8/ Der Störfall im Kernkraftwerk Würgassen Atomwirtschaft 18 Nr. 12 (1973), 584

/9/ The Role of the Man-Machine Interface in Systems Reliability, Proc. wie /2/

/10/ J.F. Ablitt: A Quantitative Approach to the Avaluation of the Safety Function of Operators on Nuclear Reactors AHSB (S) R 160

/11/ A.D. Swain: Human Reliability Assessment in Nuclear Reactor Plants SC-R-69 1236

XI. KRITIK DER OTWAY'SCHEN METHODE DER RISIKOBERECHNUNG

Das Problem der Vollständigkeit und Anzahl der möglichen Unfälle bei der Risikoanalyse

Um bei der Risikoanalyse eines Kernkraftwerkes oder einer anderen Großanlage zu brauchbaren Aussagen zu gelangen, ist es notwendig, alle denkbaren Störfallmechanismen, die eine Gefährdung nach sich ziehen können, in die Analyse einzubeziehen.

Dies bedeutet aber, daß alle möglichen initierenden Ausfälle oder Störungen sowie alle möglichen ursächlichen Verkettungen erkannt und probabilistisch erfaßt werden müssen, was bei einem komplizierten System, wie einer Kernenergieanlage außerordentlich schwierig ist.

Um ohne die detaillierte Durcharbeitung sämtlicher Störfallmechanismen zu einer realistischen Aussage über das Gesamtrisiko zu gelangen, wurde von Otway folgender Weg vorgeschlagen:

Zugrunde gelegt wird eine stetige (i.a. monoton fallende) Abhängigkeit r (P) zwischen Unfallwahrscheinlichkeit und Aktivitätsabgabe. Durch Anwendung von Faktoren, die Abstand vom Kernkraftwerk und Dosiswirkung berücksichtigen, wird die Aktivitätsabgabe r (P) in eine Todeswahrscheinlichkeit M (P,s) für einen Menschen im Abstand s umgerechnet.

Das Gesamtrisiko durch einen Reaktor wird nun angegeben als die Summe der biologischen Risiken von allen denkbaren Unfällen, gewichtet mit deren Unfallwahrscheinlichkeiten.

Die Anzahl dieser Unfälle wird, als konservative obere Grenze, als unendlich angenommen.

Es folgt der Schluß, daß das Gesamtrisiko R (s) für einen Menschen im Abstand s durch das Integral

$$R(s) = \int_{P_1}^{P_2} M(P,s)\, dP$$ gegeben ist.

Diese Schlußfolgerung kann aber auch unter den angegebenen Annahmen nicht aufrecht erhalten werden: Nach der obigen Definition (Gesamtrisiko = Summe der biologischen Risiken, gewichtet mit den Unfallwahrscheinlichkeiten) erhält man zunächst

$$R(s) = \sum_i M_i P_i$$

Geht man zum Grenzfall unendlich vieler möglicher Unfälle über, so folgt jedoch nicht $P_i \to dP$, denn weiterhin muß jeder Unfall mit dem Wert seiner Eintrittswahrscheinlichkeit und nicht mit einem Wahrscheinlichkeitsintervall gewichtet werden. Vielmehr würde die Summe $\sum_i M_i P_i$ in diesem Fall unendlich groß werden und das Gesamtrisiko R (s) = 1, da für großes $\sum_i M_i P_i$ die genauere Gleichung $R(s) = 1 - e^{-\Sigma M_i P_i}$ anzusetzen ist. Das Problem liegt hier darin, daß die Unfallwahrscheinlichkeit davon abhängt, wie fein zwischen den Unfallmöglichkeiten differenziert wird. Wird die Unterscheidung zunehmend feiner gewählt, so geht die Anzahl der potentiellen Unfälle gegen unendlich, die Eintrittswahrscheinlichkeit des Einzelfalls jedoch gegen Null. Otway benutzt jedoch Unfälle mit endlicher Wahrscheinlichkeit als Fixpunkte für seine Interpolation - also muß auch die Zahl der Unfälle endlich angenommen werden. In der Tat entsprechen die von Otway berechneten Gesamtrisiken auch nicht einer unendlichen Unfalldichte auf der r(P)-Kurve sondern viel mehr einer Dichte von etwa 1.7 Unfällen pro Zehnerpotenz auf der P-Achse (unter der Voraussetzung von Äquidistanz in ln P). Dies läßt sich durch einen Vergleich von Integral und geometrischer Summenformel oder durch eine numerische Auswertung von Fig. 2 in /1/ leicht verifizieren.

Daraus ergibt sich unmittelbar:

Ist für einen Differenzierungsgrad, der den angegebenen Wahrscheinlichkeiten entspricht die tatsächliche Unfalldichte etwa gleich oder kleiner als 1.7 Unfälle pro Zehnerpotenz auf der Wahrscheinlichkeitsachse, so sind die Schlußfolgerungen von Otway richtig bzw. konservativ.

Liegen die Unfälle jedoch dichter, so wird das Risiko dementsprechend unterschätzt.

Die Darstellung des Gesamtrisikos in Form eines Integrals ist allerdings dann möglich, wenn die Wahrscheinlichkeit P nicht für jeden einzelnen Unfall definiert ist sondern als kumulative Wahrscheinlichkeit für alle Unfälle deren Wirkung oberhalb einer bestimmten Grenze, etwa des Mortalitätsrisikos M (s,P) im Abstand s von der Anlage, liegt. Dann ist die Wahrscheinlichkeit, daß ein Mortalitätsrisiko M (s,P) im Intervall $(M_1(s,P_1), M_2(s,P_2)$ erzeugt wird gleich $P_1 - P_2 = \Delta P$ und das Gesamtrisiko im Abstand s wird.

$$M_{ges}(s) = \int_0^1 M(s,P)\, dP$$

Hierbei ist jedoch immer die kumulative Definition von P zu beachten.

Um zu einer Aussage über das Gesamtrisiko eines Kernkraftwerkes zu gelangen, ergibt sich also in jedem Fall die Notwendigkeit, die Gesamtheit aller möglichen Störfälle und ihre Eintrittswahrscheinlichkeiten im Detail zu untersuchen. Eine Interpolation oder Extrapolation mit Hilfe einiger weniger exakt durchgerechneter Störfallabläufe ist sicher nicht hinreichend.

/1/ Otway, H., Erdmann, R.
Reactor Siting and Design from a Risk Viewpoint
Nucl. Eng. and Design 13 (1970) 365

XII. RISKS FROM THE STAGES OF THE FUEL CYCLE

(1) Accident conditions (during facility operation) in

(1a) Fuel reprocessing facility
(1b) Liquid waste storage facility
(1c) Waste solidification facility
(1d) Solid waste storage facility

(2) Accident conditions in final waste disposal facility

(3) General risk considerations

The last section includes an overall consideration of the risks in which an attempt is made to place these risks in perspective.

The assumption utilized in the calculations are the following:

(i) Fuel reprocessing and waste solidification facilities have a capacity of 1500 t/year

(ii) All fuel (LWR[+)] and LMFBR[++)]) has a cooling time of 150 days before reprocessing, average burnup 34,000 MWd/t. The LWR is assumed to be a PWR[+++)] operating with an equilibrium uranium fuel cycle. The LMFBR is assumed to be fueled with plutonium from an LMFBR economy and the core and blanket (radial and axial) are mixed proportionally at reprocessing.

+) LWR: Light Water Reactor
++) LMFBR: Liquid Metal Fast Breeder Reactor
+++) PWR: Prossurized Light Water Reactor

(iii) Waste solidification occurs at 5 years after reprocessing and final waste disposal takes place 5 years after solidification

(iv) The average annual aeolian dilution (X/Q) is 10^{-7} sec/m^3 for all considerations and for groundwater (X/Q) is 10^{-1} sec/m^3

(v) One ton of reprocessed fuel, both LWR and LMFBR, produces one cubic meter of high level liquid waste .

(1) Accident conditions (during facility operation)

An accident is possible in any of the operations from fuel reprocessing to final waste disposal. For example, an accident could be a process malfunction, due to an operator or equipment error, which would result in loss of decontamination efficiency in the treatment systems for airborne effluents. Other possible accidents are waste handling accidents, solvent fires, chemical explosions, and criticality incidents in the fuel reprocessing facility. In liquid waste storage the release of radioactive materials could result from either tank corrosion, loss of cooling, hydrogen explosion or external causes (earthquake, sabotage,

flood, etc.). Storage of solid wastes could not lead to any radiolytic hydrogen formation and therefore the possibility of a hydrogen explosion does not exist. However, the other possibilities for release by liquid waste storage also exist in the storage of solid wastes.

These above mentioned accidents, their probability of occurrence and their consequences are discussed below for each step of the activities shown in Fig. III.3 of chapter III ("Das Risiko des nuklearen Brennstoffzyklus").

(1a) Fuel reprocessing facility

Confinement and ventilation systems in fuel reprocessing facilities remove particulates of nonvolatiles dispersed under accident conditions to such an extent that the upper limit accidents are controlled by the release of such volatile and semi-volatile materials as the noble gases, iodine, ruthenium, cesium, and tellurium. The site boundaries for all plants are estimated to be determined by the whole-body dose resulting from the release of volatile "fresh" fission products from a nuclear excursion.

The following would be representative of the spectrum of accidents, and their consequences, for a 1500 t/year facility

Accident type	Consequence (maximum accidental inhalation dose)	Frequency
Process malfunction		
e.g. 100-fold decrease in decontamination efficiency for 30 minutes	0.16 mrem to the bone 0.006 mrem to the whole body	0.33/year
Breach of process off-gas confinement	0.29 mrem to the thyroid (200 mrem to the thyroid)+)	≤0.20/year
Fuel handling accident involving cladding failure	0.3 mrem to the whole body 2.5 mrem to the thyroid (1750 mrem to the thyroid)+)	0.05 to 0.075/year
Design basis (upper limit) accidents e.g. nuclear excursion	0.2 mrem to the whole body 13.0 mrem to the thyroid (9100 mrem to the thyroid)+)	≤0.025/year

+) Thyroid dose assuming grass-cow-milk pathway

(1b) Liquid waste storage facility

Almost any high-level waste management scheme involves an interim storage of the wastes as liquid. The reason being that there are practical and economic advantages to be gained by allowing many fission products with short and intermediate half-lives to decay prior to additional waste processing. For safety reasons it is assumed that any type of storage facility would be located in an area that is tectonically stable and in which the geologic materials in the surrounding vinicity have a low permeability and a high ion exchange capacity. These last criteria are advantageous to hamper the movement of any ground released activity.

The causes of activity release could be considered to be one of the following:

(i) tank corrosion

(ii) loss of cooling

(iii) hydrogen explosion

(iv) external cause (e.g. earthquake, sabotage, flood, etc.).

However, it is the opinion of most safety analysis people that the most likely mechanism of a major release and impact to the public would be a loss of cooling incident.

The loss of cooling, as well as an inoperative ventilation system for the tanks, could be caused by a loss of power, operation error or neglect, flood, hurricane, earthquake, or sabotage. The worst possible time for this accident to occur would be when the tank was newly filled and the heat generation rate at its peak.

With a permanent loss of cooling the tanks would self-boil in a matter of a few hours, and would boil to dryness in something of the order of 100 hours. If the wastes were still contained at this time a temperature of more than 1000°C would be reached in the center of the tank. The semi-volatile components of the wastes, e.g. cesium and rutherium, would be released to the atmosphere from the self-heating wastes because of their relatively low vapor pressure. Assuming almost complete release of cesium and rutherium over a period of 300 hours the maximum off-site doses would be approximately 10^6 rem to the lungs (inhalation). The dose would fall rapidly with distance from the tank. The magnitude of the possible dose suggests that significant engineering safety measures must guarantee a small probability for this accident.

(1c) Waste solidification facility

Since not much experience has been obtained in the solidification of high-level liquid waste from high-burnup fuel there is not much known about possible accidents and their consequences. The most likely accident would possibly be a process malfunction which would result in a loss of decontamination efficiency. The cause of such an accident could be either operator error or equipment malfunction.

(1d) Solid waste storage facility

The leakage of activity from containers holding solid wastes could be caused by defective sealing, by release of over pressure built up in-

side the container, or by abnormally high corrosion rates. In any case the leakage rate would be slow from the solid, and could be detected by monitors so that remedial action could be taken.

The loss-of-coolant accident would probably be the most severe accident in a solid waste storage facility as in the case of liquid storage. However, since the wastes would be at least several years older than the liquid wastes, due to the time lag in solidification after reprocessing, the heat generation rates per unit volume would be correspondingly smaller. In addition, the waste may be combined in the solidification process with an amount of inert material. Therefore, the likelihood that the waste could reach the melting point of stainless steel is small. If the waste container does fail, by overheating or by rupture from collapse of the surrounding structure, the volatile components of the wastes would be released to the atmosphere.

Release rates for volatile elements from ceramic wastes have been measured to be of the order of 0.5 to 1.0% of the content per hour. A typical solid waste container would contain, roughly, the wastes from one to three tons of reprocessed fuel. Assuming the wastes have aged five years before they are solidified, the typical waste container would contain approximately 3.0×10^5 curies of cesium and rutherium. Therefore, the release from one container would be of the order of 3000 curies/hr., or a maximum dose to the lungs of 10^2 rem.

(2) Accident conditions in final waste disposal facility

Before we can consider here the risks from a final waste disposal facility we need to understand the time behaviour of the properties of the waste and the relative ecological importance of the various components

of the waste. Typically, radioactive wastes are characterized by curies (disintegration/sec) per unit volume of the waste as a function of the time from the date that the reactor fuel was reprocessed. This type of characterization is not ideal since the biological effect of the waste is only partially determined from the curies. More important is the type of decay particle and its energy, which are inherent properties of the decaying isotope. In addition, it is important to know the relative ease with which the isotopes move through our environment, the extent to which they are reconcentrated by organisms directly, or indirectly, involved in man's food chain, and our body's critical organ's characteristic rate of accumulation and elimination. Therefore, to properly consider the hazards of a final waste disposal facility it is necessary to have some sort of an index incorporating all of these factors for each radioactive isotope. The establishment of such a true index is a very difficult problem and can only be partially accomplished today due to the lack of sufficient data.

As a first approximation to such an index, which we shall call a hazard index, we use the reciprocal of the established maximum permissible concentration of the isotope in water, MPC_w (Ci/m^3). In other words, the hazard index (HI^i) of Q^i curies of isotope i in a radioactive waste mixture is defined as

$$HI^i = Q^i / MPC_w^i. \qquad (1)$$

The use of the MPC value for water is realistic as the most probable mechanism for the release of the radioactive material from the storage facility (assuming underground storage) would be by

water transportation. The units of the hazard index are volume (m^3) of water required to dilute the radioactive isotope to acceptable limits. The total hazard index of the waste is found by summing over all isotopes present;

$$HI = \sum_i HI^i = \sum_i \frac{Q^i}{MPC_w^i} \qquad (2)$$

It has to be emphasized that even though this hazard index definition is used currently, there are some severe shortcomings involved in the definition. The basic procedure in setting the maximum permissible concentrations for the general public is to calculate that amount of each radioisotope in water or air which after 50 years of continuous intake or inhalation would result in a dose to the critical body organ equal to the maximum permissible dose. The criteria for chronic exposure of the public should, however, be related directly to maximum permissible doses rather than to MPC's since the latter do not explicitly consider perhaps more limiting pathways of exposure than those caused by inhalation of air or ingestion of water. Special considerations should also be given to the specific location of the facilities as there may be mechanisms available for the reconcentration of the radioactive isotopes and pathways for ingestion by the public.

The hazard index, as defined by Eq. (2), has been calculated for the spent fuel composition of several different reactors and their fuel loadings for a time span of 1 to 10^6 years after reprocessing of the fuel. The results of these calculations are shown in Fig. XII.1 for a pressurized light water reactor. Qualitatively the curves for the other reactor types and fuel loading are not very different. It was assumed that reprocessing of the fuel occurs 150 days after dis-

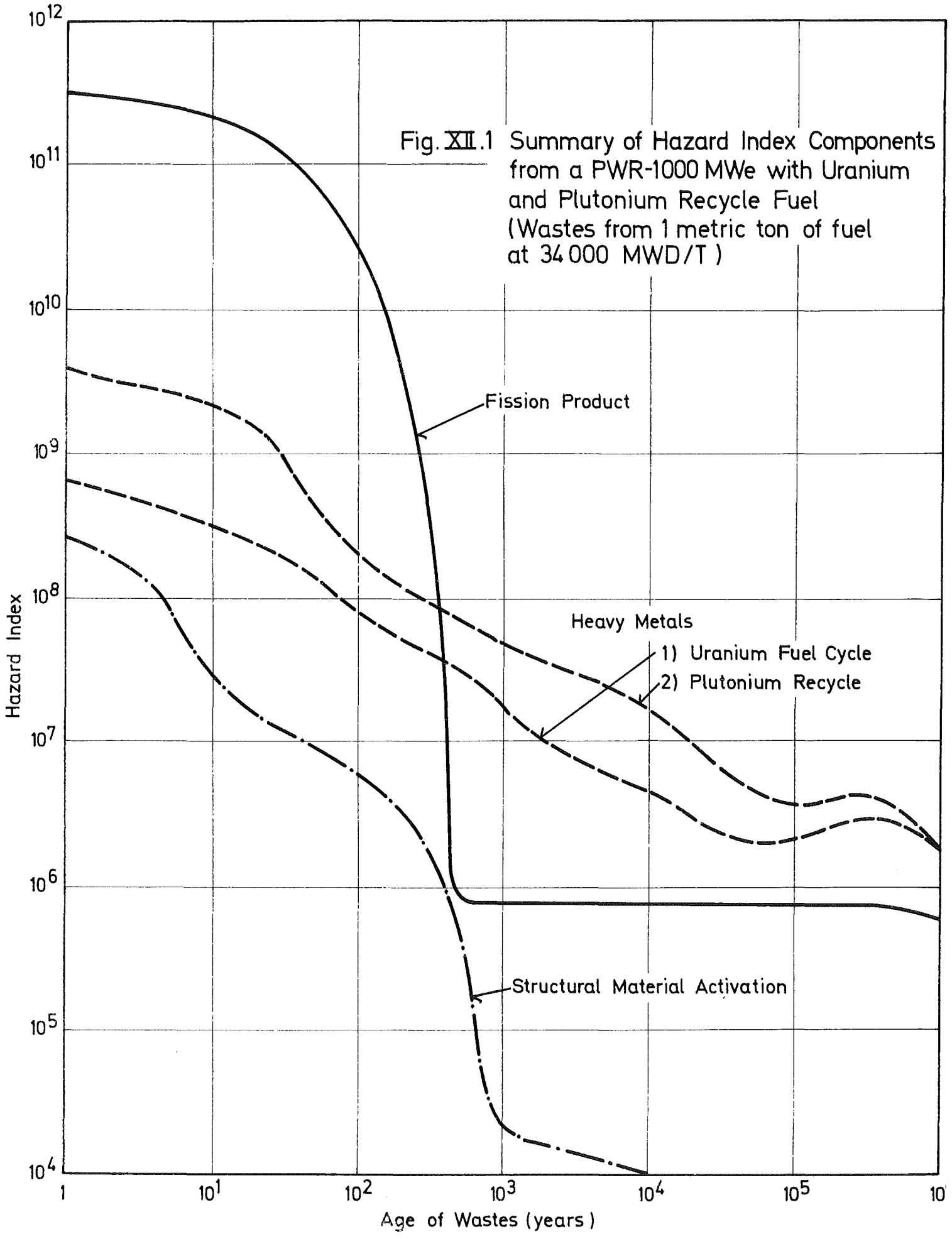
Fig. XII.1 Summary of Hazard Index Components from a PWR-1000 MWe with Uranium and Plutonium Recycle Fuel (Wastes from 1 metric ton of fuel at 34 000 MWD/T)
Fission Product
Heavy Metals
1) Uranium Fuel Cycle
2) Plutonium Recycle
Structural Material Activation
Hazard Index
Age of Wastes (years)
10^{12}
10^{11}
10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
1
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10

charge from the reactor and that the plutonium and uranium losses to the waste stream are 1.0% of the quantity present in the spent fuel. The results of these calculations are given per ton fuel (1000 kg). No losses are assumed for any of the fission products, as for example ^{85}Kr and ^{3}H which do not follow the waste stream. The curves are, therefore, not meant to represent a particular waste composition but rather to illustrate the relative importance of the individual isotopes present.

From the fission product curve one notices that the isotopes fit into two distinct classes, those that essentially vanish within 1000 years and those that are practically constant over the 10^6 years time span. The two isotopes that determine the envelope are ^{90}Sr and ^{129}I. The fission products determine the total waste hazard up to about 600 years, after which time the heavy metals dominate. The difference in the hazard of the fission products and heavy metals from 600 years to 10^6 years is only 1 to 2 orders of magnitude.

For the consideration of the safety, or risk to the public, of a final waste disposal facility one is faced with a very difficult problem, namely that it is necessary to consider a very long time span, equal to that of a geological time scale. A very important question at this point is: How long a time should we consider the waste as dangerous? Obviously not to the point that the last atom has decayed. Therefore it may be convenient to define a point after which time we would not consider the waste as dangerous. A possible means of doing so may be by comparing the wastes to existing natural radioactive sources, as uranium and thorium ore deposits.

Utilizing the salt deposit concept of the BRD for the disposal of high-level solidified wastes one calculates that approximately 505 tons of salt are directly associated with the wastes from 1 ton of reprocessed fuel. Using the definition of the hazard index as given by Eq. (1) one finds:

(i) 1.0 gm of natural uranium in equilibrium with its daughters

$$HI = 15.1\ m^3\ H_2O\ /\ gm\ U$$

(ii) 1.0 gm of thorium in equilibrium with its daughters

$$HI = 3.78\ m^3\ H_2O\ /\ gm\ Th$$

Assuming an average concentration of uranium and thorium in the earth's crust of 4 ppm and 12 ppm, respectively, one computes a hazard index for 505 tons of average earth's crust of

$$HI\ (\text{ave. earth's crust}) = 5.35 \times 10^4.$$

A typical uranium ore deposit is generally of the order of 0.2% U_3O_8. Thorium is closely associated mineralogically with uranium and is generally found in uranium ore. We shall assume a Th/U ratio of one. Therefore, 505 tons of typical uranium ore would have a hazard index of

$$HI\ (\text{uranium ore}) = 1.68 \times 10^7.$$

From Fig. XII.1 one sees that the hazard index for our fuel reprocessing wastes falls below HI(uranium ore) in about 10,000 years. From these arguments it would appear that the wastes should not be considered "dangerous" after the main hump due to the fission pro-

ducts is away. Even if we consider the time period to 10,000 years we have considerably reduced our problem. In other words we need concern ourselves, in a safety/risk analysis, with events possibly leading to accident conditions over a period of a few thousand years and not literally millions.

After the waste facility has reached its designed capacity it will be permanently sealed and, for many years thereafter, guarded against unintentional entry. The ground surface of the facility will probably be monitored also for many years after closure for the purpose of detecting releases. However, one could not expect these activities to continue for the time period of 10,000 years. During such a period of time geologic processes can play a very important role along with other factors.

A consideration of the events which could lead to the release of radioactive materials over long periods of time from the waste disposal facility has resulted in the fault tree shown in Fig. XII.2. This fault tree was not intended to serve for the calculation of the probability of the top event. This is presently not possible as geology has been a science with very limited predictive capabilities. However, from the fault tree one is able to get a logical ordering of the events.

Many of the factors in the fault tree can be designed against by careful selection of the location of the waste facility. In addition, the geologic processes are very regional dependent so that one cannot, in general, make a statement concerning the possible effects of these processes. Under the assumption that what has not happened in the past will not happen in the near future ($\sim$ 100,000 years), a site would be selected that is tectonic stable, experiences a low rate of erosion, and has no record of volcanic activity. This assumption is not necessarily valid in the world of today in which the influence of man on his environment is ever increasing.

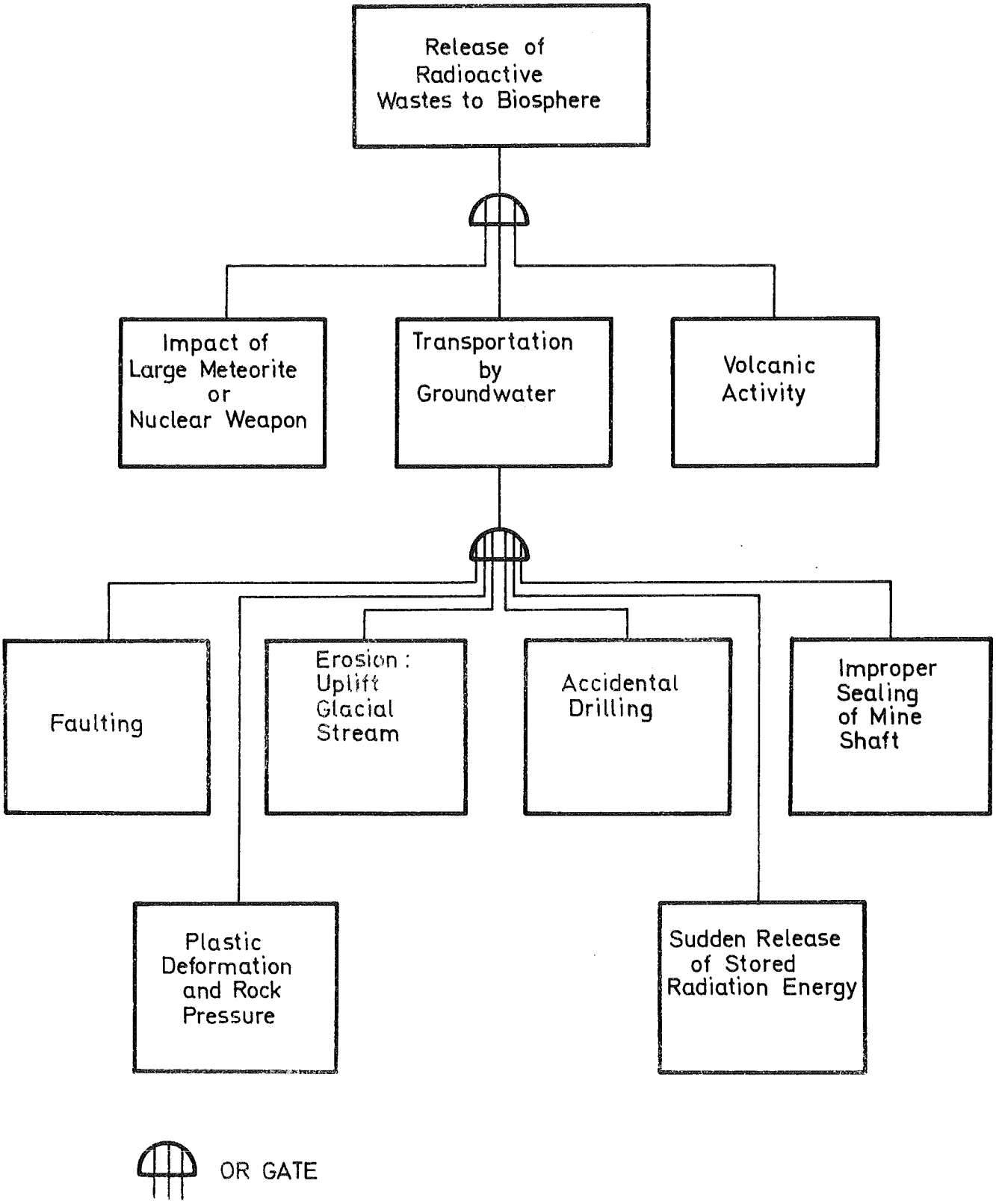

Fig. XII.2 Fault Tree of Salt Mine Used for Storage of Radioactive Wastes (after closure of the mine)

(3) General risk considerations

Remarks concerning accident conditions during facility operation

It is probably instructive to place the risks from the potential accidents in the fuel reprocessing, liquid waste storage, waste solidification, and solid waste storage facilities in perspective. To do this we can postulate upper limit accidents (large releases) and find an upper accident probability which would limit the expected risk from each facility to 30 mrem/yr.

(i) Fuel reprocessing facility

We postulate for the upper limit accident here a 5% release of all fission products and 1% of the heavy metals. For this purpose we assume that 1/200 of the total amount of fuel reprocessed in one year is available in the facility in an unfavorable form (in the process of reprocessing), i.e. 1/200 x 1500 t = 7.5 t. A summation of the curies from 5% of the fission products and 1% of the heavy metals present in the fuels, divided by their corresponding MPC values give

$$\left.\sum_i \frac{Q^i}{MPC_A^i}\right|_{LWR} = 1.59 \times 10^{15} \ (m^3/t)$$

$$\left.\sum_i \frac{Q^i}{MPC_A^i}\right|_{LMFBR} = 3.84 \times 10^{15} \ \left(\frac{m_A^3}{t}\right)$$

where Q^i = curies of radionuclide i and MPC_A^i = corresponding maximum permissible concentration in air. Utilizing the larger of the two values, namely that for the LMFBR[+)], the equation for the calculation of the upper accident probability limit is

$$P\left[1/\text{sec}\right] \times \sum_i \frac{Q^i}{MPC_A^i}\left[\frac{m_A^3}{t}\right] \times FA\left[t\right] \times \frac{X}{Q}\left[\frac{\text{sec}}{m^3}\right] \times 500\left[\frac{\text{mrem}}{\text{yr}}\right] \leq 30\left[\frac{\text{mrem}}{\text{yr}}\right]$$

where P = accident probability

$\frac{X}{Q}$ = average annual aeolian dilution (10^{-7} for our calculations)

FA = quantity of spent fuel involved in the accident

$$P\left[1/\text{sec}\right] \times 3.84\times10^{15} \times 7.5\times10^{-7} \times 500 \leq 30\left[\frac{\text{mrem}}{\text{yr}}\right]$$

$$P\left[1/\text{sec}\right] \leq 2.1\times10^{-11}\ \text{sec}^{-1}$$

or on a yearly basis

$$P \leq 6.6\times10^{-4}\ \text{yr}^{-1}$$

+) Hereafter we shall not distinguish between the LWR and LMFBR and only use the largest value from them.

(ii) Liquid waste storage

Assuming that the liquid wastes are stored for 5 years between fuel reprocessing and waste solidification, the total waste quantity in storage at any given time for a 1500 t/yr throughput would be

$$FA = 1500 \text{ t/yr} \times 5.0 \text{ yr} = 7500 \text{ m}_w^3$$

assuming that one ton of fuel produces one cubic meter of high-level liquid wastes. For the upper limit accident we shall assume that all of the semi-volatile radionuclides and 5% of the remaining fission products are released to the atmosphere. The ratio of the curies to the corresponding MPC values for these radionuclides at the midpoint of the total liquid waste storage period (2.5 years) is, selecting the larger value of the two reactor types

$$\sum_i \frac{Q^i}{MPC_A^i} = 1.48\text{x}10^{15} \left[\frac{m_A^3}{m_w^3}\right]$$

The calculation of the upper accident probability is as performed in the previous subsection.

$$P \left[1/\text{sec}\right] \times 1.48\text{x}10^{15} \times 7500\text{x}10^{-7} \times 500 \leq 30 \left[\frac{\text{mrem}}{\text{yr}}\right]$$

$$P \left[1/\text{sec}\right] \leq 5.4\text{x}10^{-14} \text{ sec}^{-1}$$

$$P \leq 1.7\text{x}10^{-6} \text{ yr}^{-1} .$$

Assuming a tank capacity of 3000 m_w^3, the accident probability per tank per year is

$$P \leq 4.25 \times 10^{-6} \text{ yr}^{-1} \text{ tank}^{-1} \quad ,$$

(iii) Waste solidification facility

The waste solidification facility considered has a throughput of 1500 t/yr. As mentioned previously, the waste solidification is assumed to take place 5 years after fuel reprocessing. Our upper limit accident is assumed to be a total release to the atmosphere of all the semi-volatiles radionuclides. As in the fuel reprocessing facility we assume that 1/200 of the annual throughput would be involved in the accident, i.e. $\frac{1}{200} \times 1500\ m_w^3 = 7.5\ m_w^3$. At 5 years after fuel reprocessing

$$\sum_i \frac{Q^i}{MPC_A^i} = 5.91 \times 10^{14}\ m_A^3/m_w^3$$

for the semi-volatiles in the waste. The upper accident probability is calculated as follows:

$$P \left[1/\text{sec} \right] \times 5.91 \times 10^{14} \times 7.5 \times 10^{-7} \times 500 \leq 30 \left[\frac{\text{mrem}}{\text{yr}} \right]$$

$$P \left[1/\text{sec} \right] \leq 1.38 \times 10^{-10} \text{ sec}^{-1}$$

$$P \leq 4.3 \times 10^{-3} \text{ yr}^{-1} \quad .$$

(iv) Solid waste storage

Solid waste storage is assumed to be for a period of 5 years after solidification and before final disposal. Therefore a total capacity needed for the facility is 1500 t/yr x 5 years = 7500 t, i.e. the wastes from 7500 t of spent fuel. Again, for the upper limit accident we assume total release to the atmosphere of all the semi-volatiles present in the wastes and that the accident would occur at the midpoint of the total storage time (7.5 years after fuel reprocessing). In this case our ratio curies to MPC values is

$$\sum_i \frac{Q^i}{MPC_A^i} = 5.5\times10^{14} \left[\frac{m_A^3}{m_w^3}\right]$$

and the accident probability

$$P\left[1/\text{sec}\right] \times 5.5\times10^{14} \times 7500\times10^{-7} \times 500 \leq 30 \left[\frac{\text{mrem}}{\text{yr}}\right]$$

$$P\left[1/\text{sec}\right] \leq 1.45\times10^{-13}\ \text{sec}^{-1}$$

$$P \leq 4.6\times10^{-6}\ \text{yr}^{-1}$$

Assuming that an individual waste cylinder contains the wastes from 2.5 t of reprocessed fuel, the accident probability per year per cylinder is

$$P \leq 4\times10^{-3}\ \text{yr}^{-1}\ \text{cylinder}^{-1}$$

To summarize, the permissible upper limits of the accident probabilities, assuming an expected accident risk of 30 mrem/yr, are collected in Table 7.

Table 7 Permissible Upper Limit of Accident Probabilities

Facility	Probability
Fuel reprocessing	$6.6 \times 10^{-4}\ yr^{-1}$
Liquid waste storage	$4.25 \times 10^{-6}\ yr^{-1}\ tank^{-1}$
Waste solidification	$4.3 \times 10^{-3}\ yr^{-1}$
Solid waste storage	$1.5 \times 10^{-3}\ yr^{-1}\ cylinder^{-1}$

From these considerations it appears that the most stringent safety requirements have to be meant in the liquid waste storage portion of our simplified fuel cycle. As mentioned in section (1b) one has to engineer against the permanent loss-of-cooling accident.

Remarks concerning accidents in final waste disposal facility

As we have done previously we can also attempt here to find an upper limit of the accident probability which would give us an expected accident risk of 30 mrem/yr. This is much more complicated here because of the time dependence of the hazards of the waste (see Fig. XII.3) and the continuous accumulation of the waste in the facility. However, one would expect that if the wastes were added to the facility at a constant annual rate an equilibrium value of the hazard index would be ultimately reached. The equilibrium value would only be a function of the annual rate of addition and the hazard index of this amount. The approach to an equilibrium value is shown in Fig. XII.3 for the case of a constant yearly addition of a quantity of waste having an initial hazard index of HI = 4.14×10^{11} m^3. The equilibrium value is reached in 800 years and is roughly 21 times the constant yearly addition. However, 95% of the equilibrium value is achieved in only 190 years.

The advantage of using the equilibrium value in our calculations is that the time dependence drops out of our problem and that we do not need to consider the total quantity of wastes stored. The permissible limit of the accident probability so calculated, for the equilibrium value, would be then the true upper limit.

The hazard index of the waste composition at 10 years after fuel reprocessing is, as defined by Eq. (1),

$$HI = \sum_i \frac{Q^i}{MPC_w^i} = 2.13 \times 10^{11} \ m^3/m_w^3 \ .$$

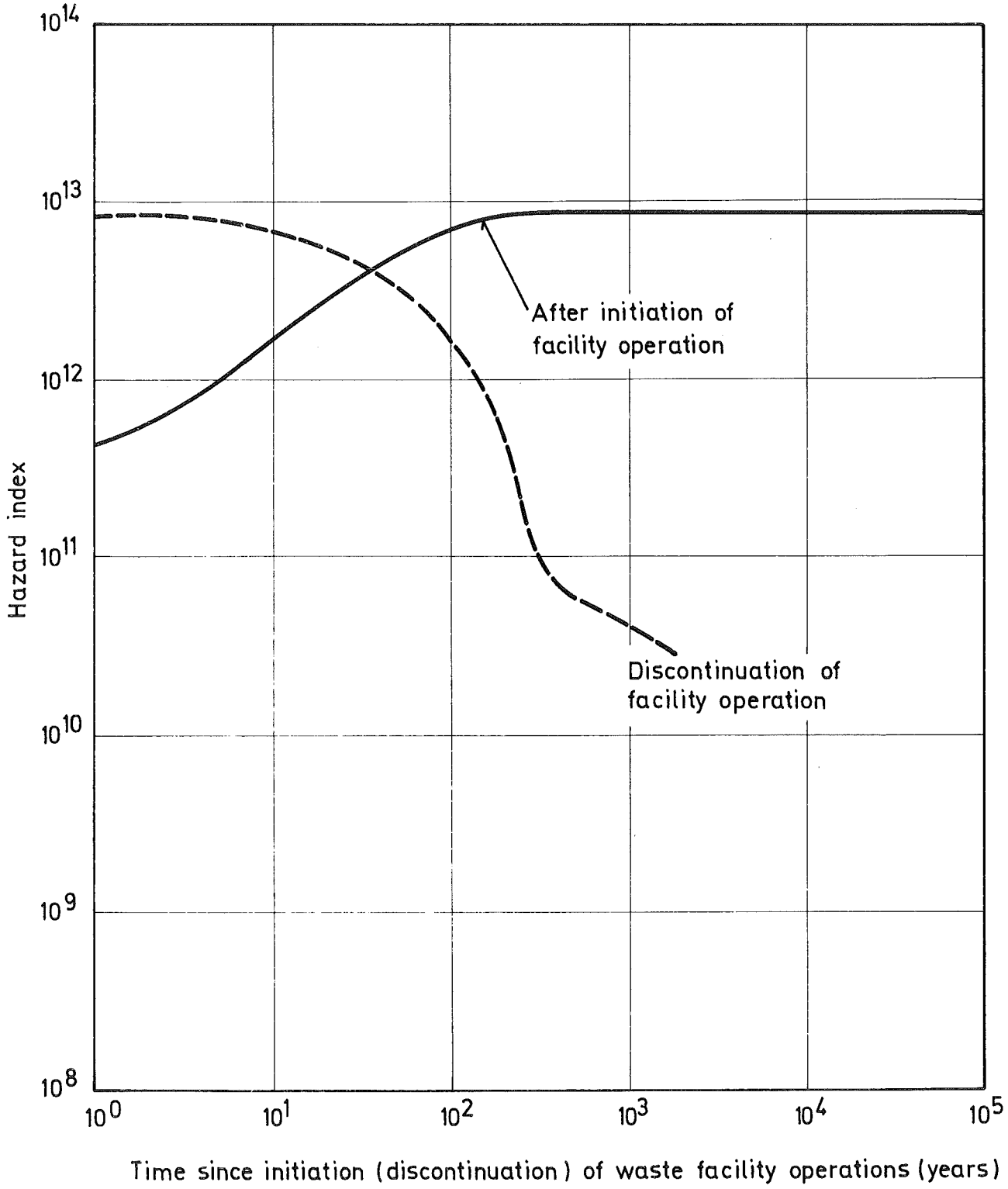

Fig. XII. 3 Hazard Index of Total Waste Storage Facility at a Constant Yearly Rate ($Hi(t) = 4.14 \times 10^{11} m^3$) of Addition

To support the facilities (fuel reprocessing, etc.) as described in the previous sections, the annual addition rate would be 1500 m_w^3/year. Therefore the equilibrium hazard index achieved is

$$HI_{eq} = 2.13 \times 10^{11} \text{ m}^3/m_w^3 \times 1500 \ m_w^3 \times 21$$

$$= 6.75 \times 10^{15} \text{ m}^3.$$

The leach rate measured for various types of solidified wastes ranges typically from 10^{-4} to 10^{-7} gm/cm^2/day. If we utilize the higher value, 10^{-4} gm/cm^2/day, and assume the waste cylinders to be 20 cm in diameter with a density of 3.0 gm/cm^3, the fraction of the waste leached by water is calculated to be

$$f = 0.77 \times 10^{-10} \text{ sec}^{-1}.$$

It is unreasonable to assume that if an accident does occur in the waste disposal facility that all waste cylinders would be simultaneously exposed to a leaching action of water. One would suspect that the probability a certain fraction of the waste cylinders be exposed to water in an accident would exhibit a behaviour, on a log-log scale, as shown in Fig. XII.4.

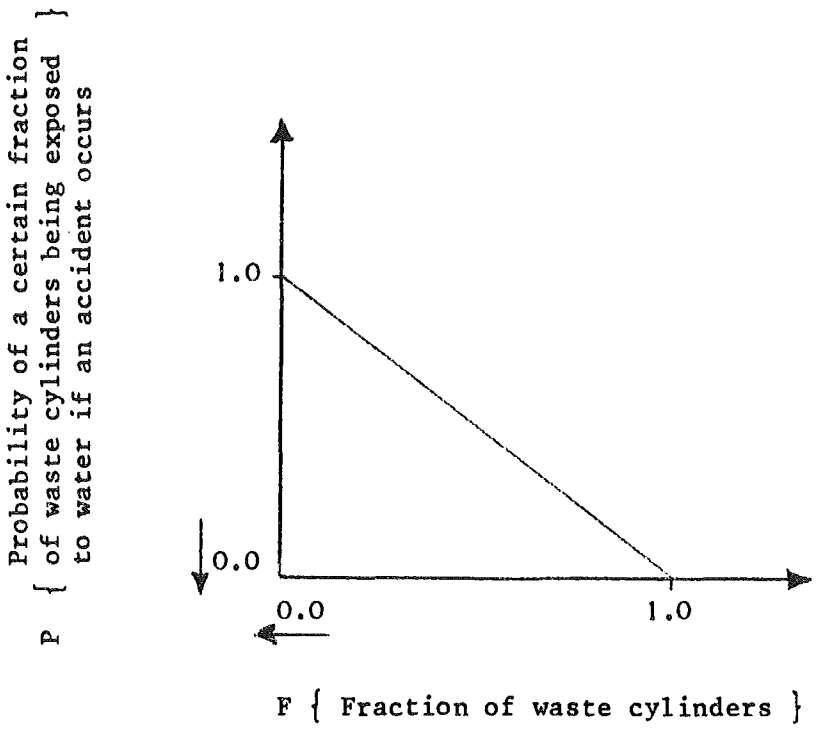

Fig. XII.4 Probability vs. Fraction of Waste Exposured in an Accident

In the following calculations we shall use the product PxF as the parameter, assuming an <u>expected</u> risk of 30 mrem/yr. Therefore

$$PxFx6.75x10^{15}\left[m^3\right]x0.77x10^{-10}\left[sec^{-1}\right]x10^{-1}\left[\frac{sec}{m^3}\right]x500\left[\frac{mrem}{yr}\right]\leq 30\left[\frac{mrem}{yr}\right]$$

where we have assumed $(\frac{X}{Q})$ of $10^{-1}\left[\frac{sec}{m^3}\right]$ for groundwater and have neglected any filter action of the ground soil. Solving for PxF

$$PxF \leq 1.15x10^{-6}.$$

Literature

1) Peter E. Mc Grath

Radioactive Waste Management: Potentials and Hazards from a Risk Point of View

Kernforschungszentrum Karlsruhe, KFK-1992 (1974)

2) Siting of Fuel Reprocessing Plants and Waste Management Facilities

Compiled and Edited by the Staff of the Oak Ridge National Laboratory, ORNL-4451 (1970)

3) The Safety of Nuclear Power Reactors and Related Facilities

U.S. Atomic Energy Commission, WASH-1250 (1973)

4) Barnwell Nuclear Fuel Plant, Environmental Report

U.S. Atomic Energy Commission, DOCKET 50-332-27 (1972)

5) Proceedings of the Conference Management of Radioactive Wastes from Fuel Reprocessing, OCED/IAEA, Paris, Dec. 1972

6) Environmental Radiation Dose Commitment

An Application to the Nuclear Power Industry, U.S. Environmental Protection Agency, EPA-520/4-73-002 (1974)

7) Recommendations of the International Commission on Radiological Protection, Publication 2 (1959)

XIII. A NEW CONCEPT IN RISK - ANALYSIS OF NUCLEAR FACILITES

Vorbemerkungen:

Die Betrachtung von Kernenergierisiken führt immer auf die Frage, ob Risiken als hinreichend niedrig angesehen werden können, d.h. die Zumutbarkeit dieser Risiken. Es handelt sich aber in jedem Einzelfall um ein Entscheidungsproblem, z.B. bezüglich der Standortwahl oder letztenendes um die Entscheidung: Kernenergie ja oder nein. Wie meist bei solchen Fragen, liegt auch bei der Kernenergie ein mehrdimensionales Entscheidungsproblem vor. Schon der Begriff der 'Zumutbarkeit' impliziert, daß gewisse Risiken, die von Null verschieden sind, eineindeutig auch mit Nutzenaspekten verbunden sind und also ein Kompromiß zu schließen ist. Hier ist es unvermeidlich, daß Werturteile eine große Rolle zu spielen beginnen. Allein aber schon bei der Frage z.B. der Verrechenbarkeit von langfristig eingegangenen Risiken, wie bei Endlagerung radioaktiver Abfälle gegenüber kurzfristigen Risiken, wie beim Abtransport der Abfälle ins Weltall; oder bei der Verrechenbarkeit kleiner häufiger gegen große seltene Belastungen treten Bewertungsfragen auf, die nicht mehr objektiv leistbar sind. Für die Handhabung solcher Entscheidungsprobleme, die ja immer darauf hinauslaufen, zunächst scheinbar nicht Verrechenbares verrechenbar zu machen, gewissermaßen zu aggregieren zu einer Maßzahl, sind eine Reihe von Modellen vorgestellt worden. Es sei im einzelnen auf diese Modelle hier nicht eingegangen. Eine grobe Beschreibung der Hauptdenkrichtungen sei jedoch skizziert.

Eine Richtung betrachtet das Entscheidungsproblem als Spiele gegen die Natur. Man hat auszuwählen zwischen einer Reihe von Strategien (wobei Abschuß des radioaktiven Abfalls in den Weltraum eine andere wäre als Endlagerung), deren Auszählungen beispielsweise durch Vergleiche mit Lotterien zueinander in Beziehung gebracht werden können und abhängig sind von Zuständen der Natur. Kenntnisse bzw. Teilkenntnisse solcher Zustände der Natur machen es möglich 'optimale' Strategien auszuwählen. Optimal bezieht sich dann auf die Einstellungsstruktur des Entscheidenden, der verschiedene Formen der Risikobereitschaft bzw. der Risikoaversion wählen kann /1/.

Hilfreich für praktische Probleme erscheinen psychometrische Verfahren wie sie beispielsweise bei Torgeson /2/ beschrieben sind bzw. bei H. Raiffa /3/ zum Einsatz kommen. Danach werden die Ausprägungen von Handlungsoptionen bezüglich verschiedener Beurteilungsaspekte über 'Befragungen' und Vergleichslotterien in Nutzwertfunktionen transformiert und diese gegenseitig fixiert (Utility Theory). Es existiert reichhaltige Literatur über die diesbezüglichen Befragungs- und Erhebungstechniken /4, 5/. Am Ende ist ein Gesamtnutzenwert jeder Alternative ermittelbar. Probleme dieses Vorgehens liegen in der Auswahl der Befragten, in der Vielzahl von sozialpsychologischen Parametern, die auf die Nutzeneinstellungen der Befragten Einfluß nehmen und in der Kombination der Einzelantworten zu Gruppenentscheidungen. Neue organisatorische Maßnahmen für die Entscheidungsverfahren wären erforderlich. Zum Teil können aber schon Expertenbefragungen mit Hilfe von 'Delphi-Techniken' /6/ weiterhelfen.

Einfacher, aber im Grunde ähnlich sind Methoden, die von der Festlegung normativ ermittelter Funktionen und ihrer Verankerung an wenigen, allgemein verbindlich festgelegten Schlüsselwerten ausgehen (wie z.B. Sensitivitätsschwellen, Protestschwelle).

Die Verrechenbarkeit verschiedenartiger Beurteilungsaspekte wird fast gänglich aufgegeben bei dem Konzept der Erfüllung von Anspruchsniveaus nach H. Simon /7/. Hier gibt man die Ermittlung einer Nutzenfunktion und damit die Ermittlung einer 'besten' Lösung auf und bestimmt lediglich zulässige Lösungen, die dadurch gekennzeichnet sind, daß sie in allen Beurteilungsaspekten die Anspruchsniveaus erfüllen, d.h. vorgegebene Standards einhalten. Dieses zum Teil bei Normalbetriebsrisiken geübte Vorgehen müßte jedoch noch wesentlich ausgebaut werden auf die vielfältigen bei Unfallsituationen anstehenden Risikofragen (Grenzwahrscheinlichkeit für Eintritt von Unfallereignissen abhängig von Schadensgröße pro Ereignis, zeitliche Nachhaltigkeit des Schadens, Vorwarnmöglichkeit etc.). Auch hier kommt man jedoch um die Einbeziehung von Werturteilen bei der Festsetzung des Anspruchsniveaus nicht herum. Das Vorgehen von Ch. Starr (z.B. /13/), beispielsweise die Akzeptierbarkeit von Risiken aus empirischen Analysen über das bisherige Bevölkerungsverhalten bei den verschiedensten Technologien zu ermitteln,

reicht nicht hin. Es müssen vielmehr auch unter Einsatz von Verfahren der numerischen Taxonomie (z.B. /8, 9/) die Abhängigkeiten der Einstellungsstrukturen der Bevölkerung bezüglich verschiedenartiger Risiken näher ermittelt werden und insbesondere die Abhängigkeit vom Informationsstand berücksichtigt werden.

Im Folgenden soll das Vorgehen gemäß der oben erwähnten Utility Theorie noch etwas detaillierter vorgestellt werden [+].

[+] Diese Überlegungen erfolgten zusammen mit L.D. Maxim and F.X. Cook Jr. von der Mathematica Inc., Princeton, New Jersey, U.S.A.

Introduction:

The purpose of this section is to address the area of risk analysis, in particular to point out gaps in the methodology of risk analysis and to show cause for viewing the approach to risk analysis from a different perspective. More specifically, we contend that the presently utilized concept of risk (expected fatalities per exposed population per year) is inappropriate. Instead, we propose to handle the problem with a mathematical approach termed utility theory.

To explore our ideas it is instructive to follow the illustrative flow chart for risk analysis shown in Figure XIII.1. Briefly, the analytical approach to the analysis involves the following elements:

-- Identification of "Events" of interest (i.e., events associated with the release of radioactive material).

-- Development of Boolean expressions which describe the circumstances (subsystem or element failures) under which these events can occur -- perhaps supplanted by stylized pictorial representations (e.g., fault trees).

-- Development of models which evaluate the consequences of these events (e.g., mortality risks) in terms of the magnitude of release and exogenous factors (e.g., weather patterns, population densities, etc.).

-- Evaluation of the likelihood of these consequences by exercising the models with data.

This type of analysis has been extensively employed to analyze the safety of reactor systems (c.f. Otway, et. al. /10, 11/ and Otway and Erdmann /12/. However, one area of the process shown in Fig. XIII. 1 in which analytical techniques have been conspicuously absent is that of providing an explicit structure by which the consequences of different decision alternatives can be meaningfully compared and set in relation to a norm (risk acceptance). For example, such a norm would be that used to define the exclusion radius of a nuclear facility. It is this particular area of the process that we have identified, somewhat tongue-in-cheek, as the methodology gap.

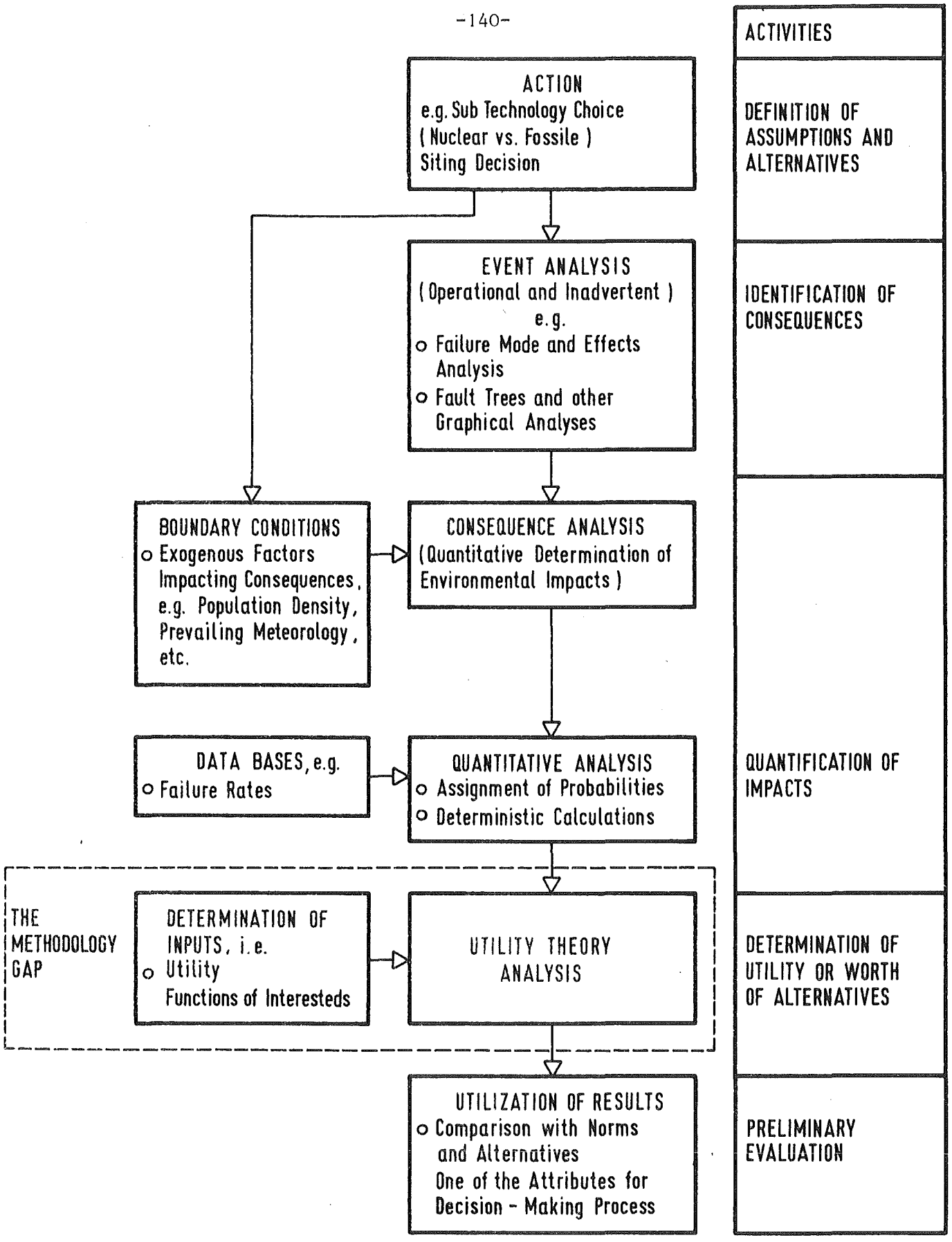

FIG. XIII.1 ILLUSTRATIVE FLOW CHART : RISK ANALYSIS

Shortcomings of present methodology

The most notable attempt to bridge the "methodology gap" has been made by Chauncey Starr (see for example Starr /13,14,15/). Starr's basic methodology involves a comparison of expected risks versus expected benefits for various voluntary activities -- like driving a car -- and involuntary ones -- like having a nuclear power plant located near your home. Measures of benefit are monetary. An example is the monetary value of the time saved by driving a car rather than using public transportation. Measures of risk are expected or average number of deaths per million population per hour of exposure to the risk. For example:

> "The estimate of the risk associated with the use of electric power is based on the (expected) number of deaths from electric current; the (expected) number of deaths from fires caused by electricity; the (expected) number of deaths that occur in coal mining, weighted by the percentage of total coal production used to produce electricity; and the (expected) number of deaths attributable to air pollution from fossil fuel stations." /13/

The results of Starr's work are shown in the frequently published curve, here reproduced as Figure XIII.2. With this curve he proposed that

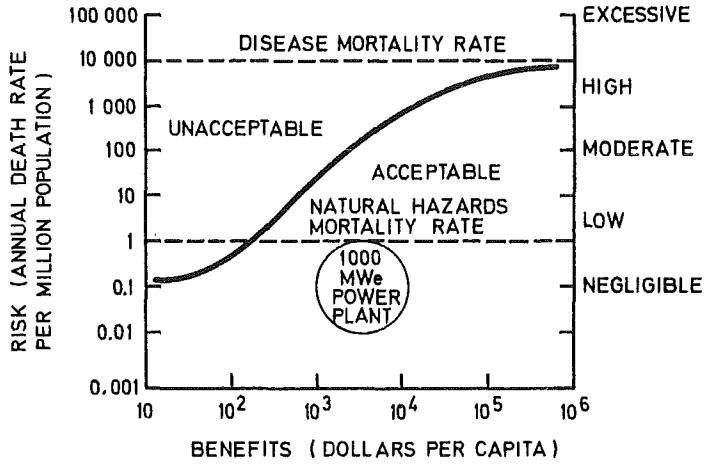

Fig. XIII.2 Benefit-risk Pattern for Involuntary Exposure

if the expected health hazard of a power plant as calculated for example by Otway (cf. Starr /15/), was below the curve, then the power plant is ... "within the socially acceptable range of risk". A comparison of the health hazards of fossil power plants with those of nuclear plants (see Starr, et. al./16/) , for example shows that the expected health hazard associated with nuclear power plants is less. Both types of plants were, however, in the range of public risks "...due to other activities of man which have general societal acceptance." Does this comparison truly imply that nuclear power is to be preferred in this particular attribute? How should the very small probability of a large scale disaster with a nuclear power plant be weighed?

As an illustration of the problem here, suppose that we were considering two alternative power plants. System A is characterized by a 50% chance of six deaths and a 50% chance of zero deaths. The expected number of deaths is three. System B has a 10^{-5} chance of three hundred thousand deaths; the expected number of deaths is also three. Based on mortality risks only, would most people be indifferent to alternatives A and B? Probably not; therein lies the failure of the expected value measure.

This point is born out in the ongoing emergency core-cooling systems (ECCS) controversy. For example, Hausknecht and Erdmann /17/ showed that the results for the annual average risk of the Starr et. al./16/ report were negligibly influenced by assuming an ineffective ECCS. Yet, the Union of Concerned Scientists, a Cambridge, Massachusetts, based coalition of scientists, will probably not be satisfied with anything short of full-scale demonstration of the effectiveness of an emergency core-cooling system.

One of the early pioneers in reactor risk analysis, F.R. Farmer, recognized that risks of the same average number of fatalities may be incommensurate. For example, Farmer/18/ states that parallel lines of equal slope-1 on a plot of accident probability/curies release join points of equal risk in terms of curies released per year, although "....it may not represent an equal risk of casualties. Furthermore, it is likely that most people would apply a relatively heavier penalty against the possibility of a large release than a small release."

He proposed an acceptable-risk criterion as a line on the probability-release curve of greater negative slope, namely a slope of -1.5 to reduce by three orders of magnitude the frequency of an event whose severity increases by two orders of magnitude. We agree, in principle, with Farmer's observations but contend that this problem can be solved by a mathematical approach termed "utility theory".

The meaning and application of Utility Theory

Utility theory is a mathematical theory in which we attempt to measure people's attitudes or preferences toward multiple objectives (e.g., improving quality of air and providing needed increase in electrical power) by means of numerical utility functions. As it is probably relatively safe to assume that utility functions are not widely known in the nuclear field we shall illustrate the meaning and use of utility functions below for a problem involving money, rather than fatalities. This digression will allow a clearer explanation of concepts and theory.

Suppose that you are offered a choice between two alternatives, A and B. If you select Alternative A, you receive $100,000, tax-free. Alternative B, on the other hand, offers a 50% chance of receiving $200,000 tax-free and a 50% chance of receiving nothing. Even though both alternatives have identical expected values of $100,000, most individuals would not be indifferent between the alternatives; they would select "A". Thus, in this instance, expected monetary value (EMV) would not be a good predictor of many individuals' preferences for the two alternatives.

In order to determine a given individual's actual indifference point, the amount received under Alternative A would be varied (downward, if the individual is risk adverse) until the individual was indifferent to the alternatives. Imagine, for example, that the individual was indifferent between A and B, if A would return $40,000 tax-free. (The returns on B are the same as before.) In effect, then, $40,000 is the price that the individual would accept in return for Alternative B. The value $40,000 is called the "certainty monetary

Equivalent" or CME for Alternative B. By definition, the individual's expected utility is the same for a certain $40,000 and Alternative B. Stated another way, when an individual has no preference (is indifferent) among a set of alternatives, then the expected utilities of those alternatives are identical. In the present example:

$$U(40,000) = 0.5 \times U(200,000) + 0.5 \times U(o) \qquad (1)$$

where U(x) denotes the utility of an amount X.

The foregoing result represents one point on the individual's personal utility curve for money. To construct the curve itself, it is first necessary to define two reference points on the curve. The procedure is similar to assigning numerical values of temperature to the freezing and boiling points for water, the choice is arbitrary. Suppose that the following two points were chosen:

$$U(0) = o$$
$$U(200,000) = 100$$

These data are then substituted into Eq. (1), which is solved for U(40,000) as follows:

$$\begin{aligned} U(40,000) &= 0.5 \times U(200,000) + 0.5 \times U(o) \\ &= 0.5 \times 100 + 0.5 \times o \\ &= 50 \end{aligned}$$

Additional points on the curve would be found by determining the individual's preferences among other alternatives, such as the two shown below.

C: tax-free $10,000 with certainty
D: 50-50 chance at tax-free $40,000 or nothing

These kinds of procedures would be repeated until sufficient points had been obtained. The complete utility curve would then be drawn.

There are three general types of utility curves: concave (risk-averse), linear (EMVer), and convex (gambler). These are depicted in Figure XIII.3. Once an individual's utility curve has been

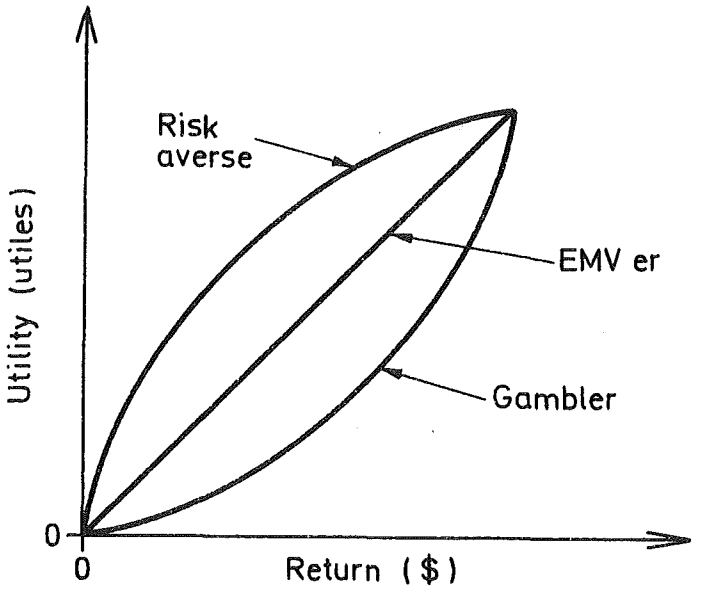

Fig.XIII.3 General Types of Utility Curves

constructed, it can be used to predict how he will act, if he is rational, or how he should act in order to be rational.

This method illustrated above for assessment of numerical utilities is called the standard gamble method. The method, by far the most widely used of the 24 known methods /19/ for assessing numerical utilities, is applicable to non-monetary as well as monetary attributes. Thus an individual's personal utility function for fatalities, air emissions, solid waste, or any other attribute can be assessed using the standard gamble method. This assessment is sometimes straightforward and sometimes not.

Ellis and Keeney /20/, and Keeney /21/ describe in detail the assessment of the utility functions of government officials for such attributes as air emissions (measured as daily sulfur dioxide concentrations), health effects (measured as the per capita decrease in

the number of days of bed disability per year), and mortality (fatalities). That work is a valuable precedent to applying Utility Theory to nuclear power decision problems.

To illustrate the application of utility theory suppose the utility function for the relevant interested parties for fatalities has been assessed using the standard gamble method. The utility curve could appear as shown in Figure XIII.4. A utility of zero has arbitrarily been assigned to the maximum possible number of fatalities. A utility of 100 utiles has been assigned to zero fatalities.

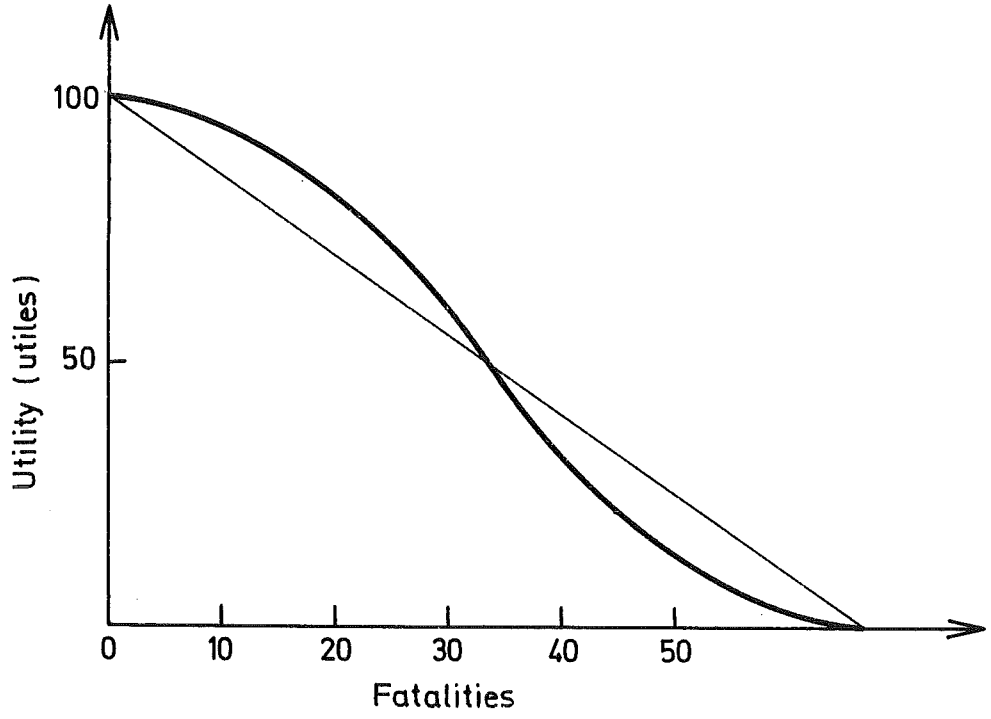

Fig. XIII.4 Hypothetical Utility Function for Fatalities

For a given case, the expected utility is computed from the utility function and the probability mass function of fatalities. More specifically, a mapping is made from the accident probability-fatality curve to utility and then integration is performed to find the expected utility. For example, suppose for a hypothetical power plant that

there are only three possible accidents, having respectively 10 fatalities from an accident with a probability of 10^{-4}, 20 fatalities with a probability of 10^{-5}, and 30 fatalities with a probability of 10^{-6}. The expected utility would be

$$E(U) = 10^{-4} \times U(10) + 10^{-5} \times U(20) + 10^{-6} \times U(30)$$

Reading the value of the utilities from Figure XIII.4,

$$E(U) = 10^{-4} \times 95 + 10^{-5} \times 76 + 10^{-6} \times 55$$

$$= 0.010315 \quad \text{(illustrative)}$$

The alternative with the highest expected utility would be preferred, in this particular attribute. It must be emphasized that the expected utility of an attribute of an alternative (nuclear or fossile) has no meaning by itself. It can only be used for the basis of relative comparison between two or more alternatives. But used in this manner the method incorporates automatically into the comparison people's attitudes or preferences.

It is, of course, the case that a comparison of different types of energy system alternatives can only be performed realistically when all relevant attributes are considered. Risk is only one attribute of many. Therefore, the comparison of two or more alternatives on the basis of risk is not conclusive. In addition, it is also necessary to consider the collection of activities, from extraction of raw materials to final power transmission, which are necessary to develop power. The problem of considering the full dimensionality of our energy system alternatives can also be treated by the application of utility theory, but in a slightly different manner, a good illustration of which is given by Turban and Metersky /22/. In our illustration we have only used utility theory for the treatment of variability.

Concluding Remarks

The sole purpose of the preceding example was to illustrate the concept and application of utility theory to risk evaluation of power plants. We firmly believe that utility theory can be utilized to

close the "methodology gap" in risk evaluation. There are, however, still some very important questions to be answered before the proposed method can be fully implemented. For example, a sampling of such questions would be the following:

(a) Whose utility function should be assessed?
(b) How can the utility function of several different interested parties be combined?
(c) For whose benefit is all this done?

It is our view that these issues can be resolved.

Literaturverzeichnis:

/1/ Krelle, W. "Präferenz und Entscheidungstheorie", Tübingen (1968)

/2/ Torgeson, W. "Theory and Methods of Scaling", New York (1967)

/3/ Raiffa, H. "Decision Analysis, Introductory Letters on Choices under Uncertainty, Massachusetts (1968)

/4/ Osgood, C. et.al. "The Measurement of Meaning"

/5/ Paweik, K. "Dimensionen des Verhaltens", Bonn (1971)

/6/ Jantsch, E. "Technological Forecasting in Perspective", Paris (1966)

/7/ Simon, H. "Models of Man", New York (1957)

/8/ Jardine, N. et.al. "Mathematical Taxonomy", New York (1971)

/9/ Green, P. et.al. "Multidimensional Scaling and Related Technologies in Marketing Analysis", New Jersey (1970)

/10/ Otway, H.J., et.al. "A Risk Analysis of the Omega West Reactor", Los Alamos Scientific Laboratory, LA-4449, March 1970

/11/ Otway, H.J. "The Application of Risk Allocation to Reactor Siting and Design", Los Alamos Scientific Laboratory, LA-4316, May, 1970

/12/ Otway, H.J. and R.C. Erdmann, "Reactor Siting and Design from a Risk Viewpoint", Nucl. Eng. Design 12, 1970

/13/ Starr, C., "Social Benefit vs. Technological Risk: What is Our Society Willing to Pay for Safety?", Science 165, 1232-38, 1969

/14/ Starr, C. "Benefit-Cost Relationships in Socia-Technical Systems", paper presented at Colloquium on Benefit-Risk Relationships for Decision-Making, Washington, D.C., April 26, 1971

/15/ Starr, C. "Benefit-Cost Relationships in Socio-Technical Systems", Proc. of a Symposium on Environmental Aspects of Nuclear Power Stations, IAEA New York, N.Y. 10-14

/16/ Starr, C., M.A. Greenfield, and D.F. Hausknecht, "A Comparison of Public Health Risks: Nuclear vs. Oil-fired Power Plants", Nuclear News, p. 37, October, 1972

/17/ Hausknecht, D.F. and R.C. Erdmann, "Comments on ECCS Risk", Letters to the Editor Nuclear News, p. 36, November, 1973

/18/ Farmer, F.R., "Reactor Safety and Siting: A Proposed Risk Criterion", Nuclear Safety, Vol. 8, No. 6, 539-548, Nov.-Dec., 1967

/19/ Fischburn, Peter C. "Methods of Estimating Additive Utilities", Management Science, 13, 435-453. (1967)

/20/ Ellis, Howard M. and Ralph L. Keeney, "A Rational Approach for Government Decisions Concerning Air Pollution", in Alvin W. Drake, et.al. (Eds.), Analysis of Public Systems, Cambridge, MIT Press, 376-400 (1972)

/21/ Keeney, Ralph L. "A Decision Analysis With Multiple Objectives: The Mexico City Airport", The Bell Journal of Economics and Management Science Vol. 4, No. 1, 101-117 (1973)

/22/ Turban, Efraim, and Morton L. Metersky, "Utility Theory Applied to Multivariable Systems Effectiveness Evaluation", Management Science 17, 817-828 (1971)

C. ZUSAMMENSTELLUNG DER BEACHTETEN VERÖFFENTLICHUNGEN

Ablitt, "An Introduction of the Syrel Reliability Data Bank"
SRS/GR/14

J.F. Ablitt, "A Quantitative Approach to the Evaluation of the Safety Function of Operators on Nuclear Reactors"
AHSB (S) R 160

Allis, Chalmers, Linearity of Nuclear Instruments and Proposed Revised Control Mode, LAC-4130, Docket 115-4, August 1, 1969.
Available at USAEC Public Document Room.

H.P. Balfanz, "Methoden zur Systemanalyse", Fortbildungsseminar der KTG "Statist. Methoden zur Beurteilung von Auslegung, Sicherheit und Verfügbarkeit von KKW" (Berlin, März 1974)

H.P. Balfanz, Sicherheitsanalyse-Plan (Anwendung verschiedener Sicherheits- und Zuverlässigkeitsanalysen zum richtigen Zeitpunkt und zu speziellen Problemen) IRS-W-2 (April 1972)

W. Bastl, Die Zuverlässigkeitsanalyse als Mittel zur Objektivierung der Beurteilung technischer Systeme
2. Informationstag des LRA, Januar 1974

W. Bastl, Reliability of Nuclear Plant
MRR 125, Juli 1973

W. Bastl, P. Kafka, Research and Development Activities in the Field of Reliability Analysis for Nuclear Power Plants.
IAEA, Panel of Experts on "Method of Assessment for Assuring Reliability of Nuclear Power Stations"
Wien, 28. Mai - 1. Juni 1973

W. Bastl, The Redundant Safety System and its Equipment
Internationale Studientage für Moderne Kraftwerke, Lüttich, Oktober 1974

W. Bastl, E. Nieckau, Zuverlässigkeitsuntersuchungen an elektronischen Geräten des Reaktorschutzsystems
LRA-Festschrift 1974

J.R. Beattie, "Risks to the Population and the Individual from Iodine Release", Symp. Containm. Siting of Nucl. Pow. Pl. (1967)

G.D. Bell, "Safety Criteria" Nucl. Eng. Des. 13 (1970)

J. Berkemann, Technokratie und verfassungsrechtliche Prinzipien, in: Technokratie als Ideologie, Verlag Kohlhammer (1973) S. 193

J. Blombach, W. Rosenhauer, H. Zeibig, Reliability Techniques Covering the Operational Conditions of Reactor Systems (Liverpool, 1974)

A.J. Bourne, A.E. Grenn, Techniques of Quantitative Reliability Analysis, Nucl. Eng. and Design 13 (1970) 1911 ff.

J.H. Bowen, Techniques of Consequence Assessment, Nucl. Eng. and Design, Vol. 13 (1970) 236

T.W.T. Burnett, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors. Westinghouse Electric Corporation, April 1969 (WCAP-7306)

S.H. Bush, Advisory Committee on Reactor Safeguards, to G.T. Seaborg, AEC, Dockets 50-352 and 50-353, August 10, 1971, Available at USAEC Public Document Room.

L. Caldarola, Cosiderations for a European Contralized Reliability Data Bank System
KFK 1928, October 1973

L. Caldarola, Considerations for a European Centralized Reliability Data Bank System, International Seminar on Reliability Data Banks - Stockholm, October 1973, FTLA-Report, A 16: 41 (Nov. 1973)

L. Caldarola, "New Definition of Reliability, Continuous Lifetime Prediction and Learning Processes", Nato Conference on Reliability, Liverpool July 1973 and KFK 1847

L. Cave, "Safety Evaulation Probability Methods for GCR's" Nuclear Engineering 13 (149), October 1968

A.G. Colombo, G. Volta, Mutlistep Reliability Analysis and Optimization of Complex Systems, paper presented at the CNSI-Specialist Meeting on: The Development and Application of Reliability Techniques to Nuclear Plants (Liverpool, 8-10 April 1974)

W.C. Coppersmith, C.L. Kling, A.T. Shosler, B.M. Tashjian, Reactor Protection System Diversity, Combustion Engineering, Inc., February 1971 (CENPD-11)

Cornell "Bayesian Statistical Decision Theory and Reliability-Based Design" International Conference on Structural Safety and Reliability, Washington D.C., (April 1969) Pergamon Press 1972

E.L. Crow, R.S. Gardner "Confidence Intervals for the Expectation of a Poisson Variable", Biometrika, 46, 1959

E. Dressler, P. Kafka, Considerations on the influence of mechanical components on the reliability of nuclear power plant systems
Paper to be presented at the 2nd Conference on Structural Mechanics in Reactor Technology, Berlin 10. - 14.7.1973

E. Dressler, Eine neue Methode zur näherungsweisen Berechnung der Zuverlässigkeit und Verfügbarkeit von Reaktorsystemen
Kerntechnik, Heft 12, 1972, S. 574 - 581

E. Dressler, H. Spindler, Einfluß der Reparaturzeit von Sicherheitssystemen auf das mit Reaktorstörfällen verbundene Risiko
Veröffentlichung in Vorbereitung

E. Dressler, Mathematische Grundlagen der Zuverlässigkeitstechnik
KTG-Fachseminar, Berlin, März 1974

E. Dressler, Programme zur Berechnung der Zuverlässigkeit von Reaktorsystemen, MRR 93, November 1971

E. Dressler, H. Spindler, Verbesserung der Verfügbarkeit von Sicherheitssystemen durch zeitlich gestaffelte Prüfungen
atw, März 1974

Z. Doron, H. Albers, "An Extension of the Quantitative Probability Approach", Nucl. Eng. Des. 9 (März 1969)

S.J. Ditto, "Effect of Operating Experience on Safety-System Design", Nuclear Safety 6 (2), Winter 1964-1965

S.J. Ditto, "Redundancy and Coincidence in Reactor Safety Systems", Nuclear Safety 2 (4), June, 1961

Ellis, Howard M., Ralph L. Keeney, "A Rational Approach for Government Decisions Concerning Air Pollution", in Alvin W. Drake, et.al. (Eds.), Analysis of Public Systems, Cambridge, MIT Press, 376-400 (1972)

E.P. Epler, "Common Mode Failure Considerations in the Design of Systems for Protection and Control, " Nuclear Safety 10 (1), January-February 1969

E.P. Epler, "Dangers in Safety Systems", IRE Transactions on Nuclear Science, NS-8(4), October, 1961

E.P. Epler, "HTRE-3 Excursion, " Nuclear Safety 1(2), December, 1959

E.P. Epler, "Safety-System Reliability vs. Performance, " Nuclear Safety 6 (4), Summer, 1965

E.P. Epler, "The ORR Emergency Cooling Failure," Nuclear Safety 11(4), July-August, 1970

R. Erdmann, W. Kastenberg, M. Meleis, "The Development of Siting Criteria for Nucl. Power Plants", Project Clean Air, UCLA (Aug. 1970)

F.R. Farmer, Letter to the Editor, Nuclear Safety 10(4), July-August 1969

F.R. Farmer, "Reactor Safety and Siting: A Proposed Risk Criterion", Nuclear Safety, Vol. 8, No. 6, 539-548, Nov.-Dec., 1967

F.R. Farmer, Siting Criteria - A New Approach, Symp. on Containment and Siting of Nucl. Power Plants, Wien (1967)

P.C. Fischburn, "Methods of Estimating Additive Utilities", Management Science, 13, 435-453 (1967)

Fothergill "The Analysis and Presentation of Derived Reliability Data from a Computerized Data Store" Seminar on Reliability Data Banks, Stockholm, (October 1973), FTLA-Report, A 16: 41 (Nov. 1973)

L.G.Frederick, An Analysis of Functional Common-Mode Failures in GE BWR Protection and Control Instrumentation, General Electric Company, July, 1970 (NEDO-10189)

Freudenthal "Intorductory Remarks to the International Conference on Structural Safety and Reliability", Washington D.C., (April 1969)- Pergamon Press 1972

J.B. Fussell, A Formal Methodology for Fault Tree Constructions, Nuclear Science and Engineering 52, p. 421 - 432 (1973)

J.B. Fussell, G.J. Powers, R.G. Bennetts, Fault Trees - A State of the Art Discussion, IEEE-Trans. on Reliability R-23, p. 51-55 (April 1974)

J.B. Fussell, Special Techniques for Fault Tree Analysis Aerojet Nuclear Company, National Reactor Testing Station, Idaho Falls, March 1974

J.B. Fussell, Synthetic Tree Model - A Formal Methodology for Fault Tree Construction
Aerojet Nuclear Company, National Reactor Testing Station, Idaho Falls, ANCR 1098 (March 1973)

G.R. Fallagher, "Failure of N Reactor Primary Scram System," Nuclear Safety 12(6), November-December 1971

W.C. Gangloff, An Evaluation of Anticipated Operational Transients in Westinghouse Pressurized Water Reactors, Westinghouse Electric Corporation Mai, 1971 (WCAP-7486)

Gangloff, Loftus, "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients", Westinghouse Electric Corporation - WCAP - 7706, July 1971

Gangloff, "Probability Investigations into Anticipated Transients Without TRIP" ASME Winter Annual Meeting, Detroit, Michigan, USA, November 1973

N.R. Garner, J.A. Huetinck, Equipment Aging Analysis, An Extension to Reliability, Symp. Reliability of Operation in the Process Industries, San Juan (Mai 1970)

Garrick, Gegker, Pomrehn, "Some Aspects of Protective Systems in Nuclear Power Plants", IEEE Trans. Nucl. Sci. NS-12 (16): 22-30 (Dec. 1965)

B.J. Garrick, Principles of Unified Systems Safety Analysis, Nucl. Eng. and Design, Vol. 13 (1970), No. 2

Gnedenko, Belajajew, Solowjew, Mathematische Methoden der Zuverlässigkeits-theorie II", Akademie Verlag, Berlin 1968 (Kap. 5)

S. Großner, L. Weil, A Reliability Analysis of the Safety Shut-Down-System of Nuclear Reactor
CSNI Specialist Meeting, Liverpool 8th - 10th April 1974

S. Großner, Experimentelle Bestimmung des Betriebs- und Ausfallverhaltens einer Taktüberwachungseinheit, MRR 130, August 1973

S. Großner, Experimentelle Bestimmung des Betriebs- und Ausfallverhaltens eines Trennverstärkers, MRR 129, August 1973

S. Großner, Zuverlässigkeitsuntersuchungen an elektronischen Bausteinen
2. Informationstag des LRA, Januar 1974

P. Green, et al., "Multidimensional Scaling and Related Technologies in Marketing Analysis", New Jersey (1970)

W. Häfele, "Die Kernenergie in der technischen Welt der Zukunft", Nuclear Inter-Jura 1973, Karlsruhe

W. Häfele, Seminar über Zuverlässigkeitskontrolle, Kernforschungszentrum Karlsruhe (1972)

S.H. Hanauer, Advisory Committee on Reactor Safeguards, to G.T. Seeborg, AEC, Docekt 50-321, Mai 15, 1969, Available at USAEC Public Document Room.

S.H. Hanauer, C.S. Walker, Design Principles of Reactor Protection Instrument Systems, USAEC Report ORNL-NSIC-51, Sept. 1968

D.F. Hausknecht, R.C. Erdmann, "Comments on ECCS Risk", Letter to the Editor Nuclear News, P. 36, November 1973

F.W. Heuser, P. Kafka., "Möglichkeiten und Grenzen der quantitativen Sicherheitsbeurteilung", KTG-Seminar, Berlin (März 1974)

F.W. Heuer, W. Rosenhauer, Projektbezogene Anwendung von Zuverlässigkeitsmethoden, 1 und 2. Teil in KFK 1811, Einführung in Methoden und Probleme der Zuverlässigkeit, G. W. (Januar 1974)

H. Hörtner, Die Versagensmöglichkeiten von Armaturen und deren Berücksichtigung in Fehlerbaumanalysen
MRR 109, Dezember 1972

H. Hörtner, P. Kafka, Forschungsvorschlag zur Erarbeitung quantitativer Methoden der Sicherheitsbeurteilung von Kernkraftwerken
MRR - I - 4, Februar 1973

H. Hörtner, B. Wohak, Gewinnung von Zuverlässigkeitsdaten aus Betriebserfahrungen, KTG-Fachseminar, Berlin, März 1974

H. Hörtner, Probleme der Zuverlässigkeitsanalyse in der Kernkraftwerkstechnik
2. Informationstag des LRA, Januar 1974

H. Hörtner, W. Bastl, Reliability Analysis of a PWR-Emergency Core Cooling System, CREST-Meeting on Complex Systems and Nuclear Plants, München (Mai 1971)

H. Hörtner, E. Dressler, E. Nieckau, H. Spindler, Reliability Investigation of the Reactor Safety System Used to Control a Loss-of-Coolant Accident SCNI Specialist Meeting, Liverpool, 8th - 10th April 1974

H. Hörtner, P. Kafka, Sicherheitsanalysen für Kernkraftwerke, LRA-Festschrift 1974

I.M. Jacobs, "Safety-System Design Technology", Nuclear Safety ((3), Spring, 1965

Jacobs, "The common mode failure study discipline" IEEE Trans. on Nuclear Science, 17 (1) pages 594 - 598, February 1970

Jantsch, E., "Technological Forecasting in Perspective", Paris (1966)

N. Jardine, et al., "Mathematical Taxonomy", New York (1971)

I. Jaschke, Methods for Determining and Improving the Reliability of Electrical Supply Systems, 1968 CREST-Meeting on Electrical Supply Systems (EUR 4517 e)

W.E. Jordan, Failure Modes, Effects and Criticality Analysis, Proc. 1972 Ann. Symp. on Reliability and Maintainability, p. 30-37

P. Kafka, Ausgewählte Bearbeitungsschwerpunkte auf dem Gebiet der Sicherheit von Kernkraftwerken
Vortrag, Seminar der Frauenhofer-Gesellschaft, Februar 1974

P. Kafka, Die Störfallanalyse als Grundlage zur Abschätzung und Festlegung der sicherheitstechnischen Bezugsgrößen Kernkraftwerk - Umwelt
Vortrag Reaktortagung 1973, Karlsruhe 10 - 13. April

P. Kafka, Fortschritte in der Technischen Systemanalyse am LRA, Informationstag des LRA, Juni 1972

P. Kafka, Grenzkriterien zur Auslegung von Kernkraftwerken, KTG-Fachseminar, Berlin, März 1974

P. Kafka, Rahmenprogramm für die Entwicklung von quantitativen Methoden zur Sicherheitsbeurteilung von Kernkraftwerken, MRR - I - 16, März 1974

P. Kafka,
Störfallanalyse zur Abschätzung und Beurteilung des Eintrittes und des Ausmasses von Störfällen an einem Druckwasserreaktor vom Typ Biblis
Interner Zwischenbericht, Juli 1972

W. Kargl, Untersuchung über die Erstellung eines Programmsystems zur Speicherung und Auswertung von Daten des RWE-Modellfalls.
MRR-I-1, April 1973

R.L. Keeney, "A Decision Analysis With Multiple Objectives: The Mexico City Airport", The Bell Journal of Economics and Management Science, Vol. 4, No. 1, 101-117 (1973)

O. Kellermann, "Unfallanalyse in der Kerntechnik", IRS-TÜ 13 (1972)

O. Knecht, H. Keil, Graphische Analyse von Reaktorstörfällen
Atom und Strom, Folge 7/8, Juli/August 1968

B.V. Koen, Carnino, A., Reliability Calculations with a List Processing Technique, IEEE-Trans. on Reliability R-23, p. 43-50 (April 1974)

W. Krelle, "Präferenz und Entscheidungstheorie", Tübingen (1968)

G.C. Laurence, "Reactor Safety in Canada", Nucleonics, 18(10), October, 1960

H. Lurz, Optimierung zweier Simulationsprogramme zur Berechnung der Systemzuverlässigkeit, T.U.M. Diplomarbeit, 13.9.1973

P. McGrath, R. Papp (GfK), D. Maxim, F. Cook (Mathematica Inc.), "A New Concept in Risk Analysis of Nuclear Facilities", Nuclear News, 17 (Nov. 1974)

P.E. McGrath, Radioactive Waste Management: Potentials and Hazards from a Risk Point of View
Kernforschungszentrum Karlsruhe, KFK-1992 (1974)

M. Meleis, R. Erdmann, "The Development of Reactor Siting, Criteria Based upon Risk Probability", Nucl. Safety, Vol. 13, 1 (Jan. Febr. 1972)

L. Merz, "Philosophie des Reaktorschutzes. Determinist. und probabilist. Thesen zur Reaktorsicherheit", Atomwirtschaft (März 1970)

L.A. Michelotti, Analysis of Anticipated Transients without Scrams, General Electric Company, March, 1971 (NEDO-10349)

K.B. Misra , An Impoved Algorithm for System Reliability Optimization with Mixed Redundancy
CSNI Specialist Meeting, Liverpool 8th - 10th April 1974

K.B. Misra, Reliability Optimation of a System with Mixed Redundancies
MRR 132, Oktober 1973

V.A. Moore, Jr., S.H. Hanauer, "Status of Power Reactor Control and Instrumentation in the United States", First Meeting of the International Atomic Energy Agency Working Group on Nuclear Power Plant Control, March 15-19, 1971

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 Ann. Symp. on Reliability and Maintainability, San Francisco, 1972, p. 565-577

E. Nieckau, Abschätzung der Zuverlässigkeit von Steuerketten der Betätigungsebene, MRR 121, April 1973

E. Nieckau, Abschätzung der Zuverlässigkeit von Bausteinen der Meßwert- und Signalverarbeitung von Reaktorschutzsystemen, MRR-I-3, Februar 1973

E. Nieckau, Zuverlässigkeitsbestimmung von elektronischen Bausteinen mit mehreren gleichzeitig ansteuerbaren digitalen Eingängen, Tagung 1973 "Technische Zuverlässigkeit", Nürnberg, 23. - 25. Mai

D.S. Nielsen, The Cause Consequence Method as a Basis for Quantitative Accident Analysis, Report Risö-M-1374 (1971)

D.S. Nielson, Practical Experience with Quantitative Reliability Methods as Decision Help (paper presented at the SRS-annual Meeting 1973)

D.S. Nielson, O. Platz, B. Runge, Probabilistic Evaluation of a Redundant Protection System Based on a Cause-Consequence Diagram, Danish Atomic Energy Commission (to be published)

C. Offe, Das politische Dilemma der Technokratie, in: Texte zur Technokratiediskussion, Euroäische Verlagsanstalt (1970), S. 156

O'Neil, Jordan "Safety and Reliability Requirements for Periodic Inspections of Pressure Vessels in the Nuclear Industry" I Mech E (1970)

C. Osgood, et al., "The Measurement of Meaning"

Otway and others, "A Risk Estimated for an Urban-Sited Reactor" Nuclear Technology, Vol. 12, October 1971

H. Otway et al., "A Risk-Analysis of the Omega West Reactor, LA-4449, Los Alamos (July 1970)

H. Otway, "The Application of Risk Allocation to Reactor Siting and Design", LA-4316, Los Alamos Scient. Laboratory (June 1969)

H. Otway, R.C. Erdmann, "Reactor Siting and Design from a Risk Viewpoint", Nucl. Eng. Design 12, 1970

H. Otway, "Risk vs. Benefit: Solution or Dream", Los Alamos, LA-4860 (Nov. 1971)

D.F. Paddleford, Analysis of Public Safety Risks Associated with Uncontained Fission Product Release from a 1000 MWe Nuclear Power Plant, paper presented at the CSNI-Specialist Meeting, (Liverpool, 1974)

F. Pasquill, "The Meteorological Magazine", Vol.90, 1063 (Febr. 1961)

K. Paweik, "Dimensionen des Verhaltens", Bonn (1971)

A. Perlis, Computers, 1973, Britannica Yearbook of Science and the Future

H. Piper, "Siting Practice and Its Relation to Population", Nucl. Safety Vol. 14, No. 6 (Nov. - Dec. 1973)

C.A. Phillips, R.G. Warwick, " A Survey of Defects in Pressure Vessels Built to High Standards of Construction and its Relevance to Nucl. Primary Circuit Envelopes" AHSB (S) R 162 (1968)

Powers, Tompkins, Fault Tree Synthesis for Chemical Processes AI ChE Journal Vol. 20, p. 376-387 (March 1974)

H. Raiffa, "Decision Analysis, Introductory Letters on Choices under Uncertainty, Massachusetts (1968)

N. Rasmussen, "The Approach of the United States Atomic Energy Commission Study to be Public Risks of Power Reactors", The Nuclear Controversy in the USA II, Mai 1974, Luzern

N. Rasmussen, Reactor Safety Study an Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH 1400 (Draft), USAEC, August 1974

Th. L. Regulinski, Human Performance Reliability Modelling in the Time Continuous Domain

Richards "Technology Transfer through GIDEP" Annual Reliability and Maintainability Symposium of the IEEE, Los Angeles (January 1974)

Richards and Dahl "The New Approache to Reliability Data Exchange" Nato Conference on Reliability Testing and Reliability Evaluation, The Hague (Sept. 1972)

Richardson J., "Comparison of U.K. and U.S. Requirements for Safety and Siting of Nuclear Power Plants", Nucl. Engin. International (Nov. 1973)

G. Richter, G. Memmert, Berechnung von Zuverlässigkeitsdaten komplexer Systeme mit analytischen Methoden, Institut für Kerntechnik der TU Berlin, Oktober 1973, Bericht TUBIK 28

R. Salvatori, Manager, Licensing Engineering, Westinghouse Electric Corporation, to P.A. Morris, Director of Reactor Licensing, May 21, 1971 (E-L-215)

R.L. Scott, Jr., "A Review of Safety Relate Occurrences in Nuclear Power Reaktors from 1967-1970, " USAEC report ORNL-TM-3435, Mai 26, 1971

R.L. Scott, Safety-Related Occurrences in Nuclear Facilities as Reported in 1969, USAEC Report ORNL-NSIC-87, August 1971

E. Siddall, "Reliability of Reactor Control Systems," Nuclear Safety 4(4), June, 1963

E. Siddall, "Reliable Reactor Protection", Nucleonics 15 (6), June, 1957

H. Simon, "Models of Man", New York (1957)

D. Smidt, "Das Lebensrisiko verringern", Die Zeit (8.6.1973)

H. Spindler, Zuverlässigkeitsuntersuchung der Gleichstromversorgung eines Kernkraftwerkes am Beispiel des KW-Biblis, Block A, MRR-I-18, März 1974

A.D. Swain, Human Reliability Assessment in Nuclear Reactor Plants, SC-R-69 1236

A.D. Swain, Shortcuts in Human Reliability Analysis SLA-73-5530, Proc. of the Nato Advances Study Institute on Genoric Techniques in Systems Reliability Assessment, University of Liverpool, July 1973

H. Schelsky, Der Mensch in der wissenschaftlichen Zivilisation, in: Auf der Suche nach Wirklichkeit, Verlag Dietrichs, (1961), S. 439

C. Starr "Benefit-Cost Relationships in Socia-Technical Systems", paper presented at Colloquium on Benefit-Risk Relationships for Decision-Making, Washington, D.C., April 26, 1971

C. Starr, "Benefit-Cost Studies in Scio-Technical Systems", paper presented at Colloquium on Benefit-Risk Relationship for Decision-Making, Wash., D.C. (April 1971)

C. Starr, "Sicial Benefit vs. Technological Risk: What is Our Society Willing to Pay for Safety?", Science 165, 1232-38, 1969

C. Starr, M.A. Greenfield, D.F. Hausknecht, "A Comparison of Public Health Risks: Nuclear vs. Oil-fired Power Plants", Nuclear News, p. 37, October, 1972

H. Stute, Auslegung von Reaktorschutzsystemen, TÜ 14 Nr. 2 (1973) 86

J. Tattersall, et al., "A Discussion of Nucl. Plant Safety with Reference to Hazards Experienced by the Community", Genfer Konferenz (1971) A. Conf. 49 P 671

J.R. Taylor, A Formalization of Failure Mode Analysis, Report Risö-M-1654 (1973)

J.R. Taylor, A Semiautomatic Method for Qualitative Failure Mode Analysis, paper presented at the CSNI-Specialist Meeting on: The Development and Application of Reliability Techniques to Nuclear Plants (Liverpool, 8-10 April 1974)

W. Torgeson, "Theory and Methods of Scaling", New York (1967)

D.R. Towill, Recent Developments in the Prediction of Human Operator Performance

E. Turban, M.L. Metersky, "Utility Theory Applied to Multivariable Systems Effectiveness Evaluation", Management Science 17, 817-828 (1971)

H. Uchida, "Safety, Environment and Licensing Problems of Nucl. Power Plants in Japan", Nucl. Engin. International (July 1973)

Vesely, A Time Dependent Methodology for Fault Tree Evaluation Nucl. Eng. and Design, Vol. 13 (1970), No. 2

Volta et al., "Cumulative Damage Stochastic Models and Distribution of Strength of Steels and Graphite", NATO-Conference on Reliability Data Banks - Stockholm (October 1973), FTLA-Report, A 16:41, (Nov. 1973)

G.G. Weber, State of Reliability Effort in Europe (review for the Special Issue of IEEE Trans. on Reliability, Vol. R-23, August 1974)

L. Weil, Experimentelle Zuverlässigkeitsuntersuchungen an Komponenten neuzeitlicher Schutzsysteme, Tagung über Regelung und Instrumentierung von Kernkraftwerken, Brüssel, März 1972

L. Weil. Zuverlässigkeitsuntersuchungen am Trennverstärker eines Reaktorschutzsystems, MRR 120, März 1973

L. Weil, E. Dressler, Zuverlässigkeitsuntersuchung der Energieversorgung für die Sicherheitseinspeisepumpen des Kernkraftwerks Obrigheim, MRR-V-1, März 1973

L. Weil, Über die Zuverlässigkeit elektronischer Reaktorschutzkomponenten modernster Schaltungstechnik, Kerntechnik, Heft 11, 1972, S. 540

Wiliams, "Common mode failures in US commercial power reactors", Thesis, University of Tennessee, June 1972

Wilson "Estimating Pipe Reliability by the Distribution of Time to Damage Methods" GEAP 10452 (March 1972)

B. Wohak, W. Kargl, Ein Informationssystem zur Gewinnung von Zuverlässigkeitsdaten für Kernkraftwerkskomponenten,
2. Informationstag des LRA, Januar 1974

B. Wohak, H. Hörtner, Establishment of Reliability Data for Power Plant Components by Means of an Information System, Eingereicht bei den IEEE-Transactions on Reliability, Dezember 1973

C.W. Zabel, Advisory Committee on Reactor Safeguards, to G.T. Seaborg, AEC, Docket 50-272, June 21, 1968, Available at USAEC Public Document Room.

Barnwell Nuclear Fuel Plant, Environmental Report U.S. Atomic Energy Commission, DOCKET 50-332-27 (1972)

"Der Brookhaven-Bericht", WASH-740, IRS-TÜ 2 (1973)

Nordic Working Group on Reactor Safety, Cause-Consequence Diagrams, A Graphic Method for Description and Analysis of Failure Sequences in Complex Process Systems,NARS Publication 2 (December 1972)

Commercial Nuclear Power Plants, Southern Nuclear Engineering, Inc. October, 1971

"Consequences of Major Accidents in Large Nucl. Power Plants", Report WASH 740 USAEC, Wash. D.C. (1957)

Consolidated Edison Company of New York, to Division of Compliance (AEC), Flux Flow Computer Causes Automatic Reactor Trips When Spurious Signals Occur, Docket 50-3 Indian Point 1, September 3, 1969, Available at USAEC Public Document Room.

"Controversy Unabated; Safety Report Anticipated", Nucl. News (Mid. Febr. 1974)

Supplementary Criteria und Requirements for RDT Reactor Plant Protection Systems, Division of Reactor Development and Technology, United States Atomic Energy Commission, December, 1969 (RDT C 16-1T)

Criteria for Protection Systems for Nuclear Power Generating Stations", The Institute of Electrical and Electronics Engineers, Inc., 1971 (IEEE Standard 279).

Dairyland Power Cooperative, to Division of Reactor Licensing (AEC), LACBWR Reactor Water-Level Instrumentation, Docket 115-5, April 7, 1970, Available at USAEC Public Document Room.

Environmental Radiation Dose Commitment, An Application to the Nuclear Power Industry, U.S. Environmental Protection Agency, EPA-520/4-73-002 (1974)

"Evaluation of Risks from Radiation", ICRP Com No. 1,
ECRP-Publ. 8, Pergamon Press (1966)

Federal Register

Fehlerbaumanalyse - Erläuterungen und Anwendungen, DIN 25 424
(Beide Fachnormenausschuß Kerntechnik, FNKe 3.3)

General Electric Company, to Director of Reactor Licensing (AEC),
Safety-System Relays, Docket 50-263 Monticello, July 29, 1970.
Available at USAEC Public Document Room.

General Principles for Reliability Analysis of Nuclear Power
Generating Station Protection Systems, IEEE Standards Committee,
IEEE Trial-Use Guide, IEEE Std. 352 (1972)

"Guide to the Application of the Single Failure Criteria to Nuclear
Power Generating Station Protection Systems (Draft Seven), IEEE
Joint Committee on Nuclear Power Standards, April 19, 1971.

Description of Human Factors Reports by Sandia Laboratories

Proceedings of the Conference Management of Radioactive Wastes from
Fuel Reprocessing, OCED/IAEA, Paris, Dec. 1972

The Role of the Man-Machine Interface in Systems Reliability

"Nuclear Safety: Calculating the Odds of Disaster"
Science 185 (Sept. 1974)

Operating Experiences, USAEC, Division of Reactor Licensing,
Reactor Safety Bulletins.

Pacific Gas and Electric Company, Humbolt Bay Unit No. 3 Operations Report,
Docket 50-133, February 19, 1969. Available at USAEC Public Document
Room.

Pacific Gas and Electric Company to Division of Reactor Licensing (AEC),
Forced Shutdown at Humbolt Bay Unit 3 and Level Indication Leak, Docket 50-133,
October 2, 1970. Available at USAEC Public Document Room.

Ablauf von Planung, Bau und Inbetriebnahme des KKW,
Atomwirtschaft 17 Nr. 2 (1972), 98

Quantitative Safety Analysis, Staff on the Safeguards Division, AHSB, UKAEA,
Nucl. Eng. and Design 13 (1970) 183-244

Recommendations of the International Commission on Radiological
Protection, Publication 2 (1959)

"Report on the Integrity of Reactor Vessels for Light-Water-Power
Reactors". WASH-1285 (January 1974)

"Results of Interviews with Proponents and Opponents of Nuclear
Power in the USA" Report of the Company "Bedaux-Mathematica"
(Dec. 1973) (priv. comm).

The Safety of Nuclear Power Reactors and Related Facilities U.S.
Atomic Energy Commission, WASH-1250 (1973)

Siting of Fuel Reprocessing Plants and Waste Management Facilities
Compiled and Edited by the Staff of the Oak Ridge National
Laboratory, ORNL-4451 (1970)

Systematic Failure Study of Reactor Protection Systems. Babcock and
Wilcox Company, September, 1970 (BAW-10019)

Der Störfall im Kernkraftwerk Würgassen, Atomwirtschaft 18 Nr. 12 (1973) 584

Störfallablaufanalyse DIN 25 419, Blatt 1 (November 1973)
(früher: Graphische Darstellung von Störfallabläufen)

Weapon System Safety Analysis Requirements, Deptmt. of the Air Force,
Space and Missile Systems Organization, Air Force Systems Command, 1968

"Wiederfelser Entwurf", Neugestaltung des Genehmigungsverfahrens im Umwelt-
schutz, Evang. Akademie Baden (Febr. 1973)