H. Hirsch, T. Einfalt, O. Schumacher, G. Thompson

IAEA SAFETY TARGETS AND PROBABILISTIC RISK ASSESSMENT

State of the Art, Merits and Shortcomings of Probabilistic Risk Assessment

Report prepared for Greenpeace International, August 1989
by Gesellschaft für Ökologische Forschung und Beratung mbH, Hannover

The Authors

Dr. Helmut Hirsch (Principal Investigator), Gesellschaft für ökologische Forschung und Beratung mbH, Hanover

Dr Thomas Einfalt, Gesellschaft für ökologische Forschung und Beratung mbH, Hanover

Dipl.Phys. Otfried Schumacher, Forschungsbüro Kollert & Donderer, Bremen

Dr Gordon Thompson, Institute for Resource and Security Studies, Cambridge, Mass.

With Contributions from:
Dr Ilse Tweer, Buxtehude,
Prof. Dr. Eckhard Gimmel, University of Hamburg
MHB Technical Associates, San Jose, Ca.

This report is printed on unbleached recycled paper

Contents

PREFACE:

This report was prepared for GREENPEACE International. The work was started in October 1988, and concluded in June 1989. The overall planning and coordination of this study was performed by the chief contractor, the Gesellschaft fur okologische Forschung und Beratung mbH, Hanover, Federal Republic of Germany.

The main body of the report consists of 17 sections, addressing the most important problems of PRA. The sections are grouped into 5 parts: An introductory part; topics concerning level I of PRA (events leading to core damage); topics concerning level II of PRA (containment behaviour); topics relevant for both level I and II; and topics concerning what we have called the "real world"- level.

Each section consists of introduction and summary of main problems, followed by a detailed background discussion.

Overall responsibility for the content of this report rests with the four authors.

The authors would like to express their gratitude to all those who have contributed to this study by providing information and background material, or by conducting various tasks which were vital for the completion of the report. In particular, we wish to thank Lutz Gärtner, Hannover; Lothar Hahn, Wiesbaden; Patricia Huntington, Cambridge/Mass.; Björn Kjellström, Trosa; John Large, London; Steve Sholly, San Jose/Ca.; the Commissariat l'Energie Atomique, Institut de Protection et de SuretéNucléaire, Fontenay- aux-Roses; the Groupement des Scientifiques pour l'Information sur l'Energie Nuclaire, Orsay; and the International Atomic Energy Agency, Division of Nuclear Safety, Vienna.

Helmut Hirsch
Hannover, June 10, 1989

H. Hirsch, T. Einfalt, O. Schumacher, G. Thompson

IAEA SAFETY TARGETS AND PROBABILISTIC RISK ASSESSMENT

State of the Art, Merits and Shortcomings of Probabilistic Risk Assessment

Executive Summary

Report prepared for Greenpeace International, August 1989
by Gesellschaft für Ökologische Forschung und Beratung mbH, Hannover

SUMMARY AND CONCLUSIONS:

Nuclear power plants represent a considerable hazard. They have the potential for accidents leading to large catastrophic releases of radioactive substances. Yet on the other hand, nuclear power plants are designed and built with numerous complex safety systems to control their hazard potential. Experience shows that this control is not perfect.

In order to obtain quantitative measures for nuclear power plant hazards, the method of "probabilistic risk assessment" (PRA) was developed. In PRAs, it is attempted to determine the probability of severe reactor accidents with the aid of complex mathematical and phenomenological models. (In so-called "full-scope" PRAs, accident consequences are also assessed, and the overall "risk" is determined, accounting for both probabilities and consequences. Those steps lie outside the scope of this study.)

Probabilistic risk assessment is used quite extensively in many countries today. Frequently, PRA results have been used to "prove" to the public how small nuclear power plant risks really are. Recently, the policy importance of PRA has become even greater.

In the wake of the Chernobyl accident, the International Atomic Energy Agency (IAEA) formulated safety targets for nuclear power plants. The probability of an accident with severe core damage is to be below 10^{-4} (1:10.000) per plant operating year. The probability of large, early releases is required to be lower by a factor of at least ten. This applies to present-day plants. For future plants, improved targets should be achieved.

IAEA claims that, at present, the targets are already met in those cases where "well-managed circumstances" prevail. According to the IAEA, PRA studies performed in different countries yield results which are consistent with IAEA safety targets.

The application of safety targets expressed in terms of probabilities clearly relies on the use of PRA. Without PRA, such targets are meaningless since there would be no way to check whether they are fulfilled.

It is interesting to note that, even if results of PRAs performed so far are accepted uncritically, they do not altogether display the consistency with IAEA targets that is claimed. For example, about two-thirds of the PRAs performed so far in the U.S. which take both internal and external events into consideration as accident initiators result in severe core damage frequency above 10^{-4}/yr.

It is also important to recognize that PRA results do not usually reflect the "as found" condition of the plant. Inevitably, opportunities are identified during the course of a PRA study to make changes in plant systems and procedures, so as to reduce core damage probability. Unfortunately, these changes are usually reflected in the published study without an indication of their impact on the estimated core damage probability. Thus, the PRA results usually reflect the "as fixed" plant state.

Reporting only the "as fixed" core damage probability, rather than including the "as found" core damage probability as well, can lead to distorted perceptions when results of a limited number of PRAs are used to draw industry-wide inferences. This practice can result in an underestimate of the generic risk of core damage accidents because those plants which have not yet been analysed could have a higher "as found" core damage probability, rather than the lower "as fixed" core damage probability which might be inferred from published PRAs.

However, there is a more basic question related to PRA: Are probabilistic safety targets at all useful for policy purposes? More precisely: Can PRAs give reliable estimates for severe core damage frequency, and the probability of early containment failure (leading to particularly large releases)? It is the purpose of this study to analyse the underlying assumptions, the methodology and the results of probabilistic risk assessment in order to identify its merits and shortcomings.

Data Base

PRAs rely on input data such as the frequencies of accident initiating events, or component failure rates. Their first problem is the lack of fully adequate data bases. There are no clear-cut criteria as to how the basic data are to be determined, and there is no uniform practice of documentation. A large

amount of arbitrariness is involved when selecting data for a particular PRA, and when combining data from different sources. Also, data collection and compilation is a complicated and lengthy process. Hence, data banks can never be up-to-date. There are delay times of several years between data generation and data access for PRA. Rare events, new phenomena etc. will thus not be included in data banks immediately.

The arbitrariness in data base selection can, in principle, be reduced by using plant-specific data. However, this is not possible in practice; the use of generic data cannot be avoided. Furthermore, even insofar as plant-specific data are available, they must be collected first. The plant must have operated more than ten years in order to generate any usable data (even then, their bandwidth of uncertainty will be considerable). Hence, the PRA will be finished at a time when the plant is already entering the latter part of its operating life - whether targets are met or not, is thus more or less decided a posteriori!

Basic questions of Methodology

The first methodological problem of a PRA is that its completeness can never be guaranteed. Due to the complexity of the system under study, possible accident initiators or accident sequences are bound to be overlooked, or underestimated in their severity. Indeed, there are severe omissions even in recent major PRAs, demonstrating the persistence of this problem.

Another major problem is the uncertainty of the results. All input values of a PRA are random variables. In order to estimate the failure probabilities of complex safety systems, those input variables are combined with the aid of complex logical structures (so-called "fault trees"). Their uncertainty margins propagate through the analysis of those fault trees. Hence, the results - severe core damage frequency, and other probability statements - are also random variables beset with a considerable bandwidth of uncertainty.

Thus, it is not appropriate to only consider the expectation value (mean value) of severe core damage frequency when checking whether safety targets are met. Even with the mean value well below 10^{-4}/yr, the probability that the unknown "true" value is higher than 10^{-4}/yr can still be considerable. A

conservative approach demands that the 95%- or 99%-fractile be taken as the yardstick (by definition, the value of a random variable is smaller than the 95%-fractile in 95% of all cases). If the latter is selected, there is hardly a PRA performed so far whose results conform to the IAEA safety targets. The IAEA does not comment on this problem and gives no hint as to which yardstick they consider appropriate.

This problem is exacerbated by the fact that uncertainty bandwidths of input variables are often underestimated in PRAs. Thus, the results are more uncertain than claimed. The bandwidth of uncertainty of the results is further increased by correlation between input variables (input variables which are correlated are expected to vary according to a common pattern, and not independently of each other).

In addition to this, and worse still, correlation between variables also leads to an increase in the expectation value (the mean) of severe core damage frequency. Nevertheless, this problem is usually ignored in PRAs; no correlation is assumed for computational convenience. It can be shown that high correlation leads to such large error margins as to render the results of PRAs practically meaningless, unless the error margins of the input variables are small indeed.

Dependent Failures

Dependent failures occur when several components fail simultaneously or consecutively, due to a common influence. Dependent failures play a major role in NPPs, as in all complex systems with several parallel trains serving the same purpose. For some important safety systems, they are indeed the dominant failure mode. Yet dependent failures are extremely difficult to incorporate in PRAs. The methodology is focused on independent failures, and dependent failures must be added in fault trees as an afterthought. Usually, the treatment of dependent failure in PRAs is not complete, even in major recent studies.

The database for dependent failures is particularly small. This can lead to extremely large uncertainty of results. The data base is further reduced by the necessity of data screening, to account for design differences which may render particular data inapplicable to a plant under study.

Rather substantial dependent failure rates can often be found in the literature, emphasizing the important role of dependent failures. In some cases, on the other hand, very low values for dependent failure rates are derived. These values, however, cannot be regarded as reliable.

Dependencies between failure rates and initiating events are not sufficiently allowed for in PRAs. This results in an underestimation of system failure probabilities, since, for example, failure rates at real demands may be higher than for test demands.

Furthermore, no procedure or model is available that is well-established and capable of yielding reliable and reproducible results with a well-defined and sufficiently narrow uncertainty range. The study of the same system by different teams of analysts can lead to results differing by several orders of magnitude.

This is yet another reason why PRA results are beset with high uncertainties. The severe core damage frequency as currently estimated is likely to be too low because of incomplete consideration of dependent failures alone, even if all other problems are disregarded.

The Human Factor

In PRAs, only the most simple kind of human error (errors of omission) is taken into consideration. Even so, the contribution to severe core damage frequency is high (in some studies, over 50%). The problems associated with human error are: That there are many different kinds of human errors; that human error probability is particularly high in times of stress; the estimation of this probability is beset with many uncertainties; human error is an important potential cause for dependent failures; and different errors can be highly correlated.

Apart from "simple" errors of omission, there are many possible error modes: Errors in design, construction, fabrication, and maintenance; actions against safety rules; errors due to wrong interpretations of plant status; erroneous actions at critical points; errors of management and administration etc. PRAs attempt to include simple, or routine, human errors. Complex and gross

human errors - like those which occurred at Chernobyl, or those at the management level - cannot be included in PRAs.

The basic psychological problem is that, as measured according to simple, day-to-day experience, severe accidents have relatively low probability. Thus, the operating personnel have no acute feeling of danger, and do not, at heart, take the hazards seriously.

In a typical accident situation, the operators are required, after a long quiet period where the plant ran automatically, to react immediately, efficiently, and without error. There is a sudden change from a situation with a very low stress level, to extremely high stress. Large masses of data will suddenly pour in, and operators usually have no practical experience in dealing with such events.

Risk analysts have put considerable efforts into modelling and quantifying human behaviour. Yet the models remain far too simple and the data base for quantification too unreliable. Notably, since severe accidents are rare events, data usually are obtained from simulator exercises or expert estimations. These data do not reflect the psychological mechanisms relevant to actual accidents. Also, for purposes of PRA quantification, a subset of relevant human actions is modelled, while action sequences that are more complex and therefore difficult to model are neglected. Unfortunately, it lies in the character of those more complicated action sequences that they produce the most surprising and thus most dangerous effects. Among other events, voluntary violations of safety rules can never be quantified. Such violations can occur in many ways, and very different motives can lead to them.

Increasing automation and reliance on computers provides no way out, since it leads into the wide and dangerous field of software errors. Software errors are a special category of complex human errors and are correspondingly difficult to assess quantitatively.

Reactor Pressure Vessel Failure

Reactor pressure vessel failure constitutes a special case amongst all internal accident initiating events: If the vessel fails, it is unlikely that safety systems

will prevent severe core damage. Thus, pressure vessel failure is a whole accident sequence in itself. Even without further system failures, it is likely to lead to a severe accident. It can even be coupled with early containment failure.

In all PRAs known to the authors, the probability of pressure vessel failure is assumed to be so low (mostly below 10^{-7}/yr) that it gives no significant contribution to risk.

A different picture emerges if the problem is analysed taking into account experience with non-nuclear vessels, experiments and tests with reactor materials, and theoretical calculations in fracture mechanics. A failure rate which is lower than 10-5/yr cannot be accepted as a conservative estimate. Thus, pressure vessel failure has to be considered as a relevant risk contributor. The possibility of vessel failure with fragmentation as a cause for early containment failure cannot be disregarded, particularly for nuclear power plants with small containment types.

Containment Behaviour (level II of PRAs)

Accident sequences involving early failure of the containment typically lead to very high releases of radioactivity (although late containment failure can also lead to a significant release). Hence, the most important issue by far in level II of a PRA is to identify possible modes of early containment failure, and to assess their probability.

Potential failure mechanisms for early containment failure include:

- Reactor pressure vessel failure with subsequent missile induced containment damage
- Containment bypass
- High pressure melt ejection (HPME)
- Containment melt-through
- Hydrogen deflagration and detonation
- Steam explosions
- Certain external events.

Reactor pressure vessel failures and external events are considered elsewhere.

Two major possibilities for containment bypass are steam generator tube rupture (SGTR), and failure of containment isolation. Bypass via a connecting line also has to be taken into account. Steam generator tube rupture as a consequence of a core melt accident is not considered as a mechanism for early containment failure in most PRAs. However, SGTR as accident initiator, failure of containment isolation, and bypass via connecting lines are often considered to some extent in PRAs, as are high pressure melt ejection and containment melt-through.

Currently, there is general agreement that in case of high pressure melt ejection, the potential for early containment failure exists, and very high releases of radioactive substances can result.

There are two other major hazards, however, which are treated in far too optimistic a manner in PRAs: Hydrogen detonation or deflagration, and steam explosions.

Hydrogen Detonation or Deflagration

The generation of Hydrogen during a core melt accident is a very serious problem. It is very difficult to derive a meaningful probability estimate for early containment failure due to Hydrogen detonation or deflagration. Probability calculations as attempted in PRAs, for example in the U.S. study NUREG-1150 (draft No. 1), can be shown to be meaningless, and based on completely arbitrary assumptions.

As quantification is very difficult, only a rough qualitative assessment can be given for the likelihood of early containment failure.

Detailed calculations show that for a PWR with a large, dry containment, for example, conditions during a core melt sequence can be such that containment-destructive Hydrogen detonations and deflagrations are possible during a considerable period of time (for about 40 hours).

It is impossible to predict the exact time of occurrence of a Hydrogen burn. Conservatively, it must be assumed during an early phase of the accident, thus leading to early containment failure. A high source term will result in this case. Counter-measures as currently planned - and given credit in some PRAs

- are of limited value at best. They might even be counter-productive in some cases.

Steam Explosions

There is no current scientific basis to give a meaningful upper limit (less than one) for the probability of a significant steam explosion occurring when the molten core comes into contact with water. Thus, the only responsible way to treat steam explosions is to assume their occurrence in case of a core melt with low pressure in the primary system. The compulsion, evident in PRAs, to produce quantitative probability estimates has led to many errors and to confusion as to what the state of knowledge really is.

This point is of particular importance since in PRAs may be often assumed that only high-pressure accident sequences (leading to high-pressure melt ejection) can cause early containment failure, and therefore measures are planned in case of an accident to reduce primary pressure and to deliberately reach a low-pressure sequence. Because of steam explosions, this is rather like avoiding Scylla in order to run into Charybdis.

External Events

External accident initiating events are often not included in PRAs since it is extremely complicated to assess their probability of occurrence, and the consequences for the plant status. Yet external events give high contributions to severe core damage frequency; in some cases where they were included in PRAs, their contribution has exceeded 50%.

The most important external events are earthquakes, fires, and, in some cases, internal and external flooding. Attempts to determine the probabilities for earthquakes of different magnitudes at a given site usually lead to no more than the observation that probability decreases with increasing magnitude. Parallel to that,the uncertainty of probability estimation increases considerably at higher magnitudes. Thus, particularly for the most relevant quakes (magnitude 5 and higher), reasonably accurate probability estimates are not possible. It is noteworthy that where PRAs have considered earthquakes, their results, taken at face value, indicate a substantial contribution from earthquakes to core melt frequency.

There are many other problems associated with external events; these problems cannot all be treated within this study. As an example of "man-made" external events, the crash of a military aircraft on an NPP is considered. In countries with a high flight density, the contribution to risk is non-negligible. This problem is exacerbated by the fact the during the last years, military aircraft have developed rapidly, getting faster and heavier. Plant designers, and risk analysts, have not kept step with this "technological progress".

A special case of external events are acts of war. Military attacks are never included in PRAs, even when other external events are. It is plainly impossible to derive meaningful probability estimates. Yet it can be shown that the possibility of the destruction of a nuclear plant by conventional weapons exists, and indeed nuclear plants have already been subject to military attacks. Thus, there is no basis for the claim that the (unknown and unknowable) probability of such attacks is negligibly small. The problem is exacerbated by the fact that nuclear plants are very vulnerable to attack. For example, a small-scale air raid with conventional bombs would be sufficient to destroy a plant and possibly lead to catastrophic releases.

Accident Management

The concept of accident management has been increasingly studied and developed in recent years, and is beginning to be introduced into PRAs. The idea is that even after vital safety systems have failed, an accident can still be "managed" by improvising the use of other systems for safety purposes, and/or by using safety systems in a different context than originally planned. The aim is to avoid severe core damage whenever possible; or, failing that, at least to avoid early containment failure.

Accident management places increased reliance on operator intervention, since accident management strategies must be implemented by the plant personnel. The possibilities of simulator training, however, are limited. Hence, there is large scope for human errors. This is enhanced by a serious pressure of time in many cases, which will create high psychological stress. For this reason alone, the significant reductions in severe core damage frequency and early containment failure probability which have been claimed

in PRAs (for example, in the German Risk Study, Phase B) appear completely unrealistic.

Furthermore, accident management, even if performed as planned, might prove ineffective, leading from one severe accident sequence to another just as hazardous. In some cases, it can even be counter-productive.

Many questions still remain open in connection with accident management. In the case of the German Risk Study, certain accident management measures are considered which cannot be performed in present-day German reactors, and require complicated and expensive backfitting of safety systems. Yet those measures have already been taken into account when assessing accident probabilities.

Unexpected Plant Defects

Unexpected defects may arise from improper design, construction or maintenance, or from unexpected changes in material properties. However, all significant defects in this category share two characteristics. First, they can cause components and structures to behave in ways not consistent with plant specifications and safety regulations. Second, they will not be reliably detected through routine inspections and tests. As a result, the risk analyst will find it difficult - and in many cases impossible - to identify and ascribe probabilities to failures which might arise from unexpected plant defects.

Many cases of unexpected plant defects have been reported in the past. They include the following categories: Piping stress exceeding code limits; incorrect hardware, or incorrect installation of hardware; lack of fire seals for electrical cable penetrations; electrical wiring errors; errors in electrical, instrumentation and control circuits; and electrical and control panels not seismically supported.

In most cases, such defects cannot be included in PRAs, since they cannot all be foreseen, and there is no adequate basis for the estimation of failure probabilities.

Unforeseen Physical Processes

PRAs can only address modes of plant behaviour which are expected and which are well understood. It is therefore noteworthy that there have been several instances where hitherto unexpected processes have been identified. PRA analysts are increasingly seeking to identify and account for such phenomena. However, they cannot be certain of reliably anticipating all important phenomena.

Sabotage

Sabotage so far has never been included in PRAs, and there appears no prospect that this will change in the future, for two compelling reasons: First, it is not credible to predict the probability of future sabotage events based on the historical record to date. Second, it would be inappropriate to publish a detailed analysis of sabotage scenarios and their likelihood of success.

Thus, sabotage will remain a factor which could increase the probability of a core melt accident, or the probability of a large source term given a core melt, by an unknown amount. The historical record of sabotage suggests that this unknown quantity is not trivial.

Conclusions

Probabilistic Risk Assessment (level I and II) is not an adequate tool to determine the frequency of severe core damage, or the probability of early containment failure, or the probability of other accident categories.

Even the most "simple" aspect of PRAs (modelling accident sequences taking into account solely internal initiating events, component failures, and human errors of omission) is beset with uncertainties which yield very large error margins. The error margins are still larger when containment behaviour is considered. In many cases, this is compounded by systematic underestimation of accident probabilities.

Furthermore, many important contributors are excluded from PRAs: Complicated forms of human error; many forms of unexpected plant defects; unforeseen physical processes; sabotage; and acts of war. Many PRAs even completely exclude external accident initiating events.

Thus, the result of a PRA is not an estimate of "severe core damage frequency". It is, rather, a form of risk-indicator with a severely limited scope, useful only for limited purposes. The "true" severe core damage frequency in fact would be this indicator times an unknown factor which is larger than 1 (taking into account the inaccuracies and optimistic assumptions in those areas which are included in PRAs, as demonstrated in this study); plus another unknown factor which is larger than zero (taking into account the issues which are omitted in PRAs): Or,

SCDF = (PRA result) x (unknown factor No.1) + (unknown f. No.2)

A similar equation holds for estimates of early containment failure.

The practice of referring to PRA results as accident frequencies is thus misleading and should be abandoned. It constitutes a perversion of a methodology which has without doubt - if its limitations are kept in mind - a number of useful applications.

Therefore, the IAEA safety targets are useless for policy purposes. It cannot be reliably determined whether a particular plant meets them (although findings from current PRAs, taken at face value, suggest that most plants currently do not). Any claim that PRAs show that probabilistic safety targets are more or less met is wishful thinking and might be dangerously misleading.

H. Hirsch, T. Einfalt, O. Schumacher, G. Thompson

IAEA SAFETY TARGETS AND PROBABILISTIC RISK ASSESSMENT

State of the Art, Merits and Shortcomings of Probabilistic Risk Assessment

Report prepared for Greenpeace International, August 1989
by Gesellschaft für Ökologische Forschung und Beratung mbH, Hannover

Introductory Section

1 INTRODUCTION

Probabilistic risk assessment (PRA) is extensively used in many countries today. In 1988, the importance of estimating nuclear accident probabilities was significantly increased further: The International Atomic Energy Agency (IAEA) published "probabilistic safety targets" (i.e., limits for accident probabilities).

In its report "Basic Safety Principles for Nuclear Power Plants" (safety series No. 75-INSAG-3) the IAEA recommends the target that, for existing nuclear power plants, the probability of severe core damage should be below 10^{-4} (1/10.000) per plant operating year. Accident management and mitigation measures should, according to IAEA, reduce by a factor of at least ten the probability of large off-site releases requiring short-term responses (to below 10^{-5} per plant operating year). For future plants, improved goals should be achieved (probabilities lower by a factor of ten) (Para. 25 of 75-INSAG-3). (In the IAEA report, it is not explained in detail what is to be understood by large releases requiring short-term responses. For the purposes of our study, we assume that accidents with early failure of the containment are meant.)

IAEA claims that, at present, the targets for existing power plants are already met in those cases where "well managed circumstances" prevail (Para. 11). In particular, IAEA states that probabilistic safety assessment (better called probabilistic risk assessment, PRA) as performed so far in different countries, gives results which are consistant with IAEA safety targets (Para. 54).

The great confidence IAEA has in probabilistic risk assessment is expressed even more pointedly in another publication (IAEA, 1988):

"The chance of a severe accident occuring at a nuclear power plant is extremely small. For existing plants, conservative assessments put the probability of severe accidental damage to a reactor or its nuclear fuel at 1 in 10.000 years of operation of a well-designed plant. The picture is brighter for tomorrow's even better designed plants, with a 1 in 100.000 probability per reactor year of a severe accident. Still, if the improbable were to occur, effective accident management and containment measures at these plants would reduce (by a factor of 10) the likelihood of significant environmental releases of radioactivity and the concurrent need for off-site emergency response."

Clearly, statements of this kind presuppose that reliable and accurate methods exist to determine accident probabilities.

Since the Chernobyl accident, the IAEA has significantly expanded its own activities in the field of PRA, following a

high priority recommendation of the Chernobyl Post Accident Review Meeting. The IAEA activities concentrate on:

- guidance on how to perform PRA and to interpret results;
- fostering the use of PRA results;
- human reliability analyses.

Eighteen states are participating in the IAEA inter-regional programme on probabilistic risk assessment. Under this programme, among other activities, the PSAPACK (Integrated PC Package for PSA level I) was developed (Boiadjiev, 1988). This package is specially recommended for training purposes.

In level I of PRA, it is attempted to estimate the probability of severe core damage accidents by describing, step by step, sequences leading to severe core damage. Complex fault trees and event trees are used, thus combining the failure probabilities of individual plant components.

Fault trees are employed to determine the overall failure probability of a safety system. Many different individual component failures are combined in a fault tree, at the end of which is the single event "system failure". The overall probability of system failure can, in principle, then be determined: It is the sum of the probabilities of all combinations of individual failures leading to system failure. (This is a somewhat simplified picture. The possibility of dependent failures in reality makes fault tree analysis much more complicated, see section 7) An example of a fault tree (from the U.S. study NUREG-1150) is given in fig. 6.1.

Event trees are used to determine the probability of severe core damage resulting from a particular initiating event. In this case, an individual event (e.g., small-break LOCA) is at the beginning of the tree. The tree then branches out, modelling possible accident sequences: The safety systems required are listed, and for each safety system, the tree branches further (according to whether it is operational, or not). At the end, there are several event sequences, some corresponding to severe core damage, and some to a controlled accident. The probability of each sequence is determined by multiplying the probabilities of the individual steps; safety system failure probabilities being provided by the fault tree analyses. An example for an event tree (from the German Risk Study) is given in fig. 1.1.

Furthermore, in level II of PRA, the probabilities of different failure modes of the reactor containment (if a severe core damage accident has occurred) are assessed taking into account the load the containment is exposed to in various circumstances, the probabilities of containment isolation failure, etc. The amounts of radionuclides released (the source term) for different accident sequences are estimated. Finally, in level III of PRA, the consequences of the released radioactive materials to public health are calculated (level III).

The purpose of this study is to analyse the most recent PRAs, regarding existing plants as well as the potential for

improvments, in order to investigate whether they can credibly support the IAEA's claims and targets. The study concentrates on the estimation of probabilities (hence, it contains only short references to source terms, and will not deal with level III at all). Thus, the main question is: How large is the probability for a reactor accident with severe core damage, and the conditional probability for early containment failure (accompanied by particularly large releases) after severe core damage; and how accurately can those probabilities be estimated?

The authors are aware of the fact that source term estimation today is one of the main issues of the ongoing debate on nuclear hazards, and that no risk study is complete without consequence estimation. The almost complete omission of those topics does not imply that we regard them as unimportant. However, it is the aim of this study to deal with the "probability aspect" of PRA, and in particular, with the IAEA's probabilistic safety targets.

An important issue in connection with risk studies is the definition of the concept of risk. In PRAs, the risk of an accident category is defined as the product of probability and consequences. In view of the unique character of accidents with very large consequences, it can be doubted whether this definition is adequate. An alternative concept giving more weight to low-probability, high-consequence accidents might be called for. This problem, however, transcends scientific analysis and is not further discussed here.

The study deals exclusively with Light Water Reactors (Pressurized, and Boiling Water Reactors), which constitute about 75 % of the world's commercial power reactor population (trend: increasing share), and for which most PRAs have been performed so far. To a large extent, the results will also be applicable to other reactor types (Gas-Cooled Reactors, Heavy Water Reactors, the Soviet RBMK design, Fast Breeders, etc.). However, it must be noted that those reactor types do not completely share the accident vulnerabilities and accident phenomenology as discussed in this study for Light Water Reactors.

It is interesting to note at the outset of this study that current PRA results - even if accepted uncritically - do not support the IAEA's claims. In the US, 38 PRAs have been performed so far (until January 1989) for 22 different plants. All of them dealt with core damage accidents initiated by internal events; only 16 included external events (such as earthquake, fires, plane crash etc.).

Severe core damage frequency due to internal events alone was above 10^{-4}/yr (the IAEA target) in 14 cases (37 % of the total of 38). In the subset of PRAs where it was determined, severe core damage frequency due to internal plus external events was above 10^{-4}/yr in 10 cases (63 % of the total of 16) (MHB, 1989).

Furthermore, a simple calculation demonstrates that even if IAEA safety targets were met, severe accidents in nuclear power plants would be relatively frequent events. With about 480 power reactors operating world-wide in 1990, a severe core damage frequency of 10^{-4}/yr results in an overall accident probability of about 0,05/yr (thus, if the number of operating reactors remained constant, one severe accident would, on average, occur every 20 years somewhere in the world).

We wish to emphasize that it is not the only purpose of PRAs to give quantitative estimates for accident probabilities, and risks. On a purely technical level, PRAs can be used and are used as a tool to identify in a systematic way design and/or operational weaknesses in a nuclear plant. PRAs can be useful when analysing particular safety systems, comparing alternative designs etc. Those limited applications of PRA are not the subject of this study; the problems and shortcomings identified here render such applications difficult and complicated in many cases, but do not altogether preclude them.

We are also well aware of the fact that risk analysts in many countries are working hard to further develop PRA methodology, and to overcome PRA weaknesses. It is only natural that in a complex field like risk analysis, perfection cannot be achieved, and different factors are modelled with significantly differing reliability and accuracy. Furthermore, it is not the fault of risk analysts that some risk contributors completely defy every attempt at quantitative probability estimation.

Our concern lies with the fact that PRA results are claimed to give meaningful estimates for overall accident probabilities, and thus can be used as a basis to decide whether nuclear plant risks are acceptable or not. It is this application of PRA results, and this application alone, that our criticism is aimed at.

Before entering the discussion of the limits and shortcomings of PRAs, an overview of PRA development and current use is given. As PRA was "invented" and first applied in the United States, and most PRA work to date is still performed in this country, the development and use of PRA in the U.S. receives special attention.

2 DEVELOPMENT AND USE OF PRA IN THE UNITED STATES

2.1 REACTOR SAFETY ANALYSIS PRIOR TO INTRODUCTION OF PRA

WASH-3

At an early stage in the development of nuclear reactors, it was understood that reactors could suffer accidents which liberated radioactive material from their fuel, with the possible release of that material to the surrounding environment. This potential was recognized in 1950 by the Reactor Safeguards Committee of the US Atomic Energy Commission (AEC), in its report WASH-3 (AEC, 1950).

Accordingly, WASH-3 articulated the concept of an "exclusion radius," defined as the radius of a circle around the reactor within which people would not be permitted to live. The formula adopted for this radius R (in miles) was:

$$R=0,01(P)^{1/2}$$

where P is the reactor thermal power in kW. Thus, a 30 MWt reactor would have an exclusion radius of 1,7 miles (2,8 km), while a 3000 MWt reactor (typical of modern commercial reactors) would have an exclusion radius of 17 miles (28 km).

The Reactor Safeguards Committee was particularly concerned about reactivity accidents, in which a surge of power leads to fuel melting and disruption of the reactor structure. Just such an event occurred at Chernobyl Unit 4 in 1986. Less attention was paid by the Committee to the possibility of fuel melting due to inadequate removal of decay heat after reactor shut-down (Okrent, 1981). This latter scenario, which became a reality at Three Mile Island Unit 2 in 1979, has become the major preoccupation of analysts studying the safety of light water reactors.

It was soon realized that the WASH-3 exclusion radius would allow few sites in the United States to qualify for larger reactors. Thus, within a year or two of publication of WASH-3, pressure developed for a relaxation of the exclusion radius. It was instead argued that a containment building could be constructed around the reactor, so that large quantities of radioactive material would not reach the environment even in the event of fuel melting. The first reactor built under this principle was the Submarine Intermediate Reactor, which was equipped with a spherical steel containment and built at West Milton, New York, at a site with a reduced exclusion radius. In 1957, the first "commercial" nuclear reactor entered service at Shippingport, Pennsylvania. This reactor was equipped with a containment building and was located at a site with an exclusion radius much smaller than that recommended by WASH-3 (0,4 miles instead of 4,8 miles). All subsequent commercial reactors in the United States have followed this precedent (Okrent, 1981).

WASH-740

As plans developed for a commercial nuclear power industry, concern arose that the industry's growth would be stifled by fear of liability for damage to the public in the event of a release of radioactive material. To provide a technical basis for consideration of this problem, the AEC submitted to the Congress in March 1957 a report, designated WASH-740, with the title "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants" (AEC, 1957). Six months later, the Congress passed the Price-Anderson Act, which limited the industry's liability in a major accident to $560 million, of which all but $60 million was at the time underwritten by the US government. This law, said then to be a temporary measure to encourage private industry to enter the nuclear field, was unique in shielding an entire industry from full liability for potential public damage arising from its operations.

WASH-740, prepared for the AEC by the Brookhaven National Laboratory, evaluated potential accidents at a hypothetical 500 MWt reactor. Source term estimates were made for three "hazard states", which correspond to progressive degradation of the three major barriers (the fuel cladding, the reactor coolant system boundary, and the containment) against release of radioactive materials. The three hazard states were:

(i) Major damage to the first barrier (the fuel cladding) but no release outside the reactor vessel. A subjective estimate was made that the probability of such an event would fall in the range of 10^{-2} to 10^{-4} per year for a typical reactor.

(ii) A situation in which there is not only major damage to the core but sufficient fuel damage or melting to lead to release of the radioactive materials outside the reactor vessel. However, it was assumed that the containment remained intact, thus preventing a major release of radioactivity to the environment. This hazard state is similar to the accident conditions assumed in the 1960s in TID-14844, described below. The authors of WASH-740 subjectively estimated a probability of 10^{-3} to 10^{-4} per reactor-year for this hazard state.

(iii) Major damage to the core and cladding, complete melting or substantial melting of the core, and failure of the last barrier (the containment). The subjectively estimated probability of this hazard state was given as 10^{-5} to 10^{-9} per reactor-year.

The probability estimates mentioned above were not the product of scientific analysis. Indeed, the authors of WASH-740 concluded that it was "essentially impossible to assign dependable quantitative values" to the probability of system failures leading to serious accidents. Instead, the authors sought expert opinion. All the experts contacted felt that the probability of a major accident was "low", but many of them declined to make even an order-of-magnitude guess as to its

magnitude. Others were willing to make guesses about the probabilities of particular hazard states.

The "Maximum Credible Accident" and 10 CFR 100

During the 1950s, many in the AEC and the nuclear industry convinced themselves that the most serious accidents, such as the third hazard state identified in WASH-740, were so unlikely as to be not credible for practical purposes. Thus developed the concept of a "maximum credible accident", which found a formal expression in the AEC's first generic reactor siting regulations, 10 CFR 100, which were promulgated in 1962.

The 10 CFR 100 regulations were based upon an AEC report designated as TID-14844 (DiNunno et al, 1962). That report asserted that the maximum credible accident (now referred to as the "design basis accident" or DBA) would result in a release to the containment building atmosphere of 100 percent of the noble gases, 50 percent of the iodine, and 1 percent of the remainder of the fission product inventory. The containment was assumed to remain intact and to leak at a small, predictable rate (0.1 percent of volume per day). Although arbitrary and without scientific foundation, the hypothesis of a maximum credible accident -- and its associated TID-14844 source term -- has had a profound effect on safety regulation and design of nuclear plants. The TID source term became widely used by the AEC and its regulatory successor, the US Nuclear Regulatory Commission (NRC). It provided the basis for a source term incorporated in NRC Regulatory Guides 1.3 and 1.4, which provide the basis for accident evaluation in utility-submitted Final Safety Analysis Reports (FSARs). Also, it is used in site suitability assessments and in establishing safety equipment environmental qualification standards. Until 1979, the TID source term (and the low population zone established under 10 CFR 100 using the TID source term) formed the basis for offsite radiological emergency planning. It has also been used in defining what constitutes radiological sabotage (deliberate acts must result in offsite doses exceeding the 10 CFR 100 limits to be officially classified as radiological sabotage).

The occurrence of a partial core melt accident at Three Mile Island Unit 2 (a 880 MWe PWR) in 1979 demonstrated conclusively that the assumed maximum credible accident was no such thing. Yet, NRC regulations still rely heavily on that out-dated concept.

WASH-740 Update

In mid-1964,in anticipation of the expiration of the Price-Anderson Act in 1967, the AEC commissioned Brookhaven National Laboratory to revise the WASH-740 study. Many AEC officials hoped that the new study would show that the consequences of a severe accident would be lower than were estimated in WASH-740. However, the Brookhaven team soon concluded that there was no basis for such a finding. Indeed, because larger reactors were being proposed in the 1960s, the public health consequences of

a severe accident were predicted to be considerably greater than were estimated in WASH-740 (Ford, 1982).

The AEC's steering committee for the study also hoped that new information could lead to a scientific finding that the probability of a severe accident was very low. However, the Brookhaven team refused to work on this problem, believing that there was no dependable statistical basis for estimating accident probability. As the minutes of one steering committee meeting noted (Ford, 1982):

"The matter of probability was brought up, and the BNL [Brookhaven National Laboratory] representatives stated that, in their opinion, no significant scientific progress could be made and they proposed not to study it.....The BNL people.....insisted that they not consider probabilities of accidents."

By late 1964, as the study neared completion, the steering committee became concerned about the implications of the study's publication. Records show that they were reluctant to publish any report that could "strengthen opposition to further nuclear power." According to the minutes of another meeting, they believed that the "impact of publishing the revised WASH-740 report on the reactor industry should be weighed before publication." In fact, the AEC suppressed the study, and its contents only came to light following a 1973 request under the Freedom of Information Act. The AEC commissioners merely sent to the Congress a letter along lines suggested by the Atomic Industrial Forum (an industry lobbying group), indicating that accident risks were comparable to those assessed previously, except for the larger size of reactors currently planned, and asking that the Price-Anderson Act be extended (Ford, 1982). It was.

WASH-1250

In July 1973, the AEC issued what was to be its last major reactor safety analysis, designated WASH-1250 (AEC, 1973). While largely a descriptive volume, WASH-1250 contains a section which summarizes the state of "expert" opinion at that time regarding accident probabilities. Based on a series of papers on the then-emerging discipline of probabilistic risk analysis, WASH-1250 estimated the probability of an accident leading to the release of 5 million Curies of fission products to be about 10^{-4} per reactor-year. The report also concluded that the mid-range estimate for the probability of a LOCA leading to the release of 20.000 Curies of iodine was about 10^{-10} per reactor-year.

2.2 THE REACTOR SAFETY STUDY; WASH-1400

In 1972, faced with upcoming Congressional hearings on further renewal of the Price-Anderson Act, and with increasing controversy over the safety of nuclear power reactors, the AEC commissioned a 3-year study of accident probabilities and consequences. MIT professor Dr. Norman Rasmussen was named to

head the study, whose budget was $3 million. This exercise generated the first nuclear nuclear plant PRA, which was published in final form in October 1975 by the NRC under the title "Reactor Safety Study," but is often known under its AEC designation WASH-1400 (1975).

This study sought to evaluate the risk posed by the operation of the first 100 reactors planned for the US. Analyzing all 100 reactors would have taken decades and many tens of millions of dollars, so two "representative" reactor designs were chosen: the Surry PWRs and the Peach Bottom BWRs. Surry Units 1 and 2 are three-loop Westinghouse PWRs with large dry subatmospheric containments and power outputs of 775 MWe; they began operation in 1972 and 1973, respectively. Peach Bottom Units 2 and 3 are General Electric BWRs with Mark I containments and power outputs of 1065 MWe; they began operation in 1974.

The typicality of these facilities has been extensively questioned since WASH-1400 was published, and the results of a later followup program which applied the same analytic techniques to four additional reactors (the RSSMAP studies) clearly indicate that the two reactors analysed in WASH-1400 are not typical at all.

WASH-1400 calculated core melt probabilities for the Surry and the Peach Bottom reactors. The PWR core melt probability was calculated to be about 6E-5 per reactor-year; the BWR core melt probability was calculated to be about 3E-5 per reactor-year. WASH-1400 itself acknowledged that these results reflected a higher core melt probability than had been previously anticipated. Prior to the publication of WASH-1400, "conventional wisdom" and expert opinion held that the probability of core melt accidents was 10^{-6} per reactor-year or lower. In comparison, the upper bound (95th percentile value) core melt probability for light water reactors generally was calculated by WASH-1400 to be about 3E-4 per reactor-year.

Releases from potential reactor accidents were broken down into a number of categories. There were seven PWR core melt release categories, designated PWR 1 through PWR 7, and two PWR design basis accident release categories, designated PWR 8 and PWR 9. Five BWR release categories were identified, of which categories BWR 1 through BWR 4 represented core melt accidents and category BWR 5 represented design basis accidents. Table 2.1 summarizes the estimated probability and release characteristics for each of the above categories.

In its draft version, published in 1974, WASH-1400 received heavy criticism, notably from a study group of the American Physical Society (Lewis, 1975). Although some of the deficiencies in the draft were corrected, the final version was also severely criticized. For example, in August 1977, the Union of Concerned Scientists published a book-length review of WASH-1400, concluding that its assertions on nuclear risks could not be trusted (UCS, 1977). Among the problems identified as plaguing this application of PRA were the following:

* Much of the elementary data on the reliability of plant components were incomplete, uncertain, or unavailable;

* For most of the WASH-1400 analysis, failure of one component was assumed to be independent of failures of other components. That is, "common mode" failures were largely ignored;

* WASH-1400 generally assumed that current reactor designs were adequate, overlooking possible intrinsic design deficiencies; and

* WASH-1400 was lax in addressing major problems that contribute to nuclear risks, such as aging and degradation of plant components, earthquakes, sabotage, and terrorism.

As a response to these and other criticisms, the NRC established a Risk Assessment Review Group, which submitted its report in September 1978. The Review Group reported that while WASH-1400 was a "substantial advance" over previous assessments of reactor risks, the Review Group could not determine whether its accident probabilities were too high or too low (Lewis, 1978). The Group also drew attention to WASH-1400's "questionable methodological and statistical procedures." A summary of the Review Group's findings appears here as Appendix 2A.

In January 1979 the NRC issued a policy statement retracting its endorsement of the WASH-1400 risk estimates: "the Commission does not regard as reliable the Reactor Safety Study's numerical estimate of the overall risk of reactor accident."

2.3 RECENT DEVELOPMENT OF PRA

Growth in Use of PRA

Since the publication of WASH-1400, a considerable number of PRAs have been completed. Table 2.2 summarizes their findings in terms of the probability of core melt. It will be noted that core melt probability is, according to present custom, attributed separately to "internal events" (equipment failures, operator errors, etc.) and "external events" (floods, earthquakes, etc.) Also, it will be noted that some plants have been the subject of up to three separate PRAs.

PRA methodology has become relatively standardized, particularly since publication by the NRC of the "PRA Procedures Guide" (NRC, 1982b). Figure 2.1 illustrates this methodology, and shows how outputs may be generated at Levels 1, 2 or 3. The PRAs whose results are summarized in table 2.2 were conducted at one or another of these three levels.

An illustration of the Level 1 results generated by contemporary PRAs is provided by figures 2.2 and 2.3. These show the statistical distributions of core melt probability (described as "frequency of core damage" in figures 2.2 and 2.3) which were generated in a recent PRA for Three Mile Island Unit 1 (a 792 MWe PWR). It will be noted that core melt probability is predicted to be relatively high in this PRA; the 95th percentile total core melt probability is 9.4E-4 (roughly 10^{-3}) per reactor-year.

The phrases "core damage", "severe core damage", and "core melt" have been used interchangeably in PRAs. This is because the sophistication of PRA is insufficient to discriminate between sequences which lead to full core melt and those which lead to lesser outcomes. The difficulty has been explained in the Seabrook PRA (PLG, 1983):

"At one stage of the study, the possibility of specifying additional plant states to distinguish between core melting and core damage short of melting was considered. The idea was rejected, however, upon finding that the time interval between onset of core damage and full scale fuel melting is short in comparison with the time interval between the initiating event and the time of core damage for risk significant scenarios. Therefore, there was a physical basis for the assumption that given the onset of core damage, the conditional likelihood of core melt approaches unity."

More recently, PRA analysts have gained confidence that they can discriminate among core damage sequences. Notably, the second draft of the NRC's NUREG-1150 study (see below) identifies core damage sequences in which core melting is arrested before the molten material penetrates the reactor vessel. Detailed review of that draft and its supporting documents (such review was not possible during the preparation of our report) will reveal the basis, if any, for this new confidence.

NUREG 1150

For the past several years, the NRC has been working on an update of the Reactor Safety Study. A draft report on this work was published in February 1987, with the designation NUREG-1150 (1987). In June 1989, a second draft was published, employing a completely different format and drawing upon a modified set of analytic procedures. Also, many of the conclusions in the first draft have been substantially modified. As our report goes to press, most of the supporting documents for the second draft of NUREG-1150 (hereafter designed NUREG-1150/2) have not been published. Therefore, we have not reviewed the basis for the findings in NUREG-1150/2. However, some of those findings are presented here for purposes of illustration. In both drafts, five plant designs have been studied -- three PWRs (Surry, Zion, Sequoyah) and two BWRs (Peach Bottom, Grand Gulf).

Figure 2.4 shows the core melt probability (severe core damage frequency) estimated in the first draft of NUREG-1150 for each

of the five plants. The range of core damage frequency is expressed in a "box and whisker" format, in which the box represents the range of mean core damage frequencies generated by various sensitivity studies, while the whisker is meant to represent extremes of the 5 to 95 percent confidence bands. Figure 2.5 provides a more detailed illustration of this format, which has been severely criticized -- in fact, described as "erroneous and misleading"-- by members of an NRC panel which reviewed the draft NUREG-1150 (Kastenberg, 1988).

From the same version of NUREG-1150, the estimated probability of early containment failure, following a core melt, is shown in figure 2.6. Here also, the range of probability is represented in a dubious manner. NUREG-1150 describes the form of presentation thus (NUREG-1150, 1987):

"The horizontal lines within the vertical bars represent the individual sample results from the uncertainty analysis and provide a qualitative indication of the concentration trends within the range, based on the judgment of experts."

In its second draft, NUREG-1150 employs a format which, at least superficially, appears more scientific. This format is illustrated by figure 2.7, which shows the estimated core damage frequency from internal initiators, for the five plants considered. The probability density functions and frequency ranges which are shown in figure 2.7 have an appearance which suggests that a rigorous, statistically-based analysis was used. Unfortunately, this appearance is deceptive. The underlying probability distributions were generated primarily by "expert judgment" (i.e., guesses).

Whereas only internal initiating events were considered in the first NUREG-1150, the second draft estimated core damage frequency from earthquakes and fired for two plants - Surry and Peach Bottom. The results are shown in figure 2.8. It will be noted that two sets of results are shown for earthquakes -- the "Livermore" and "EPRI" results. These reflect earthquake predictions make at the Lawrence Livermore National Laboratory and the Electric Power Research Institute, respectively. Although the Livermore group found severe earthquakes to be more frequent than did the EPRI analysts, the authors of NUREG-1150/2 found both sets of predictions to be "equally valid" (see also section 13.3.1).

NUREG-1150/2 does not present estimates of the conditional probability of early containment failure in a format which allows direct comparison with the estimates shown in figure 2.6. Instead, that probability is shown separately for different types of accident sequences. Again, a superficially scientific format is used, although the underlying analysis relies primarily upon expert judgment. The issue of early containment failure is pursued at greater length in section 10, below.

It is common to find that PRAs for different plants show differing significance for particular initiating events. This

point is illustrated by figure 2.9, which shows the differing contributions of various initiating events to core melt probability for the five reactors examined in the draft NUREG-1150. However, the NUREG-1150 exercise also allows comparisons to be made among PRAs done for the same plant. Table 2.3 shows such a comparison, in which the draft NUREG-1150 results for the Grand Gulf BWR are compared with those from the NRC's RSSMAP study (published in 1981) and from the industry-sponsored IDCOR study (published in 1984). Although the total core melt probability estimated in these three studies varies by only a factor of four, the estimated contributions of particular initiating events vary more widely. For example, the estimated contribution of station blackout varies by a factor of eighty if the IDCOR and NUREG-1150 results are compared. This suggests that the overall estimates of core melt probability should be viewed cautiously.

Like all PRAs, the two drafts of NUREG-1150 have not attempted to account for sabotage as an initiating event, offering the following rationale for this position (NUREG-1150, 1987):

"The risk of sabotage has not been included in the results of this report. It is the staff's opinion that the likelihood of a specific threat is very dependent on the changing political and social climate. The applicability of historical data pertaining to a threat of sabotage to a nuclear plant in the future is less obvious than for hardware data or information on human error probabilities."

"As Found" versus "As Fixed" PRA Results

It is important to recognize that the results of a PRA do not usually reflect the "as found" condition of the plant. Inevitably, opportunities are identified during the course of a PRA study to make minor (or sometimes major) changes in plant systems and procedures, so as to reduce core damage probability. Unfortunately, these changes are usually reflected in the published study without an indication of their impact on the estimated core damage probability. Thus, the PRA results usually reflect the "as fixed" plant.

For example, the recent PRA for Three Mile Island Unit 1, while apparently an intermediate product which will be further modified, nonetheless reflects some of these sorts of changes. The following changes are identified (PLG, 1987):

-- Changes were made to the surveillance procedures, the alarm response procedures, and operator training literature relevant to the reactor building emergency cooling water system, so as to permit a greater chance of operator recovery of the system.

-- Emergency procedures were revised and additional hardware was procured to improve the control building ventilation system. These changes incorporate the use of emergency fans to cool engineered safeguards electrical equipment in the event that normal control building ventilation is lost.

-- The makeup and purification system operating procedure and the engineered safeguards system status checklist were revised to provide additional assurance that the correct lubricating pump is selected for makeup (HPI) pumps.

-- Modifications made to the emergency feedwater and the heat sink protection system during the 1986-1987 refuelling outage were incorporated into the PRA.

-- In the early stages of the PRA study, the instrument air dryer transfer valve was identified as a major contributor to loss of instrument air. The complete air dryer assembly was replaced and includes a new type of transfer mechanism.

Unfortunately, the Three Mile Island PRA does not provide an estimate of the "as found" core damage probability. In fact, very few published PRAs have dealt explicitly with the issue of what was the core damage probability for the plant at the time the analysis was begun. Virtually every PRA study performed has resulted in changes of procedures and/or hardware which have reduced estimated core damage probability. This is not surprising, since identifying and implementing such changes is a key motive for performing a PRA.

Reporting only the "as fixed" core damage probability, rather than including that "as found" core damage probability as well, can lead to distorted perceptions when results of a limited number of PRAs are used to draw industry-wide inferences. This practice can result in an underestimate of the generic risk of core damage accidents because those plants which have not yet been analysed could have a higher "as found" core damage probability, rather than the lower "as fixed" core damage probability which might be inferred from published PRAs.

There are some PRAs for which "as found" and "fixed" results are available. For example, the NRC staff (and consultants) conducted a detailed review of the PRA for Indian Point Units 2 and 3 following its submittal to the NRC in 1982. For Indian Point Unit 2, the NRC staff estimated the "as found" core damage probability to be 1,0E-3 per reactor-year, while the "as fixed" core damage probability was estimated to be 3,5E-4 per reactor-year. For Indian Point Unit 3, the NRC staff estimated the "as found" core damage probability to be 6,8E-4 per reactor-year, while the "as fixed" core damage probability was estimated to be 3,5E-4 per reactor-year (Rowsome, 1982).

Another perspective on the "as found" versus "as fixed" issue is provided by the PRA for Oconee Unit 3. This study included potential external events, one of which was a turbine building flood caused by a failure in the component cooling water system which could result in a lake draining into the turbine building (which leak could not be stopped). As the analysis progressed, it was discovered that a very large core damage probability would result from such floods, and measures were implemented to reduce the risk. The final PRA estimated both the "as found" and "as fixed" value for these floods -- the "as found" core damage probability was estimated at 6,4E-3 per reactor-year, while the "as fixed" value was estimated at 8,8E-5 per reactor-

year, a reduction in probability by a factor of about 73 for this class of accident (Sugnet, 1984).

A final example is offered for illustration. The Calvert Cliffs plant, until the early 1980s, had a remote, manually initiated auxiliary feedwater system. The 1980 PRA for this plant under the RSSMAP program estimated the "internal events" core damage probability at 1,5E-3 per reactor-year, with a large contribution from loss of main feedwater scenarios. After implementation of a fix, this PRA estimated the core damage probability at 4,0E-4 per reactor-year, a reduction by a factor of about 3,8. A later PRA conducted for Calvert Cliffs under the IREP program estimated the "internal events" core damage probability at 1,3E-4 per reactor year, a reduction by a factor of about 12 (Sholly, 1986).

2.4 CURRENT APPLICATIONS OF PRA

Implications of Severe Accident Studies for Regulatory Change

NUREG-1150 is the latest in a series of NRC or AEC-sponsored studies on severe accidents. Like its predecessors, NUREG-1150 will be used as a basis for changes in the NRC's safety regulations. Figure 2.10 illustrates this process. As will be seen from the following discussion, the NRC is increasingly relying upon probabilistic analysis as a basis for its regulations.

NRC Safety Goals

When the present generation of nuclear plants was being designed and the construction sites were being chosen, the regulatory framework was "deterministic". Plants were designed according to "general design criteria" (NRC, 1986a) and it was believed that these criteria, supplemented by normal care in plant construction and maintenance, ruled out core melt accidents as credible events.

After the 1979 TMI accident, this position became unsustainable. Yet, the NRC found itself in the position of regulating plants whose design and siting were based on a demonstrably false hypothesis. An attempt has been made to overcome this basic problem on the basis of probabilistic arguments. Most prominently, the NRC has articulated a set of "safety goals" (NRC, 1986b).

The primary safety goals are qualitative. These are supported by "quantitative objectives", designed to gauge achievement of the qualitative goals. Finally, a quantitative "general performance guideline" is provided, which apparently will be the measure actually used in regulatory implementation. Figure 2.11 summarizes each of these three levels of the safety goals.

The magnitudes of core melt probability which appear in table 2.2, combined with the probabilities of early containment failure (following a core melt) which appear in figure 2.6, suggest that many -- perhaps all -- US nuclear plants do not

meet the NRC's general performance guideline. From the various industry and NRC-sponsored PRAs, one can readily conclude that the probability of a large release is well above 10^{-6} per reactor-year. Presumably, the NRC and the industry will seek to resolve this problem in two ways. First, they will seek "improved" analytic methods which reduce the estimated probability of core melt and early containment failure (as is done in NUREG-1150/2). Second, they will engage in plant modifications, procedural changes, and operator training which purport to reduce those probabilities.

Specific Regulatory Applications of PRA

The NRC is beginning to apply PRA findings in a number of regulatory areas, including (NUREG-1150, 1987):

* containment leakage requirements;
* equipment qualification for accident conditions;
* requirements for hydrogen control during severe accidents;
* siting criteria (for possible future plants);
* focussing the effort of NRC safety inspectors;
* assessing the effectiveness of existing regulations; and
* implementing the backfit rule.

For illustration, consider the last-mentioned application, implementing the backfit rule. This rule (10 CFR 50.109) requires the NRC to determine if a proposed safety modification to one or more nuclear plants is cost-effective, or, more specifically, "to determine whether: (1) public health and safety or common defense and security are substantially improved; and (2) the costs of implementation of the backfit are justified" (NUREG-1150, 1987).

Figure 2.12 shows some sample results of the type of analysis which is involved in implementing the backfit rule. In this case, a variety of safety modifications to the Peach Bottom BWRs are considered. The cost of each modification is estimated, and compared with the associated "benefit". Now, the cost can in principle be estimated objectively. By contrast, the purported benefit is an indicator representing "the monetized value of the averted risk" (NUREG-1150, 1987), and is in part derived from PRA findings. Clearly, there is much room for debate about this indicator, not least about the monetary value which should be assigned to a human life lost due to radiation exposure arising from an accident.

As part of its general move towards probability-based safety regulation, the NRC has recently required its licensees to conduct "individual plant examinations". These may either be Level 1 PRAs (internal initiating events only) or cheaper studies which provide similar information. At a later stage, it is anticipated that licensees will be required to extend this work to include external initiating events and to cover the areas treated in Level II PRAs (Crutchfield, 1988).

Although these plant-specific studies may be useful in identifying safety deficiencies at particular plants, it is unfortunate that the NRC is permitting studies at a lower level of sophistication than is usual for PRAs. Our criticisms of PRAs will, of course, apply with greater force to these cheaper studies.

3 STUDY OF ACCIDENT PRECURSORS

3.1 DEVELOPMENT OF PRECURSOR ANALYSIS

When the 1975 Reactor Safety Study was being prepared, there was a very limited data base of equipment failures and operator errors at nuclear plants. This was noted by the NRC's Risk Assessment Review Group, which proposed two sets of actions to improve the data base (Lewis, 1978):

"First, areas in which there is a paucity of data should be particularly examined to uncover how better data can be obtained. Second, as new data, including additional reactor-years, recorded events and failures, and better component reliability estimates are made, these must be entered into the process in a formal and continuing manner."

The Review Group was also concerned that the Reactor Safety Study might not have identified all significant accident sequences. They concluded (Lewis et al, 1978):

"It is important, in our view, that potentially significant sequences and precursors, as they appear, be subjected to the kind of analysis contained in WASH-1400, in such a way that the analyses are subjected to peer review."

In response to these recommendations, the NRC instituted the Accident Sequence Precursor (ASP) program, which is conducted at Oak Ridge National Laboratory. The purpose of the ASP program is to identify and study events at US nuclear plants which were potential precursors of severe accidents. Relevant events are selected from the licensee event reports (LERs) which nuclear plant licensees are required to submit to the NRC. Events are considered to be accident sequence precursors if they meet the following formal definition established under the ASP program (Minarick, 1988):

"A historically observed element in a postulated sequence of events leading to some undesirable consequence. For purposes of the ASP Study, the undesirable consequence is usually potential severe core damage. The identification of an operational event as an accident sequence precursor does not of itself imply that a significant potential for severe core damage existed. It does mean that at least one of a series of protective features designed to prevent core damage was compromised. The likelihood of potential severe core damage, given an accident sequence precursor occurred, depends on the effectiveness of the remaining protective features and, in the case of precursors that do not include initiating events, the chance of such an initiator."

ASP reports have now been published for events which occurred in the periods 1969-1979 (Minarick, 1982), 1980-1981 (Cottrell, 1984), 1984 (Minarick, 1987), 1985 (Minarick, 1986), and 1986 (Minarick, 1988). In each of these reports, LERs for the period in question are screened in a series of steps so as to

identify those events (typically a few tens of events per year) which were significant accident precursors. Then, the precursor events are examined individually, and an estimate is made of the probability that each event would have proceeded to a severe accident.

3.2 METHODOLOGY FOR ANALYSIS OF PRECURSORS

The first stage in ASP analysis is to screen LERs for the period in question. This process is illustrated by figure 3.1, which shows how LERs for 1986 were screened.

Over 2800 LERs were initially examined, and 1320 LERs were selected for detailed review. Events selected included:

* events commonly identified as initiating events in PRAs (including loss-of-feedwater events, loss-of-offsite-power events, and small-break LOCAs);
* all events in which reactor trip was demanded;
* all support system failures, including failures in cooling water systems, instrument air, instrumentation and control, and electric power systems;
* any event where two or more failures occurred;
* any event or operating condition that is not predicted within, or proceeds differently from, the plant design basis; and
* any event that, based on the reviewers' experience, could have resulted in or significantly affected a chain of events leading to potential severe core damage.

Then, the 1320 selected events were reviewed in detail, to determine if the event was a likely initiator of a core damage sequence or if it represented a failure which could have exacerbated a sequence of different origin. On this basis, 34 events were selected as precursors. Events in this group showed at least one of the following attributes:

* occurrence of a typical core damage initiator (such as a loss-of-offsite-power event, a steam-line break, or a small-break LOCA);
* a failure of a system (or all required trains of a multiple-train system) required to mitigate the consequences of a core-damage initiator; or
* degradation in more than one system required to mitigate the consequences of a core-damage initiator.

The 34 selected precursors for the year 1986 included the following:

* loss-of-offsite-power, small-break LOCA, and small steam-line break initators (8 events);
* loss-of-feedwater (LOFW) initiators with failures in systems required for LOFW mitigation (2 events);
* failures of redundant systems required to mitigate postulated core-damage initiators (18 events);

* degradation in multiple systems required to mitigate postulated core-damage initiators (2 events); and
* reactor trips with failures of redundant systems required to mitigate core damage following a reactor trip (4 events).

After selection, the precursors are analysed to estimate the probability that each one would have proceeded to severe core damage or would have left the core vulnerable to damage. This is done by mapping each precursor onto the appropriate standardized event tree. A variety of standardized event trees have been developed within the ASP program for seven classes of PWR plant and three classes of BWR plant, while a few plants are sufficiently unique as to require their own event trees.

Figure 3.2 illustrates one of the standardized event trees, in this case for loss-of-offsite-power events for a PWR of Class G. At each node of the tree, movement upward indicates success of a safety function, while movement down indicates a failure of that function. Thus, movement downward at the first node of the tree shown in figure 3.2 indicates a failure of reactor trip (RT) after loss-of-offsite-power (LOOP). This precipitates a condition known as "anticipated transient without scram" (ATWS). Other safety functions shown on figure 3.2 are: emergency power (EP); auxiliary feedwater (AFW); challenge or reseat of power-operated relief valve/safety relief valve (PORV/SRV); termination of secondary-side relief; high pressure injection (HPI); high-pressure recirculation (HPR); and containment spray recirculation (CSR).

The occurrence of a precursor event provides an empirical value for the probability of failure at a particular node of the event tree. However, probabilities must also be assigned to all other nodes in relevant parts of the tree. The data base used for these probabilities is partly drawn from within the ASP program and partly from other sources; also, it is partly generic and partly plant-specific. This is a weakness in the ASP methodology.

More generally, the following potential sources of error in ASP methodology have been acknowledged by ASP analysts (Minarick, 1987):

* the accuracy and completeness of information in LERs is sometimes questionable;
* the use of standardized event trees may lead to plant-specific features not being accounted for;
* the combination of generic and plant-specific data means that modeled responses will tend towards a generic response;
* the recovery credit for a failed system involves engineering judgment;
* systems observed to operate successfully during a precursor event are assumed to have independent failure probabilities;
* many probability values used in the ASP program were developed using an assumed equipment test interval of one month, which may not be representative;

* test intervals are assumed to be identical for periods of plant operation and shut-down; and
* the analysis can be influenced by subjective judgment on the part of the analysts.

3.3 RESULTS TO DATE

For illustration, consider the 34 precursors which were identified from LERs for the year 1986. These precursors were estimated to have conditional core damage probabilities ranging from 3,3E-3 (for a small-break LOCA at Catawba Unit 1) to 3,6E-10 (for unavailability of low-pressure core spray at Hatch Unit 2). A total of six events were estimated to have conditional core damage probabilities of 10^{-4} or higher. In brief, these events were (Minarick, 1988):

* At Catawba Unit 1 a small LOCA occurred, initiated by a loss of control power to the letdown orifice valve, which caused the valve to fail open. Following the flow surge, a line rupture occurred downstream of the failed valve's flange. Letdown isolation valves were subsequently closed to contain the LOCA. (Estimated conditional core damage probability: 3,3E-3).

* At Turkey Point Unit 3, following a loss of turbine governor oil pressure and subsequent rapid load decrease, the unit was tripped. During the transient, a primary-side PORV opened but failed to close fully. The operators closed the PORV block valve, and the unit was stabilized. (Estimated conditional core damage probability: 1,4E-3).

* A LOOP occurred at Robinson Unit 2 following a transient when a bus lockout occurred in the 115-kV switchyard. The B emergency diesel generator (DG) was out of service at the time. This DG was subsequently started manually and loaded to restore power to its emergency bus. (Estimated conditional core damage probability: 3,0E-4).

* At Indian Point Unit 2 an inadvertent reactor trip from 100 percent power occurred, and in the ensuing transient AFW was demanded to recover dropping steam generator (SG) levels. However, one motor-driven AFW pump tripped and the turbine-driven AFW pump failed when the steam supply line became overpressurized, resulting in a relief valve lift. SG levels were maintained by the remaining AFW pump. (Estimated conditional core damage probability: 2,9E-4).

* At Catawba Unit 2 all four atmospheric dump valves inadvertently opened during a test for loss of control room function. A transient ensued with SG depressurization, and a main feedwater pump tripped on low suction pressure. Loss of letdown-flow control occurred and high-pressure-injection (HPI) flow from the charging pumps was demanded. Because of the test configuration and valve labeling errors, HPI flow requirements were not met. The test was terminated, allowing HPI to actuate. (Estimated conditional core damage probability: 1,1E-4).

* At Indian Point Unit 2, all 12 condenser steam dump valves inadvertently opened, resulting in a transient and safety injection (SI) actuation. SI train B failed to actuate, but train A actuation closed the main steam isolation valves (MSIVs), ending the high-steam-flow condition. (Estimated conditional core damage probability: 1,0E-4).

If one summed over just these six incidents, and noted that about 100 reactor-years of plant operation were accrued in the United States during 1986, then one would find a core damage (core melt) probability of 5,5E-5 per reactor-year for 1986. However, repetition of that calculation for the most significant precursors (conditional core damage probability of 10^{-4} or higher) observed during 1985 (Minarick, 1986) would lead to a core damage probability of 1,6E-4 per reactor-year for 1985. Clearly, a multi-year summation will give a more accurate indication of core damage frequency, as year-to-year variations will be smoothed out. Also, all precursors (not just the most significant group) should be included.

The ASP program has not published a summation of core damage probability over all precursors for all the years for which it has analysed LERs. However, the first precursor report (Minarick, 1982) did provide an estimate of average core damage probability for the period 1969-1979. This estimate is shown in figure 3.3, where it is compared with other estimates. The ASP estimate ranges from 1,7E-3 to 4,5E-3 per reactor-year, and is much higher than estimates made by WASH-1400 and other studies. That high probability reflects the occurrence of one actual core damage event (at Three Mile Island Unit 2) and two serious incidents (at Browns Ferry Unit 1 and Rancho Seco) during the period 1969-1979.

Although the periods 1980-1981 and 1984-1986 did not exhibit events of such severity, they did show a similar frequency of occurrence of the more significant precursors. This point is illustrated by table 3.1, which shows the frequency (per reactor-year) of precursors which had estimated conditional core damage probabilities exceeding 10^{-3} or 10^{-4} in the periods 1969-1979, 1980-1981, and 1984-1986. No significant differences arise when the various periods are compared.

One of the interesting findings from the ASP exercise has been that dependent failures are very significant. These are failures which arise from design defects, maintenance and testing errors, or other problems which cause more than one item of equipment to fail. Such dependent failures may not be manifested in routine tests but could occur if a safety system were actually needed. In illustration, one data base for failure of high-pressure injection shows 4 failures during 2000 test demands (failure per demand = 2,0E-3) but 1 failure during 4 actual demands (failure per demand = 2,5E-1) (Ballard, 1985).

An analysis by G.M. Ballard (Safety and Reliability Directorate, UKAEA) of the precursors identified for the period 1969-1979 has shown that 69 of the total of 169 precursors involved dependent failures. Moreover, the 73 most significant

precursors included 30 examples of dependent failures. Many of the dependent failures involved multiple failures of essentially identical components. This is now a well-known problem which can in principle be addressed in PRAs and which can be partly avoided through use of staggered maintenance and testing of components. However, there were also 14 incidents in which dependent failures involved non-identical components. Of these incidents, 2 involved internal fire and flood (which can in principle, be accounted for in PRAs). The remaining 12 incidents involved either difficult-to-identify design linkages between safety systems or incorrect operator actions (Ballard, 1985). (Regarding dependent failures, see also section 7 of this report.)

3.4 LIMITS OF ASP ANALYSIS

In principle, ASP analysis can provide a statistically defensible estimate of core damage probability under "normal" conditions. As operating experience is accrued, the range of uncertainty of that estimate can be narrowed. The present uncertainty range is unknown, and this is a matter which deserves consideration within the ASP program.

However, the core damage probability generated by ASP analysis will always represent a lower limit to the actual probability. Increments of probability -- often un-knowable in principle -- will arise from "abnormal" conditions such as:

* gross operator errors (as at Chernobyl Unit 4 in 1986);
* gross maintenance errors;
* design, construction or maintenance defects which do not become evident until systems are exposed to stresses arising under unusual conditions (eg an earthquake within the design basis) or in an accident environment;
* dependent failures of identical or non-identical components which do not become evident until systems are exposed to unusual conditions or an accident environment; or
* sabotage.

4 SHORT SURVEY OF PRA IN EUROPE

4.1 WEST GERMANY

In the FRG, PRA efforts started early, inspired by the US Rasmussen-Study (WASH-1400).

The German Risk Study (Deutsche Risikostudie Kernkraftwerke, DRS), performed by Gesellschaft für Reaktorsicherheit for the Federal Ministry for Research and Technology, was begun in 1976. Phase A of this study was concluded in 1979, although some of the technical reports appeared as late as 1981. The German Risk Study is a level III PRA for the Biblis B PWR, including external accident initiating events. In Phase A, the methodology was fairly close to WASH-1400; as in WASH-1400, some initiating events were explicitly excluded and reserved for treatment in Phase B (e.g., secondary-side events like steam line break, and steam generator tube rupture). The data base employed was generic.

Phase B started in 1981. The methodology was developed further, and additional initiating events were included. The data base is partly plant-specific, partly generic. Official publication of this study, originally expected for late 1988/early 1989, took place on June 30, 1989. Only a summary of results is available to date (DRS B, 1989).

In the period 1985 - 1987, a "German Precursor Study" was also performed by Gesellschaft für Reaktorsicherheit for Biblis A and B. Due to the small basis of operating experience on which this study is based, it is of very limited use.

Further, more limited level I analyses have been performed during licensing procedures for nuclear power plants (e.g. for Brokdorf, Grohnde, Philippsburg-2), analyses of certain safety systems have been performed by the plant manufacturer KWU (Balfanz, 1987).

4.2 UNITED KINGDOM

PRAs for Light Water Reactors were introduced in the UK at the beginning of the 80s, in connection with the Sizewell project. US know-how was extensively employed. The two major efforts are:

-- The Probabilistic Risk Analysis contained in the Sizewell B PWR Pre-Construction Safety Report, submitted in 1982 by the CEGB. It was a level III PRA including external events for Sizewell B; the data base was, of course, generic (US plants).

-- The Sizewell B Probabilistic Safety Study (WCAP 9991), 1982, performed by Westinghouse Corporation (WEC, 1982), scope as above.

Further work based on those PRAs (revisions, sensitivity studies etc) has been performed since.

4.3 SWEDEN

PRA studies were started early in Sweden. In the period 1976 - 1978, three studies on the probabilities of large releases in Swedish BWRs were carried out on the initiative of the Swedish Energy Commission (on Barseback 1 by Studsvik Energiteknik AB and the US-firm MHB Associates, and on Forsmark 3 by Asea-Atom AB).

In 1982, a new initiative began: Level I PRAs are now performed for all nuclear power plants by the utilities, and are reviewed by the Swedish Nuclear Power Inspectorate (SKI), in the framework of the ASAR (As Operated Safety Analysis Report) programme. At present, PRAs for 10 out of 12 plants are available; the remaining plants (Ringhals 3&4) are planned to be analysed and reported by 1990.

The PRAs include internal initiating events only; external event analyses are being planned or are in progress. Several studies have a scope which is further limited since certain types of transients are not considered (Carlsson, 1987).

4.4 FRANCE

Systematic PRA efforts were introduced in France relatively late. Probabilistic methods have been used since 1980 as a support for defining technical specifications of safety-related systems. In the period 1983-1985, partial analyses have been undertaken for the future 1400 MWe N4 PWR units. Beginning in 1986, a level I PRA for one of the 4 Paluel NPPs was performed. External events are not taken into account. Levels II and III of PRA are considered to contain too many uncertainties and are thus not performed (Moroni, 1986; Villemeur, 1987).

4.5 OTHER COUNTRIES

PRA efforts of limited scope have been undertaken in many European countries; e.g., Switzerland, Finland, and Italy.

4.6 EASTERN EUROPE

No PRAs were performed or planned in the Soviet Union and other Eastern countries before the Chernobyl accident. V. Legasov, in his famous "Memorandum" published on May 20, 1988 in Pravda, stated that no institution in the Soviet Union is competent to perform a PRA (Legasov, 1988). In the last years, however, the Soviet Union has engaged in efforts, particularly within the IAEA framework, and is attempting to buy PRA know-how in the West - among others from West German firms.

Level I of PRAs

5 DATA BASE

5.1 INTRODUCTION

In order to determine the overall probability of a given accident sequence, data characterizing each individual step of the sequence are required. Those data fall into different categories:

- probabilites of initiating (internal and external) events;
- failure rates for components;
- failure rates for human behaviour;
- characteristics of core melt progression;
- behaviour of containment in different sequences.

In this section, we deal with internal initiating events and component failure rates, i.e., with the part of the problem associated with level I of PRA (except human behaviour which is a topic of such crucial importance that it merits special treatment).

Regarding the initiating events, there is a wide spectrum ranging from comparatively frequent occurrences (e.g., loss of main feedwater in a PWR, with a frequency of occurrence in the order of magnitude of one per year); to rare events which have not been observed in operating practice so far, but which can by no means be excluded from consideration (e.g., large-break LOCA, or reactor pressure vessel failure). It is clearly a major problem for the risk analyst that it is necessary to include events which have not occured yet, and for which there are no data available. The number of different initiating events considered in a PRA usually is about 10 to 20.

Of enormous scope and complexity are the data describing component failure rates. There are numerous pumps, valves, instruments, electrical switches and devices, etc., the functioning of which will be required to prevent core melt after certain initiating events. Furthermore, there are different failure modes for most components, e.g.: a valve may fail to open, or to close; with different probabilities in each case. A pump may fail to start, or, having started, it may fail to deliver; or it may fail after having operated properly for some time. Failure to start on demand may be caused by a defect which occurred in a component while it was idly on stand-by; or it may be caused by difficulties in getting an intact component started. The first contribution to the "failure on demand" probability would be dependent on the time since the component was last used or tested; the second would depend on the complexities of getting the component started.

Thus, the amount of data required in a PRA is large. For example, the German Risk Study (Deutsche Risikostudie Kernkraftwerke. DRS), e.g., lists 1457 functional elements which occur in its fault trees. For each element, a failure rate must be given (DRS A 2/II, 1981). The failure rates themselves vary considerably, e.g., the failure rate per hour

of stand-by time for different components as given in the German Risk Study varies by almost 4 orders of magnitude (from 2,5E-5/hr down to 4E-9/hr).

Frequencies of initiating events, and failure rates of components, are never known with absolute accuracy. Strictly speaking, each failure rate or event frequency is a random variable. In order to arrive at meaningful results in a PRA, information is required on the distribution of those random variables; most importantly, on their possible deviation from the mean value, and on the amount of correlation between the different variables. Even disregarding all other complexities and problems of a PRA, this statistical character of its input alone means that a PRA can never calculate accident probabilities; it can only estimate them.

Data used in PRA come from different sources; in particular, it is important to distinguish the following levels:

- general industry experience;
- data from fossil-fueled power plants;
- data from nuclear power plants;
- data from the NPP being analysed ("plant-specific" data).

Although there is a vast amount of data available, the selection and compilation of the data for a PRA is by no means trivial or straightforward.

5.2 SUMMARY OF MAIN PROBLEMS

The importance of a sound data base for a PRA can hardly be exaggerated. It is well known that even the most sophistcated computer models cannot yield results which are better than their inputs. The requirements which have to be fulfilled can be pointedly summarized as follows:

"A sound determination of failure rates clearly presupposes that a large number of parts of the same kind are observed for a long period of time under completely identical conditions, and that the failures are registered during this observation" (Lindackers, 1982).

The same applies, of course, to the determination of initiating event frequencies. Unfortunately, there are no generally recognized, rigidly applied criteria determining how many individual parts must be observed for which period of time to allow meaningful determination of failure rates and event frequencies; and there are no clear-cut rules to decide which parts may be regarded as belonging to one statistical population which is characterized by one failure rate.

Furthermore, there is no uniform practice for the registration of failures, and the documentation of failure rates. The problem lying at the bottom of this lack of uniformity and consistency in the data base for PRAs is simply that in the vast majority of cases, PRAs have to use data which were collected for other purposes, and hence do not constitute

results of observations which were, a priori, planned with the specific purpose of creating inputs for a risk analysis. For example, the Licensee Event Reports of the USNRC are designed for regulatory purposes, not PRAs (Apostolakis, 1985). The main purpose of the IAEA's Incident Reporting System is to facilitate exchange of information on significant events between nuclear plant operators and licensing authorities. The reports vary greatly in detail and methodology of description, although efforts are under way to improve uniformity. Data to be found in the literature are often incomplete and contain only information relevant for the specific purpose for which they were compiled. Thus, there may be no differentiation for different failure modes, very sketchy description of the data sources, or only certain types of failures may be reported (e.g. those leading to long repair times) (DRS A 3, 1980).

As long as this situation prevails, the choice of data for a PRA contains a large degree of arbitrariness. Many problems could, in theory, be avoided if exclusively plant-specific data were used. However, for comparatively rare events (e.g., certain accident initiators, and common mode failures), this will simply not be possible for lack of observations. Even for other events, the data base will often be small, leading to very large uncertainties in the estimation of failure rates and event frequencies; and it will be necessary for the plant to have operated for many years before meaningful estimates will be available.

Additional arbitrariness is introduced because there are often several methods, each equally plausible, to combine different data sets to obtain a larger data base for a PRA. The end result can vary significantly according to the method being used.

Progress has been made towards the establishment of data bases for nuclear power plants. In principle, it appears possible that reasonably uniform, well-classified and mutually compatible data bases will be established; although this would require much time and energy, and the political and economic obstacles for a world-wide integration are formidable. Even if this aim were reached, however, risk analysts would face two constraints which can never be overcome:

o Due to the complexities of data collection and compilation, generic data bases can never be completely up-to-date. A lead time of several years between an observation and its availability in a data bank has to be allowed for. Occurrence of rare events, possible new phenomena, plant ageing, technological change and other developments, and new criteria for data collection will be reflected in the data bases with inevitable delay.

o If only plant-specific data are used, processing can undoubtedly be faster. But in order to collect sufficient data, a risk assessment based on plant-specific data can be performed only after much of the plant's lifetime is over: The results may come too late. Even so, generic data will have to be used to supplement plant data.

5.3 BACKGROUND

In the present-day data situation, arbitrary choices and simplifying assumptions have to be made right at the beginning of compiling a data base. The first simplification lies in assuming constant failure rates and event frequencies. It is not taken into account that failure rates will generally be higher at the beginning of a power plant's operational life, or for new types of components in the time after they have been fitted. It is also assumed that components remain "as good as new" during their service time. Degradation through repeated repairs, or simply through ageing, are not allowed for.

The properties of the random variables which characterize failure rates and event frequencies are generally chosen for convenience, i.e. to make the calculations as simple as possible, rather than with the aim of an adequate representation of reality. Usually, it is assumed that the variables are distributed according to a lognormal distribution (i.e., their logarithms follow a normal, or Gaussian, distribution). The advantage of this assumption is that multiplication and, to some extent, addition of lognormally distributed variables is fairly straightforward mathematically; it is easy to describe the bandwidth of uncertainty; and the bandwidth of uncertainty, when combining a large number of variables by multiplication and/or addition, does not escalate dramatically, if the random variables are uncorrelated (i.e., if their fluctuations are subject to random errors only, and not to systematic errors), as is generally assumed.

A lognormally distributed random variable is characterized by its median M (i.e., the 50%-fractile) and, most commonly, by the variation factor K_{95} (simply denoted as K thereafter), being the ratio of the 95%-fractile to the median ($K=F_{95}/M$ and also, by the properties of the lognormal distribution, $K=M/F_5$, F_5 being the 5%-fractile). K is a measure for the bandwidth of uncertainty associated with the variable. The mean or expectation value E of the lognormal distribution is not equal to the median. It is larger than the median, the ratio growing with K (see fig. 5.1).

The fundamental problem is that the use of the lognormal distribution cannot be justified theoretically, or empirically. According to mathematical theory, the failure rate of a complex component will be lognormally distributed if the failure rates of its parts can be described by independent distributions, and common-mode failures can be neglected. It must be doubted whether those conditions hold in the majority of cases. Furthermore, empirical investigations of data on failure rates do not yield unambiguous evidence that the lognormal distribution is appropriate. In many cases, it would seem more appropriate to use other distribution models (e.g., the log-cauchy distribution), or "robust" methods which are independent of assumptions concerning the distributions. Those alternative methods would allow a more realistic description of error propagation and would lead to much larger uncertainties in the

final results - less convenient perhaps, but giving a more adequate picture of reality.

Choosing distribution functions is a very complex and fundamental problem of PRAs. We are not entering a more detailed discussion here since this problem has already been discussed at length in a study by the Öko-Institute (Öko, 1983), on which the preceding paragraph is based.

Furthermore, the individual random variables may be, to varying extents, correlated. This can lead to a large bandwidth of uncertainty when they are combined (this problem is treated further in section 6).

The sources of reliability data are in most PRAs arbitrarily selected and combined in an arbitrary manner. This is due to the lack of a consistent, comprehensive data base. In the German Risk Study, Phase A, data were taken partly from the general literature, and partly from a special evaluation of operating experience at the Biblis A and Stade plants (9 reactor years in all; note that the reference plant for the German Risk Study is Biblis B). The weight each source is given varies from component to component, depending on the respective quality for the data available. Even so, additional arbitrary assumptions were required in some cases because otherwise the data would not have been detailed enough to serve as input for the fault tree evaluation. For example, several sources did not differentiate between the two failure modes "failure to start" and "successful start, subsequent failure during operation" for pumps, and the data were arbitrarily divided. Furthermore, the literature sources, in part, were not independent (DRS A 3, 1980; Öko, 1983).

Thus was violated a very basic principle of statistical methodology: First to plan the data sampling and evaluation procedure, and then take and evaluate the data sample, rather than choosing the evaluating procedure so that it fits conveniently the data samples obtained. The consequence is that the uncertainty of the results of the German Risk Study in fact is much larger than claimed.

There is not much improvment in Phase B of the German Risk Study, as far as can be inferred from preliminary publications of results. In Phase B, it is aimed at using only plant-specific (Biblis B) data, wherever possible. The problem of arbitrariness of data sources is thus avoided. However, on the other hand, the plant-specific data base is extremely small in some cases. The observation period is 3 years or less, and the failure rates given are, e.g., about 3E-5/hr for emergency feedwater pumps, and 1E-5/hr for component cooling water pumps. Taking into account the number of pumps in the plant, this implies that the data base for emergency feedwater pumps consists of about 8 failures in all, and for component cooling water consists of about 5 failures - a data base insufficient for reasonable statistical estimation. Nevertheless, the authors of the study claim that for the examples given here, the variation factor K is as low as 2,4. A conservative

analysis shows, however, that K should be at least twice that number.

In some instances, generic data had to be used in Phase B: For safety valve failures, certain initiating events, and common mode failures. Hence, it was not possible to avoid the arbitrary combination of different data bases (Hörtner, 1987).

In principle, a methodology is available for the systematic combination of generic data with plant-specific information, with the aid of Bayes' theorem (see, e.g., Mosleh, 1985).

The Bayesian approach in mathematical statistics is, in general, subject to controversy. We cannot go into the details of the differences between "Bayesian" and classical "frequentist" theory here. It is sufficient to show that use of Bayes' theorem in PRA can lead to inconsistencies and arbitrary assumptions, or even assumptions which lead to a bias in the results. This can be shown by discussing the methodology of the German Risk Study, Phase B.

The starting-point is Bayes' theorem for a failure rate l:

$$f(l/J) = f(l).L(J/l)/\int f(l).L(J/l).dl$$

where

f(l/J).....probability density function of l, given the information J (posterior distribution)

f(l).....p.d.f. of l without knowledge of J (prior distribution)

L(J/l).....Likelihood-function, i.e. probability distribution of information J for a given value of l

and $\int$ denotes integration from 0 to ∞.

At first, a two-stage approach was attempted in the German Risk Study. In the first step, the prior distribution was based on data from Phase A, while data from Swedish, US and German nuclear power plants constituted the information J. In the second step, the posterior distribution resulting from the first step was taken as a prior distribution, and plant-specific observations from Biblis B provided the information J. Result: A plant-specific distribution incorporating prior information.

The arbitrariness here lies in defining the different levels of information for each step. The prior information of the first step (from Phase A) is mixed: It contains data from non-nuclear plants, but also from nuclear power plants. The information J in the first step contains data from various plants. It is by no means evident that this is the only logical and methodologically correct manner of grouping the data. Indeed, it seems much more plausible to consider the data from non-nuclear plants as prior information, and all nuclear plant data

(from Phase A plus information J) as the second set of information.

Looking at both steps, it seems highly arbitrary that data from two German plants (Biblis A and Stade) are grouped together with Swedish and US data, whereas data from Biblis B are taken as a separate data set. Several other ways of combining the data seem at least as plausible. For example, Swedish and US data could be taken as one set of information, and data from the three German NPPs as another. Or, the number of steps could be increased by one. At first Swedish and US data could be introduced into Bayes' theorem; then Stade and Biblis A data; and finally Biblis B data. There are further possibilities which we will not elaborate here. The point is not to propose an alternative application of Bayes' theorem, but to make it clear that the combination of data by this theorem can contain a large amount of arbitrariness in practice. The resulting failure rate distribution can vary greatly depending on how the data are integrated; in particular, the uncertainty bandwidth can be artificially reduced if data are divided into several sets and then combined by Bayes' theorem, rather than taken as one set with one distribution.

Apart from those considerations, it seems highly arbitrary that Phase B of the German Risk Study selected, apart from plant-specific data, data from 8 Swedish, 1 US and 2 other German NPPs for consideration as prior information. Why not a more complete data base, or why not include French instead of Swedish, or Japanese instead of US data? It is a fair guess that convenience of data acquisition was the chief criterion in making this particular selection, rather than a systematic analysis of what would constitute the most adequate dta base.

In its attempt to combine generic with plant-specific information, another problem became apparent in the German Risk Study, Phase B: For about 50 % of component failure rates, the plant-specific distributions deviated quite markedly from the generic information. Therefore, it was decided - for all failure rate distributions - not to use the generic prior information at all. As the generic failure rates were often significantly lower than the plant-specific ones, this practice may be laudable insofar as it is conservative. It demonstrates, however, another arbitrary point in the combination of data: There are no strict and cogent rules to decide which data are relevant for the case under study, and which should not be used.

In the absence of relevant prior information, a so-called noninformative prior was used in the German Risk Study to determine the posterior probability density function. Although a noninformative prior, in Bayesian statistics, is supposed to be a "neutral" function which does not modify the information at hand, there are again several choices open. The special Γ-distribution used in DRS is a mathematically convenient choice, but does in fact influence the results: By its use, the posterior distribution is artificially shifted to smaller values (Martz, 1984).

Another illustrative example for the arbitrariness involved in data base selection is the Probabilistic Safety Study of Sizewell B, prepared for the CEGB by Westinghouse (WEC, 1982). In this study, which is based on data from the US PWR population, at least 21 % of the operating data base was excluded. The omissions are not explained; some appear rather convenient since they involve reactors where serious accidents have occurred (TMI-2, Crystal River 3, Rancho Seco). Thirty-four important precursor events were neglected in the Westinghouse study because of those omissions (Thompson, 1983).

The selection of incomplete data bases, as well as the arbitrary assumptions of narrow distributions for failure rates in spite of insufficient data bases - as in the German Risk Study (see 5.4) - lead to a general underestimation of the bandwidth of failure rates, and hence finally to an underestimation of the uncertainty of the final severe core damage frequency result (compare also 6.3.3).

The emergence of well-organized data bases can potentially reduce arbitrariness both in selecting and combining data. The available mass of data has certainly grown considerably in the past years. At a recent international conference on Probabilistic Safety Methods, one speaker even coined the term "data deluge" (Fragola, 1985). Yet the same author continues to remark: "... despite the waterfall of raw information being generated by over 70 (NPPs) on a daily basis in the US alone, and individual successes, the advance in published and available data has not improved as dramatically". He describes four major US data bases which all have their strong and weak points. No single data base covering a large number of years of operating experience for all US plants in a consistent manner seems to be available. However, there is significant potential for future improvement.

As it appears that the largest amount of work on data bases has been performed in the United States, a more detailed report on PRA data bases in the U.S. has been prepared for this study by MHB Technical Associates (Appendix 5A).

In Europe, efforts are under way in the European Community (with Swedish participation) to set up appropriate data bases. In the framework of ERDS (European Reliability Data System), data on operational history of nuclear plant components, abnormal occurences, and unit productivity are being collected. The fourth sub-system, however, the Reliability Parameter Data Bank, was still in its definition phase by 1987 (Amendola, 1987).

The PSAPACK (Integrated PC Package for PSA level I) recently published by IAEA (Boiadjev, 1988) also contains a reliability data base module compiled from 21 sources and containing about 1000 records. This data base, however, contains many poorly documented records. It also contains (as do other reliability data bases, e.g., IEEE 500-1984 in the US) a considerable number of data derived from expert judgment, and not directly from operating experience. It is known since the first critical reviews of WASH-1400 that such data are of little value. Apart

from the arbitrariness involved in determining failure rates by expert estimation, there is a general bias involved - the values tend to be too low, as "people tend to be too confident" (Apostolakis, 1985).

With growing complexity and size of data banks, the problem of providing adequate access for the risk analysis will also grow. Work is under way to develop expert systems ("intelligent" interfaces) in order to allow users access to data banks in natural language. It remains to be seen how the problems of incompleteness and vagueness of information in the data bank, and also of possibly incomplete or imprecise queries, can be solved efficiently (Amesz, 1985).

Further development of data bases may face severe problems: It cannot be taken for granted that a continuous and growing budget will be made available for such efforts, and that political or economic (e.g., commercial secrecy) factors will not prove serious obstacles. Even under optimal circumstances, however, one problem is bound to remain: The unavoidable lead time between the moment when data are generated, and the time they are available for PRA. Mounting experience and further development in the electronic data processing sector can potentially decrease this lead time. Increasing amounts of data and, possibly, new methodological approaches and regulatory requirements (necessitating a reorganization of data collection) may, on the other hand, counteract this trend.

In the past, the delay between the closing of the data base for a PRA study, and the conclusion and publication of this study, was in the order of several years: e.g., 4 years for the German Precursor Study; about 2-3 years for the German Risk Study, Phase A; possibly more for Phase B; 1 to 2 1/2 years for the US Precurror Studies; and 2 1/2 years for the Swedish SKI-ASAR on Barsebäck (1985).

Thus, PRAs are bound to give a picture of a past state. Rare events occurring for the first time can render them obsolete (like the Biblis A incident in December 1987 - an almost-LOCA with containment bypass, which demonstrated that the significance of this accident sequence is considerably greater than was assumed in the German Risk Study, Phase A). New phenomena can necessitate the inclusion of whole new types of accident sequences (e.g., Hydrogen generation at TMI-2 in 1979 was a phenomenon which had not been foreseen in its acutal severity). Plant ageing may increase the importance of certain failure modes and events (e.g., through neutron embrittlement of reactor pressure vessels). Furthermore, any technological changes, plant modifications, new criteria for data collection etc. will not enter the data banks immediately. This problem is particularly severe when nuclear power use continues to grow. The higher the growth rate, the larger the number of reactor-years - at any given point in time - which are not yet properly included in data bases.

In principle, and with an established methodology, the collection and processing of plant-specific data could be faster than the creation of equivalent data banks for large

reactor populations. But for some failure modes, it will be impossible, in the long run as well as now, to work without generic data. Furthermore, setting aside this point, a PRA using plant-specific data is more or less a posterior analysis. In order to obtain a reasonably reliable data base, an observation period of more than 10 years (often much longer) will be required. Adding to this a couple of years to perform the PRA, the results might not be available before a time when the operator will have to begin thinking about plant decommissioning. Considering this, the risk analyst is caught on the horns of a dilemma: Neither the use of generic, nor of plant-specific data can yield accurate results which are available at an early date.

6 BASIC METHODOLOGICAL QUESTIONS

6.1 INTRODUCTION

The subject of this section is the methodology of level I of a PRA, i.e. the question: Given a nuclear plant, and a suitable data base, how can the severe core damage frequency (SCDF) be estimated? This question covers the problems encountered in constructing fault trees and event trees, and in combining basic data on failure rates and initiating events with their aid. A crucial point is that practically all input data are not precise numerical values which can be simply combined by multiplication and addition. The inputs in fault and event trees are random variables which can assume different values with varying probability. Thus, the result - the SCDF - will also be a random variable with, possibly, a considerable bandwidth of uncertainty attached to it.

We do not deal with the basic principles of fault tree and event tree construction. A critical discussion of this step would have to concentrate in great detail on individual PRAs. This lies outside the scope of this study. We can also not enter the discussion on the merits of basic alternatives to the fault tree/event tree methodology. One possibility - the modelling with the aid of Markov-processes - which might be better suited to describe the dynamics of accident sequences, is discussed at length elsewhere (Öko, 1983).

A partial alternative to the usual fault tree/event tree methodology is the "precursor"-approach based on the evaluation of incidents which actually occurred. This approach is treated in section 4.

There are some methodological problems which are of such crucial importance that they are treated at length in separate sections of this study. Common cause/common mode failures (the failure of several components of the same kind at the same time, due to a common influencing factor, which can only with great difficulties be incorporated in the fault tree/event tree methodology) are treated in section 7. The whole complex of "human error" is addressed in section 8. In this section, we briefly discuss the problems of constructing models by combining event trees and fault trees, which lead to the question of completeness in a PRA, which is obviously crucial if the analysis is to give meaningful results. Furthermore, we explore the consequences of the fact that SCDF as determined in a PRA is a random variable. Finally, the problems of possible correlations of input random variables and their influence on error propagation through the fault tree/event tree models are treated.

6.2 SUMMARY OF MAIN PROBLEMS

A severe problem which continues to plague PRAs is that their completeness can never be guaranteed. Even in a restricted

framework (level I, internal initiating events only, exclusion of complex forms of human errors, assuming the plant is built as designed), there always remains the possibility of unknown accident sequences which would increase the estimated SCDF. The analyst can choose among different approaches (event tree oriented, or fault tree oriented) when modelling accident sequences, each of which has its particular shortcomings. Furthermore, the importance and/or frequency of recognized accident sequences are often overlooked, and it may be wrongly assumed that their contributions are "covered" by another sequence or class of sequences. Even major PRA efforts performed so far show severe omissions: e.g., of steam generator tube rupture sequences in NUREG-1150 and the Westinghouse PRA for Sizewell B; or of the V-sequence (LOCA through connecting line which bypasses the containment) in the German Risk Study, Phase B. In the latter case, the V-sequence was at first considered to be a negligible contributor to SCDF; the study had to be revised, however, after a very severe precursor to the V-sequence occured at Biblis A in December 1987.

In principle, progress appears to be possible in regard to PRA completeness through accumulation of further experience, better peer reviews, and an open and efficient exchange of information between PRA teams. However, budgetary constraints as well as political and economic obstacles can render such progress difficult. Furthermore, there is persistent reluctance on the part of many risk analysts to take into account controversial expert opinion. Also, it must be noted that improved procedures will also be more time-consuming and would result in increased delays between the collection of basic information for a PRA and its completion and publication. For this reason alone, PRA results can only be regarded as lower bounds for the (unknown) "real" values of accident probabilities, today as well as in the future.

A problem which is associated with the use of PRA results in decision-making is the fact that their level I result - SCDF - is a random variable and not a single value. In order to determine, e.g., whether the basic IAEA criterion (frequency of SCD less than 1E-4/yr) is fulfilled, is it sufficient that the mean (expectation value) of SCDF is below this limit? This does not appear satisfactory because even then, the probability that the actual SCDF is higher than 1E-4/yr can still be significant. For example, the mean SCDF as determined in the German Risk Study, Phase A, was 0,9E-4/yr. Yet, the probability of SCDF being higher than 1E-4/yr is about 30 %, even accepting the rather small uncertainty range as given by the authors of this study. A more reasonable and conservative criterion would be, e.g., to demand that the 99%-fractile of SCDF must be below 1E-4/yr (i.e., the probability of SCDF being higher than 1E-4/yr would be below 0,01). If this criterion were applied to existing PRA results, however, it would be fulfilled in almost no case.

The problems of error propagation, and of correlation between failure rates, are treated here at some length. We show that, even if all input random variables can be assumed to be

uncorrelated, the bandwidth of uncertainty of the result is considerably larger than that of the individual inputs. In many PRAs, however, by assuming small, optimistic variation factors for the input data, the SCDF bandwidth is usually kept artificially low. This is of particular importance if not the mean, but the 99%-fractile (or the 95%-fractile) of SCDF were used as the decisive yardstick.

This problem is significantly exacerbated by the fact that the input variables are to some extent correlated - their deviations from the mean value will to some extent fluctuate systematically, and not completely randomly. Systematic fluctuations add up to considerably larger error margins in the final result. Furthermore, because of the intrinsic characteristics of a system whose components have failure rates close to zero, this increase in the variation factor alone - all other things being equal - will lead to an increase in the expectation value of SCDF. Thus, underestimation of variation factors and of correlation will lead not only to unrealistically small and misleading error margins (and hence to 99%-fractiles which are too small); it will also lead to an underestimation of mean SCDF. The problem of correlation is ignored in present PRAs; zero correlation is generally assumed for computational convenience.

A numerical example is provided here using a comparatively simple fault tree from the first draft of NUREG-1150. It demonstrates the crucial influence of correlation of individual variables. It shows that high correlation leads to such large error margins as to render the results of PRAs practically meaningless, unless the error margins of the input variables are small. It must be noted that our calculations are based on the assumption that probability distributions are lognormal, which is an arbitrary assumption tending to underestimate error margins.

6.3 BACKGROUND

6.3.1 Completeness

The topic of completeness of a PRA is, in this section, treated in a restricted sense only. The most serious problems which render it impossible to perform a really complete PRA (one that takes into account every relevant factor) are: The unpredictability of complex human behaviour; the fact that a real plant will differ from idealized plant models because of design deficiencies, use of components of low quality, etc.; the difficulty of quantifying the probability of external events; the large uncertainty associated with physical phenomena affecting containment integrity (regarding level II); and similar points. All those aspects are important and are treated in other sections of this study.

In this section, we concentrate on the one part of a PRA where, in principle, the highest accuracy and reliability of results can be achieved: The modelling of accident sequences leading to severe core damage (level I), initiated by internal events, and

disregarding complex forms of human error. The key questions are whether past PRAs have been complete in this respect; and if there were deficiencies, are they likely to be resolved in the future?

In PRAs, accident sequences are modelled using event trees and fault trees. At first, event trees are constructed for different initiating events. Then, fault trees are compiled for the calculation of the unavailabilities of the various functions contained in the event tree (for examples for event and fault trees, see figures 1.1 and 6.1). When performing this modelling exercise, the analyst has considerable freedom of choice: A large number of event trees could be used, each describing a specific accident sequence, combined with relatively simple fault trees. Alternatively, the analysis could be based on a small number of event trees, one for each class of accident sequences under consideration, with very detailed and complicated fault trees. Of course, compromises between those two extremes are also possible.

It has been suggested that this situation represents a dilemma (Hahn, 1985): An event tree oriented approach (large number of specific event trees) could be more adequate to model the dynamics of accident sequences, but increase the danger of overlooking sequences; whereas a fault tree oriented approach could, in principle, achieve better completeness (since each event tree covers a whole class of sequences), but would neglect the dynamics of the sequences, which cannot be incorporated into static fault trees.

On the other hand, it could be argued that employing a large number of event trees might make it easier to approach completeness. We do not need to pursue this point further here - it is a question of optimization within PRA methodology, and not directly relevant for our work.

The point which is relevant for this study is the inherent difficulty to achieve completeness in a PRA - either because of the omission of initiating events, or because of the omission of a particular sequence developing from an event which was included in the analysis, because the fault trees employed do not adequately reflect the dynamics of the accident.

It should also be noted that event trees and fault trees are binary systems (only two states are possible: component functions perfectly/component fails completely). Partial failure of components usually is not taken into account. However, in some cases partial failures can have worse consequences thatn complete failures (for instance, dropt of voltage which leads to unpredictable behaviour of electrical systems; intermittent function of a pump leading to flow instabilities).

It is also clear that empirical knowledge of plant behaviour is limited. Thus, the full spectrum of sequences leading to SCDF is not known. The consequence is that "an evaluation of all known and quantifiable sequences, even if this is done as realistically as possible, will provide inevitably an

underestimate of the real (severe core damage frequency) because the values of those sequences not analysed have to be added to the result based on the sequences which have been analysed. This fundamental problem of incompleteness leads to the conclusion that even the best conducted and realistically based evaluation can only give a lower bound to the real value" (Hahn, 1985). With a somewhat different emphasis, another expert states that "generally the safety analyses performed for plants have included either explicitly or implicitly the failure sequences that have occurred. However, less satisfactory is the indication that in some cases the relative importance and likely frequency of the actual event sequences may have been significantly underestimated by the safety analyst" (Ballard, 1986).

The problem of underestimation of the importance and frequency of a sequence is of course closely connected to the fact that completeness cannot be achieved by explicitly treating all possible sequences in a PRA. Usually, classes of sequences (categorized according to the initiating event) are considered; and each class is implicitly expected to include a number of sequences which are less frequent and/or lead to smaller consequences than those explicitly studied. However, a particular sequence, which has not been explicitly considered, may place heavier demands on safety systems than those explicitly analysed in its class. Or, the frequency of a whole class of sequences may be underestimated because important events have been omitted from the analyses (Hahn, 1985).

Furthermore, classes of sequences may be included in a PRA in the sense that they are mentioned, only to be dismissed, through faulty reasoning, as negligible.

Hence, the important question is not whether all relevant accident sequences are in some way, however vaguely or implicitly, included in a PRA. The question is whether the significance of all relevant sequences has been correctly recognized.

Experience shows that this has usually not been the case in PRAs performed to date. For example, in the USNRC's Draft Reactor Risk Reference Document (NUREG-1150, 1987), accident sequences initiated by steam generator tube rupture were not treated for the Surry and Sequoyah PWR . It was argued that their effects were covered by another sequence (the V-sequence: LOCA outside containment via the low-pressure-injection system). However, the contribution of steam generator tube rupture to severe core damage frequency is highly significant; in the case of Surry, it can be about as much again as the overall frequency assessed in the first draft of NUREG-1150 (Kastenberg, 1988). In the Westinghouse Sizewell Safety Analysis (WEC, 1982), steam generator tube rupture with stuck-open secondary pressure relief valves, as well as other sequences were omitted (Thompson, 1983; Hahn, 1985). In the German Risk Study, the V-sequence was included in Phase A (DRS A, 1979). It was then dropped from further consideration in Phase B because no significant contribution to SCDF was expected (GRS, 1986). In the end, it was included again

(Heuser, 1989); it is plausible to assume that the reason for this latter change of attitude was not new, deeper theoretical insight resulting from continuing work on the Risk Study, but rather the fact that the PWR plant Biblis A experienced a very severe precursor to SCD via V-sequence in December 1987.

A class of accident sequences systematically excluded from detailed treatment in all PRAs performed so far are those initiated by reactor pressure vessel failure, because this event is assumed to be too unlikely. In fact, it can be shown that the reasoning behind this assumption is questionable. This point has been treated in connection with Phase A of DRS (Öko, 1983), and is taken up here in detail in section 9.

Effective peer review, efficient and open exchange of information between risk analysts, and growing experience with PRAs could in principle permit PRA analysts to come very close to the goal of completeness in the restricted sense discussed here, although absolute certainty that nothing has been overlooked can of course never be achieved.

However, considering that in practice there are budgetary constraints, tight deadlines, as well as changes in plant design etc. which need to be taken into account, it must be feared that future PRAs will still be plagued by incompleteness and unjustified omissions, and the significance of some accident sequences will only be acknowledged after they have in fact occurred.

It must also be noted that improved review and critical discussion of PRAs, in order to better achieve completeness and to improve quality, would generally require additional time and hence would increase the delay time between data gathering (at the plant under study) and the availability of the final PRA results. The quality of the results might thus be improved, but their usefulness diminished (compare section 5).

6.3.2 Randomness of PRA results

It has already been pointed out (section 5) that the individual event frequencies and failure rates which are combined by means of fault and event trees to yield the frequency of severe core damage are random variables. That is, they are not simple numbers which are known with certainty, but variables which can assume different values. The reason is partly that two components are never completely alike; thus, even two pumps of the same type, produced by the same company, will not have exactly the same failure rate; two pieces of pipe, even if produced in the same manner from the same material, and having equal diameter and wall thickness, will not have exactly the same probability to break, etc. This kind of uncertainty is aggravated by the fact that often, in order to determine, e.g., a failure rate, observations must be drawn from components which are not exactly identical (e.g., different types of valves) in order to obtain a data base sufficient for statistical estimation. In part also, the random variations come from the fact that our body of experience is limited; if

only a small number of failures has been observed for one type of component, the exact failure rate could not be determined even if all components involved were exactly identical (this kind of statistical uncertainty does not vanish completely with a growing data base, but it becomes small if estimates are based on large numbers of observations).

In practice, therefore, the risk analyst has some idea of the value a given variable is most likely to have, and of the bandwidth within which it will almost always lie. The exact probability distribution is, however, unknown. Assumptions are made according to convenience - i.e. distributions are selected, which can be easily handled mathematically, as long as they roughly fit to the data.

The question of arbitrariness and convenience of assumptions was already discussed in section 5 and will be further discussed below. At this point, we discuss a different aspect of the problem.

The SCDF, as calculated in PRAs, is a function of random variables (failure rates and event frequencies) and, thus, is itself a random variable. Ignoring, at this point, the questionable assumptions and methodological shortcomings identified here, and taking PRA results as they are presented by risk analysts, a severe problem of interpretation arises: What exactly does it mean if IAEA demands that the frequency of severe core damage should lie below 1E-4 per year? Is it sufficient for the mean (expectation value) of this frequency to be below 1E-4/yr? This does not appear to be a very satisfactory criterion, since even when the mean lies well below 1E-4/yr, there may still be a considerable probability that in fact SCDF is higher than 1E-4/yr.

For instance, in Phase A of the German Risk Study, a mean severe core damage frequency of 0,9E-4/yr was calculated. Even accepting the rather small error factors as given by the authors of this study, there is a probability of 30 % that the SCDF will be higher than 1E-4/yr. Phase B of this study arrives (without accident management) at a core damage frequency which is lower by a factor of 3 (according to preliminary results). If we assume that error margins will be roughly like those in Phase A, we would arrive at a probability of about 5 % that the severe core damage frequency is higher than 1E-4/yr.

The situation is similar for the US study NUREG-1150 (first draft). The results are presented in a different, somewhat confusing manner (there is not simply one probability distribution for SCDF, but several cases - the base case and sensitivity studies - which are presented using the format of "box-and-whiskers". This format has been criticized as unscientific and misleading (Kastenberg, 1988); nevertheless, the point is clear that values much higher than the mean value of the base case can have non-negligible probabilities. For example, for the Grand Gulf BWR, with a base case mean SCDF of 2,8E-5/yr, the base case still yields a probability of 5 % that SCDF will be above 1E-4/yr. For sensitivity study 4 (diesel generator failure rate increased), there is a probability of

about 50 % that SCDF will be higher than 1E-4/yr. The same holds, in principle, for the results of the second draft of NUREG-1150 (NUREG-1150/2, 1989), which are presented in different manner.

Thus, it appears more appropriate to select a different yardstick, e.g., the 95%- or the 99%-fractile of the SCDF distribution. If the 99%-fractile were adopted (there is a probability of 99% that the value of a random variable is lower than its 99%-fractile), and taken as the measure of SCDF which ought to be below 1E-4/yr (according to IAEA safety targets), the IAEA targets would not be met in 36 out of 39 US PRAs performed until January 1989, and neither would they be met in both phases of the German Risk Study.

It should be noted that uncertainties are even higher when dealing with containment behaviour in a PRA, so that the probability distribution of the conditional probability of early containment failure (given severe core damage) is broader and less clearly defined than that of SCDF. Similar considerations regarding mean value and fractiles apply.

6.3.3 Error propagation and correlation

It is evident from the above discussion that, in order to draw meaningful conclusions from the results of level I of a PRA, it is not sufficient to consider only the median or mean SCDF. Some measure for the bandwidth of uncertainty is also required. Yet, there is no straightforward solution to the problem of combining the error margins of individual failure rates and event frequencies which in combination (by multiplication and addition according to the fault and event trees constructed) yield the SCDF.

We have already stated in section 5 that usually for convenience, it is assumed that basic rates and frequencies are lognormally distributed. This assumption alone leads to an artificially small error margin for the SCDF. In addition, the variation factors of the distributions are often too small. Another assumption is made in PRAs which keeps the error margin low: That all individual random variables being combined in fault and event trees are not correlated. It turns out that this is an unjustified simplification which leads not only to underestimation of the uncertainty in the final result, but also to a considerable optimistic bias in the mean value of SCDF.

Therefore, this point will be discussed in some detail here. To begin, let us take the nuclear plant being studied by a PRA at a given moment in time, and (as a thought experiment) let us assume there is an omniscient creature (not unlike Laplace's demon), which we will call the PRA-demon. The PRA-demon can, without delay, determine all failure rates and event frequencies for the given plant at the given moment with absolute accuracy (from the viewpoint of classical statistical theory, this means: The demon can predict the behaviour of the whole plant, given that exactly the same conditions as in the

moment under study will hold forever, for any period of time she chooses; and hence can determine with any desired degree of accuracy what the rates and frequencies are for those conditions).

The risk analyst, being less than omniscient, asks the PRA-demon for a table of the values of all random variables at an arbitrary moment. Then the analyst compares those values with his/her own estimated means, which represent averages over a certain period of observation, and also over a certain number of plants, insofar generic data are used. If the random variables are all completely uncorrelated, some of the demon's values will be higher than the analyst's estimates, and some will be lower, by varying degrees. There will be no pattern in the deviations between the two sets of values (formulated with more mathematical rigour: If such a comparison is performed many times, there will be no pattern in most cases; there might be a pattern occasionally, but it would be meaningless, produced by pure chance). On the other hand, if all random variables are completely correlated, comparison of the analyst's estimations with the demon's tables would always display a rigid pattern: The demon's values would either all be larger, or all be smaller than the analyst's, and they would either all be larger by a large degree, or by a small degree, etc. That means that the "actual" failure rates would either all be higher, or all be lower, than the analyst's mean values, etc. (In fact, the inaccuracies of the analyst's data do not result solely from the averaging process of their estimation. There will also be inaccuracies associated with data collection and compilation, which will, to some extent, blur the rigid pattern arising from correlation. The smaller those inaccuracies, the clearer the pattern of correlation will emerge in the comparison between analyst's and demon's values.=

If there is a partial correlation, the pattern of deviations would not be rigid, but it would show clear trends, i.e., the majority of deviations going in one direction.

It is in fact well-known that correlations between failure rates can and do exist (Apostolakis, 1986). Nevertheless they are usually not included in PRAs. This may be due to mathematical convenience, and/or to the belief that the error due to their omission is small compared to other error factors occurring in PRAs. It will be shown that this belief is false, and that correlation alone can lead to margins of error which are so large that the results are practically meaningless.

It is fairly obvious that the failure rates of nominally identical components will be highly correlated. Indeed, it has already been suggested that complete correlation should be assumed in that case, and that omission of this correlation (as is customary) may have a significant impact on the result (Apostolakis, 1985; Apostolakis, 1986).

However, correlations can be important in other circumstances:

O Insofar as generic data are used in a PRA, there will be a common trend in actual plant data: Because of the effects of

varying levels of quality control, maintenance and repair, personnel training, general "safety culture", etc., and also because groups of components which were produced at about the same time under similar circumstances may have been used in the plant, there will be correlations among data. Thus, failure rates will generally tend to be lower than their means, or generally higher. This correlation certainly will not be complete, as there is always some random fluctuation; but it could be rather high.

o For both generic and plant-specific data bases, there will be correlation between actual failure rates at different points in time (as would be determined, in our thought experiment, by the PRA-demon). General "safety-consciousness" may vary considerably (during long periods of uneventful operation, after severe mishaps, etc.), which will affect the quality of plant supervision, maintenance and repair work, and the like; trends may be produced by plant ageing, by the introduction of new equipment, etc.

To illustrate the effect of correlations, we will use the lognormal distribution, for convenience, and because it is chosen in PRAs. This choice is permissible for our demonstration, because we do not attempt to actually estimate SCDF but want only to illustrate the importance of one particular factor. It has to be kept in mind, however, that use of lognormal distributions excessuvely simplifies the calculations and falsely reduces uncertainty margins. The lognormal distribution has already been discussed in section 5.3 (for graphic representation, see fig. 5.1). For the topic under consideration here, it is important to recall that the expectation value E of the lognormal distribution is not only larger than the median, but its ratio to the median grows with K. For example, for K=3, E/M=1,24; for K=10, E/M=2,66; and for K=30, E/M=8,48. This ratio grows rapidly for high values of K and reaches, e.g., 279,7 for K=250.

The consequence of this characteristic of the lognormal distribution is that - all other features being equal - growing uncertainty of PRA results leads by itself to higher values of the expectation value of SCDF. This is not a purely mathematical peculiarity of the lognormal distribution. Rather, in this particular respect, the lognormal distribution is an accurate mirror of underlying properties of the system under study. Failure rates and event frequencies are probabilities; as such, their possible range of values is limited to the interval from 0 to 1. They are mostly located rather near the zero end of this interval. Thus, in their random fluctuation (whatever the distribution), they cannot fluctuate symmetrically on both sides. A random fluctuation towards zero - towards the "safer" side - must be smaller than one towards one - towards higher risk. This basic asymmetry grows more marked the larger the fluctuations (the larger the K value). If the median is kept constant, the expectation value is more and more determined by large outliers.

When adding or multiplying lognormally distributed variables, the K value of the result will be the larger the larger the

correlation between the variables (since uncorrelated fluctuations will partly compensate each other, whereas correlated fluctuations will always reinforce each other). For example, when one multiplies two lognormally distributed variables with, say, K=5, the distribution of their product will have K=9,74 for complete lack of correlation, and K=25 for complete correlation. The median will be the same for both cases. The expectation value will be larger by a factor of about 2,6, as will be the 95%-fractile.

When one adds lognormal variables, the expectation value of the sum is the same for the correlated and the uncorrelated case. The median of the sum is smaller in the correlated case. However, the 95%-fractile is larger in case of correlation.

(Note that when the input variables are uncorrelated, an increase in K will always lead to an increase of the 95%-fractile of the result. If the expectation value of the input variables is kept constant, increase in K will not lead to an increase of the expectation value of SCDF in the uncorrelated case.)

As an example, we have taken a simple fault tree from the first draft of NUREG-1150 (for an auxiliary feedwater system with 4 valves and 3 pumps plus their drivers; see figure 6.1, and also figures 7.2 and 7.3) with failure rates for individual components as given in NUREG-1150, and calculated the frequency of the top event. The calculation was performed

- for different K-factors of the individual failure rates (from K=3 to K=10, a typical bandwidth for K-factors in PRA studies);

- for complete correlation, complete lack thereof, and one intermediate case.

The calculations and their results are fully documented in 6.4. In short, the results show the following:

For K=7 (individual failure rates), the expectation value for the top event in the case with partial correlation is higher than the uncorrelated case by a factor of about 4, in the case with full correlation by a factor of approximately 12. The bandwidth of the results, as expressed by the square of the K-factor, is higher by a factor of 60, or 830. In absolute terms, the bandwidth is about 80 in the uncorrelated case, 4600 in the partly correlated, and 65.000 in the fully correlated case. The results stretch across several orders of magnitude and are thus practically meaningless.

Only for the smallest K-factor considered (K=3), are the results reasonably well-determined. Even in this case, the expectation value is larger by a factor of 3 in the fully correlated case, with a bandwidth of about 500.

Thus, the influence of correlation alone can be sufficient to render PRA results practically meaningless. Only in a small fringe area in the space of possible probability distributions

for individual failure rates (i.e., the range with small K factors) can some degree of accuracy be reached, if correlations are present. At the present stage of data bases, such small variation factors can hardly be reached.

(The example also demonstrates the importance of realistic K-factors for the individual input variables, quite apart from the influence of correlations. For the case of no correlation, the bandwidth of the top event frequency is, for K=10, larger by a factor of 16 than for K=3. The expectation value is also larger (by a factor of 7) because in our example, we have kept the individual medians constant when varying K-factors.)

It is clear that the subject of correlations, neglected in present PRAs, requires high priority. Methods for modelling correlations, and for determining correlation factors from raw data, need to be developed and introduced in PRAs. Given the complexity of the topic, however, the only reliable way to come to terms with the correlation problem appears to be to consistently make very conservative assumptions - i.e., assume complete or high correlation whenever in doubt.

6.3.4 Concluding remark

The difficulties of performing even an accurate level I PRA seem overwhelming. All the problems with variation factors, error propagation, correlation etc. could only be completely solved if "actual" data for event frequencies and failure rates were available. Unfortunately, even the concept of "actual" values is unscientific, since it is impossible in principle to observe those actual data. The only way out would be a metaphysical one, with the help of a PRA-demon. (This demon would also have to have capabilities for instantaneous computation, as well as instantaneous data collection, in order to avoid not only the problems of data and methodological uncertainty, but also of time delays.) Unfortunately, such a being either does not exist, or if she exists, it is not known how she could be recruited for a PRA.

6.4 SUPPLEMENT: MONTE CARLO SIMULATION OF FAILURE RATES

Basic approach and assumptions

Let F(R) be the failure rate for a given component R. We assume that P(R) is lognormally distributed with a median value M(R) and a variation factor K(R) (see chapter 5.3). Furthermore, we assume that it is possible to represent P(R) as

$$P(R) = P_c(R) * P_u(R) * M(R) \qquad [6.1]$$

where

$P_c(R)$ is the contribution of the correlated part of P(R)
$P_u(R)$ is the contribution of the uncorrelated part of P(R)

and both, $P_u(R)$ and $P_c(R)$ are lognormally distributed with median 1. Thus, the extent to which P(R) is correlated to the

failure rates of other components can be expressed by an appropriate choice of $K_c(R)$ and $K_u(R)$. According to the multiplication rules for lognormally distributed variables, the following equation must hold:

$$\ln^2(K(R)) = \ln^2(K_c(R)) + \ln^2(K_u(R)) \qquad [6.2]$$

Depending on the underlying assumption on correlation, $K_c(R)$ can be assigned a value between 1 and $K(R)$, thereby uniquely determining the value of $K_u(R)$.

This is a very simple model for the incorporation of correlations in fault tree analysis. The issue of correlation is in need of substantial further study, and it must be assumed that realistic models will be considerably more complex. However, we regard our model as sufficient to illustrate the considerable influence of correlation on PRA results.

The NUREG-1150 fault tree

For a demonstration of the influence of the K-factor and the correlation on the system failure rates, we have chosen a simple fault tree from the first draft of NUREG-1150, Appendix J (figure 6.1; see also figures 7.2 and 7.3). This fault tree does not include dependent failures. Having a negligible failure rate, the valve C and its associated tank have been left aside. Using simple Boolean algebra, the fault tree can be evaluated as follows:

$$\begin{aligned} \text{UNAVAIL} = {} & v_1*v_2*v_3 + v_1*v_2*v_4 + v_1*v_3*v_4 + v_2*v_3*v_4 + (t+p_3) * \\ & ((v_1+v_2)*(m_2+p_2) + (v_3+v_4)*(m_1+p_1) + (m_1+p_1)*(m_2+p_2)) \end{aligned} \qquad [6.3]$$

where, to save space, v_i, m_i, p_i and t denote the failure rates $P(v_i)$, $P(m_i)$, $P(p_i)$ and $P(t)$ from NUREG-1150 (first draft), Appendix J, table J13.15, and where UNAVAIL is the system unavailability, corresponding to the fault tree top event.

The following Monte Carlo simulation is focused on the statistical properties of the UNAVAIL random variable.

In order to faciliate calculation, we assume that the correlated part is common to all components (valves, drivers, and pumps), i.e.

$$P_c = P_c(v_i) = P_c(m_i) = P_c(p_i) = P_c(t) \ ,$$

and this value is included in the individual random variables using formula [6.1].

We also select a uniform K-factor for all components. These two restrictions do not affect the representative qualities of the results.

Furthermore, we assume that the component failure rates as given in NUREG-1150 are median values, thus:

$M(v_i) = 4,3 * 10^{-3}$ per demand
$M(m_i) = 1,65 * 10^{-3}$ per demand
$M(p_i) = 1,65 * 10^{-3}$ per demand
$M(t) = 3,15 * 10^{-2}$ per demand

Monte Carlo simulation of the selected fault tree - methodology

Six independent Monte Carlo simulations have been conducted, each consisting of 1000 simulation runs. In each simulation run, 11 values are created, being realizations of 11 independent, lognormally distributed random variables, to be used for the 11 basic failure rate variables ($P_u(v_1)$, $P_u(v_2)$, $P_u(v_3)$, $P_u(v_4)$, $P_u(p_1)$, $P_u(p_2)$, $P_u(p_3)$, $P_u(m_1)$, $P_u(m_2)$, $P_u(t)$, P_c). The statistical properties of the six sets of 11 000 random variables each are as follows:

	5%-fractile	median	95%-fractile	mean
data set #1:	0,225	0,985	4,816	1,540
data set #2:	0,215	0,985	4,459	1,494
data set #3:	0,219	0,966	4,714	1,495
data set #4:	0,224	0,991	4,773	1,547
data set #5:	0,217	0,985	4,545	1,503
data set #6:	0,222	1,008	4,693	1,542

There is reasonable agreement between the data sets. This shows that reliable results could have been obtained by only using one set of 11 * 1000 values.

For the simulation, two steps are necessary:

(1) A value for the K-factor K(R) and a correlation case (total, intermediate, or no correlation - see below) are selected. For each individual failure rate, simulated values $P_c(R)$ and $P_u(R)$ are chosen. The correlation case, common to all components, determines the variability of $P_u(R)$ and $P_c(R)$ through the values $K_u(R)$ and $K_c(R)$ using formula [6.2]. The basic data sets have to be "squeezed" or "spread" according to those K-factors. The simulated individual failure rate results now from multiplication of $P_u(R)$, $P_c(R)$ and M(R), the median failure rate from NUREG-1150, e.g.

$P(v_1) = P_u(v_1) * P_c * M(v)$
$P(v_2) = P_u(v_2) * P_c * M(v)$
etc.

(2) the simulated individual failure rates have to be added and multiplied according to formula [6.3], yielding the probability for unavailability of the whole system (**UNAVAIL**).

Monte Carlo simulation of the selected fault tree - results

The points to be demonstrated are:

- an increasing K-factor for individual failure rates increases the K-factor of **UNAVAIL**, the unavailability of the whole system, and

- an increasing correlation factor leads to higher uncertainties (K-factors) of **UNAVAIL**.

The 95%-fractile is the value which, with a probability of 95%, the failure rate will not exceed. The expectation value (mean) of a lognormally distributed variable is always higher than the median. Apart from the K-factor, median, mean and 95%-fractile of **UNAVAIL** are given below (unit: failure per demand).

(1) Under the assumption of uncorrelated failure rates, the increase of individual K-factors from 3 to 10 yields an approximately linear increase of the K-factor K_Σ for **UNAVAIL**:

K	K_Σ	median	mean	95%-fractile
3	3,1 to 3,6	3,40 - 3,61 E-6	4,37 - 4,65 E-6	1,1 - 1,3 E-5
5	5,3 to 7,0	4,64 - 5,29 E-6	8,18 - 9,16 E-6	2,5 - 3,4 E-5
7	7,6 to 10,1	6,03 - 7,13 E-6	1,39 - 1,63 E-5	4,7 - 6,5 E-5
10	11,3 to 15,4	0,81 - 1,02 E-5	2,65 - 3,31 E-5	,96 - 1,3 E-4

(2) For each K-factor, three cases have been analysed: no correlation (nc, $K_C(R) = 1$), total correlation (tc, $K_u(R) = 1$), and intermediate correlation (ic, $K_C(R) = K_u(R)$). For $K(R) = 3$, the Monte Carlo simulation showed the following development:

corr.	K_Σ	median	mean	95%-fractile
nc	3,1 to 3,6	3,40 - 3,61 E-6	4,37 - 4,65 E-6	1,1 - 1,3 E-5
ic	10,2 to 10,8	2,73 - 3,24 E-6	7,03 - 8,19 E-6	2,8 - 3,4 E-5
tc	21,2 to 24,3	2,40 - 2,75 E-6	1,12 - 1,34 E-5	5,2 - 6,4 E-5

(3) The same kind of development can be observed for $K(R) = 5$, $K(R) = 7$, and $K(R) = 10$. For these cases, however, the K-factor grows to dimensions of several orders of magnitude:

K(R) = 5:

corr.	K_Σ	median	mean	95%-fractile
nc	5,3 to 7,0	4,64 - 5,29 E-6	8,18 - 9,16 E-6	2,5 - 3,4 E-5
ic	29,0 to 34,7	3,15 - 4,02 E-6	2,11 - 2,61 E-5	,91 - 1,3 E-4
tc	87,9 to 107,3	2,33 - 2,84 E-6	4,70 - 6,52 E-5	2,1 - 2,8 E-4

K(R) = 7:

corr.	Kr	median	mean	95%-fractile
nc	7,6 to 10,1	6,03 - 7,13 E-6	1,39 - 1,63 E-5	4,7 - 6,5 E-5
ic	59,0 to 77,2	3,61 - 4,82 E-6	5,05 - 6,77 E-5	2,1 - 3,5 E-4
tc	224,1 to 285,3	2,29 - 2,90 E-6	1,39 - 2,17 E-4	5,4 - 7,6 E-4

K(R) = 10:

corr.	Kr	median	mean	95%-fractile
nc	11,3 to 15,4	0,81 - 1,02 E-5	2,65 - 3,31 E-5	,96 - 1,3 E-4
ic	120,0 to 166,6	4,36 - 5,92 E-6	1,40 - 2,23 E-4	5,2 - 9,3 E-4
tc	604,4 to 804,2	2,24 - 2,97 E-6	4,72 - 9.97 E-4	1,4 - 2,1 E-3

Thus, it is of vital importance to correctly assess the uncertainty bounds of the failure rate (K-factor) and the correlation between failure rates. A wrong assessment of these parameters may lead to considerable errors in fault tree quantification.

For instance, if it is assumed that K(R) = 3 and failure rates are uncorrelated, whereas in fact, K(R) = 7 and there is intermediate correlation, a twenty-fold underestimation of the uncertainty bounds is the consequence (more complex fault trees may even yield higher underestimation rates). The real expectation value is underestimated by more than one order of magnitude and the 95%-fractile by a factor of 30.

Inspite of the limitations of our numerical simulation, our findings can be generalized. The incorrect assessment of failure rate properties (K-factor and correlation) may lead to serious misinterpretations of PRA results.

7 DEPENDENT FAILURES

7.1 INTRODUCTION

Failures of safety systems or components in case of demand are not just isolated random events. Their occurrence is influenced by a variety of dependencies. These dependencies arise from interactions on different levels, and also from interactions between those levels. Systems and their individual components, initiating events, the environment of equipment, and human activities in planning, design, construction, operation, maintenance and accident management influence each other in many ways.

With growing data bases and the development of analytical methods in the last years, it became clear that

> " the ability to estimate the risk of potential reactor accidents is largely determined by the ability to analyse statistically dependent failures " (Fleming, 1983)

To highlight the importance of this field, it was even said:

> " Indeed the consideration of independent failures of the components of multiply redundant train systems has almost become of academic interest only " (Ballard, 1985)

Table 7.1 shows a classification of dependent failure types that are encountered in probabilistic risk assessment (PRA).

Intersystem and intercomponent dependencies are in fact more or less the same. They are treated as two different categories in PRAs because of the two-step approach usually employed: At first, individual system unavailabilities are determined by means of fault tree analysis. Subsequently, those are combined in event trees to assess core damage frequency. It is clear that, where such an approach is used, intersystem and intercomponent dependencies have to be treated separately and by different methods.

Nuclear power plants employing Light Water Reactors of current design are equipped with redundant active safety systems. This reduces the overall failure probability and allows for single failures without disabling the whole system. The degree of redundancy varies according to the regulations in different countries from (n+1)-systems (2*100% or 3*50%) which allow for one single failure to (n+2)-systems (3*100% or 4*50%) which permit one single failure while another subsystem undergoes repair (Anderson, 1986).

Diverse systems are sometimes installed in especially vulnerable areas. Examples are the boron injection system as a second reactor shutdown system, or turbine driven pumps in addition to the motor driven pumps of the auxiliary feedwater

system. In contrast to redundant systems where an additional safety margin is achieved by multiple identical subsystems, diversity has the potential of reducing the impact of dependent failures.

However, diversity does not imply complete independence. Therefore, this reduction in impact is limited. Of the total number of 69 dependent failures identified by the US Precursor Study for the period 1969-1979, 14 involved diverse systems (Ballard, 1985).

Dependent failure analysis therefore is focused on dependencies that can lead to failure of two or more redundant or even diverse systems or components. It must be emphasized, however, that the failure probability of a single component is also influenced by dependencies (see Chapter 7.3.4.1).

When analyzing the dependent failure probability of multiple systems, two basic aspects have to be dealt with (see table 7.1):

- Common Cause Initiating Events

- Intersystem/Intercomponent Dependencies

Common cause initiating events are all events which have the potential of causing failure of multiple systems. The best-known type of events in this class are the external events, for example earthquakes and plane crashes, as well as internal fires or floods. One difficulty in analyzing this class of events is that the usual procedure of fault tree analysis (definition of a top event - system unavailability - which is traced to the failures of individual components) is turned around. Here we are dealing with an initiating event and its loads on relevant systems. The task is to find out what might happen as a consequence, and what is the probability of occurrence. (External initiating events are discussed in section 13 and will not be treated further here.)

Human action as a common cause initiating event is associated with a very high uncertainty range in probabilistic risk assessment (Fleming, 1983). No complete specification of the events which have to be analysed is available. Obviously, however, the human potential for errors is unlimited, even disregarding intentional acts like war or sabotage, which are not included in PRAs.

A detailed treatment of "Human Errors" can be found in section 8. In discussing dependent failure analysis, however, this topic cannot be omitted. Human errors also play a major role regarding the second class of dependent failures identified above, the intersystem/intercomponent dependencies. In fault tree analysis of stand-by systems it must be taken into account that each valve may have been left in a wrong position after the last maintenance, each motor might be inoperative since the time of its last repair and each instrument might be miscalibrated, just to mention the most typical errors. In addition there is always the possibility of

design and construction errors making a component inoperable at the time when operation is demanded. Furthermore, it is not known what the operator will really do when confronted with an unexpected, potentially serious situation. Many such cases are reported in the history of dependent failures (NRC, 1982b; Ballard, 1985; Ballard, 1986; Meslin, 1989).

Looking at the examples of dependent failures in table 7.1, it could seem that human interaction is the only type of dependency which involves uncertainty. The problem of shared equipment and functional dependencies can, in principle, be treated by fault tree analysis according to the NRC Procedures Guide (NRC, 1982b). The case of physical interaction could be regarded merely as a matter of calculating loads and subsequent failure probabilities, and thus could be dealt with by applying well established science and engineering experience. In fact, however, the situation is more complicated. For many dependent failures which have occurred, the dependencies causing the failure were not identified.

For example, gas bubbles were found in all four trains of the high pressure injection system at Grohnde PWR (FRG) in March 1985. In the event of a demand for the system, this could have led to complete system unavailability. No explanation could be found (NUA/IRS 614, 1986).

In the next chapters the methods currently in use for dependent failure analysis in probabilistic risk assessment will be discussed. It is beyond the scope of this study to treat every single method and model proposed in the literature for analyzing dependent failures. Thus, we focus on those methods which have been used in official PRAs so far. The discussion will be restricted to multiple failures of redundant and diverse systems and components, sometimes referred to as common cause failures (CCF). These can occur both as initiating events (for example failure of residual heat removal due to CCF of the corresponding pumps) and as failure following an initiating event (for example CCF of diesel generators in case of station blackout). No distinction will be made between these categories.

7.2 SUMMARY OF MAIN PROBLEMS

Although dependent failures are considered only to a very limited degree in most PRAs, it has become evident that they are major contributors to the overall risk of nuclear power plants. Therefore, the adequate treatment of dependent failures is of special importance for achieving reliable overall results.

In view of the almost unlimited number of possible dependencies in such a complex system, completeness can never be achieved. Thus it must be guaranteed that the most important dependencies can be identified and treated appropriately, and that the remaining dependencies do not contribute significantly to the risk. This is not achieved by current methodology. It is questionable whether it will be achieved in the future.

Dependent failures can be divided into two classes. For the first class, the causal relationship can be clearly identified and can be included in a PRA by fault tree analysis. For the second class, identification of the causal relationship might be possible but it cannot be included in a PRA. "Operator error causes loss of two redundant systems" is an example for the first class, while a "design error in redundant pump controls" is a typical example for the second class.

This section deals mostly with dependent failures of the second class.

To overcome the difficulty which arises because these failures cannot be included explicitly in PRAs, the usual procedure is to deal with them statistically. Based on experience, failure rates are estimated not only for single independent component failures but for multiple failures as well. These failure rates have to be incorporated into the fault and event tree analysis. They are supposed to cover all possibilities for multiple failure.

The main problems of this methodology are:

- This methodology is, in principle, suitable for redundant, i.e. multiple identical systems only. Dependent failures of diverse systems cannot be systematically considered. Possible dependencies between completely different systems cannot be modelled. In fact, analysis of common cause failures is, at present, always restricted to multiple failures of redundant systems. Experience, however, has shown that many observed dependent failure events have involved diverse systems.

- Although common cause failures are major risk contributors, their occurrence is very rare. Thus the data base is in many cases not sufficient to perform a meaningful statistical evaluation, even when using generic data. As a consequence, CCF estimations are beset with very high uncertainty ranges.

- The extrapolation of generic data to plant-specific conditions leads to a further reduction of the available data, and is based merely on engineering judgment and the analyst's "degree of belief", rather than on established scientific methodology. Thus, the results as obtained from the data base by different analysts can differ by several orders of magnitude. This is an indicator of the extent of the uncertainties.

- Classical fault and event tree methodology is not a very suitable method for analysis of common cause failures. Thus, a priori assumptions have to be made concerning the importance of dependent failures, which assumptions are again based on engineering judgment and degree of belief.

7.3 BASIC PROBLEMS OF CCF ANALYSIS

Probabilistic risk assessment suffers from the problem that its methodology is primarily focused on the evaluation of independent failure modes, whereas in fact dependent failures are the main contributors to severe core damage frequency, as has been revealed by recent studies. Fleming even concludes:

> " It is interesting to note, however, that every time an attempt has been made in a PRA to extend the modelling of dependent events below the component level, new, important, and sometimes dominant contributors to risk and system unavailability have been identified. It is unfortunate that we seem to experience the greatest difficulties in analyzing such important risk contributors as common cause events, while, ironically, much less controversy surrounds the analysis of such non-contributors as the unfortuitous coincidence of many independent events " (Fleming, 1986).

In studies performed earlier, for example the German Risk Study Phase A (DRS, 1979), it was concluded that common cause failures do not generally play a major role. The only exception which was admitted concerned the emergency power supply by diesel generators. A subsequent evaluation of generic data for CCFs for motor operated valves and stand-by pumps by Hennings (1985) comes to the conclusion that the inclusion of CCF-rates in the fault tree "Failure of Core Cooling after Loss of Off-Site Power" would lead to an increase in system unavailability by less than a factor of two.

With this approach, only a small set of possible dependencies can be accounted for. Furthermore, the results of the data screening procedure cannot be regarded as adequate and conservative, as will be discussed later. Hence, the increase by a factor of two must be regarded as a lower bound.

Figure 7.1 shows an estimate for the common cause contribution to SCDF, for the four US plants (Surry, Peach Bottom, Sequoah and Grand Gulf) which were analysed in the draft NUREG-1150 (1987).

For the base case shown in figure 7.1, the CCF rates were reduced artificially by interpreting generic mean values as 95%-fractiles. Therefore, the upper bound values should be used for comparison and interpretation. NUREG-1150 (draft) further underestimates CCF rates, since only intercomponent common cause failures were considered. This significantly affects the contribution of common cause failures to the severe core damage frequency.

In the PRA for Sizewell B (WEC, 1982), the conclusion was drawn that common cause failures play only a minor role. Increasing the CCF rates for nearly all safety relevant systems by a factor of five only yielded an increase by a factor of four for severe core damage frequency (Vavrek, 1985). As was pointed out

by Hahn, however, the CCF probabilities are seriously underestimated in the Sizewell B study due to unrealistically low cut-off values (Hahn, 1985). Recalculation of CCF rates for some systems, based on generic data, resulted in significant increases of system unavailabilities (ranging from a factor of three for the high pressure injection system to a factor of 300 for the reactor scram system).

Including dependent failures into the methodology of probabilistic risk assessment is a very difficult task. First of all, data are very rare, and therefore plant specific data cannot be used. However dependent failures are often thought to be highly plant specific (NUREG-1150, 1987). Thus, the use of generic data is highly questionable.

Furthermore, generic data bases often provide only unspecific and insufficient information on the background of the events. Thus, the application of these data to the circumstances of the plant under study is based merely on uncertain assumptions, engineering judgment and the "experience of the analyst" rather than on a reliable and systematic methodology.

Another problem is that the analyst must seek to identify all possible dependencies in the plant under study. This goes beyond the capability of classic fault tree analysis. Therefore, dependencies on the intercomponent level have to be included explicitly into the fault tree structure. The result is that the system fault trees, which are already very complicated, become even more complex. In many cases, fault trees have to be simplified again in order to make them less unwieldy. This simplification again requires assumptions, guided by judgment alone.

On the intersystem level, two methods have been recommended by the US PRA Procedures Guide (NRC, 1982b). One method is to explicitly incorporate dependencies into the event trees with defined boundary conditions. The availability of one train of a safety system is, thereby, linked to the availability of another train. The other method is to link system fault trees and analyse the result for possible dependencies. Again, restrictions have to be made, since data handling becomes the major problem for both methods.

Finally, the available data have to be incorporated into a model, and this model must be applied to the identified dependencies. Usually a parametric model is used, like the β-Factor or the Binomial Failure Rate model which will be described later. It might be assumed that this is the most accurate step in the whole procedure. However, the treatment of events which have not yet actually occurred, and are therefore accompanied by substantial uncertainty, cannot be based on reliable methods.

In addition to being affected by the uncertainty of the underlying data, system unavailability is affected by uncertainties arising from the statistical procedures used, the engineering judgment applied in all steps, and last but not

least the possibility that the analyst simply overlooked potential contributors.

In the next chapters, these basic problems will be discussed in detail and illustrated by examples.

7.4 COMMON CAUSE ANALYSIS IN PRA

7.4.1 CCF Models

7.4.1.1 Description of CCF Models

In recent years, various models have been developed to include common cause failures in probabilistic risk assessment. Table 7.2 summarizes the treatment of CCFs in some selected PRAs.

All models mentioned in table 7.2 are parametric models. Although other types of models are available (Fleming, 1983; NRC, 1982b), only parametric models have been applied succesfully in PRA up to now. Therefore, only the parametric models will be discussed here.

The available models are:

- Square Root and other Coupling Methods

  The square root model used in the Reactor Safety Study assumes that the failure rate of two components is the geometric mean of the values for total independence and total dependence. In the German Risk Study Phase A, this method was developed further for human errors by considering several types of coupling.

- Cut-Off Method

  The cut-off method assumes that, by adding further redundancy, the system unavailability cannot be reduced beyond a certain value. This value is added to the probability of independent failure for a redundant item of equipment in order to derive the overall reliability of the system. For Sizewell B, cut-off values of 10^{-5} and 10^{-3} were used.

Both models are ad-hoc methods with no empirically founded justification. Therefore, they are only suitable for sensitivity analysis, to get a feeling for the possible unaccounted contribution of CCFs in PRAs that consider independent failure modes only.

- Marshall-Olkin-Model

  The Marshall-Olkin-Model is a very general model for describing a system of several trains. For each combination of multiple and single failures, a failure

rate must be specified. The time of occurrence of each combination is assumed to be exponentially distributed.

Since the data which would be required are not known in most cases, the Marshall-Olkin-Model is usually not used in PRA.

- β-Factor Method

The β-Factor method was the first method which linked independent and dependent failure rates. The factor β denotes the fraction of the sum of all (dependent and independent) failures that is due to dependent failures. The β-Factor method was originally intended to be used for two-fold redundancy only. Its application to systems with higher redundancies is believed to overestimate the system unavailability.

The main characteristic of the β-Factor method is that the determination of β is based only on the evaluation of experience, and no assumption is made as to the probability distribution of multiple failures. Furthermore, common cause failures are treated statistically. No specifications are necessary concerning the underlying cause of failure events.

In case of insufficient data, a value of β=0,1 is often assumed as a reasonable estimate for all components (DRS, 1979; Watson, 1986).

- Basic Parameter Model (BPM)

- Multiple Greek Letter (MGL)

The BPM and MGL models both are extensions of the β-Factor method to higher redundancies. Both models have been shown to be equivalent (Fleming, 1986). Differences between the BPM and MGL models can arise because the input variables usually cannot be determined uniquely from the available data. For both models, as many parameters have to be determined as there are trains in the system. For these parameters, the same holds as was said about the β-Factor.

The main simplification in the BPM and MGL model is that the failure rates are regarded as dependent only on the number of trains that are involved (symmetry assumption). No distinction is made among the various combinations of component failures which can lead to the same number of failed trains.

As an example contrary to this assumption, note that in German PWRs two of the four trains of the decay heat removal system are interconnected with the heat removal system of the spent fuel storage pool. For such system configurations, the assumption of symmetry is not valid.

Both models are restricted to the analysis of redundant systems. Dependent failures of diverse systems cannot be modelled.

- Binomial Failure Rate (BFR)

The BFR model is a specialization of the Marshall-Olkin-Model, originally intended to be used in cases where data are sparse. In addition to the assumption of symmetry as made in the BPM and MGL model, the number of failed components is assumed to be binomially distributed in the BFR model. The probability of the occurrence of dependent failures ("shocks") has to be determined as well as the conditional probability that the component will fail in case of the occurrence of the shock.

A more general version of the BFR model distinguishes between "lethal shocks" which affect all redundant components of the system, and "non-lethal shocks".

The BFR model always includes four parameters, regardless of the degree of redundancy of the system.

The main difficulty in using the BFR model is that, based on observed failure rates, assumptions have to be made regarding what constitutes a "non-lethal shock" and a "lethal shock". This again must be guided by engineering judgment.

As will be discussed later, the assumption of a binomial distribution is not validated by experience and must be regarded as totally arbitrary.

The BFR model, like the BPM and MGL models, cannot be used for modelling dependent failures of diverse systems.

The BFR, BPM and MGL models are recommended by the first draft of NUREG-1150 and by Fleming (1986) for use in PRAs, on the basis of the authors' experience in application and their judgment that the underlying assumptions are reasonable.

- Multiple Dependent Failure Fraction (MDFF)

The MDFF model is an extension of the β-Factor method. Like the BPM and the MGL models, it requires the determination of as many parameters as there are trains in the system. Data on probabilities for the occurrence of single and multiple events are the input for the calculation of Marcovian transition rates. Thus, assumptions are made implicitly as to the probability distribution of the number of affected trains.

Concluding, we note that the more advanced parametric models can be divided into two categories. BPM and MGL (as well as the β-Factor method) are purely empirical models, whereas BFR and

MDFF are semi-empirical models, which make use of assumptions about the probability of dependent failures, to supplement the empirical data.

The problem is that when sufficient data are available, there is no need for additional assumptions, whereas if the data base is not sufficient, additional assumptions are required, but are to a large extent arbitrary.

As will be discussed later, the data base is often very poor, particularly for failures of highly redundant systems. Thus, at present, none of these models can be expected to yield reliable results.

7.4.1.2 Comparison of CCF Models

The first draft of NUREG-1150 and Fleming (1986) compared the β-Factor, the Basic Parameter, the Multiple Greek Letter and the Binomial Failure Rate models. A simplified auxiliary feedwater system of typical US design with two motor driven and one turbine driven pump and a shared condensate storage tank was analysed. Four motor driven and one manual valve complete the system. In figures 7.2 and 7.3 the schematic of the components and a reliability block diagram are shown.

Table 7.3 shows Fleming's results for the different CCF-models. In addition, results are shown for the case with all β-Factors equalling 0,1 and for the case of independent failures only. Both were calculated by the authors using PSAPACK (Bojadjiev, 1988), following the procedure described by Fleming (1986).

The most significant result is that, if only independent failures are considered, the system unavailability is underestimated by nearly three orders of magnitude. Applying the β-Factor Model is shown to be slightly conservative compared to the more sophisticated methods. Setting all β-Factors equal to 0,1 is not a conservative approach.

Regarding the BPM, MGL and BFR models, Fleming and NUREG-1150 (draft) conclude that a good agreement between these models is achievable, provided there is a consistent general framework for systems analysis and a consistent interpretation of the underlying data base.

However, it is possible that the consistent interpretation of the data base leads to distortions in the application of the different models. For example, the parameters of the BFR model, in particular the conditional probability for component failure in case of non-lethal shocks, were deliberately fitted to the results of the other models.

Thus, it might be useful to look into the characteristics of these models using a more fundamental example.

Hirschberg has performed a comparison of the MGL, the β-Factor, the BFR and the MDFF models, using a rather detailed data base

for redundant diesel generators as input (Hirschberg, 1985) (see table 7.4).

Obviously, the main difficulty is the treatment of the quadruple event, no occurrence of which had been observed. For the MGL method and the direct data evaluation, Hirschberg assumes one quadruple failure as upper bound. The other two models do not require such an assumption. Fleming (1986) recommends the use of a noninformative prior ß-distribution, and the calculation of a posterior distribution for the model parameters according to the data base and applying Bayes' Theorem. The mean value of this posterior distribution can then be taken as input for the model. In table 7.5 and figure 7.4 the results of the calculation are presented for the three possible common cause failure situations 2 of 4, 3 of 4 and 4 of 4. To supplement Hirschberg's results and for the sake of comparison the MGL model was also applied to this case by the authors, following the Bayesian procedure of Fleming (1986) and assuming no quadruple failure.

The agreement between the different models is not as good as was achieved in the NUREG-1150 comparison, but the discrepancies between the models for the 2 of 4 and the 3 of 4 cases can be regarded as well within the expected uncertainty range. For these cases, the sophisticated models do not offer any advantages compared to the relativly simple ß-Factor model.

The crucial point is the 4 of 4 case, for which all approaches must be considered arbitrary due to the lack of data. This point gains additional significance since in some more recent PRAs, for example in the Phase B of the German Risk Study (DRS-B), a success criterion of 1 of 4, rather than 2 of 4 as assumed earlier, is assumed for many safety systems (Hörtner, 1986a).

There is good reason for the assumption that failure of 4 components is less likely than failure of two or three components. Furthermore, it is quite understandable for risk analysts to attempt to calculate the corresponding probabilities in spite of all problems. Without empirical data, however, even the most advanced and complex models will not produce reliable results.

Therefore, the conservative ß-Factor model should be used in such cases, which are quite frequent in the field of CCF analysis. An additional advantage of using this model is that its incorporation in fault tree analysis is much less complicated than for other models.

7.4.2 Fault Tree Analysis

It is very difficult and complicated to include dependent failures into fault tree analysis. Even when the task is limited to multiple failures of redundant components, every possible combination of CCFs has to be incorporated explicitly into the fault tree structure (see figure 7.5).

For the simplified auxiliary feedwater system of NUREG-1150 as already discussed above, the consequence was that the number of minimal cut sets was increased from 29 (for independent failures only) to 129. In full-scale applications of probabilistic risk assessment, the data handling task would thus become almost unmanageable. However, this is considered to be the only way of guaranteeing that all possible contributors are included (Fleming, 1986). Maybe use of the simpler β-Factor model (which in addition yields conservative results) is the only way to deal with this problem.

Furthermore, apart from redundant identical components, diverse components and even completely different systems can be involved in common cause failures.

In summary:

> " The number of different combinations of components that can be hypothetically linked by a single common cause event is essentially unbounded. Hence, a truly general formulation of a plant-level dependent events model is very difficult to express, and when expressed, impossible to solve. Keeping the number of possibilities allowed for in the models at a manageable level will continue to require judgment guided by feedback from operating experience. Such judgments, however, are not unlike the numerous judgments that need to be made by a systems analyst to account for independent events" (Fleming, 1986).

The situation becomes even more complicated when intersystem dependencies have to be considered. For reactor types where the redundant safety systems consist of multiple trains with few interconnections (for example the German KWU plants), system fault trees usually are constructed separately for each train and are then combined to event trees. The recommended procedure of defining boundary conditions for the event tree (see 7.3) and thus explicitly incorporating the dependencies (NRC, 1982b), which seems to be the most common approach to CCF analysis, is of limited value because of the possibility of overlooking potentially important dependencies.

Another possible method would be fault tree linking, followed by a careful search for possible dependencies, and subsequent application of a parametric model. The problem with this method is that the parametric models do not consider the mechanisms leading to common cause failures. They only deal with probabilities (see 7.4.1.1). Thus, dependencies like "physical interaction" or "human interaction" (see table 7.1), once identified for a specific plant or accident sequence under study, have to be incorporated separately.

We conclude that classical fault and event tree analysis, developed for independent events that were originally assumed to be risk-dominating, is not an appropriate methodology to assess the impact of dependent failures. To combine this

methodology with a model for common cause analysis leads to an immense expenditure of analytical work, and requires considerable judgment. No PRA has ever completely achieved this task.

7.4.3 Data Collecting and Processing

Data collecting and processing is the most important step of the analysis of dependent failures, especially if parametric models are used. These models are not concerned with the type of the dependency and the cause of the failure; they concentrate on probabilities only.

The types of dependent failures which can occur, and their impact, depend on the design of the plant under study, the conditions during accident sequences, and the organisation of testing and maintenance at this plant. Therefore, the usual procedure applied in CCF-analysis is to begin by collecting data on rates for independent and dependent component failures, subsequently screening these data for application to the special system configuration to be analysed. Although some systematic procedures for the second step have been proposed (Watson, 1986; Mancini, 1986; Fleming, 1986; NRC, 1986b), unequivocal and reproducible results are very difficult to obtain.

7.4.3.1 Data collecting

The main problem with collecting data for the analysis of common cause failures is the fact that these events are very rare, although CCFs as a class are major contributors to the severe core damage frequency.

For example, let us assume that there is an operating experience of 2000 reactor-years which provides a data base for a PRA. This is far more experience than that on which PRAs are usually based (see e.g. (Fleming, 1986; Meslin, 1989; Hennings, 1985)). Furthermore, we assume that one common cause event has been experienced for a certain redundant system, this being the required minimum for any meaningful calculation (see Chapter 7.4.1). The probability for this common cause failure as calculated from the data base would then amount to about 5,7E-8 per hour of operation.

CCF-rates which are considerably lower than this value have been published, ranging, for example, from 1,2E-8/hr to 6,4E-12/hr (Hennings, 1985). It is difficult to envisage a data base which would permit the reliable estimation of such low values.

Thus, the uncertainty of very low failure rate estimates is considerable. As a hypothetical example, let us assume that there are 20 years of operating experience for a plant under study. We assume further that for a particular CCF event, which has not yet occurred in the plant, a failure rate of 1,2E-8/hr is selected from a generic data base. If this event then

suddenly occurs in the plant, the estimated failure rate will change dramatically. The new value (as calculated from one occurrence in 20 reactor-years) will be 5,7E-6/hr, an increase by a factor of almost 500. This gives an indication of the uncertainty of CCF failure rate estimates.

Another problem of data collection is that it is usually assumed in PRAs that component failure is independent of the accident-initiating event.

For example, if there are ten years of operating experience for a single component or a system, and testing is performed once per month, 120 test demands result. Let us assume that 5 real demands occurred during this period, and that 1 failure at real demands and 9 at test demands were observed. According to common PRA-methodology, independence between failure rate and initiating event (real demand, or test) would be assumed. This would lead to an estimated failure rate of 0,04 per year (one real demand per 2 years; 10/125 failures per demand).

In fact, as pointed out by Ballard, the failure rate would be 0,1/yr (1 real demand per 2 years; 1/5 failures per real demand). There must be a distinction between test and real demands. During tests, parts of the system are often examined separately, without checking the complete system. Furthermore, the load on a system is quite different for real demands than for tests (see also section 3.3).

A typical example is the incident at the Brokdorf nuclear power plant described in section 8.3.1.1.3. In this case, the power supply from all four emergency feedwater diesel generators would have been unavailable in case of a real demand (station blackout). This defect had not been discovered by testing for 2 years.

Therefore, in the U.S. Precursor Study (Minarick, 1982) it was decided to count the two failure rates separately. The failure rate then was calculated as follows:

$ESF = 1/T\ (n_1 + (N-n_1)*(n_1+n_2)/(X+N))$ where

ESF = failure rate per year (Event Sequence Frequency)
T = operating experience in years
N = number of real demands
X = number of tests
n_1 = failures at real demands
n_2 = failures at tests

The possibility of double-counting was accepted in the Precursor Study in order to avoid underestimation with certainty.

Applying this approach to our example yields a failure rate of 0,132/yr.

To illustrate this point with another, more realistic example, the Diesel Generator example considered above (7.4.1) was reevaluated.

The probability of failure of at least two components (2 of 4) increases from 1,32E-2 for the original data evaluation (see table 7.5) to 5,27E-2 per demand for the Precursor Study method. The probabilities of three- and four-fold failures (3 of 4 and 4 of 4) do not change since there are no such demand failures in the data base.

It becomes evident that current PRA methodology systematically underestimates the probability of single and multiple failures of components and systems because of the erroneous assumption of independence of failure rates and initial events.

7.4.3.2 Data Screening

It is generally accepted that generic data require interpretation and screening before they can be used for the analysis of a specific plant. Plant design, organisation of maintenance etc. have to be taken into account.

This screening procedure further reduces the poor data base. Furthermore, in most cases the screening appears to result in a decrease of failure rates.

For example, generic β-Factors were arbitrarily declared in the draft NUREG-1150 to be 95%-fractiles of a lognormal distribution with a variation factor K=4, although they had been explicitly denoted as mean values in the source from which they were taken. This led to a reduction of the β-Factors by a factor of almost 3.

Hennings (1985) screened generic data for stand-by pumps and motor operated valves for application in the reference plant of the German Risk Study, Biblis B. Table 7.6 shows the results: Starting from all available data ("not fault tree specific"), all events which were supposed to be irrelevant, or to be included in other fault trees were excluded, leaving those which were directly relevant for the fault tree of the systems under study ("fault tree specific"). Some events were also "shifted" to instrumentation failures and control or support system failures. For the pumps, the data base was thus reduced to zero. For the valves, only data for 2 of 4-failures remain. The corresponding probabilities are reduced accordingly.

Three general conclusions can be drawn:

-- The data base for CCFs is simply too limited to yield reliable results. This applies particularly after screening to exclude data from plants with differing designs.

-- Design differences between the plant under study and the plants from which the data base originates can lead to overlooking dependencies which arise from the particular design of the plant under study.

-- Often, screening leads to a reduction of the number of events, whereas the underlying operating time or number of

demands remains unchanged. This leads to an underestimation of failure rates.

Even when plants are in fact comparable, data evaluation is by no means straightforward:

> " The most extensive use of judgment in data analysis is made at the level of data collection from the plant operating records " (Mosleh, 1986)

Available sources of data such as the US LER (Licensee Event Report) do not provide enough information to be used as a base for analyzing dependent failures (see also section 5).

In many cases, it is impossible to determine whether an observed multiple failure was a multiple independant or a dependent failure. In this case, a possible approach is to introduce weighting factors which reflect the analyst's "estimation of the degree" to which the events which cannot be classified are dependent or independant failures.

The resulting uncertainty can be very high. For example, Fleming (1983) estimates ß-Factors for motor driven valves, based on a review of 200 incidents. Although only 13 of these events could not be classified, this led to a notable uncertainty for the ß-Factor: This factor was estimated to be between 0,029 (all unclassified failures assumed to be independent), and 0,117 (all unclassified failures assumed to be dependent).

It might be argued that a factor of four does not represent an unacceptably high uncertainty, and that such a factor can easily be accomodated in an uncertainty analysis. However, this factor of four describes the uncertainty of only one of the input parameters of a PRA. Furthermore, the ß-factor represents only the simplest type of common cause failures, namely the 'more than one' failure mode. For failures of three- and four-train redundant components, the uncertainty of the corresponding factors is much higher.

7.4.4 Overall Uncertainty

In the preceding discussion, the different steps of CCF analysis and their basic difficulties were addressed. If the complete procedure is applied in a PRA, the calculated unavailability of systems has a high uncertainty.

This is illustrated by a study performed by Poucet (1987). This study, the Common Cause Failure Reliability Exercise, deals with the problem of identifying, modelling and quantifying dependent failures. On the basis of a real reference plant and one safety system (auxiliary feedwater system of the West German Grohnde PWR), a common set of problems was defined and analysed by ten different teams of analysts.

To begin with, all teams were provided with the same fault tree of the system, including independent failures only. They had to quantify the unavailability of the system in the event of loss of preferred power (First calculation).

In a second step a common set of parameters was used, estimated in a consistent way for the different models. The main aim was to study the differences between the models (Second calculation).

Finally, the teams were provided with a set of event reports. On this basis, the calculation had to be performed again (Third calculation). These event reports had already been used to estimate the parameters used in the second calculation.

The results (system unavailability) are shown in figure 7.6. As can be seen, the results differ by two orders of magnitude even for the third calculation.

In view of these results and the fact that only one safety system and only one initiating event were analyzed, it becomes clear that any analysis of this kind must be plagued by a significant CCF- related uncertainty. No procedure or model is available that is capable of yielding reliable and reproducible results with a well-defined and sufficiently narrow uncertainty range. Thus, one of the chief yardsticks to be applied to all PRAs is the extent to which they assess the upper bound values for common cause and other dependent failure contributions to SCDF.

8 HUMAN BEHAVIOUR IN PRA

8.1 INTRODUCTION

The "human factor" plays an important role in nuclear safety. Human behaviour can lead to accident sequence initiation or may aggravate accident sequences. On the other hand, potentially dangerous situations may be recovered by human intervention.

Accident related human actions include errors, sabotage or acts of war. Sabotage and acts of war will not be treated in this part of the study as they imply voluntary damage or destruction. (For sabotage, see section 17 of this study; for acts of war section 13.3.3.)

Deliberate human errors can occur if there is no consequence to be feared or if personal benefits are hoped for. This aspect is not excluded here.

The importance of human actions in nuclear power plants is due to the fact that

- the human error probability is high,
- the human error probability estimation is associated with an unkown uncertainty,
- human actions are potential causes for common mode errors,
- it must be assumed that different human errors are not independent.

The key question in this context is whether human behaviour can be quantified at all. Our conclusion will be that only a very limited part of human actions can be quantified (and has already been quantified). The most relevant errors, the important errors in accident situations, escape any reliable quantification effort.

8.2 SUMMARY OF MAIN PROBLEMS

Human error can occur in any domain where human action is involved. Since human actions play a vital role during the entire planning, construction and operating period of a nuclear power plant, human errors have been reported from all those stages. It must be assumed that the majority of human errors does not occur in the control room although supervision and research efforts tend to focus on this area.

Since human errors are relatively rare events, there is a considerable lack of real event data. Error quantification has therefore been based on simulator experiments or expert estimations. There has been substantial criticism concerning both practices, coming from experts belonging to the nuclear community, because

- expert opinion tends to yield overly optimistic results with an unrealistically narrow bandwidth of uncertainty,

- simulator experiments are not able to simulate the actual accident stress level, and they only yield results for a limited number of event sequences: Those which have been, and can be, subject to a modelling effort.

Current Human Reliability Assessment (HRA) studies usually concentrate on actions where the operators act according to a plant safety goal. Whilst errors of omission (failure to act) can be fairly well quantified, more difficult areas like errors of commission (doing something else instead of the scheduled action), cognition and decision based actions (e.g. errors when assessing the plant status when data are lacking), and dependencies between different actions and between different persons have not yet been subject to a reliable quantification. Thus, it must be concluded that the following aspects are not properly taken into account:

* Errors of commission are of equal importance as errors of omission,

* errors during actions based on decision processes are more likely to occur than simple errors of omission, and their impact can be greater,

* understanding of physical processes is taken for granted; however, accidents like TMI and Chernobyl show that the personnel did not anticipate the consequences for their actions,

* there may be a conflict of goals between maintaining plant safety and operating economically,

* the personnel is neither always well-motivated nor working on an optimal stress level,

* personnel has been observed disregarding safety rules,

* error probabilities for different people working together, and for different steps in a sequence of actions, will generally be correlated.

From these facts alone, it must be concluded that human action is the most important risk factor for a nuclear power plant. Several sources assess its contribution to core melt frequency ranging from about 1/3 to 2/3.

All these quantifications can only be speculative, since there are strong indications that both the decision processes and dependencies between actions and between persons depend on the general background and the knowledge of the involved persons to such a large extent that a general quantification is impossible. Hence, the HRA tool may well be able to qualitatively indicate weaknesses in nuclear power plants, but all efforts of quantification of rare events tend to be in vain.

In order to reduce human error, increased reliance on automation has been proposed. However, all software production is as prone to error as any other advanced man-machine interaction. Thus, increased automation will merely lead to the substitution of one category of human error by another category. For software production, risk analysis and error reduction techniques lag far behind the studies on human factor analysis, and a quantification of software risk is not in sight. The most important consequences of automation would be

- introduction of unknown software and hardware hazards,

- replacement of conventional human errors by software-use related errors,

- since only routine actions may be automatized, the personnel still has the task of dealing with exceptional events (the most error-prone ones).

Only automation of basic, simple actions in order to reduce the workload of the personnel should be aimed at. In areas where the consequences are not fully known, automation is not an appropriate strategy.

Inspite of his/her deficiencies, the human being remains the most reliable element in case of unforeseen events.

8.3 BACKGROUND

8.3.1 Where can human error occur in nuclear power plants ?

Human behaviour has received little attention in probabilistic risk assessment, compared to the efforts of reliability estimation for physical components. Blackman (1986) regrets that no comprehensive study of the human factors had been conducted so far. To our knowledge, this situation has not changed since 1986. However, it is generally agreed in the nuclear community that human actions play a major role in most nuclear incidents. The estimates of their contribution to core melt frequency range from 38 % (precursors only, Minarick, 1982) to 63 % (human error induced core melt, DRS A, 1979) (see figure 8.1) in risk analyses. Reports from the chemical industry even give a factor of 90 % (Joschek, 1981).

According to the Public Citizen's Annual Nuclear Power Safety Report of 1987 for commercial US reactors, at least 2940 "mishaps" were reported in the Licensee Event Reports (LER) to the US Nuclear Regulatory Commission (NRC). Personnel error was involved in 2197 cases (74%). Many other mishaps, including some of the most serious accidents of 1987, were apparently not reported (WISE, 1989a). Among the mentioned mishaps were acts of vandalism and sabotage, unauthorized possession of firearms on plant sites, and a three-fold increase in the number of reported instances of drug use among nuclear workers.

8.3.1.1 Different aspects of human error in nuclear power plants

It is often assumed that human error concerns mostly the plant operators. In fact, however, human error interferes at various levels during plant design, construction and operation.

Embrey (1981) remarks that

> "Although attention tends to be focused on the operator in the control room, several studies ... have shown that errors in design, construction, maintenance, and testing are in fact greater potential contributors to plant failures. Human reliability data are therefore required for tasks over the entire life cycle of a plant."

Figure 8.2 shows which human error categories play a major role, apart from the relatively well analysed control room context. There has been a number of attempts to quantify, for the different fields of action in a nuclear power plant, the contribution to core melt frequency.

Scott (1981) reports a percentage of 10 % for safety related events in US nuclear power plants in each of the error categories for construction, operation and supervision, and a percentage of 5 % for fabrication, installation and maintenance errors each.

The UK Central Electricity Generating Board (CEGB) examined loss- of-generation events in nuclear power plants from 1976 to 1982 (Pope, 1986). The following contributions from different error categories were found:

operating errors	10%
design errors	20%
maintenance/testing errors	70%

The Öko-Institute distinguishes between eight human error categories, for which examples will be given (Öko, 1983):

- design errors
- construction errors
- fabrication errors
- maintenance errors
- actions against safety rules
- wrong interpretation of the reactor status
- erroneous actions at critical points
- errors of management and administration.

To complete this list, we also consider modification errors, as well as so called "Wrong Unit/Wrong Train"-errors.

8.3.1.1.1 Design, construction and modification errors

In the U.S., design and construction errors were investigated by the NRC after the Crystal River incident (1986). For further details, see section 15.2. Another example for this category is

the underdimensioning of fuses for the emergency diesels at the Biblis A nuclear power plant (Öko, 1983). Emergency diesel generators are vital to prevent severe core damage in cases of loss of off-site power.

It should also be noted that it is not only the actual state of the nuclear power plant which is important; in addition (Pope, 1986)

> "... it should be appreciated that design change (on operational plants) always involves risk and the trade-off between alternative designs requires careful consideration before implementation."

Any modification on an operational plant's design also creates the danger of erroneous actions by personnel accustomed to the old plant design.

8.3.1.1.3 Fabrication errors

The Gazette Nucléaire (Gazette, 1984) reported on a piping system for the French Chinon B2 nuclear power plant. The pipes did not meet the required standard, some of them having a diameter that was 15% smaller than acceptable.

A problem of fuel fabrication was reported by NucEng (1989b) for the French Dampierre 3 nuclear power plant.

> "... some of the fuel pellets in the rods had a diameter less than laid down in the manufacturing criteria. ... a reduction of the diameter of the pellets increases the heat accumulating in the fuel rod. This would not have any effect during normal operation but, in the case of an accident involving loss of coolant, could lead to a fuel rod temperature above safety criteria. The limit exists to prevent fusion of the pellets."

This problem may also concern other nuclear power plants in France (Dampierre 1 and 4, Cruas 4) where pellets of the same manufacturing batch had already been loaded.

Errors due to faults in design, construction, fabrication or installation should (ideally) be detected in the testing phase of a nuclear power plant. If not, it is possible that the demand of an individual component leads to the failure of a safety system. This kind of error is relatively difficult to quantify, and consequently, it has rarely been taken into account by PRA studies (Öko, 1983).

At the very least, it should be expected that counter-measures are taken immediately, after such errors have been discovered. Even this, however, does not seem to hold true in all cases, as NRC (1989b) reports that the Arkansas Light & Power company was fined because four safety related questions had not promptly been resolved.

"The time that these questions went unresolved ranged from several months for three of them to more than six years for the other. Although analyses eventually showed that all these matters had minimal safety impact, NRC believes they should have been evaluated in a timelier manner."

Although the failures must have been known for a considerable period of time, the utility did not feel obliged to act. NRC remarks that the consequences were minor. However, it must be noted that the defects concerned safety-related equipment.

8.3.1.1.3 Maintenance errors

At the Brokdorf nuclear power plant, it was found during routine inspection that all four emergency feedwater diesels were lacking important parts which would have caused component failure in case of demand. The defects were discovered 1988; the parts had been lacking since 1986. For examples from the U.S., see section 15.2.

Maintenance errors have not been taken proper account of in the German Risk Study, Phase A. It is claimed that their influence is negligible.

Figure 8.2 does not support this claim. It should be noted that maintenance actions may be causes for common mode failures in redundant systems, for example by a wrong calibration of several trains of redundant components. With the exception of monitoring channels and monitoring channel groups, this common mode aspect remains totally excluded from the German Risk Study, Phase A (Öko, 1983).

8.3.1.1.4 Actions against safety rules

During the Biblis A accident in the FRG in 1987, which was a precursor to a LOCA, a warning light was overlooked by the operators for 15 hours. This light signalled that a valve was open between the low pressure injection system and the primary circuit. The reactor operator who finally noticed this state tried to remedy the problem by slightly opening a second valve, to generate a pulse which was intended to close the first valve. Since this action was not successful, he proceeded to plant shutdown, as laid down in the guidelines. The opening of the second valve had resulted in a release of radioactive steam, bypassing the containment for 2 - 5 seconds.

In September 1988, an incident occured at Stade PWR (FRG). Valves in all four main steam lines shut because of an electronic malfunction. According to plan, this would lead to an automatic shutdown of the plant, but the operating crew wanted to avoid this and tried to manually reopen the valves. However, the automatic reactor protection system finally overruled the operators and shut the valve again. The

manipulations led to considerable vibrations of the steam lines, which at Stade NPP are particularly vulnerable to break.

At the Chernobyl nuclear power plant, the operators switched off vital safety mechanisms (see 8.3.1.3.2).

The German Risk Study, Phase A, excludes unplanned, provisional, unforeseen actions as well as actions violating the safety rules. However, there is enormous scope for [illegible] actions. The results of human creativity and fantasy in complex situations cannot be predicted (see 8.3.1.3).

8.3.1.1.5 Wrong interpretation of reactor status

At the Chernobyl nuclear power plant, the operating crew regarded an unstable plant state as sufficiently stable to conduct an experiment - the consequences are well-known (see 8.3.1.3.2).

During the Three Mile Island accident in 1979, many experts did not consider the possibility that the gas bubble that had formed inside the containment could consist of hydrogen.

A bizarre event of this type occurred at the U.S. Zion plant in 1981/82. In the spring of 1981, the plant was shut down for steam generator repairs. To prevent water from getting into the steam generators, large aluminium plates were installed in the primary pipes. The plates contained an aluminium hinge through the middle to facilitate installation and removal. When the work was completed, the personnel forgot to remove the plate from one leg of the plant. The plant was started up, and reactor coolant flow from one loop registered low. Instead of believing the instruments, the operators assumed that the instruments were incorrect, and recalibrated the flow instruments to read full flow. Eventually, the hot, borated coolant ate through the plate, thus slowly increasing coolant flow in that loop. The operators again recalibrated the flow instruments, without realizing that something was seriously amiss. Eventually, the hinge portion of the plate broke loose, and slammed into the steam generator, severely damaging a large number of steam generator tubes. The plant had to be shut down and a large number of steam generator tubes had to be repaired (NRC, 1982c).

8.3.1.1.6 Erroneous actions at critical points

> "There exist many accident conditions which "look" very similar to the operator (i.e. exhibit common symptoms) but call for different operator response. In addition, there are many different plant states which call for an identical operator response but exhibit a number of extraneous symptoms." (vonHermann, 1981)

Thus, taking action during an abnormal plant state always involves the risk of error and misdiagnosis.

On November 11, 1988 the Soviet nuclear icebreaker Rossiya narrowly escaped a nuclear accident in the port of Murmansk (WISE, 1989b). According to a UPI press report of February 20, 1989, the chief physicist gave an erroneous command. The command was apparently to open a drain valve and set off what the article called in its headline, "four minutes of nuclear danger". Thanks to the emergency protection and the further actions of the crew, WISE reports, the situation was stabilized.

Nuke (1989) reports a severe damage in the recirculation pumps of Fukushima II-3 nuclear power plant. In the beginning, the utility, Tokyo Electric Power Company (TEPCO), only found that

> "a 100 kg ring attached to the bearing of the pump had become dislocated and damaged the vanes of the pump. Also two metal pieces were missing and might have found their way into the reactor core."

Four weeks later,

> "TEPCO's investigation has already discovered 10 fragments and some metallic powder at the bottom of the reactor vessel and 13 fragments inside the jet pump. Metal pieces were also observed on 122 of the 764 fuel assemblies. The largest fragment is 10.5 cm long and weighs 9 grams. ... When the first alarm sounded on the morning of Jan. 6, signalling abnormal vibration of the pump, the operators only reduced the rotational speed of the pump and kept it operating for another 14 hours with the alarm sounding most of the time. If the pump had been stopped immediately, the rupture could have been prevented."

8.3.1.1.7 Errors of management and administration

PRAs at the current state of the art are unable to treat the influence of management attitudes and management practices on risk. They typically assume at least average training of the personnel. In addition, they cannot treat the impact on risk of "inadequate management culture" (illustrated, e.g., by the Peach Bottom incidents). Furthermore, PRAs do not examine

- whether the maintenance budget is adequate;
- whether sufficient budget is available for continuing training of operators, maintenance personnel, and others with direct influence on safety systems;
- whether management and first-line supervisors are adequately qualified for their positions;
- whether the quality assurance and engineering procedures for design reviews, and other quality assurance practices are adequate;
- whether the controls on overtime work for licensed operators and key maintenance personnel are adequate to prevent increases in errors due to excessive fatigue;
- whether substance abuse counseling and prevention programs are adequate to prevent substance abuse from

affecting operator or maintenance personnel performance;
- whether maintenance records are sufficiently in depth and used adequately to prevent clusters of failures, to preclude repetition of dependent failures, etc.;
- whether procedural compliance is adequately stressed and monitored by quality assurance and others;
- whether adequate resources are given to procedure development and revision;
- whether adequate levels of safety can be maintained during strikes, and the likelihood and influence of strikes;
- whether there is adequate staffing of operations, maintenance, and other personnel at the plant.

Thus, the human factor in fact is much broader than the consideration of human errors - it includes the totality of management practices, administrative controls, information gathering systems, budgeting, and decision-making processes by which nuclear power plants are designed, constructed, operated, maintained, and modified.

8.3.1.1.8 "Wrong Unit/Wrong Train"-errors

In France, two nuclear power plant units are usually connected to the same operating building. This has already led to several safety-relevant unit mix-up incidents.

For example, a "Wrong Unit"-incident took place July 1, 1984 at the St-Laurent-Les-Zaux plant. Convinced that he was dealing with the shut-down unit B1, the operator instead commanded the opening of the valves linking the primary circuit to the shut-down cooling circuit on B2, which was in operation. "Most fortunately the valves refused to open", noted the safety authorities. The valves failed to function because of the pressure difference between two circuits. The shut-down cooling circuit normally operates at about 30 bar. It is not designed to withstand the operational design pressure of the primary circuit, 155 bar. If the valves had not malfunctioned, the situation would have almost certainly resulted in a major break and significant LOCA outside the containment (Anderson, 1986).

In the U.S., 24 "Wrong Unit"-events have been reported between 1981 and 1985 (NRC, 1986c).

Furthermore, incidents involving mix-up of trains or components within one unit are frequently reported (e.g., 65 "Wrong Train"-events, and 41 "Wrong Component"-events in the U.S. 1981 - 1985) (NRC 1986c).

8.3.1.2 Human psychology and working conditions

8.3.1.2.1 Ergonomic analysis of working accidents in industry

An ergonomic analysis of general working conditions and behaviour in (non-nuclear) industry shows (table 8.1; Röbke, 1973) that the actions and situations encountered in nuclear power plants are exactly those which are the most errorprone.

Unfortunately, the human being does not always react in a way as to avoid risk. On the contrary,

> "if risky behaviour results in success and yields the desired effect, the human gets a confirmation of his evaluation of his proper capabilities. So he believes in an increased importance of his role, often leading to an increased self confidence."

This self-confidence may result in a wrong self-esteem where a person regards him/herself as capable of handling particular situations which in fact he/she is <u>not</u> capable of. Risk-increasing motivation strongly depends on the subjective assessment of accident probabilities.

> "If an accident sequence is a rare event with a probability of less than 1 %, the related behaviour is not felt as "less dangerous" but simply as "not dangerous at all"."

This observation (Röbke, 1973) is emphasized by the fact that 84 % of all accidents are related to violations of company-specific accident prevention rules.

Among the factors initiating the wrong behaviour are

- boredom, monotony of work,
- lack of familiarity with incoming information,
- duration of working time, working night shifts etc.,
- interest for and satisfaction due to work.

It will be shown in 8.3.1.2.2 that these problems are inherent to the tasks of nuclear workers and cannot be removed.

A question frequently asked in the nuclear community (Hall, 1985) is

> "to which level ... an engineering model of human performance [should] be anchored to psychological constructs."

If the task of including psychological factors in human performance models is taken seriously, it must be recognized that in the absence of a perceivable danger (due to its low probability), the control exercised by supervisory bodies plays an important role in motivating plant personnel. Thus, the human influence is further increased and complicated, due to human interaction on the supervisory level. A typical consequence is disobedience to safety rules issued by the

supervisory body. Such cases are frequently reported, e.g., in the U.S.NRC News Releases. They lead to a degradation of the "safety culture" because safety is not regarded as accident-related but as supervision-related; the important point is not to avoid hazardous situations, but to avoid being caught.

8.3.1.2.2 Work in a nuclear power plant and human psychology

This chapter is based on two reports (Moldaschl, 1988; Libé, 1988).

For operators, the basic working conditions have been defined by engineers. In principle, the engineers attempt to design an error-free system. As no system is completely free of errors, however, the main task of an operator is to be ready for situations

* which have never occurred before,
* which have not been anticipated in system design, and
* for which no operating experience exists.

Thus, the operator is sitting in a well-sheltered room where thousands of lights signal incoming information - a silent atmosphere, only disturbed by the everlasting sound of the printer, putting these informations on paper. The most physically strenuous of the operators' tasks is the control round, at least once every 24 hours.

In this artificial environment, the operator faces several dilemmas:

- the forgetting dilemma:
  the nuclear power plant usually works in an automatic mode. However, in case the automatic system does not function, the operator has to act
  * immediately,
  * efficiently,
  * with routine, and
  * without errors.
  As most of the routine burden has been taken off the operator's shoulders, he can rarely count on his routine and experience in such situations. (Moldaschl is comparing this task with a surgeon having to operate in an emergency after a break of several years.)

- the responsibility dilemma:
  There are fixed rules and procedures for the case that an incident occurs. However, incidents quite often include unforeseen phenomena (see Dougherty, 1985). Thus, these rules cannot be applied rigidly; they may even be counter-productive (see section 14 on accident management). In this case, the operating crew has to take the responsibility to find a compromise between a flexible interpretation of the rules (which also implies modifications of the rules) and a strict shut-down-when-

in-doubt strategy - thus, a trade-off between economic and safety requirements.

- the concentration dilemma:
  For hours, days and months the daily routine may be unbroken. But in any second an event can occur. Thus, the operator has to be very attentive to a process running smoothly by itself. This situation can be compared with a sprinter sitting at the starting point and knowing that sometimes within the next couple of hours, the race will start. He will never beat the world record !

- two information dilemmas:
  * in case of an accident, the avalanche of information coming in is very likely to surpass human cognitive capacities.
  * arriving information has already been pre-processed by the automatic system, which may interfere with the correct interpretation of the situation by the operators.

- the experience dilemma:
  Such accident and risk situations which are marked by a high stress level have rarely been encountered yet.

Nevertheless, the chairman of the German Reactor Safety Commission A. Birkhofer states that "human errors should be substituted by intelligent logic" - an approach which is inevitably further degrading the above situation, as highly qualified personnel sit idle waiting for a rare emergency which cannot be handled by the system and its "intelligent logic". A risk factor which has been severely underestimated up to now is the nuclear power plant designer's assumption that he is able to control complex technologies by means of computers only.

8.3.1.2.3 The ideal man-machine interface

In 1986, Blackman of EG&G suggested an integrated approach to man-machine interaction. He regarded the studies which had been performed to date as not sufficient. He (correctly) describes the ideal man-machine interface as

> "a machine (system) ... made to fit the potential capabilities of the man".

furthermore,

> "the human must ... be provided the proper environment for optimal performance".

In order to approach the difficulty of this task adequately, Blackman demands that it must be possible

> "to generate a model capable of predicting [human] performance"

and he continues :

"the scientific and historical literature tells us that human performance cannot be completely modelled, i.e. predicted. However, it is that same source which tells us that within defined environments human performance can be predicted sufficiently to permit planning and execution of relatively narrow missions. It is our postulate that the safe operation of a nuclear plant is one such narrowly defineable mission".

More precisely,

"... the mission oriented perspective defines the power plant as supporting the operating crew and their goals, which is the converse of the crew supporting the nuclear engineer's plant".

We have seen in the preceding chapter that this postulate cannot hold for present-day nuclear power plants where operators are mainly required for emergency situations, i.e. where the operators are supporting the nuclear plant.

8.3.1.2.4 Findings of IAEA supervisory missions

IAEA OSARTs (operational safety review teams) perform a three week in-depth review of plants' operating practices, involving up to 12 experts from IAEA, utilities and supervisory bodies. The aim is to assist the utility in improving the safety of the plant. Usually focusing on unplanned reactor shutdowns, worker exposure and equipment malfunctions, OSARTs have visited more than 24 nuclear power plants. Since 1985, they have developed a catalog of 39 indicators which serve as a yardstick to assess the current safety situation of a nuclear power plant.

These indicators show that 50 - 70% of all problems are due to human failure. Of these, 20% (= 10 - 14% of all problems) are due to poor qualification of personnel and 40% (= 20 - 28%) to personnel management and personnel support factors. Furthermore, it is said that 30 - 70% of all deficiencies would have been detectable before the error occurred, provided suitable detection mechanisms were available.

The most threatening results of the OSART missions are that (NucEng, 1988b)

* most plants had not introduced modern management tools and supervisory techniques - leading to the responsible management's ignorance concerning human performance and plant equipment status.

* at several sites manpower resources appeared insufficient to cope with all the tasks without undue stress - thus, even relatively harmless incidents can lead to a high-stress atmosphere which might render the incident more severe because of misdiagnosis or wrong actions under time constraints.

* at only a few plants were there signs of obtaining the ultimate objective, a "safety culture"; a persuasive awareness that safety must be a top priority in all planning and execution.

It appears that the working environment in nuclear power plants is often lacking vital safety mechanisms and safety consciousness.

8.3.1.3 intentional misbahaviour - A risk factor which can hardly be quantified

A very important risk factor cannot be quantified and, as a consequence, is ignored by today's PRAs: voluntary violation of safety rules. We can distinguished between

* individual and group behaviour
  the nuclear power plant employee tries to distract himself, to simplify his duties or to escape punishment after an incorrect action.

* economic and public pressure
  the utility has to demonstrate to the public that the nuclear power plant operates properly and economically. Ideally, this would require that there is no (reported) incident or accident and that the plant is always working at the scheduled power level. This can lead to attempts to avoid shut-down even in dangerous situations.

* social movement
  an employee belonging to a social pressure group may be caused to act against safety rules. The example of problems created by strikes in France is discussed below.

8.3.1.3.1 Individual and group behaviour

A discovery made by the Institute of Nuclear Power Operations (INPO) received considerable attention in 1987 when operators were found to be sleeping at work at Peach Bottom nuclear power plant. It turned out that there had been (NucEng, 1988b)

"· occasions when the control room was not manned as required by technical specifications
· one occasion when only one person was in the control room, with the units at power
· another occasion when all personnel in the control room were asleep
· playing of video games by lincensed operators on computers in the control room and in the computer room
· rubber band fights and paper ball fights by licensed operators in the control room
· one instance where a GE engineer (assigned on a shift with the operator) [General Electric had sent advisers to improve operating crew professionalism] was not permitted in the "controls" area and another instance

where a utility QA Inspector (assigned to monitor shift turnover) was "kicked out" of the control room by the shift operator crew for no just reason, and with laughter afterwards in the control room

- widespread reading of non-technical material
- hostile attitude of operators towards management
- disrespect by operators for plant procedures (i.e., operating procedures were viewed only as guidelines)
- an occasion when a radwaste shift operator was asleep on a table in the radwaste control room, covered with a coat
- an occasion when non-licensed operators locked themselves in their "shack" in the turbine building (that had its windows covered so that activity inside could not be observed) and were asleep."

These incidents were taken very seriously by INPO and NRC, and they criticised the utility (Philadelphia Electric Co.) on the management level for not being able to deal with this lack of safety consciousness on the operator level. As a consequence, the NRC suspended the Peach Bottom 2 and 3 operating licenses and the nuclear power plant had to shut down. Furthermore, the NRC proceeded to issue civil penalties against individual operators - the first time this has ever happened.

These incidents do not represent single, isolated events. This must be concluded from the NRC policy statement 10 CFR Parts 50 and 55 (NRC, 1989a) which was introduced by:

> "On a number of occasions, the NRC has received reports and has found instances of operator inattentiveness and unprofessional behavior in control rooms of some operating facilities. Reported instances include:
> (1) licensed operators observed to be apparently sleeping while on duty in the control room or otherwise being inattentive to their license obligations,
> (2) operators using entertainment devices (for example, radios, tape players, and video games) in the control room in a way that might distract their attention from required safety-related duties, and
> (3) unauthorized individuals being allowed to manipulate reactivity controls.
> Such conduct is unacceptable and inconsistent with the operators' licensed duties."

The problem is that employees can have subjective priorities incompatible with safety goals. Such subjective priorities might result from boredom (need for distractions), but also, e.g. from fear of punishment for mistakes. In the same release, the NRC describes an incident at the Oyster Creek nuclear power plant:

> "Both an NRC inspection and an investigation done by the company found that the safety limit violation occurred when the operator mistakenly had turned off the fourth of five loops in a reactor water circulation system while the plant was shut down. At the time, three of the five loops had already been closed, thereby leaving only one such

loop open. This condition constituted a violation of the NRC requirement that at least two of five loops in this system be fully open at all times. The violation lasted approximately two minutes, from 2:17 a.m. to 2:19 a.m., on September 11, 1987.

The NRC, as well as a separate company investigation, also found that the operator, after correcting his error by opening two more valves, destroyed a paper tape which provided a chronology of the event. He tore off a portion of the print-out that logs control room alarms and discarded part of it in a trash can and flushed part of it down a toilet. GPUN (the utility) subsequently fired him."

However, tougher reglementation can provoke actions that are deliberately violating these new rules because the personnel may not totally accept the tougher working conditions or may consider the new rules as less important than the old ones.

8.3.1.3.2 Economic and public pressure

High pressure from the utility or from the public to meet performance goals can lead to a phase-out of safety mechanisms. As can be seen in a report of the Institute of Nuclear Power Operations (INPO) to the Sacramento Municipal Utility District (SMUD) concerning the Rancho Seco nuclear power plant, this has lead to several incidents in the plant (Nucleek, 1989c):

"The report says the causes of the incident, which increased the feedwater system pressure to nearly three times its design pressure, include poor maintenance practices and training, poorly organized and trained engineering personnel, and insufficient management involvement.
The report, made public by SMUD, also says that plant operations and maintenance personnel "perceive that they are under undue pressure to complete tasks" and that perception "has contributed to performance problems that resulted in plant incidents." For example, the report says that during the December 12 steam generator dryout incident, the load dispatcher "expected the return of the plant to the grid and requested repeated schedule updates" from the shift supervisor. "This may have been a factor in the crew's decision to keep systems on line with multiple component failures."
Rancho Seco is under pressure to meet operating conditions Sacramento County voters approved last year. The voters, in approving an 18-month trial run for the plant, said that if the unit's performance fell below 50% for four consecutive months after December 31, 1988, the plant would be permanently closed unless the SMUD board decided continued operation was in the utility's best economic interests. In June, the SMUD board is required to hold another referendum on whether the plant should continue to operate."

It is obvious that utilities tend to reduce the duration of inspection periods as much as possible because of financial reasons. This may even lead to the violation of technical specifications (for example, having both trains of a redundant two-train system out of service at the same time, while continuing to operate). However, the possibility of such violations is not included in PRAs. It is also noteworthy that violations may occur with the consent of the licensing authority, which can grant exemptions from specifications.

A further example is the Chernobyl accident where an engineering team tried to perform an experiment which was possible during the shut-down phase of the reactor only. As the shut-down sequence could not be run as usual, the team overruled a number of safety systems in order to execute the experiment and not to have to wait another two years for the next routine shut-down operation. As the safety systems were vital to prevent the precarious state the plant was going into, it was impossible to stop the accident sequence after the initial phase of the experiment.

8.3.1.3.3 Social movement

Another issue which can hardly be quantified is the influence of a strike movement on motivation and discipline of the personnel. During the IAEA OSART mission to the St. Albans nuclear power plant in France, the IAEA team found that such a condition (NucWeek, 1989c)

> "... could potentially pose operational safety problems: the year-end strike by EdF [Electricité de France - the utility] nuclear plant operators was in full swing during the IAEA mission.
> The problem, the IAEA team said, was "the obvious interference of the strike committee's orders with the normal lines of authority and responsibility." The strike consisted of continual power level reductions, and strike leaders routinely would come into the control room to ask for power drops, even when the plant manager had received a grid request for full power. As explained February 23 by EdF's Lucien Bertron, this meant that during the strike, "the authority of the plant manager was flouted on the point of output, so would it also be on the point of safety?"

Inspite of these concerns, in this case in fact nuclear safety requirements placed restraints on the strike movement, and not vice versa. EdF personnel on strike did not drop power in some nuclear power plants because the fuel was nearly burned up, and a power drop would have caused increased pollution and an outage of several days (Libé, 1988).

8.3.2 Human actions modelling

Modelling efforts of human actions in nuclear power plants include a variety of techniques usually based on a

classification of the tasks to be performed (Birkhofer, 1986). In most cases, the efforts focus on operator behaviour, although human influence in areas like maintenance, construction & fabrication, design,...(see 8.3.1.1) is far more significant.

8.3.2.1 Approaches to classify human actions

There has been a number of classification efforts, attempting to identify individual steps of action sequences, and treat those steps separately.

Wickesson (1981) introduces three basic human error categories:
(1) human errors initiating accidents,
(2) human errors affecting systems availability,
(3) human errors during accidents.

This scheme is also cited by Öko (1983) and Anderson (1986).

Joksimovich (1988) considers five classes:

- testing and maintenance actions prior to an initiating event,
- actions which might cause initiating events,
- emergency-procedure-driven actions taken to deal with and mitigate the consequences of accident sequences,
- actions which aggravate accident sequences,
- recovery actions.

Actions involving deliberate disabling of safety equipment are also mentioned and included in the first point.

Fouco (1981) assesses human errors by
- an a-priori probability estimation and
- an a-posteriori probability estimation.

A-priori probability estimation is based on event tree and fault tree analyses, while a-posteriori estimations rely on questionnaires, simulator data and other after-action evaluations (Öko, 1983).

Rasmussen (1979) defined the notions of skill based, rule based, and knowledge based actions. Skill based are those actions which are routinely performed, rule based those for which the operator needs the support of procedures and rules, and knowledge based are those which rely on the operator's knowledge of the plant, and where no rules have yet been formulated (Hannaman, 1985a).

Pope (1986) recognizes that

> "there is little consistency between classifications and few take account of the dependence which exists between human errors."

Mostly, there is no distinction between recoverable and non-recoverable human errors. Only a few qualitative approaches deal with this subject (Orvis, 1985; Worledge, 1985).

Almost all human reliability analyses include the following classification scheme which is clearly oriented towards quantification: Human actions are divided into errors of omission (an action has not been performed) and errors of commission (a wrong action has been performed). The latter case is much more difficult to evaluate as there are hundreds of possibilities to think of. Therefore this case often omitted.

Hörtner (1986b) states that the accident probabilities of DRS-B (German Risk Study - Phase B) and DPS (German Precursor Study) include human error.

Birkhofer (1986) specifies the human errors which had actually been taken account of: Most PRAs only include planned actions. The unplanned actions may have positive or negative effects on the plant status. Therefore, neglecting them entirely excludes both positive and negative influences to the same extent, according to Birkhofer. It should be noted that, for example in Browns Ferry in 1975, operators have prevented worse consequences by intelligent and innovative actions.

A review of Licensee Event Reports of US nuclear power plants (Sabri, 1981) shows that out of 89 significant reported events, 58 % (52) involved operators, 36 % (32) the maintenance crew. Out of the 52 operator related events there were initiated

- 11 by failure to act (omission)
- 11 by improper action (commission)
- 7 by failure to follow procedures (omission)
- 6 by inadvertent action (commission)
- 6 by incorrect or incomplete performance
- 5 by oversight
- 4 by misunderstanding
- 1 by communication failure
- 1 by improper written informations

This result shows a relatively high percentage of errors of commission and of "complex" errors like misdiagnosis (misunderstanding) or errors related to other levels than the operator level (errors in procedures' writing).

8.3.2.2 Data base for the quantification of basic human actions

For a discussion of completeness and quality of human actions' data see also appendix 5A.

Several authors in the nuclear community criticize the lack of sufficient and reliable data even for basic human actions. So Pope (1986) states

"There has been [illegible] systematic collection of human data. ... It follows that there is no comprehensive body of validated data."

Also Hannaman (1985a) has found that

"the review of data sources indicates that there is no entirely satisfactory single source of data."

Ryan (1985a) reviewed HRA data from 19 PRAs. It was found that less than 1 % of the data requirements for a PRA were fulfilled by all current PRA studies. Only 10 % of the data sets collected were complete in containing information about

* personnel involved
* actions involved
* performance shaping factors (PSF)
* situation
* systems involved.

Statistics (table 8.2) show a considerable concentration of PRA work on operator analysis, whereas supervisory staff is only included in about 1 % of these cases. Bearing in mind the importance of the other fields of human action (see 8.3.1.1), this constitutes a considerable weakness. Similarly, accident situations (table 8.3), personnel actions (table 8.4), nuclear power plant systems (table 8.5) and PSF's were documented neither completely nor to an acceptably detailed level.

For these reasons, researchers try to overcome this situation by the use of one or more of the following three methods:

- real event analysis,
- simulator data,
- expert estimations.

Pope (1986) gives a rule of thumb for basic human actions quantification (table 8.6).

8.3.2.2.1 Real event analysis

suffers from data sparseness, because the important events like the Three Mile Island or Chernobyl accidents are not as frequent as a statistician would desire for this purpose. Consequently, there is no statistical base for most of the real event data at present.

Although it is stressed by utility representatives that human contributions can be positive, we must conclude from reports on real accidents and incidents that humans are far more often degrading safety either voluntarily or by mistake.

8.3.2.2.2 Simulator data

are more and more used to quantify simple and complicated human actions (see Joksimovich (1987) for a verification effort of the HCR approach by simulator). The major, fundamental drawbacks of this approach are that

* operators implicitly know that there is no real danger - therefore, they act differently than they probably would in reality,
* only incidents can be simulated which have been selected and designed beforehand by the testing team - no other cases can be analysed,
* the simulator only shows reactor responses that are well understood and have been modelled - physical processes that are not yet understood or misinterpreted cannot be correctly included,
* computer programs for the simulator might be incorrect,
* because of limitations in the range of situations covered by simulator data, recour to expert opinion must be made in the areas of stress, information interface, and training (Hannaman, 1985a).

"No series of simulator experiments can obtain data under all combinations of even a limited number of key performance shaping factors" (Worledge, 1985).

Regarding the stress factor, this last point has been demonstrated for both nuclear (Chernobyl) and non-nuclear (Vincennes, see 8.3.3.2.1.1.2) applications.

Additionally, Hardman (1988) pinpoints simulators as not being consistent with the nuclear power plants they are intended to simulate:

"Some plants were years from completion when their simulators were designed, and others have undergone continued enhancement and equipment replacement for reasons of safety and operational efficiency. Control rooms have grown in complexity as more data and aids are made available to the operator due to advances in microcomputers and graphics."

8.3.2.2.3 Expert estimations

A relatively large number of subjective estimation techniques has been developed to assess human error. At least nine of them have been used in the nuclear field, all of them (Pope, 1986)

" * being complex
* giving unvalidated results
* having a variable applicability and suitability
* are not always easy to use ".

Concerning expert estimation methodology, Mosleh (1987) criticizes that

" * many applications elicit judgmental estimates without following any formal or documented approach,
* multiple experts are commonly used. However, some applications rely on traditional group meetings, with informal procedures for aggregating conflicting opinions instead of more formal mathematical procedures,
* decomposition [of tasks] is widely used. However, the form of the decomposition is sometimes akward or not meaningful. "

This leads to
- underestimation of failure rates (because of group processes) and
- overconfidence in results (i.e. underestimation of uncertainties).

Consequently, group meetings usually do not yield good quality results, and the interdependence between expert estimations is quite high.

Although useful for qualitative assessments, expert opinion sampling must be seen as a rough and rather subjective quantification method. The attempt to obtain objective expert opinions by group meetings is questionable as human interaction tends to underestimate failure rates and uncertainty bounds.

8.3.2.2.3.1 The "Handbook" of Swain and Guttmann (Swain, 1983)

This work constitutes a major effort in this field. Based on the quantification of human actions as performed for other industries, it attempts extrapolation to similar actions in the nuclear sector. The validity of these probabilistic data is limited to situations where (Bell, 1981a):

"- the operator's stress level is optimal,
...
- the personnel are qualified and experienced, ..."

Concerning the second point, we refer to chapter 8.3.1.1.7. For the first condition, the authors remark:

"Most of the estimated HEP's [Human Error Probabilities] in the Handbook apply to routine human actions. The method for estimating the probability of human error under stressful situations is highly speculative. Therefore, such estimations are characterized by wide uncertainty bounds."

For their model, they assume

".. that all nuclear power plant personnel act in a manner they believe to be in the best interests of the plant. Any intentional deviation from standard operating procedures is made because the employee believes his method of operation to be safer, more economical, or more efficient

or because he believes performance as stated in the procedure is unnecessary."

The economic aspect in particular can lead to serious problems for the operating crew: in an emergency situation, the crew might have to decide on a compromise between safety rules and utility performance goals (see 8.3.1.3.2).

We must conclude that the common practice of using the HEP's from the "Handbook" as point estimates for high-stress situations like accident conditions, where knowledge based actions are playing their most important role (e.g. Lanore, 1987), is not a scientifically correct procedure. This view is shared by (at least) one of the handbook's authors.

8.3.2.3 Human reliability modelling

Human performance models are a means of quantification for actions beyond the basic level. They have to rely on data determined by the methods described above.

Furthermore, particularly complicated actions, like dependent actions or errors of commission, cannot be quantified. Some of the models have further deficiencies.

A precise definition of the requirements for a human reliability model was given by Hannaman (1985a) (table 8.7), emphasizing that

> "it is generally recognized that the performance of humans can be strongly affected by stress, control room instrumentation arrangement, etc. and any model of crew behavior should account for these effects."

8.3.2.3.1 The basic models

In this section, some of the conceptual models and quantification approaches employed in human reliability assessment are briefly described.

8.3.2.3.1.1 Performance Shaping Factors (PSF)

Performance shaping factors (PSF) include psychological and environmental factors affecting human actions reliability. Among these PSFs are (Embrey, 1981):

- quality of procedures
- quality of personnel training
- time available for a task
- quality of the plant state information available to the personnel
- reversibility of actions
- quality of supervision

- motivation
- presence of functionally isolated steps within the task (which are more likely to be omitted).

This structure is providing a framework. The factors themselves, however, often are not clearly defined. The crucial and most difficult task is their quantification. It is obvious that every quantification effort has to be somewhat subjective because most of the features cannot be measured directly (e.g. motivation). Usually, a ranking system has been applied, consisting of "classes" ranging from 1 to 3, 1 to 5 or even 1 to 10. In order to permit the use in detailed models, a range from 1 to 10 is required according to Wakefield (1987),

8.3.2.3.1.2 THERP

The Technique for Human Error Rate Prediction (THERP) has been developed by Swain (1963) and seems to be the most widely used model (Pope, 1986). THERP is an analytical technique which is restricted to (Öko, 1983)

* maintenance actions and
* limited actions of operators (e.g. after incidents)

A fault tree technique is being used to describe the system under study. Main problems are that THERP is based on subjective assessments at various levels in the model and that independance of actions is assumed (Knee, 1981). Furthermore, important shortcomings are the omission of knowledge based actions which, however, make up the most important category under severe accident conditions (Birkhofer, 1986).

8.3.2.3.1.3 The HCR model

The Human Cognition Reliability model (HCR) provides the time-dependent human non-response probability to a task. Key input parameters are (Hannaman, 1985a)

- three types of cognitive behaviour: skill-, rule, and knowledge-based (see 8.3.2.1),
- the median response time for a task (T^*) (from simulator data or expert estimations)
- performance shaping factors (see 8.3.2.3.1.1)

The HCR model yields a curve representing the error probability for a given action as a function of performance affecting time influence (figure 8.3). Mathematically, the HCR can be approximated by a 3-parameter Weibull distribution of the form

$$HCR = \exp\left(- \frac{(t/T^*) - a}{b} \right)^c$$

where a, b and c are derived from the PSFs and t is the time available for execution of the task.

The value obtained is very sensitive to the factors influencing operator response (PSFs), and is less sensitive to the assessment of median response time (Hannaman, 1985a).

The same authors introduce their HCR model as follows:

> "It is the human reliability assumptions that can have a dominant influence on the result of a PRA study. ... Fortunately, valuable insights of plant safety can be obtained even with rough approximations of human reliability."

Wakefield (1987) observed that computed HCR values were optimistic when applied to long time periods. He modified the HCR model in order to account for dependancies between individual actions in the same sequence. As a key problem, he mentions

> "The analysis team had great difficulty estimating the "median time to respond". Since the computed error rates are so sensitive to this parameter, the uncertainty in this parameter alone can lead to large uncertainties in the final results."

8.3.2.3.1.4 The approach in the German Risk Study, Phase A

While most of the data of the German Risk Study, Phase A (DRS A, 1979) originate from WASH-1400, a limited number of them has been modeled according to a time-dependent operator failure probability. This probability, as introduced in the German Risk Study, depends exclusively on two variables:

- the maximal admissible time tc respond (t) and
- the mean operator response time (T').

This leads to a very simple, HCR-type formula:

$$P = \exp(-t/T')$$

Psychological factors and factors which are specific to certain procedures are thus neglected. This approach is completely out-of-date.

8.3.2.3.1.5 SLIM-MAUD

The SLIM-MAUD model (Embrey, 1985) is designed to quantify error probabilities of proceduralized and cognitive tasks. It relies on task decomposition and PSFs.

The model requires a description of the event to be analysed, including a decomposition into operator tasks and subtasks. Subsequently, the PSFs are quantified, using using a scale from 1 to 9, followed by a weighting procedure for each PSF.

The result, for each task, is a value called Success Likelihood Index (SLI). From the SLI, HEPs can be derived by a simple formula. Variation of different PSFs can help in identifying measures to be taken to upgrade operator performance. SLIM-MAUD at present is the most psychology-based approach to human error modelling in nuclear power plants.

8.3.2.3.1.6 SHARP

The Systematic Human Application Reliability Procedure (SHARP) is a framework for incorporating human interactions into PRA studies (Hannaman, 1985b). It consists of 7 steps, where

- the first three (definition, screening, breakdown = identification of actions, selection of important actions, task decomposition) are defining and describing the key human interactions.

- steps 4 and 5 (representation, impact assessment) are incorporating the human actions into the system models.

- step 6 (quantification) selects the approach for human reliability quantification.

- step 7 (documentation) is intended to provide a star[illegible]d documentation framework for PRA purposes.

Thus, SHARP provides a common structure and a documenta[illegible] scheme for different human reliability quantification [illegible] used in PRAs.

8.3.2.3.1.7 The Worledge model

Worledge (1985) proposes a framework which is based on five fields of action (figure 8.4):

* diagnosis
* procedure selection
* expectation of plant reaction
* perception of plant response
* avoidance of slips

The key concept is the operator's "mental image" of the plant status. If the real state deviates from this image, the operator will react. No reaction will occur, however, if the deviation is not recognized. Thus, the model takes into account diagnosis and decision processes of the operators.

This approach is much more complete than other models, without directly leading to error quantification, however. Hannaman (1986) states that this approach expands the range of applications for the HCR model, if the two models are linked. Analyses of accidents showed that the Worledge model cannot be employed to deal with errors due to equipment malfunction or operation. Also, the area of long term actions is not adequately covered.

8.3.2.4 Incorporation into a PRA scheme

Coupling of PRA techniques and preliminary results of HRA has been attempted by some researchers. However, a consistent assessment technique is not in sight. Many questions still remain open, particularly in the fields of dependency quantification and ergonomic aspects of man-machine interaction.

Hall (1985) emphasizes the need for a better documention of PRA studies as

> "the poor and incomplete way in which they are reported would require major reanalysis prior to their use."

Wakefield (1987) reported an application of his modified HCR model in a full-scope PRA, but he also found disadvantages of the HCR model (see 8.3.2.3.1.3).

Beveridge (1985) proposes that operator actions should be directly included in the PRA event tree.

On the other hand, Potash (1981) identified several major problems

> "that inhibit any effort to handle operator error in PRA's. ...
>
> - [lack of] identification of important operator errors,
> - absence of validated models and/or techniques for estimating operator error during a transient,
> - lack of data relating to operator error during events,
> - insufficiently developed methods for dealing with dependencies between operator errors in fault trees."

Although this statement has been formulated eight years ago, it still has to be regarded as valid.

8.3.2.5 Critical review of quantification efforts

Due to the limitations of event modelling and an insufficient data base for rare events, HRA quantification efforts must be regarded with extreme caution.

Especially psychological factors (PSF's), which provoke actions outside the usual framework of behaviour, are very difficult to assess or to model. Researchers often simply omit them from their analyses. The importance of, for instance, a reliable stress assessment for quantification efforts, however, is frequently emphasized.

Bell (1981b) describes a HRA performed by Sandia National Laboratories. Although focusing on test/maintenance and accident response scenarios, the selection of human actions is limited

"to those components expected to be manipulated during the test or maintenance action (or accident response action) itself."

Thus, unexpected actions which can cause unforeseen problems are left aside. The accident response identification

"assumes that the operator is attempting to follow the proper procedure in responding to each accident sequence. This assumes a proper diagnosis of the situation."

It is questionable whether an operator in a high-stress situation will be able to analyse any accident sequence correctly, particularly if there are physical phenomena which scientifically are not yet fully understood.

The authors use the "Handbook" (see 8.3.2.2.3.1) as data base, which provides human error probability (HEP) data taken mostly from the non-nuclear industry and which cannot be used for analysis of high-stress situations.

By other authors, the importance of correct identification and quantification of dependencies is mentioned (Samanta, 1985) and ranked as equally important as a correct estimation of independent probabilities (Potash, 1981).

However, most of the reported HRA models have not included the crucial point of errors in operator diagnosis and decision-making. An internal review of HRA methods by the UKAEA (Pope, 1986)

"came to the conclusions ... that on the basis of
- identification and analysis of significant human actions
- quantification of human error probabilities
no method is entirely satisfactory, and a clear need is seen for ... [further substantial work]."

In his conclusion of a review of several papers, Hall (1985) criticizes that

" * currently qualitative results are more useful in decision making than the absolute numerical ones,...

* a PRA or HRA must be correctly documented ... "

Futhermore, he diagnoses a lack of communication between the nuclear industry experts and human factors specialists. He warns the industry of indiscriminate use of HRA techniques.

Ryan (1985a) stresses the need that

"documentation should include a complete explanation of HRA/PRA methods, data sources, and results."

Pederson (1981) also restricts the use of HRA data:

"... prediction [of quantitative errors] is only practical when one is looking for comparisons and indications of the order of magnitude of the probabilities of human errors with respect to specific objectives (i.e. reliability, availability, safety) :

- for well-defined proceduralised task sequences familiar to the human,
- for well-defined work situations for which performance shaping factors (in particular error recovery features) are known, and data can be collected."

Finally, Schurmann (1985) discusses some reflections on how human performance models are being judged by experts. His conclusion is that the aesthetic and the intuitive aspect seem to be much more important than the correct and detailed modelling. He pointedly remarks that, frequently, the human being does not even seem to be necessary for human performance models. Other models (SLIM-MAUD) are regarded as rather complex for nuclear applications. The purpose of the model needs to be very well-defined indeed; or in other words:

"If you do not know where you are going, one road is as good as the other."

8.3.2.6 Conclusions

After TMI, a number of efforts have been conducted to reduce human error: Advanced control room design, training of high risk manoeuvres on full scope plant simulators, and upgrading of procedures and instructions, for example.

After Chernobyl, it also became obvious to the nuclear community that the assumption that operators always intend to follow the safety guidelines need not necessarily be true.

All modelling efforts suffer from a number of severe shortcomings in the fields of

* data quality
* data collection procedures
* uncertainties induced by human variability
* human dependencies
* complexity of human actions
* quantification of errors of commission
* completeness of actions analysed

Additionally, a systematic approach to the human error problem substantially lacks consistency in the areas of

* classification of human actions
* quantification of basic human actions
* basic assumptions for modelling
* degree of completeness and techniques used for modelling

8.3.3 The contribution of computers to safety in NPPs

Presently, the contribution of computers to nuclear power plant safety (or hazards) has not yet been considered in PRA's. There are strong indications that the use of computers will spread in the future. Thus, a comparison of human hazards is automation hazards is called for.

8.3.3.1 The use of computers in nuclear power plants

Like other German NPPs, the Grohnde nuclear power plant is run fully automatic during normal operation. Only for start-up and shut-down procedures, human actions are necessary. Furthermore, the automatic reactor protection system overrules manual inputs in the case of conflicting actions (Grohnde, 1973).

The shut-down sequence has to be initiated by hand, and subsequently proceeds automatically.

This reliance on automation has led to problems, for example, in the Neckarwestheim nuclear power plant: After the erroneous opening of a steam valve, time consuming administrative measures had to be taken for reclosure (Śmidt, 1979).

Hörtner (1986) states that a high degree of automation implies a reduction of human error. However, chapter 8.3.3.2 will show that this applies only to traditional human errors during operation. Furthermore, new categories of human error are introduced: On the level of software development, as well as on the level of using specific software tools.

Hardware hazards can be relatively well quantified (Kersken, 1985), while it is still difficult to assess software error hazards. Before analyzing those hazards, the present situation of computer use in NPPs, as well as new developments, is discussed.

8.3.3.1.1 Present situation

The areas of computer use in nuclear power plants are limited at present; they include

* passive instrumentation and control,
  - local network technology for process control (Aschenbrenner, 1988),
  - microprocessor based reactor protection system at Sizewell B (Pepper, 1989)
  - alarms on CRTs in Loviisa (Rintillä, 1987), high degree of automation
  - CRT information, operator support system in Japan (Itoh, 1988); not (yet) relying on AI
* process computers
* monitoring of fuel status (Williams, 1988) and plant status (LaRosa, 1989)
* offline analysis (process models, GRS, 1987)

The OSAR teams of the IAEA observed that in the nuclear power plants visited "no important control function was assigned to a process computer and there were no plans to do so at any plant" (NucEng, 1988b).

An OECD survey mentioned that only Canada considered using computers to replace operators on their HWR nuclear power plants (NucEng, 1988a).

8.3.3.1.2 Trends

In order to

* take operational burden (routine work) off the operators
* give decision aids in accident situations
* automatize maintenance actions
* provide operators with pre-analysed plant status data (GRS, 1987)
* improve simulator capabilities (Hardman, 1988)

a number of software packages are under development in several countries. These software packages rely primarily on

* correct measurements of the sensors
* correct analysis tools and
* realistic simulation packages.

For the near future, they include features like

* computerized procedures (Elm, 1988; Reiersen, 1988)
* alarm avalanche suppression (Elm, 1988; Reiersen, 1988; Nedderman, 1988)
* operator decision aid systems (Elm, 1988; Itoh, 1988)

At present, research is focused on artificial intelligence and expert system approaches (see 8.3.3.2.2).

8.3.3.2 Software hazards

There are at least 4 levels of possible errors related to software use and development:

* program layout (misunderstanding between computer and nuclear experts)
* program development (logical errors)
* program coding (typing errors)
* program use (wrong or incomplete documentation)
* program modification

(The Atlantis space shuttle, for instance, always carries a manual containing the errors of the software that have been found but not corrected for fear of unforeseen consequences in other parts of the software.)

Computer scientists generally agree that it is almost impossible to produce error-free software. In particular, rare events can lead to unforeseen reactions of the program (see

8.3.3.2.1.1.3). Thus, efforts to reduce and quantify software error risk have still not reached their goal (Kersken, 1985; Barnes, 1989) and it is questionable whether they ever will.

A considerable hazard including the whole error potential described above is brought about by a change of the main computer system, as experienced on the Loviisa nuclear power plant (Rintillä, 1987). In this particular case, it was necessary to rewrite all of the software which formerly had been written in assembler language.

8.3.3.2.1 Examples of software related incidents

8.3.3.2.1.1 Accidents related to computers outside nuclear industry

8.3.3.2.1.1.1 UK weather forecast 1987

In October 1987, the British Meteorological Office failed to issue a hurrican warning for South England. According to a Defense Ministry report, the scientists had overestimated the capabilities of their computer model which included an upper limit for wind velocity (HAZ, 1988). However, the real storm, killing 20 people on the morning of October 16th and devastating large areas, featured wind speeds up to 190 km/h, well above the maximum value allowed for in the model. This storm happened to be the most severe for the last 300 years.

8.3.3.2.1.1.2 Vincennes guided missile cruiser

In July 1988, the US warship "Vincennes" shot down a civilian Iranian Airbus. The following investigation showed that the computer linked to the air warning system had classified the civil airplane as "hostile", though correctly displaying that it was in the ascent phase of the flight. Bad presentation of data, together with automatic computer tracking of the plane had led to this misinterpretation in a high-stress situation (ACM, 1989b).

To better understand the situation of the cruiser crew, it must be noted that the vessel had been engaged in a battle with Iranian vessels and that another US warship, the "Stark", had been hit by a missile only a few days earlier.

The importance of the stress factor which led to the fatal decision, has well been recognized by the Pentagon which stated that people under great stress do not "function" in the same manner as they do under laboratory conditions.

The connection between the psychological factors and the computer software which is not designed adequately for these situations, is illustrated by the tape that recorded the chronology of the buttons which had been pushed (ACM, 1989a).

> "Because of this record, we know that one officer, who was prompted by the computer to "select weapon system" as the

countdown to the destruction of the Airbus began, hit the wrong button five times before he realized that he was supposed to seslect a weapon. And we also know that another member of the Vincennes' crew was so agitated that he got ahead of the firing sequence and pushed another button 23 times before it was an appropriate part of the procedure.

I don't recount these errors to pick on the crew. I recount them because I believe that they must be considered the norm when inexperienced humans face a sudden stressful encounter."

8.3.3.2.1.1.3 X-Ray machine

According to an article which appeared in ACM (1989d), a radiation therapy machine, manufactured by Atomic Energy of Canada Ltd., has caused the death of several people because of a computer program error.

> "The radiation-therapy machine, a Therac 25 linear accelerator, was designed to send a penetrating X-ray or electron beam deep into a cancer patient's body to destroy embedded tumors without injuring skin tissue. But in three separate instances in 1985 and 1986, the machine failed. Instead of delivering a safe level of radiation, the Therac 25 administered a dose that was more than 100 times larger than the typical treatment dose. Two patients died and a third was severely burned.
>
> The malfunction was caused by an error in the computer program controlling the machine. It was a subtle error that no one had picked up during the extensive testing the machine had undergone. The error surfaced only when a technician happened to use a specific, unusual combination of keystrokes to instruct the machine. ...
>
> The Therac 25 delivers two forms of radiation: either a high-energy electron beam or, when a metal target intercepts the electron beam, a lower-energy X-ray beam. It turns out that when a nimble, experienced technician punches in a particular sequence of commands faster than the programmers had anticipated, the metal target fails to swing into place."

There are many more examples in the medical field where computer controlled machines endangered people.

8.3.3.2.1.2 Computer related nuclear incidents

Although computer use is not yet widespread in the nuclear industry, there have already been two incidents leading to safety problems in nuclear power plants. In the future, it must be expected that increasing use of systems like those described in section 8.3.3.2.2 will lead to an increasing number of more

serious problems. We briefly describe the two incidents which show two features that are alarming: both problems concerned safety related plant systems, and the second one is common to a number of nuclear power plants of identical design.

8.3.3.2.1.2.1 A software problem at the Darlington nuclear power plant (Canada)

On January 19th, 1989 Nucleonics Week (NucWeek, 1989b) reported that the Atomic Energy Control Board of Canada (AECB) was delaying fuelling of the Darlington nuclear power plant because of a "problem in the shutdown system software". This incident concerned a heavy water reactor (HWR), but analogous problems could also occur in LWRs. According to AECB director Domaratzki, this software

> "... has been under discussion between [Ontario] Hydro and the board [AECB] for the last two years. Modifications are still being made based on both Hydro's recommendations and ours."
> The four Darlington reactors, under construction since 1977, incorporate a new generation of computerized control for emergency shutdown. Emergency shutdown systems in the Hydro reactors at Pickering and Bruce are essentially dependent on "hard-wired relay logic" to trigger them, he said. The Darlington emergency shutdown systems are being to be activated "by logic that is largely software, that is primarily computer programmed"."

8.3.3.2.1.2.2 A software problem at the Nogent nuclear power plant (France)

NucWeek (1989a) reported the following:

> "FRANCE: NOGENT CONTROL SOFTWARE FOUND DEFECTIVE
>
> Existence of a defect in the software controlling the instrumentation and control (I&C) system of Electricité de France's (EdF) Nogent-2 PWR was classified as a level 1 problem by French safety authorities. The defect, discovered just before Christmas, led to the sending of erroneous messages to the control room on such things as the parameters for reactor control. A similar defect was also found in the I&C systems of Flamanville-1 and -2 and Paluel-3 and -4. All five units are in EdF's "P4" four-loop PWR series.
>
> The software did not have any direct safety consequences, said the utility. However, safety authority Service Central de Sureté des Installations Nucléaires (SCSIN) flagged the problem as needing special attention in the context of EdF's quality assurance/control program. SCSIN is concerned that a watertight QA/QC program for checking software modifications be in place to prevent such defects from being introduced along with software upgrades or changes dictated by operating experience feedback,

utility spokesman said. In the meantime, EdF has taken measures to make sure the defects at the five PWR units are compensated for by control room staff until they are corrected."

8.3.3.2.1.3 Hacker intrusion in nuclear research facilities

Hackers have been reported to enter nuclear research facilities in West Germany (KFA Jülich, KfK Karlsruhe, Hahn-Meitner-Institut Berlin), Switzerland (CERN), the United States (Lawrence Livermore Labs) and elsewhere. Any responsable nuclear power plant designer should not permit access to the vital electronic systems of the plant from outside. If there is a possibility to access the plant computer from outside, however, this might cause considerable safety problems which can hardly be evaluated quantitatively.

8.3.3.2.2 Expert systems and Artificial Intelligence

8.3.3.2.2.1 What is Artificial Intelligence ?

Artificial Intelligence (AI) is a field of computer science where it is attempted to model human problem solving ability.

This field has created a number of special sub-domains:

- pattern recognition
- robotics
- knowledge representation
- expert systems
- learning
- and others

There have been a number of spectacular results which are of considerable use in special applications: chess computers, industry robots, rapid finger print analysis, etc. However, there is no hint that the "final goal" will ever be achieved: The creation of a general-purpose "thinking machine".

8.3.3.2.2.2 What is an Expert System ?

An expert system is a simplified approach to human reasoning. Generally, reasoning is divided into two basic categories:

- the knowledge base (simulating factual knowledge) and
- the inference motor (simulating deduction capacities)

The knowledge base itself consists of data base and rule base, whereas the inference motor consists of the complete description of rule and data interaction and user interference (figure 8.5). Typically, an expert system has to handle a certain situation by applying logical rules and stored data ("experience") to provide further information or a solution to the given problem.

8.3.3.2.2.3 Application of expert systems in a nuclear power plant

The benefits and limitations of expert system use in nuclear power plants are discussed by Westinghouse's W.C.Elm (1988):

> "In situations during which man may be prone to error - such as when large amounts of data are received in a short time, when apparently contradictory data are presented simultaneously, or when man fixates on a hypothesis and ignores or misinterprets data to the contrary - a machine's effective support of man's problem-solving skills can be a valuable tool in the process of decision-making."

However, any automated interpretation of data leading to a recommended action, places the user into a dilemma:

> "When advice is output from the system, the user must decide to accept or reject that advice. Acceptance of incorrect advice may endanger the plant, as may rejection of correct advice. In essence, the user must understand the advice, and come to an independent determination of its correctness.
> Expert system designers respond to this issue as a question of how the expert system "explains" itself to the user."

Considering the well-known time constraints of operators in accident conditions, it is not very probable that lengthy explanations will be of great value. Thus, the conclusion is that

> "Systems which require "common sense" or a "deep understanding" of physical phenomena are not good candidates for expert systems.
> ... an expert system to diagnose precisely the failure(s) and correct response for all possible plant disturbances is not likely to be practical in the near term. The scope of understanding required ... exceeds the current state of the art."

To benefit from the rapid data processing capacities of a computer, an integrated expert system approach is neither feasible nor useful. Although a partial substitution of the operating crew may be possible (Nedderman, 1988), it should not be attempted to suppress valuable information about the plant status. In order to support operators in stress situations, it may be helpful, however, to use "intelligent" systems for low-level tasks like the transformation of data into information meeting the requirements of the user (e.g. alarm avalanche suppression).

Several institutions are presently developing decision aid systems of a relatively high complexity. Sonoda (1987) presents a system that is guiding the operator in fault conditions, an expert system intended to collect operator and engineering

knowledge for automatically giving skilled advice under accident conditions. The US DoE (Department of Energy) is also working in this direction. As there are still considerable deficits in understanding human decision making (Kennedy, 1986) and physical aspects in the field of degraded core analysis (Birkhofer, 1988), operational decision aid systems of this kind should be regarded with extreme care.

Artificial intelligence and expert system tools are certainly of a high value, but the area of application in nuclear power plants has to be limited to fields where processes are fully understood and where it can be guaranteed that they do not create additional risks. Under accident conditions, this usually cannot be assumed. Unless there is a satisfactory conservative solution for this problem, the application should be restricted to off-line analyses, studies and non-sensitive areas.

8.3.3.2.3 Limitations of computer use in nuclear power plants

Nelson (1981) is proposing more intensive computer use in the area of decision making. His propositions range from merely passive decision aid systems in the form of an electronical procedures guide to sophisticated learning tools which would

> "detect subtle relationships which a human operator would never notice."

This could lead to safety problems because a sophisticated learning system might draw the wrong conclusions from the complex physical nuclear power plant system.

The main limitations of real-time simulation of physical processes can be summarized as follows:

* mathematical models do not represent reality; they only provide an approximation,

* it must be expected that there are unforeseen measurement results, due to defect sensors or to unforeseen physical reactions,

* only phenomena that have been understood can be simulated; the simulation remains incomplete,

* operators may place too much confidence in simulation results relating to rare events.

A very useful application of expert system techniques may be an alarm avalanche suppression scheme which, however, should be equipped with redundant control possibilities and a manual backup.

The general tendency during a conference on Man-Machine interface in the Nuclear Industry (Feb. 1988) was that

"... four years or more will be required before we can tell what the role of AI [in the nuclear industry] will be. ...
It would be too risky to let operators become over dependent on such expert systems. ...
... changes should not be made because they are technically possible."

There is nothing we can add to these insights.

8.3.4 Automation or human control ?

There is an old, possibly Buddhist, saying which was recalled in ACM (1989c):

"There is a key that opens the gate of heaven and it is the same key that opens the gate of hell. The two gates cannot be distinguished from the outside and the only way to tell which is which, is to open it.

Obviously, it is very desirable to possess the key because it allows us to experience wunderful things, but there is also the risk of the contrary. This key is technology."

Applied to the question of computer use in nuclear power plants, it is true that this can lead to improved safety but it also bears the risk of including new dangers which cannot be dealt with by the usual procedures.

In connection with the Norwegian nuclear power plant simulator HAMMLAB in Halden, Reiersen (1988) discusses the automation of tasks that previously had been performed by the human operator. His outlook into the future shows the dangers described in 8.3.1.2 :

"In the more advanced conceptual designs now proposed for nuclear power plants, the operator is retained primarily for his supervisory skills and diagnostic capabilities. ... However, a basic issue, which must be confronted before such systems can be implemented with confidence, is whether they do indeed provide those benefits to plant performance expected by their designers."

In a much more optimistic manner, the West German nuclear industry magazine "Atom & Strom" mentions in its issue no. 6 of 1987

"... automation which is always working in the right direction ..."

and

"... graphics terminals presenting several thousand individual information points in a clear manner ..."

If automation was as easy as this, the difficulties in expert system and artificial intelligence development would never have occurred (see 8.4.2.2). All human errors could be avoided by replacing the human operator by a computer program. Unfortunately, reality does not support this viewpoint - human error interferes in the production process of software and of hardware, the use of software, etc.

A consequence of the high error probability for unfamiliar situations might be a higher level of automation of well-understood sequences, (Pope, 1986)

> "in essence reducing human involvement in the operational stage whilst increasing it at the maintenance and testing stage",

a method that has lead to the so-called "30-minutes-rule". According to this rule, all actions after the initiation of an accident are performed automatically for 30 minutes. Thus, the personnel has some time to discuss possible actions to be taken in case of unfamiliar situations, actions that might be supported by simple decision aid systems if the situation is fully understood.

This "30-minutes-rule" is implemented in Swedish nuclear power plants (Anderson, 1986), leading to

> * advantages for handling design-basis events and
> * disadvantages for unforeseen events (reliance on operator experience and decisions being unavoidable in these cases).

Practice in West German nuclear power plants is similar.

However, recent developments in accident management permitting the operating crew more freedom of action (see section 14) may jeopardize what advantages the 30-minutes rule may have, at least for design-basis events.

A trade-off between hazards of human actions and computer hazards has to take into account that more automation brings about unknown new software problems. Additionally, there is one aspect <u>increasing</u> safety (the human operator has less tasks to fulfill) and one aspect <u>decreasing</u> safety (the human operator has to face more boredom, with all its consequences).

9 REACTOR PRESSURE VESSEL FAILURE

(contribution by Dr. Ilse Tweer, Buxtehude)

9.1 INTRODUCTION

In probabilistic risk assessment, the quantification of the rate of catastrophic failure of the reactor pressure vessel (RPV) requires extreme care. There are no back-up systems for this component: RPV failure necessarily leads to severe core damage.

The determination of the failure probability of an LWR vessel from statistical data on operating commercial reactors has not been performed in PRAs so far: although no disruptive failures were yet reported from Western pressure vessels, the accumulated reactor vessel years do not yield a sufficient statistical basis. Failure rates calculated from the actually "observed" vessel years would amount to values higher than 2E-4 per vessel year.

Therefore, the estimation of RPV failure probabilities relies either on statistical data from conventional (i.e., non-nuclear) vessels, or on theoretical approaches analyzing the structural integrity of reactor vessels. In spite of the methodological difficulties, all major PRA studies come to the conclusion that the contribution of RPV failure to nuclear power plant risk is negligible (probability below 10^{-7}, or at most 10^{-6}, per vessel year).

9.2 SUMMARY OF MAIN PROBLEMS

Attempts to validate PRA estimates for RPV failure rates have to account for the severe uncertainties and oversimplifications of transient and load profiles, particularly in the case of emergency and fault conditions; for the material data base uncertainties including material degradation due to thermomechanical ageing and radiation embrittlement; for the inspection and testing deficiencies; and for the limited knowledge on stable crack growth and crack arrest mechanisms.

Intuitively, this situation would forbid any quantitative prediction of the failure rate.

If quantification is attempted nevertheless, the conservative approach aimed at highest safety would have to rely on the most conservative estimates.

In the context of extrapolating RPV failure rates from conventional vessel failure data, a conservative approach would have to consider disruptive and potentially disruptive failures. Marshall (1982, p. 103) estimates the probability of potentially disruptive failure occuring in non-nuclear class 1 vessels at 10^{-3} to 10^{-4} per vessel year. The discussion in 9.3.1.2 illustrates that no convincing reasons can establish an

additional safety margin for a nuclear vessel, compared to non-nuclear vessels.

Theoretical fracture mechanics calculations of the potential failure rate (9.3.2.1-2) have shown an extreme sensitivity to variations in the essential assumptions which are beset with high uncertainties - the resulting failure rates differ by several orders of magnitude. The largest contribution to the failure rate will result from pressurized shock events, amounting to 10^{-4} to 10^{-6} per vessel year.

Keeping in mind that a considerable number of older RPVs (which could not meet today's licensing requirements!) already has reached an operating time longer than the mean lifetime of conventional vessels (Boesebeck, 1975), a responsible analysis must insist on using pessimistic limits as the basis for safety decisions.

Thus, a failure rate below about 10^{-5} per vessel year cannot be accepted as conservative evaluation of the knowledge on the structural integrity of RPVs. In spite of claims to the contrary found in most PRAs, pressure vessel failure therefore has to be regarded as a relevant contributor to risk and the danger of RPV failure with fragmentation as possible cause for containment failure cannot be neglected.

9.3 BACKGROUND

9.3.1 RPV Failure Rate Estimation from Non-nuclear Vessel Data

9.3.1.1 Failure Rate of Non-nuclear Vessels

US, UK and German studies on conventional vessel failure distinguish the following categories:

(a) disruptive failures: rupture by failure of the shell, head, nozzles of bolting, accompanied by the rapid release of a large volume of the pressurized fluid.

(b) non-disruptive failures:
-- potentially disruptive failures: a condition of crack growth that could have led to disruptive failure if it had not been repaired;
-- non-critical vessel failures: local degradation of the vessel boundary with or without leakage, not reaching critical crack size or disruptive failure conditions (Marshall, 1982, p.102; DRS A 3, 1980, p. 27).

Table 9.1 shows the results of several studies (Marshall, 1982).

The German study group (RS 217, 1978) did not include all the registered failure events in the analysis. Only failures due to defects from design, construction and fabrication were selected, failures due to operational errors or non-specified operational conditions were eliminated. On the other hand, the

statistical base of the vessel population includes a wide range of design pressure, vessel size, and vessel function (Öko, 1983, p 89). Thus the reference value of this data base seems to be rather questionable with respect to the extrapolation to nuclear vessels.

Both selection criteria used in the German statistical failure rate determination from non-nuclear vessels (regarding the reference vessel population, and the failures which were taken into account) show the tendency to reduce the resulting failure rate. This procedure obviously is not conservative.

The UK survey (Smith and Warwick) and the UK statistics restricted to steam drums and steam receivers (better similarity to RPVs) yield higher failure rates than the German study.

It has to be noted that the distinction between disruptive and non-disruptive failures is questionable. Potentially disruptive failures would necessitate a major repair or replacement of the vessel which is not possible in case of nuclear vessels. Thus potentially disruptive failures should be counted to the disruptive failures rather than to the non-disruptive failures.

From the number of vessels and vessel service years, a mean vessel lifetime can be determined (last column in table 9.1). For all studies quoted, this mean lifetime is $\leq$ 20 years. The projected lifetime of a nuclear vessel, however, is 40 years. Thus, the temporal limit of the statistical pressure vessel data is not adequate for extrapolations to RPVs.

Fundamental doubts on the significance of the procedures used were expressed by Marshall (1982, p. 103): "The Study Group believes that there is no satisfactory way of interpreting the data on potential failure rates for conventional vessels to give a useful estimate of the possible catastrophic failure rate of LWR vessels".

9.3.1.2 Extrapolations from Failure Rates of Conventional Vessels to Failure Rates of RPVs

Based on conventional pressure vessel failure rates, the FRA estimates for RPV failure rates due to vessel rupture for PWRs are as follows:

Surry (WASH-1400, 1975, p. 63)	10^{-7} per vessel year
Biblis B (DRS A 3, 1980, p. 33)	10^{-7} per vessel year
Zion (ACSNI, 1982, p. 84)	10^{-7} per vessel year
Sizewell B (ACSNI, 1982, p. 33)	$\leq 10^{-6}$ per vessel year
Oconee 3 (NSAC, 1984)	$1,1 \times 10^{-6}$ per vessel year

(In Phase B of the German Risk Study, the estimate given in Phase A was confirmed (DRS B, 1989).)

The reasons for assuming a lower failure rate for RPVs compared to conventional vessels are the following (ACSNI, 1982, p. 33):

- more detailed stress analysis for operational transients
- higher specifications of materials
- better toughness of materials
- stringent quality control
- multiple independent and experimentally validated ultrasonic testing of welds
- repeated non-destructive testing in service
- monitoring of long-term behaviour of materials by surveillance of samples

The German Risk Study (DRS A 3, 1980, p. 28/29) claims higher quality standards which characterize the concept of "fundamental safety" (Basissicherheit; Kußmaul, 1978):

- complete load assessment for all realistic operational states and emergency events, including low-frequency, extreme transients
- complete stress analysis accounting for the loads mentioned
- optimum construction
- purity of the materials
- toughness of the materials
- easy workability of the materials
- control of the welding practice
- control of heat treatments
- multiple independent ultrasonic tests of welds after heat treatment and hydrotest
- repeated non-destructive testing in service
- monitoring long-term behaviour of material by surveillance programs

The construction of any pressure vessel is regulated by the ASME Code or similar national regulations (e.g., the AD-Regelwerk and Dampfkesselverordnung in the F.R.G.). Nuclear vessels differ from conventional vessels in size, wall thickness, the need for large attachments (cooling circuit nozzles) and nozzle arrays (control rod insertion), higher thermal and pressure transients, and the hazard of radiation embrittlement.

The extreme requirements on vessel design could not be achieved by the conventional Code regulations; more stringent specifications for materials, stress analysis and fabrication procedures, and in-service inspection had to be formulated in order to permit these nuclear "monsters" to be built.

Keeping this in mind, it is not valid to claim that those additional specifications, which take into account the special problems of nuclear pressure vessels, can lead to a reduction of the failure rate by two orders of magnitude. The authors of ACSNI (1982, p. 34) remark that the mentioned "favorable factors are offset by (i) a different environment including the effects of irradiation though the latter can be minimized by suitable choice of materials, (ii) the fact that reactor vessel walls are much thicker than walls of typical steam drums and receivers, (iii) the expectation that transient stresses will be more severe for RPVs and (iv) a restricted ability for continuous observation in service. The balance between

favorable and adverse effects is impossible to quantify in the absence of sufficient data." They conclude: "We believe, however, that the balance will be favorable and we judge, although we cannot prove ist, that the failure rate of the RPVs considered in this study is likely to be less than 10^{-6} per reactor year."

The PRA studies mentioned cover only PWR vessels. The common argumen' that BWR vessels have to withstand a pressure of 70 bar only, compared to 150 bar of PWR vessels, implying a higher safety margin, is not correct, since the wall thickness of BWR vessels is reduced according to the lower design pressure. On the other hand, BWR vessels are usually larger and therefore made of rolled plates with longitudinal welds instead of forged rings. There is no doubt that such a construction represents reduced structural integrity.

9.3.1.2.1 Load and Stress Analysis

Design pressures and temperature transients considered for an RPV have to cover the normal operating, test, incident, emergency and fault conditions, including common mode failures and human error induced accidents (a faultless operation of the emergency core cooling system in case of LOCA and a defect-free vessel are usually assumed). The stress analysis calculated on this basis has to be consistent with the material properties. The ASME Code section III requires that no unacceptable plastic deformation should develop in any part of the vessel (when subjected to the load conditions assumed) which could lead to ductile fracture; this has to include the case of repeated cyclic loads (fatigue analysis).

The Codes distinguish three categories of stress levels:
- primary stresses: bending and membrane stresses, not self-limiting.
- secondary stresses: self-limiting, can be relieved by yielding, e.g., thermal stresses and bending stresses at structural discontinuities.
- peak stresses: additive to the primary and secondary stresses, arising from local discontinuities, stress concentrations, etc.

Primary stresses are not allowed to exceed the design stress level S_m. Secondary stresses must not exceed $3S_m$.

The design stress level S_m is limited according to U.S. Code regulations (ASME Code III) to 1/3 of the tensile strength at room temperature (RT) or operating temperature and to 1/1.5 of the yield strength at RT and operating temperature of the vessel steel. The German regulations (KTA-3201.2, 1984, 7.7.3.4.) prescribe a lower safety margin of 2,7 (instead of 3) for the tensile strength at operating temperature.

It is evident that the safety factor of 3 for the tensile strength is an absolute necessity since secondary stresses are permitted up to $3S_m$, and otherwise secondary stresses could

exceed the tensile strength of the material at structural discontinuities (nozzle attachments, etc.).

The ASME Code Section I and VIII for conventional vessels requires no detailed stress analysis; the vessel thickness is determined according to the design pressure. The limiting stress level S_m prescribed by the Code is 1/1,6 of the yield strength or 1/4 of the tensile strength at operating temperature.

Nuclear vessels with an adequate wall thickness could not be designed to meet the non-nuclear Code requirements for the projected pressure range and the given low-alloy steel tensile properties. Additional prescriptions for stress analysis, particularly for the important parts of the vessel where secondary stresses might peak up to 3 S_m, had to compensate for the reduction of the safety factors for tensile strength and yield strength and the problems due to the complicated vessel geometry (nozzles, flanges, upper and lower head welds, control rod and other instrument tube insertions, etc).

Some critical comments on selected points follow.

Load Conditions and Transients

The set of operational transients during the projected reactor vessel lifetime as specified by the manufacturing company is intended to cover normal operation as well as emergency situations. It must be doubted, however, that ALL possible situations of the complex system can be covered.

"However, the design transients may not be fully representative of situations where the reactor is under manual control or undergoing commissioning or testing. In addition there have been instances of vessels being exposed to transients other than the specified design transients. These include overpressurization when the vessel is cooled and more recently, rapid cooling of the vessel, whilst still pressurized ('overcooling transients')" (Marshall, 1982, p. 62).

Stress analysis

Stress analysis calculations for complicated structures can only be performed introducing considerable simplifications. This applies particularly to the nozzle attachment regions, the penetration arrays for control rod insertion and the welds between the cylindrical shell and the upper and lower head. Welds are not treated as discontinuities. Welding-induced residual stresses and possible embrittlement of the heat affected zone (HAZ) are neglected as well as any kind of defects (cracks, crack-like flaws like slag inclusions, segregates, etc).

In reality, even specified welding materials and procedures cannot prevent the formation of defects in the welding material and the surrounding HAZ. Another problem is the existence of multiaxial stress distributions that are not covered by the

ASME Code regulations. This can result in an underestimation of vessel failure risk (Stahlberg, 1977, p. 283).

Finite element modelling is assuming increasing importance in the analysis of complex regions of the vessel structure (flange region, nozzle attachment, etc). These calculations were found to be very sensitive to the assumptions made (i.e., to structural simplifications employed) and to the detailed load conditions (Marshall, 1982, p. 64).

The uncertainties in the theoretical treatment of collective load assessment, stress analysis and defect state of the vessel would therefore require extended experimental investigations to establish a verification of the calculated stress profiles.

Experiences from German Reactor Vessels

-- The German Nuclear Code KTA-Regelwerk was published from 1979 onwards. The vessels built before that time were supposed to fulfill the ASME Code Section III requirements. Actually, the safety factor of the limiting stress level S_m for tensile strength was not 3, but only 2,7 for the RPVs in Stade, Mühlheim-Kärlich and Wyhl (TÜV, 1975b, p. 1/18). Later, the KTA regulations explicitly permitted this lower safety margin.

-- In the German Risk Study, Phase A, the authors claim that RPVs are constructed optimally to account for stress profiles. The minimization of weld seams with the aim of a more integrated construction has to be attempted to enhance structural integrity of the vessels. A reduction to 70 % for BWR vessels and 25 % for PWR vessels compared to conventional designs was expected (Onodera, 1977). Keeping in mind that most of the RPVs in service will belong to the "conventional design", no credits can be taken for optimum construction.

-- For the AEG BWR vessel design which was also used by KWU for the series '69 (Brunsbüttel, Philippsburg, Zwentendorf/Austria, Krümmel, Ohu) and '72 (Gundremmingen B, C), the circumferential weld between the cylindrical shell flange and the flat dish-type lower head ("Tellerboden") is a contested design feature. Secondary stresses in the weld region reach the value of yield strength at operating temperature (see fig. 9.1).

The KTA-Regelwerk 3201.2 (latest version from 1984) contains no specifications on this construction type (p. 62 merely states: 7. "Tellerböden" - in preparation). Kußmaul admitted that this is not an optimal design (Profil, 1978, p. 21).

-- Because of court resolutions, a wide range of fabrication details are known on the Krümmel (KKK) reactor vessel. The cylindrical shell is made of 7 rings with two longitudinal welds on each ring (longitudinal welds experience twice the load of circumferential welds, fig. 9.2).

The specified values of tensile strength at RT as well as yield strength at RT and operating temperature were not reached for 1/4 thickness and mid-thickness positions in more than 70 % of the plates for the vessel shell (deviations up to 15 %). One

plate did not have the specified thickness. The stress analysis was provided by KWU at a time when the vessel was almost completed (TUV, 1975a).

9.3.1.2.2 Purity of the Material

The ASME Code permits a wide range of major alloying elements for the commercial RPV steels SA-508 and SA-533B (comparable German steels: 22NiMoCr37 and 20MnMoNi55). The vessel producers usually define compositions more restrictively in order to get improved mechanical properties.

Very late, considerations started whether restrictions of some minor impurities could help to avoid temper embrittlement (P, As, Sb, Sn), to improve upper shelf toughness (S), to limit carbide formation and to reduce neutron irradiation embrittlement (Cu) (Marshall, 1982, p. 13/14).

Segregation effects during solidification cannot be avoided; the segregates change transformation characteristics, reduce the fracture toughness and enhance the incidence of welding defects.

Impurity segregation in the plates for the KKK vessel led to the problem of finding rather pure areas for the nozzle attachments. It was necessary to change the projected ring sequence in order to ensure better weldability, but no completely segregation-free areas were found (TÜV, 1974).

9.3.1.2.3 Workability of the Steel

Beside the fact that welding defects in the weld metal and the HAZ cannot be avoided, the low-alloy steels have shown a high susceptiblity to solidification cracking, reheat cracking and Hydrogen-induced cracking (Marshall, 1982, p. 17). Kußmaul observed a high susceptibility to stress relief cracking and relaxation embrittlement for the German RPV steel 22NiMoCr37 (Kußmaul, 1976). Based on these observations a research program was started to investigate cracking in samples from German RPVs and steam generators and to study possible effects of relaxation embrittlement in the coarse grained HAZ (SR 10, 1976). About 50 % of the samples showed either solidification or stress relief cracking, 30 % showed both.

Uncertainties concerning possible interactions of fabrication-induced cracks with residual stresses as well as the uncertainty whether simulation experiments allow statements on structural components enlarge the problem. While a complete understanding of the controlling factors for hot and reheat cracking, particularly in the HAZ, is still not possible, it seems clear that a controlled heat input during welding to prevent grain growth and a restriction of carbide-dispersion-forming elements (V, Zr, Nb) should be achieved. Impurity segregations obviously also enhance the Hydrogen-induced cracking (Marshall, 1982, p. 19).

A further welding problem is associated with the austenitic cladding at the inside of the ferritic pressure vessel. Marshall (1982, p. 21) reports under-clad cracking experience in SA-508 after 1970. Under-clad cracking observations in 22NiMoCr37 were compiled by the Öko-Institut (Öko, 1983, Vol.II, p. 99).

Marked under-clad cracking was observed in 22NiMoCr37 and 20MnMoNi55 steam generators. Strong correlations with impurity segregation were found (Czerjak, 1978).

Recent investigations on under-clad cracking in SA-508 class 2 forgings and 22NiMoCr37 (in the as-clad condition and after stress relief treatment) have confirmed that "cavitation and intergranular fissuring can occur in the presence or absence of intergranular particles (Lopez, 1987).

Stress relief tempering was usually performed at 550° C until it was found that this is the temperature range of high cracking susceptibility of 22NiMoCr37 (Kußmaul, 1976, p. 220). Kußmaul admitted that stress relief treatment above 600° C cannot avoid cracking while the critical temperature range is passed through.

9.3.1.2.4 Stringent Quality Control (Welding, Heat Treatment)

Beside the unavoidable occurence of cracking due to welding and heat treatments (as described in 9.3.1.2.3), the quality of the welds in pressure vessel steels depends on the skill and reliability of welders and on careful inspection procedures.

From KKK vessel fabrication reports it is known that the plates had been welded without the required prewelding inspection with non-destructive ultrasonic (US) testing (TÜV, 1974, p. 2). Weld defects had been found in high quality class components for the Barsebäck 2 reactor pressure vessel during the pre-service test AFTER the final manufacturing control (slag inclusions and lack of fusion in nozzle/vessel welds which had to be ground). Studies on the control methods during the manufacturing phase have shown that these weld defects have a low detection probability (SKI-ASAR, 1985, p. 43).

French programs were forced to use automatic welding procedures, since "experience has shown that in case of welding operations that are difficult to perform, because of the nature of the electrode, accessibility conditions and environmental problems, there is a need to minimize as much as possible the human factor for it increases the risk of creating defects" (Buchalet, 1979).

9.3.1.2.5 Toughness of the Material

The strength of the materials must be sufficient to guarantee structural integrity under loads up to design stress levels; the ductility of the material must accomodate the strains. With increasing temperature ferritic steels change from the low-

temperature brittle behaviour to high-temperatur ductility, characterized by the so-called upper shelf toughness. The ductile-brittle transition temperature (DBTT) or nil-ductility-transition temperature (T_{NDT}) can be determined by Pellini drop weight tests or Charpy impact tests.

The ASME Code specifies a minimum Charpy impact energy value of 68 Joule at temperatures above T_{NDT} + 33°. This specification was adopted in the German RSK-Guidelines. All operational conditions of the RPV are restricted to the upper shelf range.

With respect to these requirements, the main problem area is not the base metal but the weld regions. The upper shelf toughness of the weld metal can usually be matched quite well to the base metal properties; the critical area is the neighboring HAZ (Dahl, 1986, p. 31.1).

Fracture Mechanics

The theoretical description of the fracture properties, particularly the calculation of critical defect sizes and crack propagation behaviour, is performed by fracture mechanics. Pressure vessel steels can fail by brittle (non-ductile) fracture - the unstable crack propagation results in spontaneous rupture. This behaviour can be described using linear elastic fracture mechanics (LEFM), assuming relatively small plastic zones around the crack tip. Spontaneous fracture will occur as soon as the stress distribution around the crack exceeds a critical value, the fracture toughness K_{Ic}, which is a characteristic material property. Critical crack sizes can be calculated from measured K_{Ic} values.

Since most vessel conditions are supposed to be in the upper shelf regime where LEFM is no more valid, the relevant crack behaviour has to be described by elasto-plastic theories. Several methods (J-integral, crack-opening-displacement (COD), R6-method) were developed to analyze the critical crack behaviour in case of extended plastic deformation with the possibility of ductile failure.

Fracture mechanics calculations assume an isotropic material and neglect microstructural features (grain boundaries, dislocations, precipitates, segregations, inclusions, voids etc) and their interactions with the postulated crack, which itself has strictly defined geometric properties. This is certainly an oversimplification. In the ductile regime the crack will begin to grow at a certain stress intensity or deformation (characterized by K_{Ic} or by the crack initiation value J_i, as defined in elasto-plastic (J-integral) theory. Actually, in ductile regimes it is impossible to determine valid K_{Ic}-values, and J_i is not precisely defined); then it is supposed to run into regions with higher toughness where it will be stopped before reaching a critical size (the corresponding stress intensity for crack arrest is K_{Ia}).

There are no standard methods for the determination of J_i and K_{Ia}. The ASME Code recommends a reference fracture toughness curve (K_{IR} vs. T) based on lower bound K_{Ic} and K_{Ia} values. The

validity of this procedure is still in doubt because of sample size effects (Roos, 1986b, p. 34; Kußmaul, 1986, p. 25.56) and also ingot and section size effects (segregate distribution, grain size distribution) on toughness (Marshall, 1982, p. 29).

The ductile-brittle transition temperature also seems to depend on sample thickness, i.e. the transition might occur at higher temperatures in thicker sections. Dynamical or quasi-static conditions presumably also shift the DBTT to elevated temperatures (Kußmaul, 1986, p. 25.6). Experimental investigations have shown a saturation in the K_{Ic} and K_{Ia} versus T curves above DBTT corresponding to the upper shelf toughness (Roos, 1986b, p. 34.7), while the ASME code reference curves do not include saturation at all. A further problem arises from the fact that very different upper shelf toughness values were observed for plate materials and forgings (Marshall, 1982, p. 83).

ASME Code and KTA-Regelwerk also neglect possible toughness differences between base metal, weld metal and HAZ. Variations of additive composition can influence the weld metal toughness; the HAZ, however, remains critical.

Investigations on the failure behaviour of wide plates with welded joints using fracture mechanics calculations have shown both considerable underestimation as well as occasional overestimation of the failure loads compared to experimental results (Dahl, 1986, p. 31.15).

The unknown toughness properties of the HAZ and the uncertainties concerning residual stress distributions in the weld obviously do not allow reliable predictions of the fracture properties of wide plates. Such predictions are even more difficult for the complicated structures of real vessel components. Therefore the structural integrity of the vessel cannot be guaranteed by fracture mechanical simulations. It depends decisively on the actual fabrication quality and the reliability of fabrication and in-service testing.

"Whilst in general we are confident that welds could be comparable with base materials, quality control procedures will have to be specified carefully to avoid the use of lower toughness welds" (Marshall, 1982, p. 34).

Elasto-plastic fracture mechanical calculations are performed for reactor vessels in the UK; the German procedure is restricted to LEFM simulations (ACSNI, 1982, p. 73).

In-service degradation of the toughness properties is expected due to thermal ageing, strain ageing and neutron irradiation embrittlement.

Thermal Ageing caused by carbide precipitation and grain boundary segregation effects, especially in the coarse-grained HAZ regions, can increase the ductile-brittle transition temperature (DBTT). The authors of the British study (ACSNI, 1982, p. 32) assume that a 30°-shift might occur.

Strain Ageing and dynamic strain ageing as a result of plastic strain interactions with impurities in the material will predominantly take place in vessel parts with high stress levels or stress concentrations, such as the inner nozzle welds. A shift of the DBTT to elevated temperatures and a reduction of the upper shelf toughness are the consequences. The ACSNI authors estimate the possible DBTT shift to be 10-20°.

Increasing amounts of strain and thermal ageing reduce the fracture toughness successively (Stahlberg, 1977, p. 273). Strain ageing embrittlement is a very dangerous effect since it occurs in those parts that always experience higher loads; therefore failure could be initiated below the testing stress level.

Thermal fatigue induced cracking was found at Barsebäck 1 (1976) in the spargers for the distribution of feed water in the RPV (SKI-ASAR, 1985, p. 45). In Brunswick-1 cracks were found that begin in the pump inlet nozzle welds and propagated through the weld material into the low-alloy steel of the reactor vessel (NucWeek, 1989a, p.6). A similar problem was observed at Brunswick-2 in 1988.

Superposition of the warm prestress effect (warm prestress precluded crack extension) does not necessarily yield a better ductility (Marshall, 1982, p. 37).

Strain ageing effects are strongly correlated with material purity. Recent investigations have shown that inhomogeneities such as carbides and inclusions in the weld metal are closely related to cleavage initiation (Irwin, 1986, p. 19-3).

Neutron Irradiation Effects in pressure vessel steels cause an increase of yield strength, ultimate tensile strength and hardness, and reduced ductility, characterized by a shift of the DBTT to elevated temperatures and a drop of the upper shelf energy. The DBTT shift increases with the neutron fluence. The effect is enhanced by increasing copper content. Other impurities such as Phosphorus, Arsenic, Antimony and Tin seem to promote the embrittlement. Recent atom-probe field ion microscopic results from irradiated vessel steel welds indicate the existence of radiation-induced Cu-rich precipitates and Phosphorus-enriched Mo carbides and Phosphorus segregation at the grain boundaries (Miller, 1987).

For design purposes, the trend curves of the U.S. Nuclear Regulatory Commission Reg. Guide 1.99 Rev 1/1977 (NRC, 1977b) describe the influence of the Cu content of the DBTT-shift versus neutron fluence (fig. 9.3). The deteriorating effect of the copper content on the radiation resistance of vessel steels was not known when the first RPVs were fabricated. Later on, Cu-content was restricted to levels below 0,10 %. Therefore radiation induced embrittlement has to be suspected for all older pressure vessels, and particularly for PWR vessels because of the smaller water gap between vessel wall and core. Beltline welds suffer the highest neutron flux and therefore are of main concern with respect to embrittlement. Early German

PWR vessel welds are known to contain up to 0,28 % Cu. As a result of the alarming observations of Cu enhanced radiation embrittlement, the projected end-of-life fluence was reduced by the use of dummy rods in the outer core areas (GÖK, 1987). A limiting neutron fluence of 1E19 n/cm^2 was prescribed be the RSK-Guidelines 1981, but the facts indicate that this limit cannot be met by German PWR vessels.

Examples of Radiation Embrittlement in Specific RPVs

-- The KKS (Stade) vessel has passed the RSK fluence limit at the end of 1986. A DBTT shift of more than 120° has to be assumed from surveillance experiments, associated with a significant drop of the upper shelf energy. Only few data exist on radiation effects in the HAZ - the deterioration there might be even worse than in the weld metal (GÖK, 1987).

The RSK-Guidelines restrict the operation of an RPV to temperature-pressure ranges where the material properties are in the ductile regime (temperatures above DBTT + 33°, upper shelf energy 68 J). It has to be suspected that those requirements are not fulfilled for the beltline weld at KKS.

-- Soviet VVER-440 pressure vessels: In the pressure vessels of the Soviet-built finnish power plants Loviisa 1 and 2, embrittlement proceeded faster than expected due to a high Cu and P content, particularly in the weld. Older VVER-440 vessels with radiation-induced embrittlement have recently been annealed at 430° C to recover the original toughness properties: Novovoronezh-3 (1987), Armenskaya (1988), Greifswald/GDR (1988) (NucWeek, 1989a, p. 5). These annealing procedures might be of questionable success since recent investigations have shown that "the sensitivity to re-irradiation embrittlement is high compared to material that received the same fluence but which has not been anealed" (Hawthorne, 1988).

-- Serious radiation-induced embrittlement was also reported for Japanese RPVs (Anderson, 1986, p. J7).

-- Older US PWR vessels contain $\geq$ 0,15 wt% Cu. Cu-precipitation dominated embrittlement is is assumed (Darlaston, 1986, p.26.12).

9.3.1.2.6 Non-destructive In-service Testing

Fracture mechanics methods assume a defect-free material for the calculation of the critical size of a geometrically well-defined crack. They neglect all possible interactions of this singular crack with other possible microstructural features. Considering the simplifications in stress and loading assessment, the uncertainties of the material properties data base, possible synergisms etc, the safety of an RPV cannot be guaranteed by theoretical simulations.

The leak-before break criterion might be valid for certain parts of the structure under special transient conditions but

cannot be relied upon with respect to vessel integrity. The essential contribution to the safety of an RPV will therefore come from continuous testing procedures during service.

The ASME Code (and KTA 3201.4) prescribes a pre-service cold hydrotest (that should be repeated several times during the service life) at 1,25 times the design pressure (KTA: 1,3 times the design pressure) at a temperature above DBTT to avoid brittle fracture conditions. Marshall (1982, p. 77) does not believe that the hydrotest can "establish the absence of unacceptable crack sizes". He suspects "that it may cause some damage to lesser defects not large enough to cause failure". According to Marshall it is also questionable that hot hydrotests "provide an assurance of vessel integrity".

Radiography is a reliable tool for conventional weld quality control, but it is not applicable for most parts of an RPV. Contrast sharpness and resolution are not sufficient due to the scattering in the thick wall. The size of defects in the important depth direction cannot be measured.

Visual inspection with optical methods is applied to the inner vessel wall with the aim to discover surface cracks and environmental damage of the cladding surface. There is no other way to check the surface of the vessel for corrosive attacks.

Stress corrosion and corrosion fatigue are severe problems for the ferritic steel as soon as the austenitic cladding is damaged. Stress corrosion cracking of the clad material could occur in oxygenated water with Chlorine contamination. Experiments at the inner nozzle weld cladding have shown that the ASME III design curve (stress corrosion) is not conservative for the cladding material used in German pressure vessels (Jansky, 1985, p. 32.26).

Fatigue cracking of the clad can develop at the inner nozzle weld corner due to the high stress concentrations. The detection of clad cracking would be of foremost importance. However, it is difficult to demonstrate the detectability of surface defects by optical methods (SKI-ASAR, 1985, p. 49).

A major problem of visual inspection during service is the impossibility of access to many problem areas (the vessel bottom with control rod insertion nozzles in BWRs, coolant nozzle welds, etc) and the radiation hazards for the personnel.

Ultrasonic non-destructive testing methods will therefore constitute the central part of testing procedures. In order to achieve an effective assessment, a complete overall examination of the vessel before installation ("Nullatlas") and periodically repeated testing procedures would be desirable. In reality, the complete pre-service testing is described in KTA 3204.4, leaving open the possibility to reduce the amount of testing in the base metal and relying on similar fabrication testing. Only the possibility of testing has to be guaranteed. In-service testing covers only welds. Several critical parts of the vessel are even not accessible for ultrasonic testing (bottom nozzle areas in BWRs, parts of the nozzle welds).

Ultrasonic testing during fabrication and pre-service inspection used to be performed manually with contact probes. In-service testing requires remotely operated equipment to reduce radiation exposure to the operator. Automatic techniques are obtaining increasing importance.

Ultrasonic examination from the inside and the outside of the vessel would be desirable, but is commonly not performed. Manual examinations allow the operator to notice clusters of small defects with sizes below the specified critical value, which nevertheless can be critical if they are very close together. Automatic systems with the threshold registration level adjusted to the specified critical value cannot detect such defect agglomerations.

PISC (plate inspection steering committee) I program results have shown "considerably worse effectiveness in detecting and sentencing sets of defects compared with single defects of similar overall size" (Marshall, 1982, p. 86). Marshall estimates the effectiveness of ultrasonic testing to 50 % probability of detecting a defect size of 6 mm and 95 % probability of detecting a defect size of 25 mm.

Ultrasonic in-service testing does not permit an assured localization of cracks, and measurement of their size, extension, depth position and configuration. The transformation of registered signals into a defect topography is not possible (Stahlberg, 1977, p. 276).

Details of existing defects in the vessel that would be required for fracture mechanical failure assessment cannot be derived with sufficient accuracy from ultrasonic testing results. This did not change with improved measuring techniques: Mundry (1982, p. 112) reports that the nature, the actual size and the orientation of the detected defects cannot be determined from ultrasonic measurements. Practical experience with ultrasonic testing for the quality control of steel pressure vessels has shown that in spite of correct testing performance according to the Code regulations, the quality requirements were not always met (Werden, 1983, p. 179).

Marshall (1982, p. 94) reports that "some theoretical studies have highlighted limitations of present inspection procedures, a general conclusion being that current threshold recording levels should be reduced considerably to ensure reliable detection of planar defects".

Further problems for the ultrasonic detection of near-surface defects arise form the presence of the austenitic cladding; the influencing factors are still not understood.

Due to these problems there is no reliable possibility to ensure complete adhesion of the cladding to the ferritic steel of the vessel body. Adhesion deficiencies can facilitate fatigue cracking, particularly in areas exposed to stress

concentrations, with the subsequent danger of stress corrosion of the underlying ferritic material.

Technical problems of the ultrasonic testing originate from ultrasound coupling difficulties for contact probes and scanning difficulties in case of supplementary automation, including calibration and comparability problems.

9.3.1.2.7 Long-term Monitoring by Surveillance Programs

ASME Code (and KTA) regulations demand in-service irradiation of steel samples in positions between the core and the vessel wall so that the elevated neutron fluence at the sampling position will simulate vessel conditions in the future (due to the higher neutron fluence density at the irradiation point) (ASTM E 185, KTA 3203).

The long-term monitoring is based on the experimental analysis of these samples according to a specified temporal schedule, simulating the lifetime of the vessel. Charpy impact tests and fracture mechanical evaluations are to provide predictions of the future irradiation affected toughness properties of the vessel steel. The data on DBTT-shift and the fracture toughness reference curve K_{IR} for different neutron fluences are supposed to verify the trend curves for the linear elastic regime. Results on the Charpy upper shelf energy will be used to assess the hazards of ductile failure for future irradiation conditions of the vessel.

Several limitations, however, should be kept in mind:

-- The irradiation of the surveillance samples occurs without applying stress; whereas the vessel material experiences the irradiation under different load conditions (with spatial and temporal variation).

-- The thermomechanical history of the surveillance samples will certainly differ from the real vessel material, particularly in the welds.

-- The neutron fluence density at the surveillance samples is considerably higher than at the vessel surface. Flux density effects with interfering temperature effects on radiation-induced defects could result in significant differences between the samples and the real state of the exposed vessel.

-- Surveillance samples need to be rather small, which is limiting the extrapolation of the fracture mechanical evaluation to the vessel properties. The crack initiation and the crack resistance curve depend on specimen size and geometry.

Recent experimental studies on the validity of the surveillance programs were performed by the MPA Stuttgart using trepans from the RPV of the shut-down Gundremmingen-A BWR (252 MWe, 10 years of operation, total fluence at the vessel wall about 2,4E18 n/cm^2). The results were compared with existing

surveillance samples and additional irradiated archive material.

It turned out that "on the basis of the chemical composition (Cu and P) and the calculated local fluence the material behaviour cannot be predicted conservatively by the trend curves of the Reg.Guide 1.99, neither with respect to the transition shift, nor the drop in the upper shelf" (Kußmaul, 1987).

The irradiation effects on the archive material (identical chemical composition) exposed to the threefold neutron fluence were smaller than those in the vessel trepans. Strong orientation effects were found.

These results indicate that the sensitivity to radiation-induced embrittlement increases with decreasing neutron flux density and that orientational effects due to fabrication-induced anisotropy and/or due to applied stress distributions during irradiation exposure cannot be neglected.

Recent US investigations on ASTM-A302 B plates have confirmed the tendency of these results for high Cu content welds: "The intermediate fluence rate appears to be more damaging to the weld than the high fluence rate" (Hawthorne, 1988).

If these experimental results prove to be valid, the surveillance program would collapse completely as a consequence, because the real embrittlement of the vessel would exceed by far the simulation results from surveillance monitoring. And there would be no possibility to estimate the actual toughness properties of an in-service vessel due to the lack of knowledge on the dose rate dependence of radiation-induced embrittlement.

9.3.1.2.8 RPV Failure vs. Non-nuclear Vessel Failure - Conclusions

In 9.3.1.2.2 - 9.3.1.2.7, it was attempted to discuss the set of quality-improving factors that are supposed to substantiate the reduction of the assumed nuclear vessel failure rate by a factor of 100, compared to the conventional vessel failure rate. The real manufacturing and inspection experience as well as recently published research results were taken into account.

-- Compared to high-quality conventional vessels, no extra safety margin in the design of nuclear vessels can be assumed, on the contrary: Additional stress analysis and fabrication inspection appear to be necessary to compensate for the reduced safety factors.

-- Idealizations and simplifications in stress analysis calculations and the uncertainties concerning the completeness of design transient assumptions combined with the complicated geometrical structure of a nuclear vessel and its extreme operational conditions cannot support a reduced failure probability.

-- The majority of existing reactor vessels is far from the a[illegible]ired integral vessel layout with reduced weld lengths. In p[illegible]icular, the German BWR vessels with longitudinal welds and a [illegible]lat dish-type bottom cannot satisfy the claimed "optimum design" quality.

-- The purity of the material is not a convincing quality characteristic. The discussion as to which element should be restricted to what level to improve toughness, radiation resistance, weldability, corrosion resistance etc. continues. Many of the existing vessels were built at a time when the influence of some alloying elements or impurities on specific properties were not yet known.

-- In practice, unavoidable segregations as well as manufacturing insufficiencies have raised problems in meeting the minimum purity specifications. In very few cases details are known concerning fabrication events: virtually unacceptable defects were left unrepaired in order to avoid additional repair-induced deterioration of the component.

-- The low-alloy steels (SA-508, 22NoMoCr37) are susceptible to solidification cracking, stress relief cracking, and Hydrogen-induced cracking. Significant underclad cracking was observed.

-- Only few factual reports are known about the "human factor" concerning welding defects, heat treatment mistakes, etc. The known events involving manufacturing problems and detection deficiencies show that optimum quality cannot be guaranteed.

-- Fracture mechanics concepts c[illegible]rtainly allow the interpretation of an extended variety of observed material behaviour. Nevertheless the fundamental simplifications, together with the limitations of the specimen-size-dependent experimental data base cannot yet yield reliable results on the structural integrity of the vessel.

-- Stable growth of a postulated crack depends on the upper shelf energy, the existing constraints in the component and the course of the transient (pressurized thermal shock is supposed to be the most severe transient).

-- The upper shelf energy is a time-dependent material state, degrading during operation due to ageing, strain ageing, radiation embrittlement and possible interfering effects.

-- Crack arrest curves for shallow cracks that could initiate brittle failure could not be demonstrated to constitute reliable predictions for the behaviour of samples. The situation in the real component is significantly more complicated involving different material states due to fabrication (welds, HAZ) and operational degradation (thermomechanical ageing, radiation effects) as well as various stress profiles due to the geometrical features in the vessel, and the postulated transient.

-- Thermal ageing, strain ageing and radiation effects cause a considerable shift of the DBTT to elevated temperatures and a drop of the upper shelf energy which can differ in different parts of the vessel (welds, HAZ, inner nozzle weld corners).

-- Further degradation of the vessel integrity can originate from stress corrosion processes if clad defects (i.e., fatigue cracking in areas of high stress concentration) enable water contact with the ferritic steel. Stress corrosion of the cladding material cannot be excluded either.

-- For the non-destructive testing methods, the required effectiveness in detecting critical defects with sufficient certainty could not be confirmed.

-- The approach of long-term monitoring of the RPV material state based on surveillance programs must be regarded as entirely invalid if the recent results on enhanced radiation embrittlement at low flux densities are verified.

In view of these problems concerning design, fabrication, testing and operation, it is not appropriate to assume that the structural integrity of reactor pressure vessels is better than that of conventional vessels by a factor of 100. Therefore a failure rate of 10^{-7} per vessel year cannot be derived from "better quality".

The Öko-Institut (Öko, 1983, Vol.II, p. 121) concluded that there are no evident reasons that could justify the assumption of an RPV failure rate of 10^{-7} per vessel year as opposed to the failure rate of 10^{-5} per vessel year for conventional vessels. Therefore, a failure rate for reactor pressure vessels in the range of 10^{-6} - 10^{-4} per vessel year is assumed.

9.3.2 Theoretical RPV Failure Probability Calculations

Marshall (1982, p. 104 ff)

Marshall reviews the status of the failure rate calculations based on fracture mechanics simulations. Simplifications and statistical uncertainties limit the validity of the procedure. The problems associated with the assumptions on crack size distribution, material state and transient stresses can be summarized as follows (according to Marshall):

-- The knowledge on crack distribution in the vessel is limited; the crack height distribution is estimated from assumptions on the manufacturing process and detection probabilities.

-- The variability of crack shapes, orientation etc. is reduced to the assumption of a single crack type with specific shape and orientation.

-- Fabrication-induced cracks are assumed to be proportional to the volume of the welds - there are considerable uncertainties concerning the size distribution.

-- Theoretical assumptions on the probability of not detecting defects, or underestimating detected defects differ significantly. Experimental studies (PISC) indicated an insufficient effectiveness of the commonly used procedures.

-- The basic laws and mechanisms of fatigue crack growth are still uncertain. The equation which is generally used "may not apply over the whole range".

-- Due to the lack of empirical information on frequency and magnitude of transients during normal operation and emergency conditions, the calculations have to rely on specified design transients.

It is assumed that the magnitude of transient stress is more important than transient frequency.

The calculated failure rates in the reviewed analyses amount to 10^{-8} - 10^{-6} per vessel year.

The failure probability is shown to be sensitive to the initial crack size distribution, to the location of the crack in the vessel, to the accuracy of the transient stress intensity profile, and the crack growth rate. The nozzle regions and the bottom head are supposed to be responsible for the largest contributions.

Marshall recommends: "Particular failure probabilities should not be taken too 'literally' at present because they are sensitive to factors which remain uncertain."

Battelle Calculations for the German Risk Study, Phase B (Geiß, 1985)

The fracture mechanical analysis of failure rates in case of a thermal shock event assumes linear elastic behaviour of the material and cooling with rotational symmetry; the austenitic cladding is neglected, no credits are taken for warm prestressing.

The calculation of the failure probability depends very strongly on the crack size distribution and the fracture toughness. The assumption concerning the crack size distribution is based on ultrasonic fabrication testing results and estimates on the detection efficiency. The authors emphasize that the quantification of crack size distributions contains "the largest uncertainties".

The simulation of radiation embrittlement is derived from a copper content of 0,11 - 0,08 wt% and an end-of-life neutron fluence of 5E18/cm² (which seems quite low for PWR vessels). Because of the lack of a systematic analysis of relevant transient stresses for German reactors, assumptions from US studies were used together with parametric variations of temperature and pressure.

Depending on the postulated course of the transient, the calculated failure probabilities vary by several orders of magnitude. Extreme transients can initiate instable crack growth for relatively small crack sizes.

The amount of the temperature drop during a postulated transient appears to have the largest effect on the failure rate. Depending on the duration of the temperature drop (0 - 100 min), conditional failure rates of 3E-6 - 2E-7 for a 100° drop, and 7E-4 to 2E-5 for a 250° drop were found (fig. 9.4).

The figure illustrates the influence of the different assumptions concerning crack distribution: For a 150° temperature drop, the predicted failure rates for pressurized thermal shock differ by four orders of magnitude.

Severe thermoshock transients with a temperature drop of at least 250° (small LOCA) have a design frequency of 5 times during reactor life (Marshall, 1982, table 4.1). The contribution to the failure rate of the vessel due to thermoshock events would therefore amount to 2,5E-6 - 9E-5 per vessel year (using the KWU-crack distribution results: 3E-6 - 4E-4 per vessel year).

Both analyses show that theoretical failure probability calculations are very sensitive to the assumptions on material state and transient profile. These assumptions are characterized by extreme uncertainties.

9.4 RPV FAILURE WITH SUBSEQUENT CONTAINMENT DAMAGE

This section provides the link between RPV failure considerations and level II of PRAs.

In PRAs, the risk of RPV failure with subsequent containment damage, based on an RPV failure rate of 10^{-7} per vessel year, is assumed to be not significant (WASH-1400, 1975, app. V-46). The possibility of pressure vessel rupture with fragment missiles propelled towards the containment causing severe damage is only discussed for steam explosions.

A more recent U.S. study also comes to the conclusion that containment failure will not occur after RPV failure (Simonen, 1986). This study, however, considers only large, dray PWR containments consisting of a concrete hull with a steel liner.

The German Risk Study (DRS A FB 3, 1980, p. 34) does not exclude the possibility of RPV rupture with expelled pieces but it is assumed that the ceiling plate and the crane will prevent the pieces to reach the containment. Early containment failure following RPV rupture is therefore excluded (for a large, dry PWR steel containment).

The authors of the study performed by the Öko-Institut (Öko, 1983, Vol.II, p. 121) estimate the failure rate for the reactor pressure vessel at 10^{-6} - 10^{-4} per vessel year. They also show possible trajectories for ejected fragments (fig. 9.5) that

could penetrate the containment. Accordingly, RPV failure with subsequent containment damage will contribute significantly to risk.

The authors of ACSNI (1982, p. 87) claim that, based on their assumption of a failure rate $\leq 10^{-6}$ per vessel year, the "probability of failure with fragmentation will be considerably smaller provided upper shelf conditions apply". They "feel that the estimate of 10^{-7} per reactor year assumed in the ZION analysis may well be reasonable" and they conclude therefore "that the RPV failure with almost simultaneous containment failure may lead to a release comparable to that due to the V-accident (i.e., an extremely high release), and that this release will have a frequency of less than 10^{-7} per year".

For the planned nuclear power plant BASF-Mitte, which was to be built at the site of a chemical plant, the German Reactor Safety Commission (BAZ-110, 1977, p. I.172ff) demanded special provisions against RPV rupture. This "rupture protection system" (Berstschutz) was supposed to protect the containment and other relevant safety systems against pressure vessel fragments. The main concern was obviously a vessel failure due to longitudinal cracks, or break of the circumferential weld of the lower head. The RSK emphasized at that time that the "Berstschutz"-requirement should not be seen as a consequence of modified PRA estimates, but rather as an additional protective measure because of the siting of the reactor within a chemical plant and in an area with a high population density. (The plans for BASF-Mitte were later abandoned.)

The formation of missiles is not the only mechanism which can lead to containment failure after pressure vessel rupture. For small, pressure-suppression containments, it is likely that the capacity of the pressure-suppression system will be exceeded since coolant will escape from the primary circuit at a significantly higher rate in case of a large rupture in the pressure vessel than in case of the most severe design-basis accident (double-ended break of a main coolant pipe). Such containments will also be more vulnerable to missiles than large containments.

It is evident that probability estimates for containment failure due to RPV rupture are far more inaccurate than estimates for RPV failure alone (which themselves are characterized by a considerable uncertainty). Another factor contributing to the inaccuracy of quantitative estimates is the uncertainty of the prediction of pressurization pulse duration and pulse height during extreme transients (Ju, 1982).

It must be concluded that early containment failure due to RPV failure cannot be neglected as a risk contributor. The conditional probability of containment damage resulting from RPV failure depends on the containment type. It must be assumed to be close to unity for small designs like PWR ice condensor or BWR containments. Large, dry PWR containments will have better chances to remain undamaged. This holds especially for concrete containments with steel liners.

Level II of PRAs

10 EARLY CONTAINMENT FAILURE

10.1 INTRODUCTION

The focus of Level II of a PRA is the fraction of the radioactive inventory that is released to the environment in case of a severe core damage accident, the timing of that release, the release height, and the accompanying thermal energy (which affects plume rise). Together, these characteristics constitute the accident "source term".

Obviously the most serious consequences can be expected for accidents which involve early releases of radioactivity and high source terms. Those two aspects are closely linked, since the later the containment fails, the more time is available for sedimentation and other processes in the containment which can significantly reduce the source term. However, there are processes (e.g., evolution of Iodine from pools of water which boil when containment pressure falls) which can lead to significant releases even if the containment fails after many hours.

Within the framework of this study, it is not our aim to enter a detailed discussion on the complex questions of assessing source terms for various release modes. Instead, the subsequent discussion concentrates on mechanisms which can lead to early containment failure, and on the problem of estimating their probabilities.

We recall that the IAEA Safety Targets require, in effect, a conditional probability of early containment failure of less than 0,1 (see section 1), and that this target is assumed to be met by current reactor designs.

The most important mechanisms for early containment failure are:

-- Failure of reactor pressure vessel (RPV) and subsequent missile-induced containment destruction
-- Containment bypass via the steam generators or connecting lines or through failure of containment isolation
-- High pressure melt ejection
-- Containment melt-through (particularly for older BWR designs)
-- Hydrogen deflagration or detonation
-- Steam explosion
-- External events, for example containment penetration by airplane crash

Failure of the RPV is also a very important issue in PRA Level I and is discussed in section 9. Only a short summary is given here. Because of their special importance, and because they are consistently treated in a too optimistic manner in PRAs, questions of Hydrogen deflagration or detonation and steam explosion are treated separately in sections 11 and 12. External events are discussed in section 13. The other failure

mechanisms mentioned above are usually included in PRAs - although with some omissions - and are discussed briefly in this section.

In a level II PRA analysis, the various potential containment failure mechanisms should be examined in a systematic way. For this purpose, containment event trees have been developed. In the first draft of NUREG-1150, such event trees were developed to a complexity beyond that of previous PRAs, accounting for the following issues:

-- Conditions in the reactor coolant system and containment prior to core melt;
-- failure modes of the reactor coolant system;
-- potential for, and implications of, relevant phenomena during an accident sequence;
-- survivability of containment systems (e.g., sprays); and
-- containment failure modes.

NUREG-1150/2 has further refined this concept, introducing the idea of an "accident progression event tree". That tree begins with accident initiation and proceeds through containment failure. In this way, containment behaviour can be explicitly linked to other aspects of an accident sequence.

If empirically derived probability distributions were available for each node of such an event tree, it would be possible to calculate a credible distribution for the probabilitiy of early containment failure (absolute, or conditional upon core melt). A superficial reading of NUREG-1150/2 might lead one to conclude that this type of calculation can be done. However, the necessary data are not available, and NUREG-1150/2 relies upon "expert judgment" as to the various subsidiary probability distributions. Hence, that report's findings as to the probability of early containment failure do not have a scientific basis.

10.2 SUMMARY OF MAIN PROBLEMS

Reactor Pressure Vessel Failure

Failure of the reactor pressure vessel can lead to early containment failure, if missiles are generated. This possibility is usually excluded in PRAs. The conditional probability of containment damage as a result of RPV failure depends on the containment type. It may be close to unity for small designs like PWR ice condensor or BWR containments. Large, dry PWR containments will have a better chance of remaining undamaged. This holds especially for concrete containments with steel liners. For further details, see section 9.

Containment Bypass

Three major possibilities for containment bypass are considered:

-- Steam generator tube rupture (SGTR) at PWRs
-- Failure of containment isolation
-- Interfacing systems LOCA

Steam generator tube rupture may follow a core melt or might act as a severe core damage initiator. In both cases a pathway is opened from the reactor coolant system to the secondary cooling circuit, bypassing the containment. Considerable uncertainty exists concerning the possible failure of steam generator tubes in case of core damage accidents under high system pressure. Most PRAs do not consider this as a mechanism for early containment failure.

Spontaneous rupture or rupture of steam generator tubes as a consequence of steam line break or failure to SCRAM can initiate a core melt sequence. Failure of reclosing of secondary relief valves might then lead to a core melt accident with open containment.

Regarding failure of containment isolation, US experience suggests that containments can be expected to exceed their permitted leak rates in 30% of the time. They can be expected to have a large leak between 0,1% and 1% of the time.

High Pressure Melt Ejection (HPME)

The analysis of HPME suffers from considerable uncertainties. There is agreement, however, that in case of its occurrence the potential for containment failure exists even for the largest and strongest containments. The special importance of this mechanism lies in the fact, that it leads to an extremely high source term, as was shown, for example, in the German Risk Study Phase B.

On the other hand, avoidance of HPME by deliberate or accident-induced depressurization of the reactor cooling system might create "ideal" conditions for containment-destructive steam explosions.

Melt-Through of BWR Containments

For some older BWR containment designs such as the U.S. MARK I and the German BWR-69 the conditional probability for early containment failure may approach unity. In case of core damage accidents the steel containment will be penetrated by molten core material within a short time, which has the effect that large leak areas in the containment boundary are opened. A similar phenomenon has also been identified for PWR Ice Condensor containments. These effects are addressed in NUREG-1150 but generally not in other PRAs.

10.3 BACKGROUND

10.3.1 Containment Bypass

The containment building of a nuclear plant is penetrated by a large number of pipes of varying diameter, which carry fluids into or out of the containment. These pipes represent potential paths by which radioactivity could leave the containment in the event of a core melt accident. Such paths are often known as "containment bypass" paths.

Bypass paths fall into two basic categories:

* paths from the reactor coolant system (RCS) direct to the environment outside the containment or to buildings outside but adjacent to the containment; or

* paths from inside the containment (but outside the RCS) direct to the environment outside the containment or to buildings outside but adjacent to the containment.

An indication of the variety of potential bypass paths is provided by figures 10.1 and 10.2. First, figure 10.1 provides a highly simplified picture of the power conversion system, emergency cooling system, and containment spray/cooling system for the Oconee PWR. This diagram shows that the RCS is connected to a variety of pipes which penetrate the containment. Some of these connections link the RCS to piping systems (often outside the containment) which are designed for pressures much lower than RCS operating pressure. Indeed, it is said that a typical PWR has 20-25 valves associated with the RCS which serve as high-low pressure interfaces (Wheeler, 1989). Thus, failure or inappropriate opening of valves may connect the RCS to a low-pressure piping system outside of the containment; a rupture in that system could then create an unmitigable LOCA and a consequent core melt, as well as creating a release path for radioactivity liberated from the molten fuel. This scenario, known as an "interfacing systems LOCA", has attracted considerable attention in many PRAs.

In recent years, PRAs have generally found that interfacing systems LOCAs make a small contribution to core melt frequency. However, US operating experience -- at least for BWRs -- casts considerable doubt on this finding. In a 1985 study (Lam, 1985), the NRC examined BWR operational data from 1975 onward, looking for interfacing systems LOCAs. A total of eight precursors were identified, suggesting that the probability of an emergency core cooling system (outside containment) being pressurized to twice its design pressure is about 10^{-2} per reactor year. If the probability of failure of the system at this pressure is taken to fall in the range 10^{-3} to 10^{-2}, as the NRC's study suggests, then the probability of an interfacing systems LOCA (leading to core melt) becomes 10^{-5} to 10^{-4} per reactor-year. This probability range is two or three

orders of magnitude higher than the probability typically shown by PRAs.

A serious precursor event to an interfacing systems LOCA occurred in the German PWR Biblis A in December 1987. One of two valves separating the reactor coolant system from the low-pressure injection system had been left open at reactor start-up. To avoid the necessity of shutting down the reactor, the second valve was opened for 7 seconds to create a pressure pulse to shut the first valve. This attempt failed. Luckily the second valve did not remain stuck open like the first. This accident sequence had already been dropped from further consideration in the German Risk Study Phase B, because it had been expected to make no significant contribution to risk (see also section 6.3.1).

Also to be noted from figure 10.1 is a path from the RCS to the environment via the steam generators; this is a potentially important path for all PWRs. In the event of a rupture of steam generator tubes, a path will be opened from the RCS to the main steam lines. Attached to these lines are pressure relief valves which communicate directly to the outside atmosphere. Thus, a core melt scenario involving steam generator tube rupture and the opening of secondary side relief valves (which may stick open) will feature a direct path from the core region to the outside atmosphere. This scenario is discussed below at greater length.

For BWRs, an equivalent scenario involves leakage through the main steam isolation valves, whose function is to isolate the RCS from the power conversion system. In contrast to PWRs, however, the power conversion system of BWRs is designed for full RCS pressure. As a result, it may be possible to avoid major leakage from the power conversion system to the environment.

Turning now to figure 10.2, one finds a highly simplified picture of potential connections between the containment and the outside environment at the Surry PWRs. It will be noted that large equipment and personnel hatches penetrate the containment, as do large-diameter pipes (36 inch diameter, in the case of Surry) whose purpose is to purge the containment atmosphere.

In the remainder of this discussion, the focus is upon two issues. The first issue is the possibility for containment bypass at PWRs via the steam generators. The second issue is the potential for failure of containment isolation.

Bypass Via PWR Steam Generators

For illustration of the parameters of this problem, consider the Ginna plant, which suffered a steam generator tube rupture in 1982. This 490 MWe PWR operates with an RCS pressure of about 150 bar and a secondary side pressure of about 50 bar. Four secondary-side relief valves are provided per steam generator, venting directly to the atmosphere. These relief valves are located upstream of the main steam isolation valves and are set to open at a pressure of about 75 bar. Each of the two steam generators contains about 3300 U-shaped tubes, each tube having an outside diameter of 22 mm and a wall thickness of about 1 mm. The interfacing area per steam generator is about 4000 square meters (Sholly, 1986).

The low thermal mass of the steam generator tubes makes them vulnerable to failure by overheating during a core melt accident. This vulnerability is illustrated by figure 10.3, which shows estimated tube rupture time as a function of temperature and differential pressure (note that 1 MPa = 10 bar). Thus, steam generator tube rupture (SGTR) may follow core melt. It may also, however, be a core melt accident sequence initiator.

As an accident initiator, SGTR could lead to core melt if emergency core cooling systems were unavailable or became so during the sequence (eg, due to loss of coolant inventory to the secondary side). During such sequences, the secondary side relief valves are likely to open, and experience suggests that there is a substantial probability that one or more of them will fail to re-close. In the latter event, there will exist, even before the accident has proceeded to core melt, a direct release path from the core to the atmosphere.

Spontaneous tube ruptures are relatively common events. This is not surprising, considering the dimensions of the tube walls, the harsh conditions to which they are exposed, and the difficulty of detecting weakened tubes through routine inspection. In addition, however, SGTR could occur as a result of the primary/secondary pressure differential arising during a "steam line break" or "failure to scram" incident. An SGTR induced in this manner could lead to core melt in the same way as a spontaneous rupture.

As indicated above, SGTR could also be induced by pressure and temperature effects arising during core melt sequences which have other initiators. These effects will be relevant for sequences in which the RCS remains at high pressure up to and during core melt. During such sequences, there may be a substantial pulse of pressure on the primary side of the steam generator tubes when the molten core slumps into residual water in the base of the reactor vessel. While the core is melting, tube temperatures may become elevated due to convective heat

transfer from the core and/or deposition of radioactive material within the tubes.

The temperature effect raises an issue which is generic to high pressure core melts and which is also relevant to the phenomenon of high-pressure melt ejection. This issue is the heating of the entire RCS boundary by convective heat transfer and deposition of radioactive material. Such heating could lead to a breach of the RCS, either in the steam generators or at locations such as the "hot leg" piping or the pressurizer line. If the RCS is breached, its internal pressure would fall and high pressure melt ejection would be precluded. To date, research and regulatory attention has focused on convective heat transfer rather than on heating due to deposited radioactive material. Even with this limited focus, considerable uncertainty remains about the potential for heating of steam generator tubes (NUREG-1150, 1987). In light of this uncertainty, it can be argued that thermally induced SGTR must be considered a potential containment failure mechanism for PWRs (eg, Lyon, 1987).

NUREG-1150/2 concludes that thermally-induced failure in a hot leg is likely for some high-pressure PWR sequences, but that thermally-induced SGTR is unlikely. As with other NUREG-1150/2 findings, however, this reflects "expert judgment" rather than empirically based analysis. Moreover, NUREG-1150/2 does not consider heating of steam generator tubes by deposited radioactive material. Thus, the issue remains open.

Steam generator tubes are also vulnerable to impact by small objects circulating within the RCS. Two instances of US experience are illustrative. First, North Anna Unit 1 experienced a rupture in February 1989, induced by failure of a plug inserted in November 1985. That plug, inserted to block flow from a degraded tube, broke apart and the top portion was propelled upward inside the tube, puncturing that tube and denting an adjacent tube (Rossi, 1989). Second, at Zion Unit 1, stainless steel bolts and pieces of stainless steel hinges were found in the RCS during February 1982. These had been attached to an aluminium structure which had been inserted to block a steam generator inlet nozzle during maintenance conducted in April 1981. That structure was mistakenly left in place; the aluminium dissolved and the stainless steel components circulated through the RCS. Damage to steam generator tube ends was evident, but no tube failure arose (NRC, 1982c; see also section 8.3.1.1.5). In light of the relatively fragile nature of the steam generator tubes, these instances raise the spectre of unsuspected tube weakness (potentially important in transient or core melt conditions) or of multiple tube failure.

Failure of Containment Isolation

Each path through the containment boundary is equipped with hatches or valves, whose successful operation will "isolate" the containment. Some paths (such as equipment hatches) are

intended to be isolated at all times when the reactor is operating. Other paths (such as containment purge lines or the main steam lines of BWRs) are intended to be isolated automatically when indications of abnormal operation are received. The concept of "isolation failure" thus encompasses events which involve both passive and active failures. It also encompasses paths direct from the RCS to the containment exterior and paths from the containment atmosphere to the exterior.

A comprehensive review of data on containment isolation failure has been published, drawing upon approximately 815 reactor-years of US light-water reactor operating experience (Pelto, 1985). Data were drawn from licensee event reports (LERs) and from containment integrated leak rate test (CILRT) reports. The results of the review are summarized in table 10.1.

This table suggests that containments can be expected to exceed their permitted leak rate about 30 percent of the time. Between 1 percent and 0,1 percent of the time, they can be expected to have a large leak (typically 28 square inches in area). For about 0,005 percent of the time, they can be expected to have an enormous leak in the form of an open airlock (leak area typically 5000 square inches). Subatmospheric PWR containments or Mark I and Mark II BWR containments would be less likely to manifest significant leakage areas, because leakage may be detected by loss of subatmospheric condition or loss of inerting, respectively.

Containment isolation failure may occur under conditions not represented by the data base underlying table 10.1. Recent experience at three US plants is instructive in this respect. In each case, it was found that containment isolation was dependent upon continued successful operation of the non-safety-grade instrument air system. The discoveries were made by plant licensees in response to a generic letter issued by the NRC in August 1988, many years after these plants commenced operation.

The first example concerns the Pilgrim plant in Massachusetts (a 670 MWe BWR with a Mark I containment). In January 1989 it was discovered that the closure of containment isolation valves in vacuum breaker lines connecting the torus to the reactor building was dependent upon continuing operation of the instrument air system. Although the plant design called for accumulators to supply compressed air to these valves for 30 days after a failure of the instrument air system, a test showed that the accumulators would be depleted in less than 1 hour, resulting in a containment isolation failure (NRC, 1989c). The plant had held an operating license for 16 years when this defect was identified.

A similar problem was identified in January 1989 at Browns Ferry Units 1, 2 and 3. These units are 1067 MWe BWRs which entered service between 1974 and 1977. In February 1989, a related problem was identified at the Oyster Creek plant (a

620 MWe BWR which commenced operation in 1969). At Oyster Creek, the licensee found that air accumulators feeding the main steam isolation valves would rapidly depressurize if the instrument air system failed. Containment isolation failure would follow (NRC, 1989c).

These defects are particularly important because failure of the instrument air system could be the initiator of a core melt sequence or could arise as part of a core melt sequence of other origin. Thus, dependent failures could occur, linking a core melt sequence with a failure of containment isolation.

Containment hatch incidents are reported from French PWRs.

From 1982 - 1984, containment door seals failed during 6 incidents occurring at five French NPPs. In 5 cases, the incidents resulted in total loss of containment integrity for up to 4 1/2 hours. All incidents are potentially very serious since they involve total loss of an essential safety function.

In 3 cases, a single failure of the air supply to the door seals of a hatch simultaneously affected both doors. In the other cases, the degraded (although not yet critical) condition of the seals followed by delayed or no response from operators to the signals received in the control room, resulted in all door seals deflating. Thus, the problems arose partly from inadequate design of hatches and air supply systems, and partly from operator oversights. System modifications, changes in control room alarm design, and better training of personnel were envisaged as preventive measures (NEA/IRS 508, 1985). This example is indicative of the complexity of possible sequences leading to failure of containment isolation.

10.3.2 High Pressure Melt Ejection

For many accident sequences, it is expected that the reactor core will melt while the RCS remains at high pressure. The Seabrook PRA uses 300 psia as the dividing line between low and high pressure core melts, and estimates that well over 90% of core melts at that plant (a PWR) would be at high pressure, about half of the events involving a dry reactor cavity (PLG, 1983). PRAs for other PWR plants have indicated a similar preponderance of high pressure core melts.

For example, in the German Risk Study Phase B, almost all core melt scenarios are high pressure ones (about 97%), assuming no accident management. Taking accident management into account, it is claimed that this contribution is reduced to only about 12 % (DRS B, 1989; see also section 14).

In the event of a high-pressure core melt accident, molten material could flow into the bottom of the reactor vessel and melt through the vessel wall, while the RCS remains pressurized. Molten material could then be ejected from the

vessel at high velocity, driven by pressure inside the RCS. This phenomenon is known as high-pressure melt ejection (HPME).

The concerns raised by HPME are twofold. First, HPME provides mechanisms for the suspension of radioactive material in the containment atmosphere. Second, it can lead to a substantial increase in containment pressure, potentially leading to early containment failure. That pressure increase could have contributions from direct heating of the containment atmosphere, from combustion of the molten material, from hydrogen combustion, and from an ex-vessel steam explosion. The phrase "direct containment heating" (DCH) is often used to refer to this collection of effects.

If HPME is to occur, the RCS boundary must maintain its structural integrity until the molten core has formed a pool inside the bottom of the reactor vessel. Further, the core must melt through the vessel wall in such a way that material flows into the reactor cavity at high velocity. There are several factors which could decrease the likelihood of the core melt conditions needed for HPME, as illustrated by the following two effects.

First, an in-vessel steam explosion could blow open the lower end of the reactor vessel, thus precluding HPME. Second, the temperature of the RCS boundary might closely follow the core temperature for accidents in which the RCS is pressurized. If so, the decline of material strength in the RCS at higher temperatures could cause a loss of structural integrity, leading to depressurization before the molten core slumps into the bottom of the vessel. In addition, operators might succeed in depressurizing the RCS prior to vessel failure.

There is dispute about the likelihood of these effects, but a consensus that HPME must be considered as a potential outcome of PWR core melt sequences which begin with a high RCS pressure. NUREG-1150/2 concludes that relatively few such sequences would continue to exhibit high pressure until the time of vessel melt-through, thus downplaying the importance of HPME. However, as mentioned above, the findings of NUREG-1150/2 are not credible because of their overwhelming reliance upon "expert judgment". Some analysts feel that HPME is less significant for BWRs because high-pressure core melt sequences are less likely than for PWRs and because large quantities of molten core material may not be able to collect in the vessel's bottom head. However, BWR containments would be vulnerable to even reduced-magnitude HPME events because of the small free volume of Mark I and Mark II containments and the relatively low design pressure of Mark III containments (NUREG-1150, 1987).

Even if conditions for HPME are assumed to be satisfied, there remains great uncertainty about the magnitude of the containment pressure which will be generated. However, present estimates of the range of possible pressure loadings are such

that the potential for containment failure exists even for the largest and strongest containments (NUREG-1150, 1987). This remains true even as more sophisticated analyses (eg, Williams, 1987) demonstrate the potential role of certain factors (eg, the existence of compartments within the containment free volume) in reducing estimated peak pressure loadings. In NUREG-1150/2, it is determined that the Surry and Zion containments (of the large, dry type) have a high probability of withstanding expected pressure loadings from HPME, as does the Sequoyah containment (of the ice condensor type) if substantial ice remains present at the time of HPME. However, as mentioned earlier, the findings of NUREG-1150/2 are not credible.

It is ironic that, when the potential for HPME was first recognized, it was thought to be a phenomenon favorable to containment integrity. The Zion PRA, published in 1981, proposed HPME as a mechanism for dispersing molten core material over the floor of the containment, thus preventing a high temperature core-concrete interaction and thereby avoiding the evolution of gases (including combustible gases) and radioactive aerosols which accompany such interaction (Commonwealth, 1981). However, subsequent experiments conducted at Sandia National Laboratories have shown that HPME is a much more violent event than the authors of the Zion PRA thought, and that it in fact presents a major threat to containment integrity (NUREG-1150, 1987).

10.3.3 Melt-Through of Older BWR Containments

BWRs with Mark I containments are vulnerable to containment failure arising from penetration of the steel liner of the drywell by molten core material. Figure 10.4 illustrates this vulnerability; if molten core material pours into the reactor cavity, passes through openings in the reactor pedestal, and runs across the concrete drywell floor, it will come into contact with the steel drywell liner. Failure of that liner will open a large leak area in the containment boundary.

Failure of the liner could occur rapidly. Consider an illustrative calculation made in the draft NUREG-1150 (1987). Here, an accident at one of the Browns Ferry BWRs was assumed, involving loss of all coolant injection at scram and failure of the automatic RCS depressurization system. It was assumed that the molten core debris was spread uniformly over the concrete floor to a 6-meter radius, being bounded by the 3-centimeter-thick steel drywell liner. Estimated failure times by various failure modes are shown in table 10.2. It will be seen that melt-through of the liner is expected over a wide range of conditions, and could occur within a few minutes. By comparison, the estimated times required for the drywell to fail via the overheating or overpressurization modes are considerably greater.

The situation is similar for the five German "series-69" BWRs. The bottom part of the Containment steel hull will melt through within minutes after contact with the molten core, thus opening a pathway to the environment (TUV, 1985).

A similar phenomenon has been identified for PWR Ice Condensor containments. In the case of the Sequoyah plant, and presumably other plants of similar design, a HPME event with a relatively dry reactor cavity would be likely to deposit molten core material in a location where it would rapidly melt through the steel containment wall (NUREG-1150, 1987, Vol. 1). Further investigation may reveal a similar problem for other accident scenarios and containment types.

10.4 FINDINGS OF NUREG-1150/2 AS TO EARLY CONTAINMENT FAILURE

It has not been possible for us to review the second draft of NUREG-1150 in any depth, due to the unavailability of its supporting documents (and the fact that it was published when our study was already nearing completion). However, the findings of NUREG-1150/2 in relation to early containment failure must be mentioned, because this study has treated that issue in a more elaborate manner than any preceding PRA.

Accident progression event trees have been developed in NUREG-1150/2, which in principle could provide a logical framework for addressing the complex issues involved. An elaborate set of uncertainty calculations is performed for these event trees, in a process which would be scientifically credible were the needed data available. However, those data are not available, and "expert judgment" is resorted to. Thus, the calculations are fundamentally flawed.

In summary, NUREG-1150/2 finds that the conditional probability of early containment failure (assuming core damage) is quite low for the three PWRs studied. Table 10.3 illustrates those findings. By contrast, it is found that the two BWRs which were studied have a high conditional probability of early containment failure (mean values well above 10 % for the dominant accident sequences). These findings deserve a thorough review.

An interesting qualitative finding from NUREG-1150/2 is that the Grand Gulf BWR (with a Mark III containment) is susceptible to containment failure from an ex-vessel steam explosion. In this scenario, a steam explosion would destroy the reactor pedestal, following which the drywell wall would be expected to fail either from impact by the unsupported reactor vessel or from loading at pipe penetrations.

11 HYDROGEN DEFLAGRATION AND DETONATION

11.1 INTRODUCTION

During core melt accidents, large amounts of Hydrogen will be generated and released to the containment atmosphere. Rapid pressure increase by large scale Hydrogen deflagration or even detonation becomes possible. This constitutes a serious threat to the integrity of the containment. At this stage of an accident, the containment is the last barrier preventing the uncontrolled release of a considerable fraction of the radioactive inventory.

The real potential of Hydrogen deflagration or detonation to be a major contributor to risk was revealed by the Three-Mile-Island accident. Earlier risk analysis studies had almost completely ignored this problem, or, when they had considered it, had grossly underestimated it.

The main source of Hydrogen is the oxidation of metals, especially of Zirconium, which is used as fuel cladding material in PWRs and BWRs and additionally as a material for channel boxes in BWRs.

At temperatures higher than about 1200 K Zirconium reacts with water or steam exothermically according to the equation

$$Zr + 2H_2O \rightarrow ZrO_2 + 2H_2 + 586\ kJ/Mol$$

(Hennies, 1987)

The excess energy, in addition to the decay heat, heats up fuel and metal. For temperatures higher than 1500 K, the oxidation process becomes autocatalytic, i.e. is accelerated by the energy it releases itself.

For in-vessel Hydrogen generation, the oxidation of Zirconium is by far the dominant factor. Thus, a "Hydrogen Hazard Factor" might be defined, relating the free volume of the containment to the Zirconium inventory for different reactor types and designs.

In table 11.1 the values of this hazard factor are given for various designs of PWRs and BWRs. in operation worldwide. The difference between BWRs with their small pressure suppression containment and PWRs with large containments is clearly to be seen. Table 11.1 indicates the relative importance of introducing counter measures for different containment types. The following measures have been implemented so far:

- Nitrogen insertion of the containment for the small Mark I, Mark II, GBWR-69 and SBWR

- Electrical ignitors for Mark III BWR and ice condenser PWRs

- No measures for PWRs with large dry containments

(Anderson, 1986; NUREG-1150, 1987; RSK, 1987)

If the melt is not dispersed by high pressure melt ejection or a steam explosion, a concrete-melt-interaction will occur in most reactor types after the melt-through of the reactor pressure vessel. During this stage of the accident additional Hydrogen is produced by the oxidation of the remaining Zirconium, and the oxidation of other metals. Investigations have shown that the steam generated by the concrete-melt is completely reduced to Hydrogen as it flows upward through the melt (JTKT, 1986).

This fact is ignored in many PRAs. The additional potential of Hydrogen generation by the concrete-melt-interaction is of the same order of magnitude as it is for the in-vessel Zirconium oxidation.

This does not hold for BWRs with a steel shell containment, e.g. the German BWR-"series-69" and some US BWRs with MARK I containment, where the concrete-melt-interaction plays no major role. For these types melt-through of the pressure vessel must be assumed to be followed by containment failure after a short time anyway (see section 10.3.3).

Besides the possibility of early containment failure due to deflagration or detonation the following contributions of Hydrogen to risk have to be considered:

- Mobilization of fission products caused by deflagration. This has to be taken into account regardless of whether the containment is destroyed or not.

- In case of filtered containment venting, Hydrogen burning might damage the filter.

- Pressure buildup without ignition in BWRs can lead to over-pressure failure of the containment.

- In older BWRs, Hydrogen burning outside the containment after meltthrough might significantly increase the source term.

11.2 SUMMARY OF MAIN PROBLEMS

Analysis with an AICC combustion model (Adiabatic Isochoric Complete Combustion) shows that during core melt accidents, sufficient Hydrogen is generated and released to the containment atmosphere to endanger the containment integrity of large dry PWRs by coherent deflagration or detonation.

In addition local detonations might be possible leading to containment failure as well (ÖKO, 1988).

For the smaller containment designs of ice condensers and BWRs MARK III this hazard is increased.

For the small Mark I and II designs and the German series 69 BWRs overpressure failure of the containment is possible due to the partial pressure of the noncondensible Hydrogen even without any combustion.

Since it is impossible to predict the time of ignition, the probability of early containment failure cannot be assessed. Any probability estimates that are given, e.g., in the first draft of NUREG-1150 (1987) must be regarded as totally arbitrary.

Without countermeasures, early containment failure must be regarded to be at least probable, if not inevitable. Therefore, the earliest possible time and the case with the highest source term has to be assumed conservatively in PRAs. For large dry PWRs the earliest possibility for containment failure is at the time of vessel failure, when local detonations have to be assumed. This stage is reached 2,5 hours after the beginning of the accident sequence.

The only effective countermeasure which is available at present is Nitrogen inertion of the complete containment atmosphere. This, however, has been implemented for the small BWR containments only. The integrity of such containments is endangered by Hydrogen pressure buildup even without combustion.

Ignitors that are installed in Mark III and ice condenser containments might even increase the hazard, since they can trigger a deflagration or detonation in certain accident situations.

Other measures, like catalytic foils have not yet proven to be effective under all circumstances. For cases with rapid Hydrogen release, their capability of transforming Hydrogen to water is not sufficient.

11.3 CORE MELT ACCIDENTS IN PWRS AND BWRS

11.3.1 PWR

In the introduction to this section, we mentioned the idea of classifying the risk of a certain reactor type according to the potential Hydrogen generation during core melt accidents. In a study performed for the City of Hamburg, concerning two GBWR-69 types and two GPWRs, this approach was elaborated further (Öko, 1988).

The further treatment will be based mostly on this work, in which one of the authors of this study has participated. The influence of design differences will be discussed qualitatively.

A given containment design can be characterized by its free volume, the range of pressures which are possible in the containment during core melt accidents, and the possible masses of released Hydrogen. By applying generally accepted criteria for Hydrogen inflammability limits in steam-air-atmospheres (SNL, 1986; Tosetti, 1981) and assuming homogeneous mixture, three different states can be identified:

- The mixture is not inflammable

- The mixture is inflammable

- The mixture is detonable

In figure 11.1 this is illustrated for a large dry GPWR containment of the Convoy-type, which is comparable to large dry US containment designs (see table 11.1). The inflammability limits are listed in table 11.2 and are basically the same as those used in the code HECTR 1.5 (SNL, 1986). The maximum mass of Hydrogen that can be burnt, independent of any other restrictions, is limited by the mass of available oxygen, and is about 2500 kg.

The parameter range where failure of the containment can be expected must then be identified. First of all this depends on the system design. The German PWR is designed for static overpressure of 6,3 bar. Failure is usually assumed at 8,5 bar (Heuser, 1986). The large dry US type is designed for 4,4 bar. In NUREG-1150 (1987) its failure threshold is assumed to be 9,2 bar. Other US plants are designed for 3,2 bar only (Shunmugavel, 1986). We regard a failure threshold of 8,5 bar as representative for US designs as well.

In the next step, the pressure buildup has to be assessed. In (ÖKO, 1988) a simple AICC-model was used (Adiabatic, Isochoric, Complete Combustion). According to this model, the heat released by Hydrogen deflagration increases the temperature and pressure of the atmosphere according to basic thermodynamic equations.

Unfortunately, this approach is not conservative in every case. Although the AICC-model is regarded to yield upper-limit combustion pressures and temperatures, this only applies to Hydrogen concentrations below 15 Vol% (Berman, 1984a; Benedick, 1982; Roller, 1982). Turbulent combustion effects can lead to higher pressures (Langer, 1984; Kumar, 1984) as well as to Deflagration-Detonation-Transition (DDT) (Berman, 1986c).(For more detailed discussion on this topic see (ÖKO, 1988))

Figure 11.2 shows the AICC results for the GPWR. Since the dynamic loads of coherent detonations can be expected to be beyond the capacity of the containment structure (Gittus, 1982; Haskin, 1984; Elliot, 1982), failure must be assumed for the complete parameter region (state) where detonations are possible.

Finally, the design dependent characteristics of different containment types have to be related to possible accident scenarios. Pressures and Hydrogen masses have to be determined.

Figure 11.3 shows the "Pressure Histories" that are expected for High, Low and Intermediate pressure sequences for the GPWR (Heuser, 1986). Because of the larger containment (by 10%) and the somewhat lower thermal power, pressures for the US design might be slightly lower. This difference will not be taken into account in the further discussion. The influence of containment spray systems for US designs is not analyzed.

In table 11.3 the masses of released Hydrogen are presented for the Low pressure sequence of a core melt accident. Regarding in-vessel Hydrogen generation, it is assumed that 60 % of the Zirconium inventory (Lo case), or 90 % (Hi case) are oxidized. Ex-vessel generation is estimated according to various studies (Hassmann, 1985; Langer, 1985; Baukal, 1984). For the Lo case, these values were reduced by 25%. For the US design, these values are assumed to be a reasonable approximation.

Figures 11.4 and 11.5 show the development of pressure and Hydrogen mass with time for the Lo and Hi cases. The parameter region where containment failure occurs in case of detonation or deflagration is indicated.

The result is that for the Hi case, containment destructive deflagrations or detonations are possible, for the German PWR, during the time span from 2,5 to 42 hours after the beginning of the accident sequence, and for the large dry US PWR, during the period from 5 to 39 hours after the beginning of the accident sequence.

For the Lo case, this is possible during the period from 5 to 40 hours for the GPWR, and from 16 to 35 hours for the US PWR.

Discussion

1. High Pressure Sequence (HPS)

A similar approach has been followed in (ÖKO, 1988) for the HPS, but it must be noted that the uncertainties concerning this sequence are much higher.

Unresolved questions are:

- High pressure melt ejection and the role of Hydrogen deflagration to pressure buildup (see section 10)

- Early depressurization due to primary loop failure

- Early depressurization by accident management

As far as the issue of Hydrogen generation is concerned, the time of depressurization is particularly relevant, because it can be expected that the major part of the in vessel generated Hydrogen will be released to the containment atmosphere very

rapidly at this time. Local detonations caused by self ignition or even possibly triggered by ignitors might be the consequence. The capability of recombination systems usually is not sufficient to deal with such a rapid and massive Hydrogen release.

2. Carbon monoxide (CO)

During the melt-concrete-interaction, Carbon dioxide (CO_2) will be generated. Passing through the melt it is almost completely reduced to CO (Tarbell, 1982).

CO is inflammable. Its heat production per mole is slightly higher than that of Hydrogen. CO increases the inflammability limits. This might lead to a further reduction of the effectivity of ignitors and eventually of recombination systems (see Section 11.4).

Combustion of CO and the corresponding additional pressure buildup are not included in the calculations presented here. Thus the hazards in fact can be even more severe than indicated by the results.

3. Other Designs

All designs with relatively small containments like ice condensers and subatmospherics are more vulnerable. For ice condenser containments as considered in the first draft of NUREG-1150 (1987), the likelihood of local detonations in the ice bed region is significant.

4. Countermeasures

see section 11.4

5. Detonations

A homogeneous mixture of the complete containment atmosphere was assumed so far. This is regarded as a reasonable assumption in case fans are operating (NUREG-1150, 1987). For other conditions, this assumption is conservative if only deflagrations are considered (see (ÖKO, 1988) for a more detailed discussion). It must be noted however, that especially in multiply subdivided containments high local detonable Hydrogen concentrations are possible (Casper, 1984; Bareiss, 1985a), threatening the containment integrity (Bareiss, 1985b; Karwat, 1986).

At the time of vessel failure (2,5 hours after the beginning of the accident sequence), several hundred kilograms of Hydrogen are very rapidly released to the containment atmosphere. Since steam and Hydrogen might have been to some extent separated inside the vessel, and the released steam condensates within a short time, local detonations are most probable at this time.

Thus, containment failure has to be assumed at the time of vessel failure, even with the average concentration of Hydrogen not being high enough to lead to containment failure.

6. Ignition Time

There is no possible way to reliably determine the ignition time. Therefore it has to be assumed that ignition can happen arbitrarily at any time. This assumption is supported by the TMI-accident, where an inflammable mixture was present for 5 hours before ignition occurred (EPRI, 1985). For level II PRA the earliest possible time which involves containment failure and the case with the highest Source Term have to be assumed conservatively.

7. Containment Depressurization

- by venting

- by recovery of spray systems

might have the effect of returning from an inerted condition back again to inflammable conditions. This issue, however, requires further study. Conclusive results are lacking to date.

11.3.2 BWR

For BWRs, two issues have to be considered: Combustion and subsequent overpressure failure of the containment, and overpressure failure due to the partial pressure of the noncondensible Hydrogen without combustion.

Due to the limited Oxygen available in BWR containments with no inertion only 200 - 400 kg of Hydrogen can be burnt, dependent on design. The corresponding fraction of Zirconium that has to be oxidized is about 10 %.

Containment-destructive pressure buildup caused by deflagration is possible beginning at 190 kg (5.5%) for a GBWR-69.2 (see table 11.1). Detonations which have to be assumed to be containment destructive as well are possible from 110 kg (3.2%) on. The corresponding values for a BWR-MARK-II assuming a 9 bar failure threshold are 250 kg (8.5%) for containment destructive deflagrations and 160 kg (5.3%) for detonations.

The underlying scenario is failure of emergency power supply in case of station blackout for the GBWR-69.2 (TÜV, 1985). In this sequence, pressure buildup is caused by Hydrogen deflagration and the partial pressure of Hydrogen only. Additional steam pressure is not taken into account.

In cases where Hydrogen deflagration begins at a steam pressure of several bar (for example in case of failure of decay heat

removal systems) the necessary amount of Hydrogen required to cause containment failure is further reduced (ÖKO, 1988).

In the first draft of NUREG-1150 (1987) the fraction of Zirconium oxidized during in-vessel Hydrogen generation and release is estimated to be between 10 and 50% for BWRs. In table 11.4 the resulting air and Hydrogen pressures are listed. To complete the picture, the values corresponding to 90% oxidation of Zirconium are given.

These values must be added to a static steam pressure of about 4 bar and are superposed by dynamic loads from the steam relief into the wet well. It becomes clear that even without any combustion of Hydrogen the containment integrity is endangered by overpressure, especially for the very small containments.

11.4 COUNTERMEASURES

11.4.1 Containment Inertion

Nitrogen inertion of the complete containment atmosphere is the most drastic measure and probably the only measure that significantly reduces the risk of containment destruction by Hydrogen deflagration or detonation. However, it must be noted that during the start-up and shut-down phases the containment inertion is suspended, so that during about 1% of operating time there will be no inertion. Since it must be assumed that during these phases nuclear power plants are especially susceptible to accidents, the overall risk reduction will be considerably less than a factor of 100.

Containment intertion is implemented for small containment types only. For these designs, overpressure failure due to the partial pressure of the noncondensible Hydrogen even without combustion constitutes a comparable hazard.

Furthermore, Hydrogen combustion after melt-through of the containment might have a significant impact on the source term for those containment types, especially for the GBWR-69.

11.4.2 Ignitors

The larger US containments such as the Mark III BWR containments and the ice condenser types are equipped with ignitors for early and controlled burning of the generated Hydrogen. The main shortcomings of these systems are:

- The effectiveness of the forced ignition is questionable below Hydrogen concentrations of 8% (ÖKO, 1988). Note that the combustion induced pressure buildup can be well beyond the containment failure threshold for Hydrogen concentrations of less than 8%.

- For all high pressure melt sequences and steam explosions, and possibly other sequences as well, a very rapid release of large amounts of Hydrogen must be assumed. In these cases

containment destructive deflagrations or even detonations might be triggered by the ignitors.

- The effectiveness of the ignitors is dependent on electrical energy supply. Failure of emergency power supply in case of station blackout leads to unavailability of the ignitors, at least in some plants (NUREG-1150, 1987). Recovering of the energy supply when considerable amounts of hydrogen have already been released to the containment will lead to forced ignition and possibly to containment destruction.

We conclude that ignitors do not reduce the probability of early containment failure by Hydrogen deflagration or detonation. In fact it must be suspected that taking into account all possibilities, the probability is even increased.

11.4.3 Recombination Systems

Catalytic metallic foils have been proposed by Chakraborty to remove the Hydrogen from the containment atmosphere (Chakraborty, 1986; GRS, 1987c). The basic advantage of these foils is that they can be designed as passive systems and therefore are independent of energy supply.

However, it is questionable at present whether the catalytic foils do function satisfactorily under all physical conditions.

In any case, the recombination rate is not sufficient for accident sequences with rapid Hydrogen release. This holds especially when recombination poisons (substances which decrease the efficiency of recombination) are also released, as must be assumed for many accident sequences.

12 STEAM EXPLOSION AND α-MODE CONTAINMENT FAILURE

12.1 INTRODUCTION

During core melt accidents, it is possible that the hot molten core material will come into close contact with water. A steam explosion might occur, with the possible consequence of early containment failure.

Generation of a containment-penetrating missile by a severe in-vessel steam explosion was identified as the α-Mode containment failure in the Rasmussen Report (WASH-1400, 1975). It is one of the most controversial issues of nuclear risk assessment. (See for example (Theofanous, 1988; Berman, 1988; Marshall, 1988; Corradini, 1988; SERG, 1985))

Some earlier studies like the German Risk Study Phase A (DRS A, 1979) regarded steam explosion as the only possible mechanism for early containment failure (apart from failure of containment isolation). Therefore, the results of these studies depended significantly on the assumptions concerning the conditional probability of the α-Mode containment failure. For

example, for DRS Phase A, steam explosion induced early containment failure was by far the dominant contributor to risk, although it was assumed to occur in only 2 % of all core melt accidents.

In the meantime, other mechanisms for early containment failure have been identified (for example, high pressure melt ejection). Thus, the issue of steam explosions appears to receive less attention nowadays (NUREG-1150, 1987).

Nevertheless this is still a very important issue. If it is correct that steam explosions are possible and can be strong enough to destroy the containment, there is no countermeasure at existing plants.

The occurrence of steam explosions is governed by deterministic laws. In principle, no statistical uncertainty is involved: If the required conditions apply, a steam explosion will occur; otherwise, it will not occur. However, the problem encountered when attempting to analyze steam explosions in a PRA is that only little is known about the underlying laws and necessary conditions. Furthermore, the course a core melt accident will take cannot be accurately determined beforehand. Therefore, no definite statement can be made as to the probability of a containment- destructive steam explosion.

The only points that are really known are:

- Steam explosions can occur and they can have a considerable destructive potential

- Steam explosions have been experimentally induced with molten corium and water

- Steam explosion experiments are not reproducable. Repetition of the experiment in many cases yields other results, for unknown reasons

- The highest conversion ratio from thermal to mechanical energy observed for a steam explosion was between 5 and 17% (The value could not be determined more accurately since the experimental equipment was destroyed)

The analyst Berman has based his "Uncertainty Study of PWR Steam Explosions" on these experimental facts. His study resulted in the statement that the conditional probability of a containment destructive steam explosion lies between zero and one (Berman, 1984b; Berman, 1987). It must be emphasized that this statement is by no means trivial. It means that it is not possible to give a numerical value for the probability of this event which would be justified by experimental data. In the next sections, the phenomenon of steam explosion, and the various approaches to estimation of its probability, are discussed.

12.2 SUMMARY OF MAIN PROBLEMS

In WASH-1400 (1975) the conditional probability of early containment failure due to an energetic in-vessel steam explosion (the so called α-Mode) was assumed to be 0,01.

Due to lack both of experimental data and of appropriate theoretical models, this value must be regarded as just as arbitrary as any other value between zero and unity.

Likewise, the ultimate conclusions of NUREG-1150 (1987) that (a) the contribution to risk from this class of events can be neglected and (b) that uncertainties in the probability of α-Mode failure are not a dominant problem, cannot be substantiated. The same holds for the conclusion of Phase B of the German Risk Study (Heuser, 1989; DRS B, 1989), that steam explosions do not represent a risk relevant accident path.

The only appropriate way of treating steam explosions is to assume that they can occur -- without any judgment on probability. The compulsion to produce probability estimates so as to fulfill the task of probabilistic risk assessment has led to many errors and considerable confusion on what the real state of knowledge is.

Furthermore, the other possible effects of in- and ex-vessel steam explosions should be included in PRAs:

- possible rupture of steam generator tubes, thus bypassing the containment
- bypass of pressure suppression systems for Boiling Water Reactors
- impact on fission product transport processes
- impact on coolability of core debris
- impact on source term even when the containment is not destroyed
- weakening of structures
- Hydrogen production

Those points were not considered in NUREG-1150. It is not yet known to what extent they were taken into account in the German Risk Study, Phase B.

12.3 PHENOMENA OF STEAM EXPLOSIONS

The "classic" scenario of α-mode failure of a pressurized water reactor containment is that, during a core melt accident, parts of the molten core material slump into the residual water at the bottom of the reactor pressure vessel. Fragmentation processes lead to a very rapid heat transfer from the melt to the water, which evaporates explosively. A slug consisting of

melt and water is created, which is accelerated upwards by the explosion, and hits the reactor pressure vessel head. The vessel head fails and part or all of the vessel head is catapulted through the containment.

A similar sequence can be constructed for BWRs, but steam explosions seem less likely for BWRs, since their vessel bottom is largely occupied by control rod drives which obstruct the mixing of water and melt. On the other hand, a smaller energy release is required for failure of BWR vessels and for containment failure by overpressure or by missiles.

Experiments have shown that it is more difficult to trigger steam explosions at high ambient pressures. Therefore, for high pressure melt sequences, steam explosions are often said to be impossible. However, there are indications that steam explosions can in fact be triggered under these conditions (Berman, 1986a).

Steam explosion is of special importance in view of an often-proposed accident management measure: early depressurization of the primary cooling system, to avoid high pressure melt ejection. The dilemma arises that when preventing containment failure due to high pressure melt ejection, the possibility of a containment- destructive steam explosion has to be accepted.

Apart from in-vessel steam explosions, steam explosions can also occur after melt-through of the pressure vessel. This is dependent on the accident sequence and the design of the vessel cavity and the concrete biological shield. These factors prevent early contact of the melt with water for some designs and accident sequences.

When early water contact is possible, ex-vessel steam explosions are a threat for containment integrity as well, especially for BWRs (Haskin, 1986; Sholly, 1986; Evans, 1983).

Even when steam explosions do not induce containment failure directly, they can have some unfavourable consequences:

- Steam explosions can lead to weakening of the containment system, reducing its failure threshold for subsequent loads.

- Fission products are mobilized leading to higher source terms.

- The melt configuration might become more difficult to be cooled, because of unpredictable dispersion of the molten mass.

- In case neither the vessel head nor its bottom fail, steam explosions might induce steam generator tube rupture, thus leading to containment bypass (see section 10).

- If the vessel bottom fails, a situation comparable to high pressure melt ejection might be evoked.

- Considerable masses of Hydrogen can be rapidly generated by steam explosions (Corradini, 1983). Thus, the hazard of containment destructive Hydrogen deflagrations is increased, even for plants that are equipped with ignitors or catalytic recombination systems (see section 11).

Neither of these points is considered satisfactorily in current PRAs, where interest is focused on the α-mode, which is not regarded as a contributor to risk.

12.4 DETERMINISTIC APPROACHES

Various theories on steam explosions have been developed in the past. These are discussed elsewhere (Goedecke, 1982). The present state of the art can be summarized as follows:

> " a) Fragmentation of molten material can be calculated. In some cases the results are in reasonable agreement with experimental observations. However, in most cases it is impossible to prove the theoretical results experimentally."
>
> " b) Detonation theory models can predict an experimental result if the geometry of the experiment is one dimensional."
>
> (Körber, 1985)

In any case, containment destructive steam explosions cannot be excluded by these models:

> " For these experimental conditions even very strong supercritical cases are theoretically possible, since the hydrodynamic fragmentation mechanism proved to be highly self escalating under special triggering conditions. Thus, further theoretical and experimental investigations of triggering events are very important in order to exclude the possibility of occurrence of these very strong detonation waves under realistic conditions "
>
> (Carachalios, 1986)

The experimental base is not much more reliable than the theoretical base. Most experiments (for example, of the FITS series at Sandia National Laboratories) were performed with Iron-Alumina instead of Uranium Dioxide and with masses of around 20 kg compared to the thousands of kilograms that might be involved in real accident situations (Berman, 1986a).

Furthermore it is obviously impossible for the experimenters to produce predictable steam explosion events. Berman, commenting the RC-series concludes:

" This result seems to support the idea, that FCIs (Fuel Coolant Interactions) are not simple and predictable events but rather just the opposite - very complicated and unpredictable in many cases. "

(Berman, 1986b)

The RC-series of experiments gave valuable insights concerning the efficiency of energy conversion during a steam explosion. Earlier experiments had yielded ratios for the conversion from thermal to mechanical energy of a few percent (Oh, 1987; ATOM, 1989). For probabilistic investigations, upper bound values of 3 - 5 % were therefore usually assumed (Swenson, 1981; Berman, 1984b).

The experiments of the RC-series for the first time were performed in a rigid chamber, instead of the flexible lucite chamber of the other FITS experiments. This is more realistic for in- vessel steam explosions. RC-1, the first experiment, did not lead to an explosion, but RC-2 resulted in a very violent steam explosion, which destroyed the apparatus.

The analysis performed after this experiment was based on the damage experienced and on the readings of one instrument monitoring pressure. A conversion ratio between 5 and 17 % was estimated, with a high probability that it was above 10 % (Berman, 1986b).

Therefore, an upper bound value for the energy conversion factor of in-vessel steam explosions of at least 17 % has to be assumed.

In view of the RC-series it might furthermore be possible that steam explosions at high pressures are more likely to be triggered in a chamber with a rigid wall. This issue, however, requires further experimental investigation.

The last fundamental question is how much of the molten core material might be involved in a steam explosion. Estimations of the members of the US SERG committee (Steam Explosion Review Group) ranged from 700 kg to 24000 kg (SERG, 1985). Upper bound estimations for the German PWR were in the range between 2000 kg and 10000 kg (Körber, 1985; Friedericha, 1986). Based on analysis with the computer code MELPROG, Berman even regarded 94000 kg as a possible upper bound (Berman, 1985).

Accepting 17 % as the upper bound for the conversion factor and taking 1500 MJ as the lower bound for the mechanical energy that is necessary to destroy the containment (Berman, 1986a), reaction of 5500 kg of molten material might be sufficient for α-mode failure.

In the summary of the Phase B of the German Risk Study published recently (DRS B, 1989), a maximum mass of 10.000 kg of molten corium is assumed to participate in the heat exchange processes, and an upper bound of 10 % is assumed for the conversion factor for accident conditions.

An analysis of the dynamic loads the reactor pressure vessel is subjected to came to the result that the highest loads occur in the bottom region of the vessel. Neither the bottom nor the vessel head is expected to fail according to this analysis.

Although the details of this analysis are not yet published, it must be concluded that the assumptions concerning both upper bound values are arbitrary. In particular, there is no experimental evidence indicating that the conversion factor of a steam explosion, involving several tons of molten material, is smaller than the conversion factor of small scale experiments with 20 kg of material.

Furthermore, no analysis of other impacts of steam explosions is mentioned in the summary.

Therefore, the ultimate conclusion of the summary of DRS B, that steam explosions do not represent a risk relevant accident path, is not justified.

12.5 PROBABILISTIC APPROACH

The occurrence of containment-destructive steam explosions cannot be excluded by deterministic reasoning. Therefore, probabilities have to be estimated for PRAs. The problem is that no experimental data base is available for steam explosions with corium and water on a scale comparable to LWR accident conditions. Furthermore, steam explosions in fact cannot be regarded as statistical processes. If the "PRA demon" (see section 6.3.3) were asked whether for a specific reactor and a certain accident sequence a steam explosion would occur, the answer would always be an unambiguous yes or no.

To overcome this difficulty, two methods have been employed. One method is to try to substitute the "PRA demon" by a group of experts. The other is to use Monte Carlo Analysis to investigate the effects of existing uncertainty ranges of key parameters on deterministic calculations.

12.5.1. Expert opinion and related approaches

When expert opinions are sampled, the process is divided into several stages all of which are assumed to be necessary for containment failure to occur:

- A 'large' amount of melt accumulates in the core region.
- A 'large' fraction of this pours 'rapidly' into the lower plenum, which contains a 'large' quantity of water.
- The melt mixes 'efficiently' with the water to form a premixture.
- The premixture is 'triggered' and an energetic explosion occurs.

- A water-fuel-structure slug is accelerated upwards in the core barrel

- A missile is created from the upper head with a 'sufficient' velocity to propel it through the containment dome.

(Berman, 1986a)

Subjective conditional probabilities are then assigned to each of these steps. It is assumed that the individual step probabilities are independent. Thus, they are multiplied to yield the overall probability. If only one step-value is zero, the overall probability is zero as well.

Questioning of the members of the US "Steam Explosion Review Group" (SERG) yielded values between "physically impossible" and 0,1 for the overall conditional probability of containment destructive steam explosions (SERG, 1985).

Three basic problems are connected with this approach of expert inquiry:

(i) The reliability of the results is questionable.

In view of the numerous mistakes and errors of experts in this field in the past, revealed by subsequent experimentally gained insights, this procedure cannot be trusted very much.

For example (Berman, 1985; Mayinger, 1982):

- Spontaneous steam explosions with Corium were thought to be impossible

- Spontaneous steam explosions with saturated water were thought to be impossible

- Premixing and fragmentation of the melt was thought to be a necessary precondition for steam explosions to occur

- It was thought that supercritical pressures cannot be produced by steam explosions

- The conversion ratio of steam explosions was thought to be reduced with increasing pressure

- The theoretically possible conversion ratio was thought to be 2-3% at most.

(ii) The resulting probabilities are not to be interpreted as event frequencies but merely as a "Degree of Belief" (DOB) of the experts (Berman, 1987). According to Berman, it is impossible to assign an uncertainty range smaller than the maximum range possible (i.e. the range from zero to unity, which is trivial) to DOBs.

(iii) Obviously, the resulting probability depends on the number of steps assumed to be necessary. Thus, with an

increasing number of steps the confidance that the event will not occur increases. All such investigations therefore introduce an artificial bias towards a lower probability; there is no proof that the smallest possible number of necessary and independent variables was chosen (Berman, 1987). The number of steps selected by the different SERG members differed from three to eight (SERG, 1985).

12.5.2 Monte Carlo Analysis

A more systematic approach was pursued by Swenson and Berman to calculate probabilities or uncertainty ranges (Swenson, 1981; Berman, 1984; Berman, 1987).

Uncertainty ranges were assumed for different parameters of the low pressure core melt case, characterizing the following issues:

- mass of molten material
- mass of reacting melt
- mass of reacting water
- conversion ratio from thermal to mechanical energy
- heat content of melt
- distribution of nonreacting water and melt
- failure of bottom of vessel
- energy dissipation by core and tank structures
- void fraction of the slug
- failure of vessel head
- velocity of missiles leading to containment failure

Monte Carlo Analyses were performed with two possible outcomes for each run: Failure or non-failure of the containment.

The difference between the two studies is that Berman consistently avoided any subjective assumptions about the range of the parameters and their probability distributions. The criterion for selecting assumptions was that they were based only on experimentally founded knowledge. Therefore, uniform probability distributions (which are non-informative, i.e., do not introduce any bias) were used for the parameters.

In summary the results of these calculations are that

> " high failure probabilities are computed for substantial fractions of the physically realizable parameter space. " (Berman, 1987)

For lack of experimental evidence, the conditional probability of a steam explosion leading to early containment failure during a low pressure core melt accident must therefore be assumed to be between zero and unity.

> " No method is currently capable of credibly defending any given value of failure probability or a narrow uncertainty range." (Berman, 1987)

Topics Relevant for Both Levels I and II

13 EXTERNAL EVENTS

13.1 INTRODUCTION

In many PRAs, external influences are not considered at all. When they are, the following categories are usually considered as most important:

- earthquake;
- airplane crash;
- floods;
- tornadoes (in the US);
- fires;
- others (lightning stroke, gas cloud explosion, etc.).

Fires are actually plant internal events, in a class by themselves, but are customarily included in the "external events" category.

Acts of war are never considered in PRAs. Nuclear power plants are highly vulnerable to military attacks; but there is no basis for reliable probability estimations.

Sabotage can occur from the outside as well as from the inside; this rather special topic is treated in section 17.

External events as accident sequence initiators are particularly difficult to deal with in PRAs. When analysing the possible sequences, all basic problems of methodology and component data bases fully apply. In addition, it is necessary to investigate in which ways a particular event will apply loads to the plant, which probabilities are associated with different loads, and how NPP components will react to them.

External events can yield significant contributions to SCDF. According to the German Risk Study, Phase B, this contribution is about 12 %, mainly from earthquakes (20 % in the case with accident management considered (DRS B, 1989)). For 6 recent US PRAs for PWRs, the contribution of external events is more than 10 % in every case, and more than 60 % in three cases, again with earthquakes as the single most important factor (Garrick, 1989). In some cases, fires contribute significantly to severe core damage frequency (e.g., 30 % in one of the six PRAs mentioned above, and 16 % for the TMI Unit 1 PRA (PLG, 1987)). In the second draft of NUREG-1150 (NUREG-1150/2, 1989), external events are considered for the Surry and Peach Bottom plants. In both cases, the contribution of external events to SCDF is larger than the contribution of internal events (see figure 2.8). According to NUREG-1150/2, only earthquakes and fires, among all external events, contribute significantly to SCDF.

The detailed treatment of plant response to external loads, and its translation into PRA terms, is a difficult field where experimental investigations are expensive and computer modelling extremely complicated. (This complexity probably is

the reason why many PRAs exclude external events. Of 39 PRAs performed in the US until January 1989, only 17 include external events.)

It is outside the scope of this study to enter this field, which would require a detailed review on its own. We will restrict ourselves to the question: How accurately can the probabilities of different loads due to external events be determined? This is a very basic problem since the best plant design based on the most elaborate research will not guarantee low risk if the probability of loads higher than the limits it can withstand has been underestimated. In order to discuss this problem, we have selected two examples: Earthquakes, and crash of military aircraft. Furthermore, we will discuss acts of war in order to obtain a qualitative picture on their possible contribution to risk.

This limitation of topics treated here does not imply that other categories of external events are of no importance. As already mentioned, fire-initiated sequences emerge as important risk contributors in many PRAs and external and internal flooding is, in some cases, also an important contributor. Furthermore, there are clear indications that those event categories are not treated adequately in PRAs. For example, findings of the Fire Risk Scoping Study, performed by Sandia National Laboratory for the U.S.NRC, indicate that fire PRAs do not normally address fire vulnerabilities in several important areas, including: (a) fire-induced alternate shutdown/control room panel interactions; (b) smoke control and manual fire-fighting effectiveness; (c) adequacy of fire barriers; and (d) seismic/fire interactions (NRC, 1989d).

13.2 SUMMARY OF MAIN PROBLEMS

Apart from all other methodological problems, the analyst seeking to account for earthquakes in a PRA is faced with the impossible task of deriving meaningful estimates for the probability of earthquakes (at varying magnitudes) at a given site. The data base is of necessity weak as the picture will be different for each region. Probabilistic site analyses usually culminate in the trivial insight that earthquake probabilities decrease with increasing magnitude; and that the error margins increase rapidly with increasing magnitude. Thus, in the range of magnitudes which are most important for PRAs, i.e. from 5 (Richter scale) onwards, the bandwidth of uncertainty is large and rapidly growing (e.g., to probably more than a factor of 100 for M=7).

Earthquakes (and to some extent, other external events) have a significant potential to induce further events which may contribute to accident severity. Seismically induced fires and floods are almost never included in PRAs.

Crash of military aircraft seems, in general, to yield a lower contribution to SCDF than earthquakes. However, it is important to note that probabilities can vary considerably between sites.

Furthermore, if an aircraft actually hits the reactor building, releases must be expected to be extremely high since in many cases the containment will be destroyed immediately and remain open while severe core damage proceeds. Due to the rapid development of military aircraft in recent years, guidelines for the design of NPPs against aircraft crash, e.g., in the FRG do not guarantee sufficient protection; and load assumptions in PRAs tend to be too optimistic.

Acts of war are never included in PRAs since it is plainly impossible to give meaningful probability estimates. Yet it can be shown that the possibility of the destruction of a nuclear plant by conventional weapons exists, and indeed nuclear plants have already been subject to military attack. Thus, there is no basis for the claim that the (unknown and unknowable) probability of such attacks is negligibly small. This is exacerbated by the fact that NPPs are very vulnerable to attacks; e.g., a small-scale air raid with conventional bombs would be sufficient to destroy a plant and lead to catastrophic radioactive releases.

A general problem of the treatment of external events in PRAs is that the data bases for such events are generally weaker than for internal events in most respects (see appendix 5A).

13.3 BACKGROUND

13.3.1 Seismic risk of nuclear power plants

(contribution by Prof.Dr.Eckhard Grimmel, University of Hamburg)

Earthquakes are waves of mostly natural origin, coming from the earth's interior, which are perceived at the surface as tremors. Two measures for the strength of an earthquake are in common use: Magnitude (M) and Intensity (I).

Magnitude is calculated from instrument readings. Intensity is derived from the effects observed at the surface. The logarithmic scale for Magnitude ("Richter-Scale") has, theoretically, no upper limit. The highest value measured to date is M=8,7.

The scale for Intensity ("MSK-Scale") has 12 steps:

I	registered by instruments only
II	perceived only by very small number of people at rest
III	perceived only by a few
IV	perceived by many, dishes and windows clatter
V	hanging objects start swinging, many sleepers awake
VI	slight damage to buildings, small cracks in plaster
VII	cracks in plaster, fissures in walls and chimneys
VIII	large fissures in walls, parts of gables and roof ledges collapse
IX	for some buildings, walls and roofs collapse, landslides

X many buildings collapse, fissures in the ground, with a width of up to 1m
XI many fissures in the ground, landslides in mountains
XII significant changes at the earth's surface

The effects of earthquakes of different strengths are not only well-known; they can be experienced again and again. Unknown, however, are the place and time of the next strong quake, which, within seconds, profoundly changes the environment, suddenly replacing a human being's usual feeling of superiority by panic and fear.

Seismic measurements and the evaluation of historic records show that earthquakes, although they do occur everywhere on the globe, are more frequent and usually also more powerful in certain regions. Thus, we talk of regions with higher or lower "seismicity". Regarding the earthquake-restistant design of buildings, the following complex question arises: In which regions do we have to expect which frequency and which strengths of earthquakes?

Experts attempt to answer this question by drawing maps where earthquakes which have been measured and which are documented in historic records are marked according to their magnitude (MSK-Scale), and then lines are drawn corresponding to the same magnitude (isoseismic maps, fig. 13.1).

Using those maps, the design of buildings is appropriately strengthened to render them "earthquake-resistant".

However, the reliability of such maps is small. The time-span of observation, and thus the number of earthquakes observed so far, is much too short compared to geologic dimensions, and does not permit the determination of the real seismic risk in a region or at a particular site.

It is attempted to reduce this basic shortcoming of seismic maps by defining so-called tectonic or seismotectonic units and by assuming that the strongest earthquake which was ever observed in a tectonic unit can occur again at any time and any place within this unit (compare, e.g., KTA 2201, 1975, 3.2(5)).

However, as there are no binding scientific criteria for defining the boundaries of tectonic units, severe earthquakes, which would have significantly increased the construction costs of nuclear power plants in earthquake zones, have on occasion been "deleted" from their tectonic unit when seismic zones were defined in the F.R.G. for purposes of nuclear planning.

A particularly "inconvenient" earthquake in this respect is the quake which occured at Basle in 1356, with an authenticated Intensity I=X, and a probable Magnitude M=6,5. Basle without doubt is located in the "Upper Rhine Graben", which belongs to the Central European "Rhine-Rift-Zone" (Illies, 1977; Illies, 1979; Ahorner, 1983) (figs. 13.2, 13.3).

This decisive earthquake for its tectonic unit, according to KTA-Rule 2201, was either "overlooked" by the licensing

authorities and their seismologic experts, or it was removed from its tectonic unit by manipulation. It was claimed that the geologic and tectonic characteristics of the Basle region are such that there is a "special seismicity, differing from that of the Rhine Rift zone", which is linked to the "contact between Jura, Upper Rhine Graben, and Black Forest" (DRS A FB 4, 1980, S. 45).

Based on this dubious finding, all nuclear power plants built in the Rhine-Rift-Zone were designed, at most, against earthquakes of the Intensity I=VIII. This design is insufficient from a geologic viewpoint: During earthquakes with an intensity of VIII, ground accelerations of 1,5 - 3 m/s^2 occur, whereas for an intensity of X, accelerations of 4,5 - 15 m/s^2 are experienced.

Finally, it should be noted that the Basle earthquake may even be surpassed in the future. For example, in a comparable Rift-Zone, the Baikal-Rift in Central Asia, an earthquake with an intensity of X-XI and a magnitude of 7,9 occured on June 27, 1957 (Logatchev, 1978, p. 59).

There is a possible alternative to the problematic seismotectonic regionalisation: The probabilistic approach, i.e., to estimate the probability of future quakes of different strengths at a given site on the basis of observed earthquakes.

However, such "probabilistic site analyses" culminate in the trivial insight that the frequency of earthquakes decreases as their strength increases. Furthermore, the accuracy of the probabilistic forecast decreases with decreasing frequency - thus, there is particularly high uncertainty regarding the most dangerous earthquakes (Ahorner, 1978, p. 484) (fig. 13.4).

Anyway, what is the use of the statistical "insight" that an earthquake like the Basle quake is likely to occur once in about 1000 years (fig. 13.4), if nothing can be said about the actual time and place in the Rhine-Rift-Zone?

The fact that there has been no further earthquake of this intensity in the Rhine-Rift-Zone since 1356 certainly does not permit the conclusion that a repetition will not occur before the 24th century; and that the probability of such a quake today is still extremely small, constituting a negligible "residual risk". Neither does it permit the opposite conclusion: That after such a long period of rest, another earthquake with an instensity of X is soon to be expected.

The truth is, that an earthquake with an intensity of VIII or IX or X or even XI can, in principle, occur at any time at any place in the Rhine-Rift-Zone - perhaps tomorrow, or in 1000 or more years.

This, of course, holds for every region of the globe with seismic activity, and not only for the Rhine-Rift-Zone, which was used here as an illustrative example. It can be concluded that, in earthquake-prone regions, there is no <u>residual</u> seismic risk, but rather a <u>basic</u> seismic risk, which cannot be accepted

and tolerated in view of the very high radioactive releases which result when a nuclear power plant's structure and components are destroyed by an earthquake. From this perspective, nuclear plants must not be operated in regions where strong earthquakes occurred in the past (yet even avoiding such regions altogether clearly does not lead to zero seismic risk). Even a design taking into account the strongest earthquake which was ever observed in a tectonic unit does not guarantee sufficient protection against the extreme loads to building and components experienced during a strong quake. The risk is even higher when nuclear plant materials are weakened because of ageing.

The predictability of seismic events is further reduced by the increasing scale of human activities which can trigger earthquakes. For events like the collapse of large mines or underground nuclear tests, no parallel exists in history.

The importance of earthquakes is exacerbated by the fact that (as mentioned in 13.1) many seismic risk studies performed within PRAs indicate, taking their results at face value, a high contribution of earthquakes to severe core damage frequency. Those studies without doubt have helped in recognizing the significance of the problem. Their value cannot be completely dismissed, in spite of their severe shortcomings and limitations.

It is important to note that earthquakes have a particularly significant potential to induce other events which may contribute to the severity of an accident, or lead to a severe core damage accident even when the plant has withstood the seismic shock. Seismically induced fires have not been systematically considered in the seismic PRA literature. Seismically induced floods were analysed in the PRA for the U.S. plant Oconee; no other analysis of seismically induced floods is given in the seismic PRA literature (Prassinos, 1988).

It should also be noted that earthquake hazards (and possibly hazards from other external events) are exacerbated by the fact that the same event could initiate a nuclear accident and degrade offsite emergency response capability. Such a combination would increase public exposure to radiation. As the discussion of accident consequences lies outside the scope of this study, this point will not be pursued further here. It implies, however, that the overall importance of external events as a contributor to accident hazards may be larger than would be indicated simply by their contribution to severe core damage frequency.

<u>Addendum: Discrepancies between recent seismic hazard studies</u>

The second draft of NUREG-1150 (NUREG-1150/2, 1989) provides interesting insights into the discrepancies between seismic hazard studies, as already mentioned briefly in section 2.3. The seismic analyses in this report make use of two data sources on the frequency of earthquakes of various intensities at specific plant sites (seismic "hazard curves"): The Eastern

United States Seismic Hazard Characterization Program, funded by the NRC at Lawrence Livermore National Laboratory (LLNL), published 1989, and the Seismic Hazard Methodology for the Central and Eastern United States Program, sponsored by the Electric Power Research Institute (EPRI), published 1986. Both studies used expert panels to interpret available data.

The discrepancies between the seismic hazard curves in both studies are significant. For instance, the values given for the probability of an earthquake with a ground acceleration of 6 m/s^2 for the Peach Bottom site are as follows:

EPRI	median: 8E-7/yr	85%-fractile: 6E-6/yr
LLNL	median: 5E-6/yr	85%-fractile: 8E-5/yr

It is noteworthy that two studies performed by two institutions of renown, presumably using similar data bases and methods, differ by about an order of magnitude. According to NUREG-1150/2, the NRC staff presently considers both program results to be equally valid, and for this reason, two sets of seismic results are provided in the report.

One conclusion drawn in NUREG-1150/2 is that the distribution of the seismic-induced core damage frequency is more uncertain than the internal frequencies. Furthermore, in light of the large uncertainties, any decision making should take into account the full range of uncertainty.

In this section, we made the point that the accuracy of earthquake probability estimates is extremely low for high-intensity earthquakes. This point is well illustrated by this addendum.

13.3.2 Crash of military aircraft

Average probabilities for the crash of a military aircraft in a given country can be determined with reasonable accuracy. Determination of site-specific probabilities, however, is extremely difficult. The actual data base will be too small to allow meaningful statistical estimation. Of course, indications as to the site-specific probability may be gained when considering, e.g., proximity of airports and of zones where military training and patrol flights are performed.

However, such zones can change. Also, considering the high speed of modern military aircraft, an aircraft which has gotten out of control can rapidly reach areas far from the original flight zone. Furthermore, there is no guarantee that zoning regulations are not broken deliberately or because of navigation errors.

The overall probability in a given country can also vary with time; new types of aircraft may be introduced, the general standards of pilot's training, airplane maintenance and repair might change etc.

We have selected the case of the Federal Republic of Germany for further consideration here. The FRG is a highly militarized "front state" where many aircraft are deployed, many flights take place, and hence comparatively many crashes occur per square kilometer (Certainly more than, e.g., in the US.). The average probability of the crash of a military aircraft on an area of 10.000 m^2 (the typical size of an NPP site) is 1E-6/yr. Such a crash does not lead to severe core damage in every case; hence, the overall contribution to SCDF is not very large. However, three considerations are important:

o It can be expected that, at some sites, the probability will be significantly higher (perhaps by a factor of ten).

o The conditional probability of an aircraft actually hitting the reactor building more or less head-on (angle of incidence deviating less than 45 ° from the vertical) is about 20 %. In such cases, if the airplane is heavy and fast, the release will be extremely high since the containment will be destroyed and remain open while the accident proceeds further. Thus, the contribution of aircraft crash to accidents with early containment failure will be higher than to general SCD.

o Cases have been reported of pilots using nuclear plants as landmarks for target practice (Sütterlin, 1975). This would result in a higher crash probability; however, it seems impossible to quantify this effect.

In the German Risk Study, Phase A, it is assumed that in 50 % of the crashes, the airplane will be a Phantom; in the other 50 %, a plane which is not heavier or faster than a Starfighter. The reference plant (Biblis B) is designed to withstand even the head-on crash of a Starfighter, but not of a Phantom. Hence, DRS arrives at a frequency of 1E-6x0,2x0,5 = 1E-7/yr for an airplane crash with immediate containment damage (overall crash probability times conditional probability for head-on crash on reactor building times conditional probability of airplane being heavier and faster than a Starfighter). This result remained unchanged in Phase B (DRS B, 1989). By the same logic, the probability for airplane crash with immediate containment damage would be zero for newer plants (e.g., Brokdorf, Grohnde), since they are designed against Phantom crash; and about 2E-7/yr for older plants like Stade or Würgassen, which are not even designed against Starfighter crash.

DRS also stated that it is not expected that military aircraft with significantly higher impact loads than a Phantom will be deployed in the FRG in the future (DRS A 4, 1980).

However, reality has overtaken both plant designers and risk analysts. Today, roughly 50 % of the military planes deployed in the FRG are F-15 and Tornado, which are both faster and heavier than Phantoms (we estimate the peak load occuring when they crash to be at the very least 50 % higher than for a Phantom). It is clear that it is very difficult to predict such a development; military planners do not have NPPs in mind when developing and deploying aircraft. In the case of the F-15 and

the Tornado, it is also interesting to note that the Tornado as planned on paper by the late 70s was still considerably lighter than the Phantom, but became heavier and heavier during the development phase; and early versions of the F-15 were comparable to the Phantom, but weight was added with every new version (the F-15E, being in production since the beginning of 1988, is heavier by 50 % than the Phantom) (Janes', 1988).

Another notable point is that in DRS, the effect of any weapon load (bombs, missiles, munition) is not taken into account. We have no reliable information as to how often planes do indeed carry such weapons.

The most interesting conclusion from this discussion is not the increase in risk for the reference plant of DRS, but rather that even for the most modern German nuclear plants, the risk of severe core damage with early containment failure resulting from the crash of a military airplane is not zero, as claimed officially, but in the order of 1E-7/yr or more.

13.3.3 Acts of War

Protection against acts of war is not a design requirement for nuclear power plants, although it is claimed that protective measures against other external events - e.g., against airplane crash - will also result in a certain limited capability to withstand military attacks. Furthermore, for obvious reasons, acts of war are never included in PRAs: It is plainly impossible to assign reliable values to the probability of occurrence. There is no way to extrapolate historic evidence for the purposes of probability estimation. Global and regional political situations, military doctrines, and military technology keep changing continually and the general picture today is very different from the picture, e.g., 25 years or 50 years ago. For instance, it would be clearly nonsensical to derive probabilities for the destruction of a British or German nuclear power plant by air raid by studying the bombing offensives in World War II.

However, even if the actual risk cannot be reliably estimated, and keeps changing rapidly, there is no justification for assuming it to be negligible. Military attacks on nuclear installations can occur, and in fact have occurred in the last decades; the best-known example being the Israeli air raid on the reactor Osiraq near Baghdad at June 7, 1981.

In the case of an all-out, worldwide nuclear war, leading to large-scale destruction, radioactive contamination, and potentially a "nuclear winter", the problem of radioactive releases from nuclear power plants is more or less irrelevant. However, the possibility of conventional wars or "limited" nuclear conflicts, involving countries with nuclear power plants, exists; and the destruction of a nuclear plant can, in this case, significantly increase the damage by radioactive contamination. The assessment of the likelihood of such a scenario lies outside the scope of this study.

The vulnerability of nuclear power plants to military attacks is high. Conventional attacks by artillery, missiles, or bombs can destroy the reactor building and lead to damage of the reactor pressure vessel or to a multiple loss-of-coolant accident which cannot be controlled by safety systems. For example, a 2000 pound standard-bomb of the U.S. air force can penetrate 3,4 m of concrete (Gervasi, 1977). The protective concrete structures of NPPs are considerably thinner; the maximum thickness is about 2 m for some newer West German plants. Due to the increasing accuracy of modern weapons systems, a small-scale attack could be sufficient to destroy a plant (e.g., an F16 can place conventional bombs with an accuracy of +/- 10m; for the Tornado IDS, an accuracy of +/- 3m is claimed (Richardson, 1985)).

Acts of war also have a significant potential to induce fires at the site. Destruction of communication lines, roads etc. in the vicinity of the power plant can also severely degrade the capability for emergency response.

Furthermore, indirect effects at times of war can compromise the safety of nuclear power plants. Even when shut down, a nuclear power plant needs electricity for numerous systems to remain in a safe state. Both the electrical grid of a country, and the long-term supply of fuel for the emergency Diesel generators, are likely to break down sooner or later in case of war. A minimum number of qualified personnel must be available for plant supervision and maintenance; supply of spare parts might become necessary. Yet, Diesel generators are not designed for long-term operation. Their failure rate will be high if operated over weeks and months, even if fuel is available (Öko, 1987).

Thus, even if deliberate care is taken not to directly attack nuclear power plants during a war, and no direct attack occurs by mistake, there is a significant potential for accidents to eventually occur.

14 ACCIDENT MANAGEMENT

14.1 INTRODUCTION

Traditionally, PRAs have applied rigid criteria in order to determine which accident sequences lead to severe core damage. That is, a certain set of safety systems is required to keep the plant safe for a particular initiating event. If not all the needed functions are available, severe core damage is assumed to occur. However, a more optimistic approach is now being gradually introduced. It is conceived that, even in cases where not all required safety systems are available, the accident can still be "managed" by improvising the use of other systems for safety purposes, and/or by the use of safety systems in a different context than originally planned. The aim of such accident management is to avoid severe core damage in situations where the plant would otherwise have to be written off; or at least to avoid containment failure if SCD occurs.

Such possibilities of "accident management" are increasingly given credit in PRAs, resulting in considerable reductions in the frequencies of severe core damage and early containment failure. Accident management is a large field which we will not attempt to fully discuss here. We will restrict our treatment to those aspects which are relevant for PRA.

14.2 SUMMARY OF MAIN PROBLEMS

Accident management places increased reliance on operator intervention. Yet, the possibilities of simulator training are limited. Hence, there is a large scope for human errors - from simple omissions to complicated improvisations which aggravate the accident because the operators do not have a correct picture of the situation, or make mistakes in devising their strategies. This potential for error is enhanced by a serious pressure of time in many cases which will create high stress levels. For this reason alone, the significant reductions in SCDF and early containment failure probability which are claimed in PRAs (most notably, in the German Risk Study, Phase B) appear unrealistic.

Furthermore, accident management, even if performed as planned, might prove ineffective, leading from one severe accident sequence to another just as hazardous. It could even be counter-productive - e.g., an attempt to avoid Hydrogen detonation by controlled burning of Hydrogen can actually initiate detonation if it is implemented too late. Similar considerations hold for containment venting.

Many questions still remain open in connection with accident management. Nevertheless, in the case of the German Risk Study, credit is already taken for measures which cannot be implemented in present-day German reactors without complicated and expensive backfitting.

14.3 BACKGROUND

The field of accident management (AM) is at present developing rapidly. It is difficult to give a precise and detailed definition. Kersting (1988) attempt to sum up what it is all about:

"The concepts and measures aimed at preventing a core melt or mitigating its consequences which are not explicitly considered in the design are internationally known as accident management measures. Accident management includes all measures which are initiated in a plant to identify as early as possible deviations from design basis sequences, to diagnose and control them and terminate the disturbances with minimum damage."

This gives a reasonable picture of the idea of accident management. What it comes down to is using NPP systems in a way which was not originally planned, in order to prevent or mitigate accidents; i.e. allowing for improvisation in addition to the planned use of safety systems, or when safety systems have failed.

However, this picture is not complete. AM procedures can affect plant design if equipment has to be upgraded, or newly installed, to permit their implementation. The separation between "ordinary" safety procedures and accident management is still more fuzzy in the case of new plant designs when accident management features may be incorporated right from the start.

The idea of accident management is increasingly emphasized, and has been introduced into the public debate on nuclear safety in recent years (particularly after the Chernobyl accident). Seen from the PRA-viewpoint, accident management appears to be intended to provide the nuclear industry with a means to make up for less-than-satisfactory PRA results; either qualitatively (by pointing out that estimated SCDFs need not be taken too seriously, since AM will in fact help to avoid severe core damage in most cases), or even quantitatively by incorporating accident management into PRAs.

For our purposes, it is appropriate to distinguish three levels of accident management:

- prevention of severe core damage;
- prevention of early containment failure should SCD occur;
- preservation of long-term containment integrity in case of SCD without early containment failure.

In recent years, accident management procedures have increasingly been introduced into PRAs. It is claimed that this can lead to very significant decreases in SCDF and ECF probability. An excellent example is provided by the most recent preliminary results of the German Risk Study, Phase B. Overall SCDF is to be reduced from 3,1E-5/yr (without AM) to 5,4E-6/yr (with AM), by a factor of almost 6. The most decisive influence of accident management, however, is the reduction of the frequency of accidents with extremely high releases (early

containment failure, or containment bypass): From 3E-5/yr without AM (i.e., without AM almost every accident leads to very large releases), to 5E-7/yr with AM, i.e., a reduction by a factor of 60 (Heuser, 1989).

Similar considerations apply in France. For example, it is assumed that accident management will reduce the probability of the S_2D-sequence (a very small LOCA with coincident failure of the HPI system) at least by a factor of 10 to 100 (Bars, 1985).

Accident management is also receiving increasing attention in the U.S. In the draft NUREG-1150, accident management measures were taken into consideration when written procedures existed. In a detailed study on accident management prepared for the U.S.NRC (NRC, 1985), event trees for accident management measures were constructed. No estimation of probabilities, however, was performed.

Accident management implies increased reliance on operator intervention. Complicated procedures have to be performed, which are not encountered during routine operation or when dealing with minor mishaps. The value of simulator training is limited, since the capacity to model complex accident dynamics in the simulator is limited (and not all accident sequences are sufficiently well-understood). Thus, there is large scope for human errors; not only "simple" errors of omission, but also complicated forms of counter-productive behaviour due to hasty improvisation, misunderstanding of the situation, etc. (compare section 8.3.1.3.2). Of course, on the other hand, human creativity and intuition may also lead to unforeseen responses which prove very effective. However, the increased reliance on human intervention certainly implies very large error margins when estimating the probability of AM failure or success in a PRA, and hence leads to large error margins in the PRA results. In some countries at least, AM also constitutes a basic change of trend in the development of the general "safety philosophy". In the FRG, for example, it used to be a basic principle to limit the necessity of operator intervention during a severe accident as much as possible, and render any interventions completely unnecessary in the first 30 minutes after accident initiation.

The problem of human error in accident management is exacerbated by the fact that the time available for the initiation of procedures is often very short. Consider, for example, a transient in a PWR with failure of emergency feedwater supply, as treated in the German Risk Study. Without AM, this would lead to SCD. This could be avoided by secondary bleed and feed, i.e., dumping steam from the secondary circuit and thus lowering the secondary pressure so that alternative water supply to the steam generator can be improvised. Secondary bleed and feed, however, must begin 50 - 60 minutes after accident initiation in many cases. The time required to implement this measure, on the other hand, is about 45 - 60 minutes. Thus, decisions need to be taken immediately at the beginning of the accident sequence, and the practical implementation must start within minutes.

If secondary bleed and feed fails, primary bleed and feed might still prevent severe core damage (opening of pressurizer relief valves and high-pressure injection). If high-pressure injection fails, primary bleed alone could at least avoid core melt at high pressure, and reduce the danger of early containment failure. But again, time is a crucial factor. Furthermore, the operators may be faced with rather awkward decisions: In case of a delay in initiation of secondary bleed and feed, would it be safer to delay primary bleed and feed initiation (with the risk that, when secondary bleed and feed cannot be started subsequently, it will be too late for primary measures); or is it better to start primary bleed (risking core melt when HPI fails, even if secondary bleed and feed is implemented later, if pressurizer valves cannot be closed again in time). Similar considerations apply in case of a small LOCA; however, in this case, secondary bleed and feed alone (without HPI) cannot prevent core melt, it can only prevent the high-pressure-path (Kersting, 1988; Fischbacher, 1988).

Similarly, in case of the French investigations, the time available for the operator to install short term cooling via the steam generators in the S_2D-sequence can be as short as 20 minutes (Bars, 1985).

The high stress level in such situations will lead to a very high probability of ineffective, or even counter-productive, human behaviour (there is even the possibility that operators may overreact in a sequence which would not ordinarily lead to severe core damage, and aggravate it by inappropriate actions, thus inducing SCD).

A significant reduction of SCDF and early containment failure probability by accident management thus appears unrealistic (see part 14.4 for an exemplary discussion).

Furthermore, even if performed as intended, accident management measures may not reach their aim, or even be counter-productive. For example, in the German Risk Study, it is assumed that core melt at high primary pressure will lead to high pressure melt ejection (HPME) and ECF, whereas the "low-pressure-path" will never lead to ECF. This is the reason why, if SCD cannot be avoided at all, AM is planned to at least reduce primary pressure. However, as discussed in section 12, the low pressure sequence can be accompanied by a steam explosion which destroys the reactor pressure vessel and results in ECF.

Another measure to avoid early containment failure - the controlled burning of Hydrogen in order to avoid destructive detonation - can actually initiate the detonation it seeks to render impossible if performed too late.

Also, the restoration of cooling water to a core which is already dried-out and hot may cause a rapid Zirconium-steam reaction, leading to accelerated meltdown (Sholly, 1986, p. 9-6).

Containment venting to avoid late containment failure due to overpressure, as already introduced in the FRG, France and Sweden, and seriously considered by many other countries, is also highly controversial. Due to the pressure drop, steam will condense in the containment. Thus, Hydrogen detonations may become possible which otherwise could not occur because the containment atmosphere is inerted by high steam concentrations. (This, however, is a complex issue in need of further study.) Furthermore, containment venting could actually aggravate some accident situations, e.g., containment venting could have made the consequences of the TMI-2 accident worse (NucEng, 1989a).

All in all, many questions still remain open in connection with accident management. One important issue is the survivability of equipment needed for AM under accident conditions (NUREG-1150 J, 1987). Furthermore, it must be noted that the results of the German Risk Study concerning the significant reduction of accident probabilities by AM do not correspond to the actual plant status. Backfitting measures are necessary in German PWRs to make possible AM to the extent which is already taken for granted in the risk study. For example, in order to create primary bleed capacity, an additional relief line with two motor driven pilot valves must be installed at the pressurizer to allow opening of the safety valves from the control room (Fischbacher, 1988). The inclusion in a PRA of measures which cannot yet be performed is even more misleading than the lack of distinction between "as found" and "as fixed" PRAs (see section 2.3). In terms of section 2.3, it creates a third category of PRA results: "As envisaged".

Those findings further support the conclusions already drawn in 1986, after the Chernobyl accident, by an expert panel assembled by GREENPEACE in order to assess the hazards of present-day commercial power reactors:

"... these reactor types are technologically mature in the sense that they have, over the decades, more or less reached the limits of their potential for development and improvement. They are as good as they can get. (...) Further addition of safety systems, or further increase of sophistication of systems are likely either to bring only marginal improvements, or to have negative returns because of the increase in complexity" (Anderson, 1986).

As far as can be seen today, accident management does not have the potential to invalidate this statement.

14.4 DISCUSSION OF RESULTS OF DRS, PHASE B

We consider the accident category "plant internal transients" of DRS B. This category constitutes about 2/3 of SCDF without accident management, and is the category the frequency of which is most drastically reduced by accident management.

According to preliminary results of DRS Phase B (Heuser, 1989), the mean value of SCDF due to transients without accident management amounts to 2E-5/yr. For AM measures which serve to

avoid severe core damage, a failure probability of 0,01 is assumed. This number is given as "rough assessment", without detailed justification. There is no indication as to whether it is supposed to be the mean or the median of the failure probability distribution. Thus, with AM, an SCDF contribution of 2E-7/yr for transients is claimed.

This rough assessment appears to be unrealistically optimistic. Using different, equally plausible, assumptions, the reduction of SCDF by accident management is much less significant. For instance, let us assume that

-- due to the introduction of accident management options, the SCDF contribution due to transients is increased by 10 %, to 2,2E-5/yr (because the possibility for additional accident sequences might be created);

-- the median failure probability of accident management is 0,1, which appears to be an appropriate value for actions under high stress;

-- the variation factor K (assuming lognormal distributions) both for the SCDF contribution due to transients, and AM failure probability, equals 5;

-- and the two random variables "severe core damge frequency due to transients" and "AM failure probability" are completely correlated.

Our calculations show that the resulting SCDF (transients), with accident management, equals about 0,9E-5/yr.Thus, our assessment yields an improvement in SCDF by a factor of 2 only. Overall SCDF will be reduced by a still smaller factor.

This example is based on assumptions which are to a large extent arbitrary. It is not intended to give a reliable estimate of the reduction of SCDF by accident management. Rather, its purpose is to illustrate the considerable uncertainty associated with estimating the influence of AM on PRA results.

(The final results of DRS Phase B, published at a time when this study was in the last phase of completion, contain only slight modifications of the preliminary results discussed here. For the accident category considered here, the overall reduction of SCDF contribution by AM is claimed to be by a factor of about 80 instead of 100. The reduction of the contribution of the high-pressure path alone is still assumed to be by a factor of 100. Thus, the discussion here remains valid.)

"Real World" - level

15 UNEXPECTED PLANT DEFECTS

15.1 INTRODUCTION AND SUMMARY OF MAIN PROBLEMS

PRA analysts seek to identify failures which fall into two classes: human errors; and failures of components or structures. In each case, the failure may be random or may arise from some abnormal stress. A competent analyst will try to account for natural variations in the behaviors of people, materials and machines, and for factors such as equipment aging. However, the analyst cannot readily account for unexpected human behaviors -- such as acts of sabotage -- or for unexpected defects in the plant. The present discussion focusses on the potential for, and significance of, the latter problem -- unexpected plant defects.

Such unexpected defects may arise from improper design, construction or maintenance, or from unexpected changes in material properties due to factors such as corrosion or embrittlement. However, all significant defects in this category share two characteristics. First, they can cause components and structures to behave in ways not consistent with plant specifications and safety regulations. Second, they will not be reliably detected through routine inspections and tests. As a result, the PRA analyst will find it difficult -- and in many cases impossible -- to identify and ascribe probabilities to failures which might arise from unexpected plant defects.

By their very nature, these defects will tend to remain hidden in normal circumstances. However, plant construction and operating experience in many countries has revealed a considerable number of defects which were not detected by routine inspections and tests; and also of defects which, although detected by tests, might well have led to severe problems before they were discovered. Examples of these instances are described below. It must therefore be assumed that there are other, so far undetected, defects in nuclear power plants, but there is no basis for estimating their likelihood or significance.

Since it is impossible to review world-wide relevant plant experience within the scope of this study, this section mostly deals with US nuclear power plants. However, as some examples concerning European plants illustrate, there is no basis for assuming that US plants are unique in terms of the prevalence of undetected defects.

15.2 EXAMPLES OF UNEXPECTED DEFECTS AT US NUCLEAR PLANTS

The Crystal River Incident of 1986.

Crystal River Unit 3 is an 825 MWe PWR which commenced operation in 1977. On 9 June 1986, the plant licensee submitted to the NRC a licensee event report (LER) describing plant defects which resulted in a potential common mode failure

of a system important to safety. The defects were detected by the plant's quality assurance (QA) and quality control (QC) program during construction, but through visible structural damage which became obvious after nine years of plant operation (Hsu, 1987).

The visible damage consisted of cracking in a concrete pedestal which supports discharge piping from two heat exchangers in the nuclear service closed cycle cooling water system. Subsequently, hairline cracking was found in support pedestals for two other heat exchangers in the system. Investigation revealed that the original analysis of piping loads had been performed incorrectly, with the result that the support pedestals were not designed for the loads actually experienced. This could have led, at any time, to a failure which would have rendered both trains of the cooling system inoperable. Moreover, the same investigation showed that a rigid seismic restraint, assumed in the piping design calculations, was not included in construction documentation and, therefore, was never installed. Thus, even if the support pedestals had been sufficiently strong, the piping may not have withstood an earthquake for which it was nominally designed.

In this case, two separate but related defects arose at the detailed design level and were not detected by routine measures. Prior to their detection, a PRA analyst would have had no basis for assuming a failure from such defects. Yet, the defects could have caused a common mode failure rendering the cooling system inoperable. Such an event would have violated the "single failure criterion" and would be outside the plant's design basis.

The NRC's Generic Investigation After the Crystal River Incident

In the wake of the above-mentioned incident, the NRC searched its files for LERs describing similar design and construction defects. For reasons unknown to us, this search was confined to LERs submitted between January 1984 and September 1986. Yet, despite this limited scope, the search identified a total of 55 reports involving design and construction defects that could have led to significant failures. None of these defects had been detected by the QA and QC programs in place during plant construction or modification. Nor could most of the defects have been detected by routine tests such as pre-operational, start-up or surveillance tests (Hsu, 1987).

The 55 reports were from 34 plants; of these 55 reports, 36 referred to original design or construction problems, while 19 referred to plant modifications. Reported defects can be grouped into six categories:

(i) piping stress exceeding code limits;
(ii) incorrect hardware or improper installation of hardware;
(iii) lack of fire seals for electrical cable penetrations;
(iv) electrical wiring errors;

(v) errors in electrical, instrumentation and control circuits; and
(vi) electrical and control panels not seismically supported.

In some cases, the defects can be attributed to poor workmanship. A particularly egregious example involved Crystal River Unit 3, in an incident different from the one described above. Here, many bolts supporting ductwork for the control room ventilation system were found to be too short to provide adequate strength or to have been cut off and their heads tack welded in place, to give the appearance of proper installation. Yet, by no means all the defects can be attributed to markedly substandard workmanship. Many are typical of errors or defects which are not unusual in construction or modification of complex systems.

Defects Introduced by Faulty Maintenance

A recent NRC report (Wegner, 1989) attempts to assess the probability and implications of significant maintenance deficiencies by reviewing operational experience reported to the NRC over the period 1985 - 1988. The report's conclusions include the following statement:

> "Maintenance-related problems have been identified in many systems and components in several operating nuclear plants. The type of components and systems involved, such as motor-operated valves, solenoid valves, plant air systems, and service water systems, point out the pervasiveness of the problem and the potential for common cause failures of redundant safety equipment and systems."

In illustration of these maintenance problems, consider a case where a new type of grease was used on moter-operated valves. The new grease was qualified for accident conditions, and thus its use was part of an effort to enhance plant safety. However, the new grease had a lower viscosity, and thus migrated to a region of each valve where it inhibited the compression of a spring which was needed to operate the valve. Clearly, this problem had the potential to disable many valves at the same time.

Defects in Concrete Containment Buildings

Level II PRAs usually devote considerable attention to the probability that containment will fail under the stresses encountered in core melt accidents. This is an important point because reactor containments are not designed for core melt conditions but for lesser, "design basis", accidents. It is often claimed that containments will withstand pressures several times their design pressure, even though they are not tested in this regime. The validity of such a claim will depend upon the accuracy of the supporting analysis and the extent to which the actual containment corresponds to the "theoretical" containment which is analyzed. There is reason to believe that there may be significant discrepancies between "theoretical" and actual containments. Consider the case of

References

ACM, 1989a

ACM Committee on Computers and Public Policy Forum on risks to the public in computers and related systems
Volume 8.1, January 4, 1989

ACM, 1989b

ACM Committee on Computers and Public Policy Forum on risks to the public in computers and related systems
Volume 8.2, January 4, 1989

ACM, 1989c

ACM Committee on Computers and Public Policy Forum on risks to the public in computers and related systems
Volume 8.3, January 8, 1989

ACM, 1989d

ACM Committee on Computers and Public Policy Forum on risks to the public in computers and related systems
Volume 8.5, January 11, 1989

ACSNI, 1982

Advisory Committee on the Safety of Nuclear Installations
Some aspects of safety in pressurized water reactors
Health and Safety Executive (UK)
1982

AEC, 1950

US Atomic Energy Commission
Summary report of reactor safeguards committee
WASH-3, 1950

AEC, 1957

US Atomic Energy Commission
Theoretical possibilities and consequences of major accidents in large nuclear power plants
WASH-740, 1957

AEC, 1973

US Atomic Energy Commission
The safety of nuclear power reactors (light water-cooled) and related facilities
WASH-1250, 1973

Ahlf, 1984

J. Ahlf et al.
Das Strahlungsverhalten von Reaktordruckbehälterstählen aus dem Forschungsprogramm Komponentensicherheit
10. MPA-Seminar, 1984

Ahorner, 1978

L. Ahorner, W. Rosenhauer
Seismic risk evaluation for the upper Rhine Graben and its vicinity
J. Geophys., 44, p.481-497, 1978

Ahorner, 1983

L. Ahorner
Seismicity and neotectonic structural activity of the Rhine Graben system in Central Europe
In: A.R. Ritsema, A. Gürpinar (Ed.): "Seismicity and seismic risk in the offshore North Sea area", NATO Advanced Study Institutes Series C, Vol. 99, p. 101-111, Reidel Publ. Comp., Dordrecht, 1983

Amendola, 1987

A. Amendola et al.
Probabilistic safety assessment: Actions and priorities in the EC-frame
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

Amesz, 1985

J. Amesz et al.
The European Reliability Data System: Main developments and use
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

Anderson, 1988

Anderson et al.
International Nuclear Reactor Hazard Study
Greenpeace
1988

Andrews, 1988

W.B. Andrews et al.
A ranking of sabotage/tampering avoidance technology alternatives
NUREG/CR-4462
U.S. NRC, 1988

Apostolakis, 1985

G. Apostolakis
On the analysis and use of operating experience in probabilistic risk assessment
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

Apostolakis, 1988

G. Apostolakis, P. Moieni
On the correlation of failure rates
EUREDATA Conference
1988

Aschenbrenner, 1988

J.F. Aschenbrenner et al.
N4 PWR makes full use of distributed processing and local networks
Nuclear Engineering International
January 1988

Atom, 1987

Atom & Strom
Vol. 8, 1987

ATOM, 1988

ATOM
U.K. Atomic Energy Authority
Number 368
February 1988

ATW, 1987

atomwirtschaft - atomtechnik
Vol. XXXII
May 1987

Baker, 1988

G. Baker
Hydrogen accidentally fed into service air system at Robinson 2
Inside NRC, p. 12
18 January 1988

Balfanz, 1987

H.P. Balfanz
State of the art of probabilistic safety analysis (PSA) in the FRG and principles of a PSA-guideline
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

Ballard, 1985

G.M. Ballard
An analysis of dependent failures in the ONRL precursor study (NUREG/CR-2487)
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

Ballard, 1988

G.M. Ballard
Small incidents - precursors to disaster? or aid to safe operation?
Int. Conf. on Nuclear Risks
London, 1-2 December, 1988

Bareiss, 1985a

H. Bareiss et al.
Möglichkeiten einer lokalen Wasserstoffdetonation im SB eines DWR während eines hypothetischen Unfalls
Jahrestagung Kerntechnik
1985

Bareiss, 1985b

H. Bareiss
Untersuchung zur Möglichkeit einer kleinräumigen Detonation während eines hypothetischen Unfalls
GRS-F-145
1985

Barnes, 1988

M. Barnes
Seeking a standard framework for dependable computing
Nuclear Engineering International
May, 1988

Bare, 1985

G. Bare et al.
Introduction of accidental procedures in the event trees of the 900MW PWR PRA
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

Baukal, 1984

W. Baukal et al.
Möglichkeiten zur Wasserstoffbeseitigung
BMI 1984-083
1984

BAZ-110, 1977

Kernkraftwerk BASF - Standort BASF-Mitte und Sicherheitskonzept
BAZ Nr.110, I, pp 1?2??, 1977

Bell, 1981a

B.J. Bell, A.D. Swain
Overview of a procedure for Human Reliability Analysis
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Bell, 1981b

B.J. Bell, D.D. Carlson
IREP Human Reliability Analysis
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Benedick, 1982

W. B. Benedick et al.
Experimental Results from Combustion of Hydrogen-Air Mixtures in an Intermediate Scale Tank
Proc. Second International Conference on the Impact of Hydrogen on Water Reactor Safety
NUREG/CP-0038
1982

Bennett, 1982

H.A. Bennett
Reactor safeguards against insider sabotage
NUREG/CR-2546
U.S. NRC, 1982

Berman, 1984a

M. Berman et al.
Hydrogen Behavior in LWR
Nuclear Safety 25, 1
1984

Berman, 1984b

M. Berman et al.
Uncertainty Study of PWR Steam Explosions
Sandia National Laboratories
NUREG/CR-3369
1984

Berman, 1985

M. Berman
Comments on Draft of SERG Report
SERG 85
1985

Berman, 1986a

M. Berman
An Evaluation of the Ba[illegible] for Estimating a-Mode Failure Probabilities
Proc. Int. ANS/ENS Top. Mtg. on Thermal Reactor Safety
San Diego, California
ANS 700108
1986

Berman, 1986b

M. Berman
Light Water Reactor Safety Research Program
Semiannual Report, Oct. 83-March 84
Sandia National Laboratories
NUREG/CR-4459
1986

Berman, 1988c

M. Berman
A Critical Review of recent Large-Scale Experiments on Hydrogen-Air Detonations
Nucl. Sci. Eng. 88, 321
1988

Berman, 1987

M. Berman
A Critique of three Methodologies for Estimating the Probability of Containment Failure due to Steam Explosions
Nucl. Sci. Eng. 88
1987

Berman, 1988

M. Berman
Comments on "An Assessment of Steam Explosion Induced Containment Failure, Parts I - IV"
Nucl. Sci. Eng. 100
1988

Beveridge, 1988

R.L. Beveridge
Applied human reliability: one utility's experience
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1988

Birkhofer, 1988

A. Birkhofer, K. Käberlein
Data situation and the quality of risk assessment
EUREDATA Conference
1988

Birkhofer, 1988

A. Birkhofer, A. Jehna
Germans examine benefits of accident management techniques
Nuclear Engineering International
July 1988

Blackman, 1988

H.S. Blackman et al.
The need and direction of a human factors research program for the nuclear power industry
Proceedings of the International ANS/ENS Topical Meeting on
Thermal Reactor Safety
San Diego, U.S.A.
February 2-6, 1988

Boesebeck, 1978

K. Boesebeck
Schadenswahrscheinlichkeiten für Reaktordruckbehälter abgeleitet aus den Schadensstatistiken für Druckbehälter aus dem konventionellen Bereich
TÜ 19, Nr.10, p. 281-284, 1978

Bohn, 1988

Th. Bohn (Ed.)
Kernkraftwerke
Handbuchreihe Energie Bd. 10
Verlag TÜV Rheinland, 1988

Boladjiev, 1988

A. Boladjiev, H. Vallerga
PSAPACK - integrated PC package for a PSA level 1, Version 2.1
IAEA Division of Nuclear Safety
October 1988

Buchalet, 1979

C. Buchalet et al.
Improvement in reactor pressure vessel reliability through assembly production
Trends in RPV and circuit development, p.295-301, 1979

Carachalios, 1988

C. Carachalios et al.
The Thermal Detonation Theory in Comparison with Large Scale Vapor Explosion Experiments
Proceedings of the International ANS/ENS Topical Meeting on
Thermal Reactor Safety
San Diego, U.S.A.
February 2-6, 1988

Carlsson, 1987

L. Carlsson et al.
Qualitative review of PSA characteristics
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

Casper, 1984

H. Casper (Ed.)
Wasserstoffproblematik in der Reaktorsicherheitsforschung
BMI-1984-004
1984

Chakraborty, 1988

A.K. Chakraborty et al.
An Alternate Possibility to Remove Hydrogen from the Containment Atmosphere During Severe Accidents
ANS/ENS Top. Mtg. on Operability of Nuclear Power Systems in Normal and Adverse Environments,
Albuquerque
1988

Commonwealth, 1981

Commonwealth Edison Company of Chicago
Zion probabilistic safety studies
September 1981

Corradini, 1983

M.L. Corradini et al.
Hydrogen Generation during a Core Melt - Coolant Interaction
Proc. Int. Mtg. on Light Water Reactor Severe Accident Evaluation
Cambridge, Mass.
1983

Corradini, 1988

M.L. Corradini
Comments on "An Assessment of Steam Explosion Induced Containment Failure, Parts I - IV"
Nucl. Sci. Eng. 100
1988

Cottrell, 1984

W.B. Cottrell et al.
Precursors to potential severe core damage accidents: 1980-81
A status report
NUREG/CR-3591
U.S. NRC, 1984

Crutchfield, 1988

D. Crutchfield
Individual plant examination for severe accident vulnerabilities - 10 CFR 50.54(f)
US Nuclear Regulatory Commission
Generic letter No. 88-20
letter to nuclear plant licensees,
23 November 1988

Czerjak, 1978

H. Czerjak et al.
Zusammenhang Steigerungen - Kaltrissigkeit
4.MPA-Seminar 1978

Dahl, 1988

W. Dahl et al.
Determination of fracture mechanic properties of welded joints and comparison with the failure behaviour of wide plates
12. MPA-Seminar 1988

Darlaston, 1988

B.J. Darlaston et al.
Advances in PWR structural integrity assessment and materials technology in the United Kingdom
12. MPA-Seminar 1988

DiNunno, 1982

J.J. DiNunno et al.
Calculation of distance factors for power and test reactor sites
Division of Licensing and Regulation, US Atomic Energy Commission
TID-14844, second printing, March 1962

Dougherty, 1988

E.M. Dougherty et al.
Plant modification: applying human reliability analysis to the risk assessment of McGuire nuclear station
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1988

DRS A, 1979

Deutsche Risikostudie - Kernkraftwerke
Phase A
Ed.: GRS GmbH
Verlag TÜV Rheinland, Köln, 1979

DRS A 3, 1980

Deutsche Risikostudie - Kernkraftwerke
Phase A
Fachband 3: Zuverlässigkeitsdaten und Betriebserfahrungen
Ed.: GRS GmbH
Verlag TÜV Rheinland, Köln, 1980

DRS A 4, 1980

Deutsche Risikostudie - Kernkraftwerke
Phase A
Fachband 4: Einwirkungen von außen
Ed.: GRS GmbH
Verlag TÜV Rheinland, Köln, 1980

DRS A 2/II, 1981

Deutsche Risikostudie - Kernkraftwerke
Phase A
Fachband 2/II: Zuverlässigkeitsanalyse
Ed.: GRS GmbH
Verlag TÜV Rheinland, Köln, 1981

DRS B, 1989

Deutsche Risikostudie - Kernkraftwerke
Phase B
Zusammenfassende Darstellung
Ed.: GRS GmbH
GRS-72, Juni 1989

Elliot, 1982

J. C. Elliot et al.
Assessment of Hydrogen Combustion Effects in the BWR/6-MARK II Standard Plant
Proc. Second International Conference on the Impact of Hydrogen on Water Reactor Safety
NUREG/CP-0038
1982

Ela, 1988

W.C. Ela
How artificial intelligence can help
Nuclear Engineering International
May 1988

Embrey, 1981

D.E. Embrey, R.E. Hall
Quantification of human performance using performance shaping factors
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Embrey, 1985

D.E. Embrey
SLIM-MAUD - A computer based technique for Human Reliability Assessment
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

EPRI, 1985

Analysis of the Hydrogen Burn in the TMI-2 Containment
EPRI-NP-3975
1985

Ericsson, 1981

G. Ericsson, P. Noustainen
Importance of human errors - a tool used to assign priority levels to reactor safety improvements
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Evans, 1983

N.A. Evans
The effect of core melt-coolant interactions on severe accident risks in light water reactors
Proc. Int. Mtg. Light Water Reactor Severe Accident Evaluation
Cambridge, Mass., 1983

Fischbacher, 1988

W. Fischbacher, E. Wild
Mitigation measures for severe accidents in pressurized water reactors of the Federal Republic of Germany
in: Severe accidents in nuclear power plants
Proceedings of an international symposium in Sorrento, March 21-25, 1988
IAEA, Vienna, 1988

Fleming, 1983

K.N. Fleming et al.
On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation
Nuclear Safety 24, 5
1983

Fleming, 1985

K.N. Fleming et al.
A Systematic Procedure for the Incorporation of Common Cause Events into Risk and Reliability Models
Pickard, Lowe and Garrick
PLG0427
August 1985

Fleming, 1986

K.N. Fleming et al.
A Systematic Procedure for the Incorporation of Common Cause Events into Risk and Reliability Models
Nucl. Eng. Des. 93
1986

Ford, 1982

D. Ford
The cult of the atom
Secret papers of the Atomic Energy Commission
Simon and Schuster, New York, 1982

Fouco, 1981

H.G. Fouco, P. Gagnolet
A priori and a posteriori approaches in human reliability
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Fragola, 1985

J. R. Fragola
Reliability Data Bases: the current picture
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

Friedericha, 1986

H.G. Friedericha
Unfallarten und Freisetzungsarten
Jahrestagung Kerntechnik 1986
Fachsitzung
Ergebnisse der Phase B der Deutschen Risikostudie Kernkraftwerke
1986

Garrick, 1989

B.J. Garrick
Lessons learned from 21 nuclear plant probabilistic risk assessments
Nuclear Technology, 84
March, 1989

Gazette, 1984

Gazette Nucléaire
Vol. 59/60
Paris, 1984

Gelb, 1988

M. Gelb et al.
Results of probabilistic fracture mechanics analyses for pressurized thermal shock transients in the reactor pressure vessel of Biblis-B
11. MPA-Seminar 1985

Gervasi, 1977

T. Gervasi
Arsenal of democracy
Grove Press, 1977

Gittus, 1982

J. H. Gittus
PWR Degraded Core Analysis
United Kingdom Atomic Energy Authority
ND-R-810 (S)
1982

Hardman, 1988

R. Hardman
An escalation of expectation
Nuclear Engineering International
June 1988

Haskin, 1984

F.E. Haskin et al.
Combustion induced Loads in Large Dry PWR Containments
Proc. Second Workshop on Containment Integrity
NUREG/CP-0058
1984

Haskin, 1988

F.E. Haskin et al.
Thermal-hydraulic uncertainties affecting severe accident risks in light water reactors
Proc. of the 6th Information Exchange Meeting on Debris Coolability
EPRI-NP-4455
Los Angeles, Ca., 1988

Hasemann, 1985

K. Hasemann et al.
Bildung und Verhalten brennbarer Gase bei Störfällen und schweren Unfällen in DWR
Atomenergie-Kerntechnik 47, 2
1985

Hawthorne, 1988

J.R. Hawthorne et al.
Nucl. Engineering and Design, 108, p 221-232, 1988

HAZ, 1988

Hannoversche Allgemeine Zeitung
February 16, 1988

Hennies, 1987

H. H. Hennies et al.
Stand der internationalen Sicherheitsforschung
INFORUM
Hrg. Deutsches Atomforum
1987

Henninge, 1985

W. Henninge et al.
Dependent Failure Analysis - A Vote for a Flexible Approach
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

vanHemann, 1981

J.L. vanHemann, R.G. Brown
Light water reactor plant status monitoring
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Heuser, 1988

F. W. Heuser
Risikountersuchungen zu Unfällen in Kernkraftwerken
10. GRS Fachgespräch
GRS 64
1988

Heuser, 1989

F. W. Heuser
Basic Aspects and Results of the German Risk Study, Phase B
Proc. Int. Topical Meeting on
Probability, Reliability, and Safety Assessment
PSA 89
Pittsburgh, Penns.
1989

Hillrichs, 1987

C. Hillrichs, G. Michael
Austausch von Kernfassungsschrauben in Druckwasserreaktoren
in: Jahrestagung Kerntechnik '87
Tagungsbericht, p.703-706
Deutsches Atomforum 1987

Hirsch, 1985

D. Hirsch et al.
Nuclear terrorism: a growing threat
A report to the Advisory Committee on Reactor Safeguards of the U.S. NRC
SPNP-85-P-1, Rev.1, 1985

Goedecke, 1982

R. Goedecke
Zusammenfassung und Kritik der Modelle zur Brennstoff-Natrium-Reaktion (BNR)
in:
Aufstellung und Zusammenfassung der Arbeiten im Bereich "Core Disruptive Accidents - CDA " der risikoorientierten Studie zum SNR-300 aus dem Zeitraum September - Dezember 1981
Forschungsgruppe Schneller Brüter
1982

GDK, 1987

Gruppe Ökologie
Gutachten zu den Schwachstellen des KKW Stade
Hannover, 1987

Goldman, 1982

L.A. Goldman, P.R. Lobner
A review of selected methods for protecting against sabotage by an insider
NUREG/CR-2643
U.S. NRC, 1982

Grohnde, 1973

Sicherheitsbericht Kernkraftwerk Grohnde
1973

GRS, 1988

Gesellschaft für Reaktorsicherheit
Die Deutsche Risikostudie, Phase B
Kap. 8.1
GRS Jahresbericht 1988

GRS, 1987a

Gesellschaft für Reaktorsicherheit
SPIRIT - Ein Mehrprozessorsystem zur adaptiven Überwachung von Prozeßanomalien
Kap. 8.7
GRS Jahresbericht 1987

GRS, 1987b

Gesellschaft für Reaktorsicherheit
Beurteilung des Potentials zur Verhinderung brennbarer H2-Gemische bei Unfallbedingungen in LWR's unter Nutzung katalytisch wirkender Metallfolien
GRS - A - 1335
1987

Hahn, 1988

L. Hahn
Probabilistic safety analysis for Sizewell B
Proof of evidence for PaE, London
Darmstadt, August 1988

Hall, 1988

R.E. Hall
Human Reliability Assessment: Session summary
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1988

Hannaman, 1988a

G.W. Hannaman et al.
A model for assessing Human Cognitive Reliability in PRA studies
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1988

Hannaman, 1988b

G.W. Hannaman et al.
SHARP - A framework for incorporating human interactions i to PRA studies
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3812-SR
Palo Alto, California, 1988

Hannaman, 1988

G.W. Hannaman et al.
Status of EPRI's human reliability project
Proceedings of the International ANS/ENS Topical Meeting on Thermal Reactor Safety
San Diego, U.S.A.
February 2-6, 1988

Hirschberg, 1988

S. Hirschberg
Comparison of Methods for quantitative Analysis of Common Cause Failures - a Case Study
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1988

Härtner, 1986a

H. Härtner
Zuverlässigkeitsuntersuchungen für Sicherheitssysteme und ihr Vergleich mit Auswertungen von Betriebserfahrungen
10. GRS Fachgespräch
1986

Härtner, 1986b

H. Härtner et al.
German Precursor Study - methods and results
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1988

Härtner, 1987

H. Härtner
Zuverlässigkeitsuntersuchungen für Sicherheitssysteme und ihr Vergleich mit Auswertungen von Betriebserfahrungen
Haus der Technik
Vortragsveröffentlichungen 817
1987

Hudgins, 1985

C. Hudgins
Farley-2 tendon anchor head failures seen as possible generic problem
Nucleonics Week, p. 5-6, February 14, 1985

Hsu, 1987

C. Hsu
Design and construction problems at nuclear power plants
Office for the analysis and evaluation of operational data
U.S. NRC, AEOD Engineering Evaluation Report No. AEOD/E707, March 1987

IAEA, 1988

IAEA Topics
June 1988

Illies, 1977

J.H. Illies, G. Greiner
Eine lebendige Erdkraft entlang des Lauf des Rheins
Ber. Naturf. Ges., Freiburg i. Br., 67, p. 81-104, 1977

Illies, 1978

J.H. Illies et al.
The quaternary uplift of the Rhenish shield in Germany
Tectonophysics, 61, p. 197-225, 1978

Irwin, 1988

G.R. Irwin
Brittle-to-ductile transition behaviour in nuclear reactor vessel steels
NUREG/CP-0081
U.S. NRC, 1988

Itoh, 1988

M. Itoh et al.
Reducing the operator's burden with PODIA, A-PODIA and I-PODIA
Nuclear Engineering International
January 1989

Jane's, 1988

Jane's all the world's aircraft 1987-88
London/New York, 1988

Janeky, 1985

J. Janeky et al.
Erkenntnisse zum Rißwachstum unter zyklischer Thermoschocklast an einer Stutzenkante des HDR-Druckbehälters unter Korrosionseinfluß
11. MPA-Seminar 1985

Jokelmovich, 1987

V. Jokelmovich et al.
Simulator human reliability experiments
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

Jaksimovich, 1988

V. Jaksimovich, D.E. Morledge
Using simulator experiments to analyze human reliability for PRA studies
Nuclear Engineering International
January 1988

Joschek, 1981

H.I. Joschek
Risk assessment in the chemical industry
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

JTKT, 1988

Jahrestagung Kerntechnik
p. 223
1988

Ju, 1982

F.D. Ju et al.
Response of an LWR pressure vessel to severe accident loading
PVP Vol.82, 1982

Kastenberg, 1988

W.E. Kastenberg et al.
Findings of the peer review panel on the draft reactor risk reference document NUREG-1150
NUREG/CR-5113
U.S. NRC, 1988

Karwat, 1988

H. Karwat
Scaling and Extrpolating of Hydrogen Distribution Experiments
Proc. Third Workshop on Containment Integrity
NUREG/CP-0076
1988

Kennedy, 1988

W.G. Kennedy
Automation and artificial intelligence for increased safety
Transactions of the fourteenth water reactor safety information meeting
NUREG/CP-0081
October 27-31, 1988

Kersken, 1985

M. Kersken, H. Schüller
Zuverlässigkeit der Hard- und Software von Rechnern
Haus der Technik
Vortragsveröffentlichungen 504
1985

Kersting, 1988

E. Kersting, J. Rohde
Analysis of selected accident management measures for a PWR in the FRG
in: Severe accidents in nuclear power plants
Proceedings of an international symposium in Sorrento, March 21-25, 1988
IAEA, Vienna, 1988

Knee, 1981

H.E. Knee et al.
The nuclear power plant maintenance personnel reliability prediction (NPP/MPRP) effort at Oak Ridge National Laboratory
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Körber, 1985

H. Körber et al.
Contribution of Steam Explosions to the Source Term
International Atomic Energy Agency (IAEA)
Symposium on Source Term Evaluation for Accident Conditions
Columbus, Ohio
IAEA-SM-281/55
1985

Kolb, 1981

G.J. Kolb et al.
Reactor safety study methodology applications program: Oconee #3 PWR power plant
NUREG/CR-1659/2of4
U.S. NRC, 1981

Krummel, 1987 — Documents provided for a hearing during legal proceedings concerning the Krummel NPP, West Germany 1987

KTA-2201, 1978 — Sicherheitstechnische Regel des KTA (KTA 2201): Auslegung von Kernkraftwerken gegen seismische Einwirkungen, Teil 1: Grundsätze (KTA 2201, Teil 1), Fassung 6/78, C. Heymanns Verlag, Köln 1978

KTA-3201.2, 1984 — Sicherheitstechnische Regel des KTA (KTA 3201.2): Komponenten des Primärkreislaufes von Leichtwasserreaktoren, Teil 2: Auslegung, Konstruktion und Berechnung, Fassung 3/84 Bundesanzeiger 37, Nr. 20a, 30 January 1985

Kumar, 1984 — R. K. Kumar
The Effect of Fan-Induced Turbulence on the Combustion of Hydrogen-Air Mixtures
Proc. Fifth Int. Mtg. Thermal Nuclear Reactor Safety, Karlsruhe
KFK 3880
1984

Kußmaul, 1978 — K. Kußmaul
Die Bewertung der Sprödbruchneigung von Feinkorn- und kaltzähen Baustählen in Vergleich zu den herkömmlichen bruchmechanischen Prüfkriterien
Angewandte Bruchmechanik, TÜV-Symposium, 1978

Kußmaul, 1978 — K. Kußmaul
Die Gewährleistung der Umschließung
atw p.354-360, 1978

Kußmaul, 1988 — K. Kußmaul et al.
Einige Folgerungen aus dem derzeitigen Stand des Forschungsvorhabens Komponentensicherheit FSK II für die Sicherheitsbeurteilung rißbehafteter Bauteile
12. MPA-Seminar, 1988

Kußmaul, 1987 — K. Kußmaul et al.
Assurance of the pressure vessel integrity with respect to irradiation embrittlement - Activities in the FRG
IAEA meeting 1987

Lee, 1985 — P. Lee
Overpressurization of emergency core cooling systems in Boiling Water Reactors
Office for Analysis and Evaluation of Operational Data, U.S.NRC
AEOD/C502
1985

Langer, 1984 — G. Langer et al.
Möglichkeiten zur Wasserstoffbeseitigung, Phase 2: Wasserstoffbeherrschung bei hypothetischen schweren Unfällen in DWR
BMI-1984-027
1984

Langer, 1988 — G. Langer
Möglichkeiten zur Wasserstoffbeseitigung, Phase III/2: Gesteuerte Zündung als Maßnahme zur Wasserstoffbeseitigung bei hypothetischen schweren Unfällen in DWR
BMI-1988-088
1988

Lanore, 1987 — J.M. Lanore et al.
Interaction between thermal/hydraulics, human factors and system analysis for assessing feed and bleed risk benefits
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

LaRosa, 1988 — T.P. LaRosa, J.B. Hickman
Handling emergencies with the NRC's real time plant data link
Nuclear Engineering International
July 1987

Legasov, 1988 — K.M. Legasov
"Memoire" as quoted in Nucleonics Week
June 9, 1988

Lewis, 1975

H.W. Lewis et al.
Report to the American Physical Society by the study group on light water reactor safety
Reviews of Modern Physics, Vol. 47, Suppl.No.1, Summer 1975

Lewis, 1978

H.W. Lewis et al.
Risk assessment review group report to the U.S. Nuclear Regulatory Commission
NUREG/CR-0400
U.S. NRC, 1978

Libe, 1988

Libération
28/27 november 1988
Paris

Lindackers, 1982

K.H. Lindackers
Leistungsfähigkeit, Anwendungsgrenzen und Weiterentwicklungsmöglichkeiten von Methoden und Modellen der Risiko- und Sicherheitsforschung
Int. Symp. über Risiko- und Sicherheitsforschung, Bonn, 6-8 July, 1982

Lobner, 1982

P. Lobner
Nuclear power plant damage control measures and design changes for sabotage protection
NUREG/CR-2585
U.S. NRC, 1982

Logatchev, 1978

N.A. Logatchev et al.
Deep structure and evolution of the Baikal Rift zone
In: I.B. Ramberg, E.R. Neumann (Ed.): "Tectonics and geophysics of continental rifts", Dordrecht, p. 48-61, 1978

Lopez, 1987

H.F. Lopez
Underclad cracking of pressure vessel steels for LWRs
Scripta Met., 21, p.753-758, 1987

Lyon, 1987

W. Lyon
Steam generator tube rupture during severe accidents at Seabrook Station
Facilities Operations Branch, NRC
Memorandum to C.E. Rossi, Division of PWR Licensing-A, NRC, 3 March 1987

Mancini, 1988

G. Mancini
Collection, Processing and Use of Data
Nucl. Eng. Des. 88
1988

Marshall, 1982

W. Marshall
An assessment of the integrity of pressurized water reactor pressure vessels
The Marshall Study Group
UKAEA
Second Report, 1982

Marshall, 1988

B. W. Marshall
Comments on "An Assessment of Steam Explosion Induced Containment Failure, Parts I - IV"
Nucl. Sci. Eng. 100
1988

Marston, 1980

T.U. Marston, K.E. Stahlkopf
Radiation embrittlement: significance of its effects on integrity and operation of PWR pressure vessels
Nuclear Safety, Vol. 21, No.6, Nov./Dec. 1980

Hartz, 1984

H.F. Hartz, J.W. Johnson
Assessing compatibility with reactor safety goals using uncertain risk analysis results with application to core melt
Nuclear Safety, 25, No.3, May-June 1984

Hayinger, 1982

F. Hayinger
Wie sind Dampfexplosionen im Lichte neuerer Erkenntnisse zu beurteilen?
Atomwirtschaft
Februar 1982

Heslin, 1989

S.T. Heslin
Analysis and Quantification of Common-Cause Failures on the Basis of Operating Experience
Nuclear Technology 84
1989

MHB, 1988

MHB Technical Associates
Severe accidents at Three Mile Island unit 1
San Jose, Cal.
February 1988

Miller, 1987

M.K. Miller et al.
Characterization of irradiated A 5338 pressure vessel steel weld
Journal de Physique, 48, p.429-434, 1987

Minarick, 1982

J.W. Minarick, C.A. Kukielka
Precursors to potential severe core damage accidents: 1969-1979. A status report
NUREG/CR-2497
U.S. NRC, 1982

Minarick, 1986

J.W. Minarick et al.
Precursors to potential severe core damage accidents: 1985. A status report
NUREG/CR-4674
U.S. NRC, 1986

Minarick, 1987

J.W. Minarick et al.
Precursors to potential severe core damage accidents: 1984. A status report
NUREG/CR-4674
U.S. NRC, 1987

Minarick, 1988

J.W. Minarick et al.
Precursors to potential severe core damage accidents: 1986. A status report
NUREG/CR-4674
U.S. NRC, 1988

Moldaschl, 1988

M. Moldaschl
Bedingungen, unter denen Menschen nur noch "versagen" können
in: Frankfurter Rundschau
December 24, 1988

Morani, 1988

J.M. Morani et al.
Probabilistic safety assessment: Total loss of the heat sink in a PWR - Electicite de France
Proceedings of the International ANS/ENS Topical Meeting on Thermal Reactor Safety
San Diego, U.S.A.
February 2-8, 1988

Mosleh, 1988

A. Mosleh, G. Apostolakis
The development of a generic data base for failure rates
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1988

Mosleh, 1988

A. Mosleh
Hidden Sources of Uncertainty: Judgment in the Collection and Analysis of Data
Nucl. Eng. Des. 88
1988

Mosleh, 1987

A. Mosleh et al.
The elicitation and use of expert opinion in risk assessment: a critical overview
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

Mundry, 1982

E. Mundry
Die Bestimmung von Fehlerart und Fehlergröße mittels zerstörungsfreier Prüfung - Möglichkeiten und Grenzen
Schweißtechnik, 6, p.112, 1982

Naus, 1988

D.J. Naus
Concrete component aging and its significance relative to life extension of nuclear power plants
NUREG/CR-4652
U.S. NRC, 1988

NEA/IRS 508, 1985

NEA Incident Reporting System
No. 508: Hatch incidents at operating 900 MWe units / France
Distributed October 24, 1985

NEA/IRS 576, 1988

NEA Incident Reporting System
No. 576: Control rod faults / France
Distributed April 30, 1988

NEA/IRS 577, 1988

NEA Incident Reporting System
No. 577: Failure of the reactor trip system / France
Distributed April 30, 1988

NEA/IRS 614, 1988

NEA Incident Reporting System
No. 614: Failure of a safety injection pump during a pump testrun due to gas binding / FRG
Distributed April 7, 1988

Neddermann, 1988

J. Neddermann
Can computers replace power plant operators ?
Nuclear Engineering International
May 1988

Nelson, 1981

W.R. Nelson
Decision making in the reactor control room
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

NRC, 1977a

Nuclear Regulatory Commission
Mark I containment short term program
Safety evaluation report
NUREG-0408
U.S. NRC, 1977

NRC, 1977b

Nuclear Regulatory Commission
Regulatory Guide 1.99
Rev. 1/1977
U.S. NRC, 1977

NRC, 1982a

NRC report on the January 25, 1982 steam generator tube rupture at R.E. Ginna nuclear power plant
NUREG-0909
U.S. NRC, 1982

NRC, 1982b

Nuclear Regulatory Commission
PRA Procedures Guide
NUREG/CR-2300
U.S. NRC, 1982

NRC, 1982c

Nuclear Regulatory Commission
Power Reactor Events
NUREG/BR-0051
Vol.4, No.2
U.S. NRC, January/February 1982

NRC, 1985

Nuclear Regulatory Commission
Management of severe accidents
NUREG/CR-4177
U.S. NRC, 1985

NRC, 1988a

Nuclear Regulatory Commission
10 CFR 50 Appendix A: General design criteria for nuclear power plants
U.S. NRC, 30 April 1988

NRC, 1988b

Nuclear Regulatory Commission
10 CFR 50: Safety goals for the operation of nuclear power plants; policy statement; republication
Federal Register, p 30028-30033,
21 August 1988

NRC, 1988c — Nuclear Regulatory Commission
Wrong Unit/ Wrong Train Events 1981 - 1985
Memo by F.J. Hebdon to W.T. Russell
U.S. NRC, February 13, 1988

NRC, 1989a — NRC News Releases
No. 89-12
January 24, 1989

NRC, 1989b — NRC News Releases
April 11, 1989

NRC, 1989c — U.S. Nuclear Regulatory Commission
NRC Information Notice No. 89-28
Instrument Air Supply to Safety-Related Equipment
March 7, 1989

NRC, 1989d — NRC News Releases
July 25, 1989

NSAC, 1984 — Nuclear Safety Analysis Center and Duke Power Company
Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3
NSAC/60, 1984

NucEng, 1988a — Nuclear Engineering International
May 1988

NucEng, 1988b — Nuclear Engineering International
June 1988

NucEng, 1988c — Nuclear Engineering International
p.23
October 1988

NucEng, 1989a — Nuclear Engineering International
p. 14-17, February 1989

NucEng, 1989b — Nuclear Engineering International
April 1989

Nucleek, 1989a — Nucleonics Week
January 12, 1989

Nucleek, 1989b — Nucleonics Week
January 19, 1989

Nucleek, 1989c — Nucleonics Week
March 2, 1989

Nucleek, 1989J — Nucleonics Week
May 25, 1988

Nuke, 1989 — Nuke Info Tokyo
No. 10
April/May 1989

NUREG-1150, 1987 — Nuclear Regulatory Commission
Reactor Risk Reference Document
Draft
NUREG-1150
U.S. NRC, 1987

NUREG-1150/2, 1989 — Nuclear Regulatory Commission
Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants
Second Draft for Peer Review
NUREG-1150
U.S. NRC, 1989

Öko, 1983 — Öko-Institut
Risikountersuchungen zu Leichtwasserreaktoren
Freiburg, 1983

Öko, 1987
Öko-Institut
Untersuchung über die Sicherheit der in Hamburger Umland gelegenen Kernkraftwerke Brokdorf, Brunsbüttel, Krümmel und Stade
Teil 1
1987

Öko, 1988
Öko-Institut
Untersuchung über die Sicherheit der in Hamburger Umland gelegenen Kernkraftwerke Brokdorf, Brunsbüttel, Krümmel und Stade
Teil 2
1988

Oh, 1987
M.D. Oh et al.
A propagation/expansion model for large scale vapour explosions
Nuc. Sc. Eng., 98
1987

Okrent, 1981
D. Okrent
Nuclear reactor safety
On the history of the regulatory process
The University of Wisconsin Press, 1981

Onodera, 1977
S. Onodera et al.
Advantages in application of integrated flange forgings for reactor vessels
3. MPA-Seminar, 1977

Orvis, 1985
D.D. Orvis et al.
Treatment of system dependencies and human interactions in PRA studies: a review and sensitivity study
Proceedings: International Topical Meeting on Probabilistic Safety Methods and Applications
EPRI NP-3912-SR
Palo Alto, California, 1985

Pedersen, 1981
O.M. Pedersen et al.
Classifying and quantifying human error in routine tasks in nuclear power plants
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Pelto, 1985
P.J. Pelto et al.
Reliability analysis of containment isolation systems
NUREG/CR-4220
U.S. NRC, 1985

Pepper, 1989
J.W. Pepper, G.W. Reeley
Employing microprocessor based digital reactor protection at Sizewell B
Nuclear Engineering International
January 1989

Phung, 1983
D.L. Phung
Pressure vessel thermal shock at U.S. pressurized-water reactors: events and precursors, 1963-1981
NUREG/CR-2789
U.S. NRC, 1983

PLG, 1983
Pickard, Lowe and Garrick, Inc.
Seabrook Station probabilistic safety assessment
Main report, PLG-0300
1983

PLG, 1987
Pickard, Lowe and Garrick, Inc.
Three Mile Island Unit 1 Probabilistic Risk Assessment
PLG-0525
1987

Pope, 1986
R.H. Pope
Human Performance: What improvement from Human Reliability Assessment
EUREDATA Conference
1986

Potash, 1981

L.H. Potash et al.
Experience in integrating the operator contributions in the PRA of actual operating plants
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Poucet, 1987

A. Poucet et al.
European Benchmark Exercise on Common Cause Failure Analysis
Probabilistic Safety Assessment and Risk Management / PSA 87
Köln: Verlag TÜV Rheinland
1987

Prassinos, 1988

P.G. Prassinos
Evaluation of external hazards to nuclear power plants in the United States - seismic hazard
NUREG/CR-5042, Supplement 1, U.S. NRC, April 1988

Profil, 1978

Profil-Gespräch
44, p.21, 1978

Rasmussen, 1979

J. Rasmussen
On the structure of knowledge - A morphology of mental models in a man-machine context
Risø-M-2192
Roskilde, Denmark, 1979

Reierson, 1988

C. Reierson, E. Marshall
Evaluating operator support systems in realistic conditions at HAMBLAB
Nuclear Engineering International
January 1988

Richardson, 1985

D. Richardson
Kampfflugzeuge heute und morgen
Motorbuch-Verlag, Stuttgart 1985

Rintillä, 1987

E. Rintillä
Replacing the process computer systems at Finland's Loviisa PWR
Nuclear Engineering International
July 1987

Rühle, 1973

R. Rühle et al.
Verhaltensvariabilität des Menschen als Unfallursache
Analyse und Abwehr verhaltensbedingter Arbeitsunfälle
Inst. für Arbeitswissenschaft, TU Berlin
Forschungsberichte No. 113
Dortmund, 1973

Roller, 1982

S. F. Roller et al.
Medium-Scale Combustion Tests of H2-Air-Steam Systems
Proc. Second International Conference on the Impact of Hydrogen on Water Reactor Safety
NUREG/CP-0038
1982

Roos, 1986a

Roos et al.
On the influence of the material toughness and the state of stress on fracture of large specimens
12. MPA-Seminar, pp 30ff, 1986

Roos, 1986b

Roos et al.
Classification and characterization of materials by means of fracture mechanics parameters
12. MPA-Seminar, pp 34ff, 1986

Rossi, 1989

C. E. Rossi
Failure of Westinghouse steam generator tube mechanical plugs
Office of Nuclear Reactor Regulation, U.S.NRC
NRC Bulletin No. 89-01
1989

Rowsome, 1982

F. Rowsome
Internal NRC memorandum to James Meyer, titled "Damage State Likelihoods for Indian Point"
2 December, 1982

RS 217, 1978

RS 217
Schadensstatistische Auswertungen zum Versagen mechanisch beanspruchter Bauteile konventioneller Druckbehälter
TÜV-Arbeitsgemeinschaft Kerntechnik West, 1978

RSK, 1987

Bundesanzeiger
Bekanntmachung von Empfehlungen der Reaktorsicherheitskommission
March 5th and August 14th
1987

Rubin, 1984

S. D. Rubin
Case study report for the Edwin I. Hatch Unit No. 2 plant systems interaction event on August 25, 1982
Office for Analysis and Evaluation of Operational Data, U.S.NRC
AEOD/C403
1984

Ryan, 1985a

T.G. Ryan et al.
The adequacy of human reliability data for addressing risk reduction issues at commercial nuclear power plants
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1985

Ryan, 1985b

M.L. Ryan
Millstone-2 steam generator cleaning unmasks unexpected defects
Nucleonics Week, p.6, April 25, 1985

Sabri, 1981

Z.A. Sabri et al.
Assessment of human contributions to significant trends based on LWR past operating experience
in: Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment
Port Chester, New York
September 20-24, 1981

Samanta, 1985

P.K. Samanta
Multiple sequential failure model: A probabilistic approach to quantifying human error dependency
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1985

Schurman, 1985

D.L. Schurman
Do we need the human in human performance models?
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1985

Scott, 1981

R.L. Scott, R.B. Gallaher
Review of safety-related events at nuclear power plants as reported in 1979 Nuclear Safety
Vol.22, No.4, 1981

SERG, 1985

US Nuclear Regulatory Commission
A Review of the Current Understanding of the Potential for Containment Failure from In-Vessel Steam Explosions
NUREG-1116
1985

Shelly, 1986

S.C. Shelly, G. Thompson
The source term debate
A report by the Union of Concerned Scientists
Cambridge, Mass.
January, 1986

Shunsugavel, 1986

P. Shunsugavel et al.
An Evaluation of Structural Failure Modes for Prestressed Concrete Containments
Proc. Third Workshop on Containment Integrity
NUREG/CP-0076
1986

Silberberg, 1988

M. Silberberg et al.
Reassessments of the technical bases for estimating source terms
NUREG-0956
U.S. NRC, 1986

Simonen, 1986

F.A. Simonen et al.
Reactor pressure vessel failure probability following through-wall cracks due to pressurized thermal shock events
NUREG/CR-4483
U.S. NRC, 1986

SKI-ASAR, 1985

SKI-ASAR
Periodic safety review Barsebäck 1/Barsebäck 2
SKI-ASAR-81/82, 1985

Smidt, 1979

D. Smidt
Reaktorsicherheitstechnik
Springer Verlag Berlin, 1979

SNL, 1986

Sandia National Laboratories
MECTR. Version 1.5
User's Manual
NUREG/CR-4507
1986

Sonoda, 1987

N. Sonoda
Kansai applies experience through an expert system
Nuclear Engineering International
July 1987

SR 10, 1976

Forschungsprogramm SR 10
Zentrale Auswertung von Herstellungsfehlern und Schäden in Hinblick auf druckführende Anlagenteile von Kernkraftwerken
MPA-Bericht, Auftrags-Nr. 810 034/1
1976

Stahlberg, 1977

Stahlberg
Anwendungsmöglichkeiten und Anwendungsgrenzen bruchmechanischer Methoden bei der Beurteilung der Sicherheit von Bauteilen
Dissertation, RWTH Aachen, 1977

Stecklow, 1984

S. Stecklow, R. Heidorn
Limerick: the costly legacy of a choice made long ago
Philadelphia Inquirer
13 August 1984

Sütterlin, 1975

L. Sütterlin
Zur Auslegung kerntechnischer Anlagen gegen Einwirkungen von außen
Institut für Reaktorsicherheit, IRS-W-12
März 1974

Sugnet, 1984

W.R. Sugnet et al.
Oconee PRA: A probabilistic risk assessment of Oconee Unit 3
Nuclear Safety Analysis Center and Duke Power Company
June 1984

Swain, 1963

A.D. Swain
A method of performing a human factors reliability analysis
Report SCR-685
Sandia Corporation
Albuquerque, 1963

Swain, 1983

A.D. Swain, H.E. Guttmann
Handbook of human reliability analysis with emphasis on nuclear power plant applications
NUREG/CR-1278
US NRC, 1983

Swenson, 1981

D. V. Swenson et al.
Monte Carlo Analysis of LWR Steam Explosions
Sandia National Laboratories
NUREG CR/2307
1981

Tarbell, 1982
W.W. Tarbell et al.
Hydrogen production during fragmented debris/ concrete interactions
Proc. Second International Conference on the Impact of Hydrogen on Water Reactor Safety
NUREG/CP-0038
1982

Theofanous, 1988
T.G. Theofanous et al.
An Assessment of Steam Explosion Induced Containment Failure, Parts I - IV
Nucl. Sci. Eng. 97
1987

Thompson, 1983
G. Thompson
Sizewell B public inquiry: safety and waste management implications of the Sizewell PWR
Appendix G
Prepared for TCPA, November 1983

Tosetti, 1981
R. J. Tosetti et al.
Evaluation of the H2 Combustion and Control under Degraded Core Conditions for Pilgrim-2
Proc. Workshop on the Impact of Hydrogen on Water Reactor Safety
NUREG/CR-2017
1981

TÜV, 1974
TÜV
Stellungnahme zu den Verunreinigungen in den Mantelblechen des Reaktordruckbehälters Krümmel
MP 27.8.3; 8.15; 8.20; 8.35
1974

TÜV, 1975a
TÜV
Stellungnahme zur Festigkeit der Bleche für den zylindrischen Teil des Reaktordruckbehälters Krümmel
KE 27.8.1; KE 27.8.2.1
1975

TÜV, 1975b
TÜV Meisungsbeschluß
1975

TÜV, 1985
TÜV Norddeutschland
Untersuchungen zu Ereignisabläufen mit Kernschmelzen und Aktivitätsfreisetzung in den DWR-Anlagen KKS und KBR sowie in den SWR-Anlagen KKB und KKK
1985

UCS, 1977
Union of Concerned Scientists
The risks of nuclear power reactors
Cambridge, Mass., 1977

UCS, 1978
Union of Concerned Scientists
An analysis of chairman Hendrie's response to Senator Hart's letter of June 15, 1978
December 1978

Vavrek, 1988
Sensitivity Study of Common Mode Failure Rates for Sizewell B
Proc. Int. Top. Mtg. on Probabilistic Safety Methods and Applications
EPRI NP 3912-SR
1985

Villemeur, 1987
A. Villemeur et al.
French PWR nuclear power plants: probabilistic studies of accident sequences and related findings
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

Wakefield, 1987
D.J. Wakefield, C.D. Adams
Quantification of dynamic human errors in the TMI-1 PRA
in: Probabilistic Safety Assessment and Risk Management/PSA'87
Ed: European Nuc. Soc. and Swiss Nuc. Soc.
Köln, Verlag TÜV Rheinland, 1987

WASH-1400, 1975

Nuclear Regulatory Commission
Reactor Safety Study
WASH-1400
NUREG-75/014
1975

Watson, 1986

Watson
Analysis of Dependent Events and Multiple Unavailabilities with particular Reference to Common-Cause Failures
Nucl. Eng. Des. 93
1986

WEC, 1982

Westinghouse Electric Corporation
Sizewell B Probabilistic Safety Study
WCAP-9991
1982

Wegner, 1989

H. Wegner et al.
Maintenance problems at nuclear power plants
Office for Analysis and Evaluation of Operational Data, U.S.NRC
AEOD/S901
1989

Werden, 1983

B. Werden
Ultrasonic testing - engineering science position and range of application
Detectability and assessment of faults - control standards
DVS, 179, 1983

Wheeler, 1989

T.A. Wheeler et al.
Analysis of core damage frequency from internal events: expert judgment elicitation
NUREG/CR-4550
U.S. NRC, 1989

Williams, 1987

D.C. Williams et al.
Containment loads due to direct containment heating and associated hydrogen behavior: analysis and calculations with the CONTAIN code
NUREG/CR-4896
U.S. NRC, 1987

Williams, 1988

R.D. Williams
Integrating core design and monitoring on the desktop
Nuclear Engineering International
December 1988

WISE, 1989a

WISE News Communique
No. 307
Amsterdam, 1989

WISE, 1989b

WISE News Communique
No. 309
Amsterdam, 1989

Worledge, 1985

D.H. Worledge
Some useful characteristics of performance models
in: Conference Record on
IEEE Third Conference on Human Factors and Nuclear Safety
Monterey, California
June 23-27, 1985

TABLES AND FIGURES

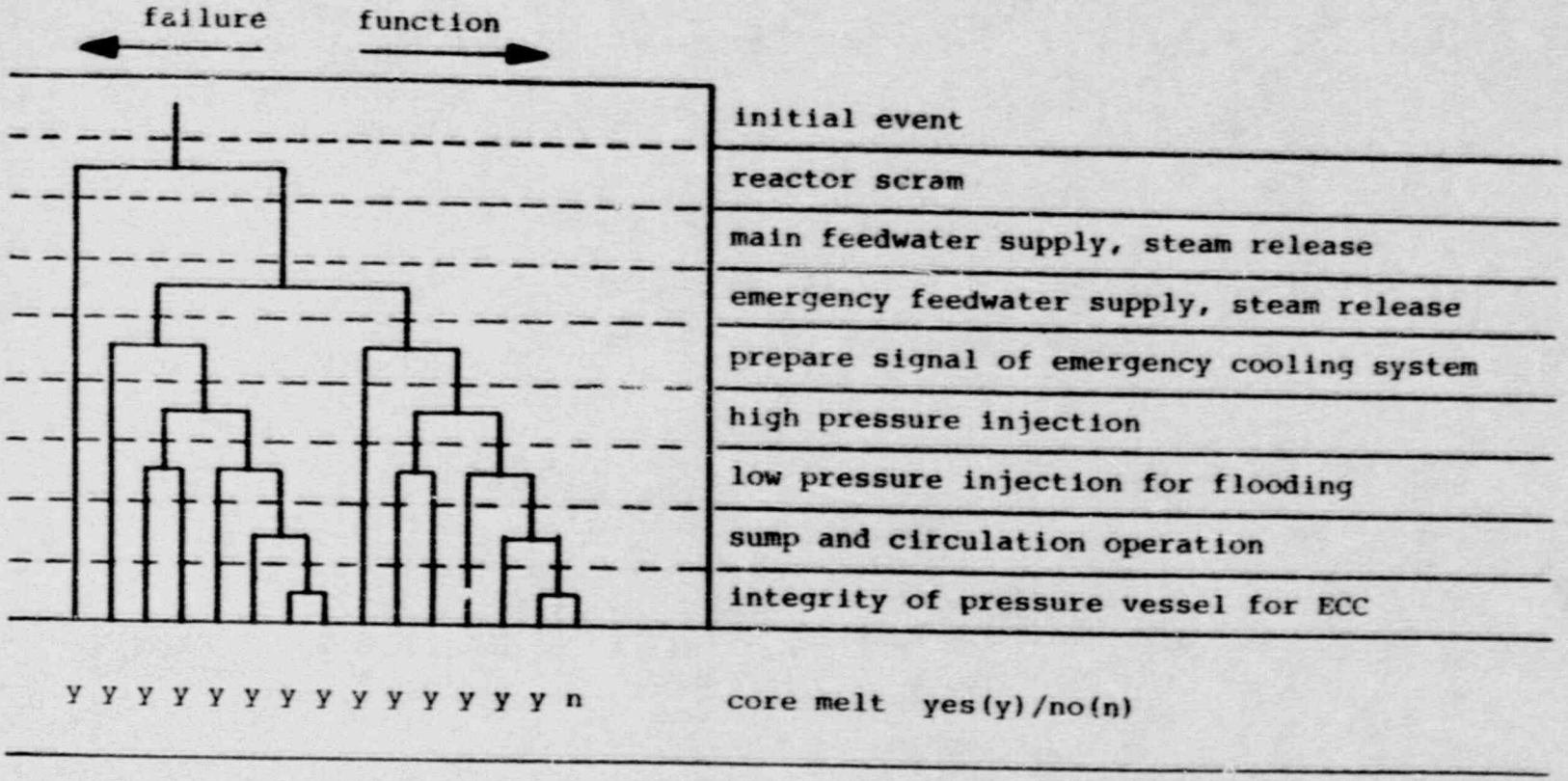


Fig. 1.1: Event Tree for "small-break LOCA" (DRS A, 1979)

Table 2.1: **Summary of accidents involving core (WASH-1400, 1975)**

RELEASE CATEGORY	PROBABILITY per Reactor-Yr	TIME OF RELEASE (Hr)	DURATION OF RELEASE (Hr)	WARNING TIME FOR EVACUATION (Hr)	ELEVATION OF RELEASE (Meters)	CONTAINMENT ENERGY RELEASE (10^6 Btu/Hr)	FRACTION OF CORE INVENTORY RELEASED[a]							
							Xe-Kr	Org. I	I	Cs-Rb	Te-Sb	Ba-Sr	Ru[b]	La[c]
PWR 1	9×10^{-7}	2.5	0.5	1.0	25	520[d]	0.9	6×10^{-3}	0.7	0.4	0.4	0.05	0.4	3×10^{-3}
PWR 2	8×10^{-6}	2.5	0.5	1.0	0	170	0.9	7×10^{-3}	0.7	0.5	0.3	0.06	0.02	4×10^{-3}
PWR 3	4×10^{-6}	5.0	1.5	2.0	0	6	0.8	6×10^{-3}	0.2	0.2	0.3	0.02	0.03	3×10^{-3}
PWR 4	5×10^{-7}	2.0	3.0	2.0	0	1	0.6	2×10^{-3}	0.09	0.04	0.03	5×10^{-3}	3×10^{-3}	4×10^{-4}
PWR 5	7×10^{-7}	2.0	4.0	1.0	0	0.3	0.3	2×10^{-3}	0.03	9×10^{-3}	5×10^{-3}	1×10^{-3}	6×10^{-4}	7×10^{-5}
PWR 6	6×10^{-6}	12.0	10.0	1.0	0	N/A	0.3	2×10^{-3}	9×10^{-4}	8×10^{-4}	1×10^{-3}	9×10^{-5}	7×10^{-5}	1×10^{-5}
PWR 7	4×10^{-5}	10.0	10.0	1.0	0	N/A	6×10^{-3}	2×10^{-5}	2×10^{-5}	1×10^{-5}	2×10^{-5}	1×10^{-6}	1×10^{-6}	2×10^{-7}
PWR 8	4×10^{-5}	0.5	0.5	N/A	0	N/A	2×10^{-3}	5×10^{-6}	1×10^{-4}	5×10^{-4}	1×10^{-6}	1×10^{-8}	0	0
PWR 9	4×10^{-4}	0.5	0.5	N/A	0	N/A	3×10^{-6}	7×10^{-9}	1×10^{-7}	6×10^{-7}	1×10^{-9}	1×10^{-11}	0	0
BWR 1	1×10^{-6}	2.0	2.0	1.5	25	130	1.0	7×10^{-3}	0.40	0.40	0.70	0.05	0.5	5×10^{-3}
BWR 2	6×10^{-6}	30.0	3.0	2.0	0	30	1.0	7×10^{-3}	0.90	0.50	0.30	0.10	0.03	4×10^{-3}
BWR 3	2×10^{-5}	30.0	3.0	2.0	25	20	1.0	7×10^{-3}	0.10	0.10	0.30	0.01	0.02	3×10^{-3}
BWR 4	2×10^{-6}	5.0	2.0	2.0	25	N/A	0.6	7×10^{-4}	8×10^{-4}	5×10^{-3}	4×10^{-3}	6×10^{-4}	6×10^{-4}	1×10^{-4}
BWR 5	1×10^{-4}	3.5	5.0	N/A	150	N/A	5×10^{-4}	2×10^{-9}	6×10^{-11}	4×10^{-9}	9×10^{-12}	8×10^{-14}	0	0

(a) A discussion of the isotopes used in the study is found in Appendix VI. Background on the isotope groups and release mechanisms is found in Appendix VII.

(b) Includes Mo, Rh, Tc, Co.

(c) Includes Nd, Y, Ce, Pr, La, Nb, Am, Cm, Pu, Np, Zr.

(d) A lower energy release rate than this value applies to part of the period over which the radioactivity is being released. The effect of lower energy release rates on consequences is found in Appendix VI.

Table 2.2: Results of US PRAs (MHB, 1989)

Plant Name (PRA Vintage)	Internal Events Core Melt Frequency (per Ry)	External Events Core Melt Frequency (per Ry)
BABCOCK & WILCOX PWRs		
Three Mile Island 1 (1987)	4.4×10^{-4}	1.1×10^{-4}
Oconee 3 (1981)	8.0×10^{-5}	N.A.
Oconee 3 (1984)	5.4×10^{-5}	2.0×10^{-4}
Arkansas 1 (1982)	5.0×10^{-5}	N.A.
Crystal River 3 (1981)	4.0×10^{-4}	N.A.
Crystal River 3 (1987)	3.7×10^{-5}	N.A.
Midland (1984)	2.8×10^{-4}	3.1×10^{-5}
WESTINGHOUSE PWRs		
Indian Point 2 (1982)	2.9×10^{-4}	6.0×10^{-5}
Indian Point 2 (1982)	7.9×10^{-5}	6.1×10^{-5}
Indian Point 3 (1982)	3.3×10^{-4}	1.5×10^{-5}
Indian Point 3 (1982)	1.3×10^{-4}	1.0×10^{-5}
Seabrook 1 (1983)	1.7×10^{-4}	5.8×10^{-5}
Millstone 3 (1984)	4.5×10^{-5}	1.4×10^{-5}
Sequoyah 1 (1981)	5.6×10^{-5}	N.A.
Sequoyah 1 (1984)	9.1×10^{-5}	N.A.
Sequoyah 1 (1987)	1.0×10^{-4}	N.A.
Zion 1 (1981)	5.7×10^{-5}	1.0×10^{-5}
Zion 1 (1984)	3.2×10^{-5}	N.A.

Table 2.2 (continued)

Plant Name (PRA Vintage)	Internal Events Core Melt Frequency (per R_y)	External Events Core Melt Frequency (per R_y)
Zion 1 (1987)	1.5×10^{-4}	N.A.
Surry 1 (1975)	6.0×10^{-5}	N.A.
Surry 1 (1987)	2.6×10^{-5}	N.A.
Haddam Neck (1986)	1.7×10^{-4}	3.8×10^{-4}
COMBUSTION ENGINEERING PWRs		
Calvert Cliffs 1 (1980)	1.5×10^{-3}	N.A.
Calvert Cliffs 2 (1982)	1.3×10^{-4}	N.A.
GENERAL ELECTRIC BWRs		
Browns Ferry * (1982)	2.0×10^{-4}	N.A.
Peach Bottom (1975)	3.0×10^{-5}	N.A.
Peach Bottom (1984)	3.6×10^{-5}	N.A.
Peach Bottom (1987)	8.2×10^{-6}	N.A.
Grand Gulf (1981)	3.6×10^{-5}	N.A.
Grand Gulf (1984)	8.3×10^{-6}	N.A.
Grand Gulf (1987)	2.8×10^{-5}	N.A.
Millstone 1 (1983)	3.0×10^{-4}	N.A.
Milktone 1 (1985)	8.1×10^{-4}	N.A.
Limerick (1981/1983)	1.5×10^{-5}	9.1×10^{-6}
Limerick (1984)	8.5×10^{-5}	9.1×10^{-6}
GESSAR-II (1982)	4.3×10^{-6}	6.0×10^{-7}
GESSAR-II (1985)	3.8×10^{-5}	6.7×10^{-5}
Oyster Creek (1980)	4.8×10^{-5} (total)	

K_{IR}	reference value for fracture toughness
KRR	Kernkraftwerk (nuclear power plant) Krümmel, F.R.G.
KKS	Kernkraftwerk (nuclear power plant) Stade, F.R.G.
KTA	Kerntechnischer Ausschuß, F.R.G.
KWU	Kraftwerk Union, F.R.G.
L(J/1)	likelihood-function for J given 1
LEFM	linear elastic fracture mechanics
LER	licensee event report
LLNL	Lawrence Livermore National Laboratory, U.S.
LOCA	loss-of-coolant accident
LOFW	loss of feedwater
LOOP	loss of offsite power
LWR	light water reactor
M	median
MDFF	multiple dependent failure fraction
MGL	multiple Greek letter
MSIV	main steam isolation valve
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission, U.S.
OSART	operational safety review team
P	reactor thermal power
PISC	plate inspection steering committee
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PSA	probabilistic safety assessment
PSAPACK	integrated PC package for PSA level I
PSF	performance shaping factor
PWR	pressurized water reactor
QA	quality assurance
QC	quality control
R	exclusion radius
RCIC	reactor core isolation cooling
RCS	reactor coolant system
RPV	reactor pressure vessel
RSK	Reaktorsicherheitskommission (reactor safety commission, F.R.G.)
RT	reactor trips
RT	room temperature
S_m	design stress level
SCD	severe core damage
SCDF	severe core damage frequency
SERG	steam explosion review group
SG	steam generator
SGTR	steam generator tube rupture
SI	safety injection
SKI	Statens Kärnkraftinspektion (Swedish Nuclear Power Inspectorate)
SRV	safety relief valve
T_{NDT}	nil-ductility transition temperature
THERP	technique for human error rate prediction
TMI	Three Miles Island
TÜV	Technischer Überwachungsverein, F.R.G.
VVER-440	Soviet type pressurized water reactor, 440 MWe

2,5E-4	$2,5 \times 10^{-4}$ etc.

ABBREVIATIONS:

AEC	Atomic Energy Commission, U.S.
AECB	Atomic Energy Control Board, Canada
AFW	auxiliary feedwater
AI	artificial intelligence
AM	accident management
ASAR	as operated safety analysis report
ASME	American Society of Mechanical Engineers
ASP	accident sequence precursor
ATWS	anticipated transient without scram
BFR	binominal failure rate
BNL	Brookhaven National Laboratory
BPM	basic parameter model
BWR	boiling water reactor
CCF	common base failures
CEGB	Central Electricity Generating Board, U.K.
COD	crack-opening-displacement
CRT	cathode ray tube
CSR	containment spray recirculation
DBA	design basis accident
DBTT	ductile-brittle transition temperature
DCH	direct containment heating
DG	diesel generator
DOB	degree of believe
DRS	Deutsche Risikostudie
E	mean or expectation value
ECF	early containment failure
EdF	Electricité de France
EP	emergency power
EPRI	Electric Power Research Institute, U.S.
ERDS	European Reliability Data System
F_5	5%-fractile
F_{95}	95%-fractile
f(I)	probability density function of I without knowledge of J (prior distribution)
f(I/J)	probability density function of I, given the information J (posterior distribution)
FCI	fuel coolant interaction
FSAR	final safety analysis report
HAZ	heat affected zone
HCR	human cognition reliability
HEP	human error probability
HPI	high pressure injection
HPME	high pressure melt ejection
HPR	high pressure recirculation
HPS	high pressure sequence
HRA	human reliability analysis
HWR	heavy water reactor
IAEA	International Atomic Energy Agency
INPO	Institute of Nuclear Power Operations
J_i	crack initiation value (from elasto-plastic J-integral theory)
K ($=K_{95}$)	variation factor of lognormal distribution
K_{Ia}	stress intensity for crack arrest
K_{Ic}	fracture toughness (critical stress intensity)

It will be noted from table 17.1 that the NRC does not regard any of these events as meeting its formal definition of sabotage, which is: "deliberate attempts to endanger public health and safety". This definition is, however, much too narrow. Events have occurred at US nuclear plants which could have initiated a core melt accident or could have been an important part of a core melt accident sequence. In the context of PRA, these events must be counted as sabotage.

Sabotage-related events at nuclear plants have also been recorded in many other countries. Appendix 17A summarizes the events which were identified in a review performed in 1983. The list of events in Appendix 17A is incomplete and excludes acts of war (such as Iranian and Israeli aerial attacks on Iraq's Tammuz-1 research reactor in 1980 and 1981). It shows, however, that nuclear plants have been a focus for violence or severe employee disaffection in many countries.

Some fear that the incidence of sabotage -- at least that of terrorist origin -- may increase. Figures 17.1 and 17.2 are suggestive in this respect. These figures show an increasing trend in the number of terrorist events worldwide over the past two decades, and a growing number of bombings of nuclear facilities outside the United States during the late 1970s and early 1980s. Whether or not such indicators rise over coming years, they point clearly to a serious potential danger.

17.3 PROSPECTS FOR REDUCING THE IMPORTANCE OF SABOTAGE

In the United States and elsewhere, efforts have been made to reduce access to sensitive areas by potential saboteurs -- both insiders and outsiders. Also, a number of plant modifications have been considered, with the objective of complicating a saboteur's task or allowing plant operators to more readily recover control of the plant after a sabotage event (eg, Andrews, 1986; Bennett, 1982; Goldman, 1982; Lobner, 1982).

Such measures create their own problems. Rigorous control of access and intense surveillance of sensitive areas will interfere with civil liberties and can reduce employee morale. Moreover, physical measures to control access (locked doors, etc.) can hinder the movement of plant personnel in an emergency, potentially exacerbating the effects of an accident. Plant modifications intended to hinder saboteurs will also hinder maintenance procedures and some emergency response actions. They may also create the opportunity for additional core melt sequences, possibly including new sabotage-induced sequences. Thus, there is no basis for believing that the importance of sabotage can be significantly reduced.

17 SABOTAGE

17.1 INTRODUCTION

To date, PRA analysts have not sought to account for the possibility of sabotage, recognizing that it is not susceptible to their usual analytic approach. However, some limited analyses have been made, seeking to draw quantitative lessons from the record of nuclear-plant-related sabotage (eg, Andrews, 1986). It is unlikely that such analyses will soon be incorporated into formal PRAs, for two compelling reasons. First, it is not credible to predict the probability of future sabotage events based on the historical record to date. Second, it would be inappropriate to publish a detailed analysis of sabotage scenarios and their likelihood of success.

Thus, sabotage will remain a factor which could increase the probability of a core melt accident, or the probability of a large source term given a core melt, by an unknown amount. The historical record of sabotage suggests that this unknown quantity is not trivial.

17.2 THE RECORD OF NPP-RELATED SABOTAGE

Table 17.1 summarizes the sabotage-related events recorded by the NRC for the period 1976 through 1983. These events all involved nuclear facilities or materials regulated by the NRC -- that is, events inside the United States. Further elaboration of these events is provided in the study from which table 17.1 is taken (Andrews, 1986):

"A total of 833 events have occurred during the period covered by the study. The majority of the events have involved bomb threats. Nine bombs have been found outside critical areas. Detonations that have occurred have not damaged safety-related equipment. Intrusions with unknown or malevolent intent have occurred 17 times. These acts were judged to have the potential to damage plant systems because the intruders were not always caught, and because they had occupied protected and important areas of the plant, unobserved, for significant amounts of time. No damage has ever been attributed to intruders. Vandalism has been the largest contributor to plant damage. Damage to single and multiple systems has occurred in plants both under construction and in operation. Three events judged to be contributors to an accident initiator have occurred. Significant events have involved the closure of emergency coolant valves, the repositioning of switches and wires, damage to diesel generators and new nuclear fuel elements, initiation of plant trips, and damage to core cooling water piping. Arson has occurred in both protected and important areas of operating and partially completed plants. Damage to multiple systems has been the most likely consequence."

reactor coolant system blowdown occurred outside primary containment" (Rubin, 1984). This event, aside from any significance it had as a potential core damage precursor, was notable in that the discharged coolant travelled through floor drains and (via an open drain hub in a room of the reactor building) created a harsh (hot and moist) environment which shut down the reactor core isolation cooling (RCIC) system. This is a classic case of system interaction which had, in a general sense, already been foreseen by the NRC and communicated to the plant licensee. Yet, the licensee had failed to adopt the NRC's suggested modifications. Apparently the licensee had either not understood or not cared about this problem.

Appendix 16A provides an account of two separate instances of system interaction which occurred at Millstone Unit 2 (an 870 MWe PWR) in January 1981. In the first instance, an operator error initiated a sequence of events which came very close to a "station blackout" condition. The event sequence shows a high degree of coupling among nominally independent sources of electricity supply. In the second instance, reactor coolant was transferred from the pressurizer to an accumulator via an unexpected route -- the nitrogen system. This also illustrates the possibility for unexpected linkages among systems.

None of the above-mentioned events led to core melt. However, they clearly illustrate the potential for unexpected interactions among plant systems. PRA analysts may be alert to the possibility of such interactions, but cannot be certain of identifying all potentially significant interactions. Thus, the probability of failure of redundant, nominally independent safety systems will in practice be greater than PRA analysts will predict.

continue. In May 1978, the NRC formally reduced its safety requirements as follows (UCS, 1978):

* the pressure safety margin was reduced from a factor of 4 to a factor of 2;

* the requirement to consider the "largest credible" force was reduced to a requirement to consider the "most probable maximum" force; and

* calculation of material strengths was permitted using "test" strength rather than "design" strength.

Even with this waiver, substantial costs and delays in plant operation arose. As an indication of those costs, the owners of the never-completed Zimmer Plant estimated that modifications to that plant's containment cost $360 million including interest, an amount 6,5 times the original $55 million cost of the containment. The owners sought to recover this amount through a $400 million lawsuit against General Electric and the plant's architect-engineer (Stecklow, 1984).

16.2.2 Unexpected Interactions among Plant Systems

The potential for unexpected interactions can be illustrated by an event which occurred at Robinson Unit 2 (a 665 MWe PWR) in January 1989. In this event, a worker using an air-operated grinder in the turbine building discovered blue flames issuing from the grinder. Elsewhere in that building, welders also observed sparks igniting flames in the vicinity of an instrument air manifold. It was discovered that the service air system had been contaminated with Hydrogen at concentrations up to 6 %, which is in the flammable range. Hydrogen concentrations exceeded flammable levels in the air systems of the turbine, auxiliary and containment buildings. Investigation showe that the Hydrogen had been introduced into the air system through errors made by a worker who was performing post-maintenance testing on the plant's turbo-generator (Baker, 1989).

This incident did not lead to an accident sequence at Robinson Unit 2, which was shut down at the time. However, if Hydrogen contamination of the air system were to occur while the plant was operating, and if high concentrations of Hydrogen were thereby to arise in and around safety-related components, there would be the prospect of multiple, dependent failures following ignition of that Hydrogen. It cannot be expected that PRA analysts would foresee such a scenario.

In some cases, an interaction might have been anticipated, without that awareness leading to appropriate action. Consider an event which occurred following a scram at Hatch Unit 2 (a BWR) in August 1982. Here, a "sustained and uncontrolled

Nevertheless, many BWR plants were built with Mark I and Mark II suppression pool containments, drawing upon these early test results (NRC, 1977a).

During the early 1970s, incidents at BWRs in West Germany, Switzerland and the United States showed that violent oscillations could arise in the suppression pool during discharge of RCS relief valves. An empirical investigation of this phenomenon conducted at one of the Browns Ferry BWRs in 1973 had to be stopped for fear of damaging the plant. During the same period, General Electric undertook large-scale testing of their new Mark III containment concept. These tests showed unexpected dynamic effects in the pool after a simulated LOCA, thereby sparking a prolonged and expensive empirical and theoretical investigation which adressed Mark I, Mark II and Mark III containment designs. For Mark I containments (other containment designs exhibit analogous effects), the following sequence of events was identified as the sequel to a LOCA (NRC, 1977a):

* expansion of a sonic wave front from the break location;
* propagation of a compressive wave in the suppression pool;
* increased pressure and temperature loading in the drywell and vent system;
* ejection of a jet of water from each downcomer into the pool;
* formation of an air/steam bubble at the exit of each downcomer;
* swelling of the pool surface as the air/steam bubble expands;
* breakup of the pool surface;
* "fallback" of elevated pool water, and formation of waves in the pool surface (this phase begins 3-5 seconds after the LOCA); and
* condensation of LOCA-generated steam over a relatively prolonged period, with the potential for "chugging" at the downcomer exits.

Analyses indicated that structural loads arising from these phenomena, or from the dynamic phenomena associated with discharge of RCS relief valves, could exceed the capabilities of containments then in operation or under construction. Containment failure could follow. As a result of this discovery, substantial plant modifications were made. Despite the modifications, the NRC was obliged to waive several containment safety regulations so the plant operation could

16 UNEXPECTED PROCESSES

16.1 INTRODUCTION AND SUMMARY OF MAIN PROBLEMS

PRAs can only address modes of plant behavior which are expected and which are well understood. It is therefore noteworthy that there have been several instances where hitherto unexpected processes have been identified. These instances give warning that other, so far unidentified, processes may be important.

One instance has been discussed elsewhere in this report. This instance is the discovery of high-pressure melt ejection (HPME) as a phenomenon which can lead to early containment failure. It is ironic that HPME was first proposed (in the 1981 Zion PRA) as a mechanism which would reduce the probability of containment failure. Upon empirical and theoretical investigation, however, HPME was revealed as a severe threat to containment integrity.

Another instance is discussed at greater length below. In this case, operating experience and empirical investigation revealed that dynamic effects could threaten the structural integrity of BWR suppression pool containments. This discovery was made after many containments had been built. Extensive modifications to plants in operation and under construction were necessary, even though the NRC waived several of its safety requirements in an attempt to accommodate the newly discovered phenomena.

Both of these incidents involved unexpected physical phenomena. In addition, however, the realm of unexpected processes also includes unexpected interactions among plant systems. Although PRA analysts are increasingly seeking to identify and account for such interactions, they cannot be certain of completing that task. In a discussion below, some instances of unexpected system interaction are described, in illustration of the problem facing the PRA analyst.

16.2 BACKGROUND

16.2.1 Dynamic Effects in BWR Suppression Pools

General Electric developed the suppression pool concept as a means of reducing the size (and therefore, the cost) of containment. The concept was tested during the period 1958-1962 using full-scale segments of the pools for the Humboldt Bay and proposed Bodega Bay BWR plants. These segments bear little resemblance to the pool designs later used.

trip mechanism was incorrectly reassembled; and in three cases, the cause could not be determined.

Only one of two trip channels was affected in each case. Nevertheless, the reactor trip system is a vital safety system and the repeated occurrence of failures at different plants is an alarming symptom - particularly as the causes could not be determined in every case. Complete failure of the trip system during a transient can lead to severe core damage.

Changes in maintenance, testing, and reporting procedures, and modifications of trip breaker coil control, were implemented as counter-measures. However, the last two incidents occurred after those measures were taken (NEA/IRS 577, 1986).

Moreover, faults in control rods which could affect the trip capability were reported 1985 for another French PWR (faults included signs of friction, cracks and broken welds). All control rods were eventually replaced (NEA/IRS 576, 1986).

Problems with control rods appear to be persistent in French PWRs. In spite of the fact that the problems are well recognized and the first counter-measures were taken several years ago, a new control rod incident occured April 1, 1989 at Gravelines-4 PWR. A control rod had broken off and fallen to the bottom of a fuel assembly, causing the control rod cluster to stick at the intermediate position. Analysis showed that the local wear on the control rod casing was far more severe than had been predicted by studies. The earlier EdF criteria for control rod wear were not correct (NucWeek, 1989d).

15.4 PROSPECTS OF PRA ANALYSTS ACCOUNTING FOR UNEXPECTED DEFECTS

Some unexpected defects could be accounted for by assuming that equipment and structures cannot withstand stresses greater than those at which they have been routinely tested. For example, Level II PRA analysts could assume that containment buildings would not withstand internal pressures greater than 115 percent of design pressure (the pressure at which leak-rate tests are conducted). Such conservative assumptions would have the effect of increasing the estimated probability of core melt, and the estimated probability of a large source term given a core melt, but would at least have an objective basis.

In many -- perhaps most -- cases, the PRA analyst will have no objective basis for assigning a failure probability. Consider the above-described case of weak piping and heat exchanger support pedestals at Crystal River Unit 3. How could an analyst predict that piping would collapse during normal operation or a mild earthquake because of errors in detailed design of apparently simple components?

would remain the problem of predicting materials properties and the characteristics of pre-existing cracks at all critical points of the vessel.

While vessels now being built -- such as for new PWRs in Britain -- are being subjected to quite rigorous inspection, earlier practices were less stringent. In-service inspection of old vessels cannot rectify this discrepancy.

Problems connected to reactor pressure vessel failure are treated further in section 9.

15.3 FURTHER EXAMPLES OF UNEXPECTED DEFECTS

Defects of Core Enclosure Bolts at KWU PWRs

The core of a PWR is surrounded by a metal structure which guides the coolant flow. In most KWU-built PWRs, this structure is secured by bolts. The material of those bolts originally was partly Inconel X 750 (used in places where particularly high operational stresses were expected), partly steel (German code No. 1.4571).

From 1978 onwards, bolt defects due to stress corrosion cracking were found in several KWU plants. This led, in some cases, to fuel rod failures due to changes in the coolant flow. Defects occured at Inconel bolts only; the number of defective bolts was quite significant. For example, in Biblis (1980/81) 48 out of 240 (Bohn, 1985); and in GKN-1 (1986) 69 out of 480 (ATW, May 1987). The defects were found during routine tests. However, it is simple chance that the number of failed bolts did not grow more rapidly during the years, and that the tests were performed sufficiently early to avoid major damage (in GKN-1, where the failed bolts were found in 1986, the most recent tests before that had been 1981).

Further bolt failure could have led to loss of integrity of the core enclosure, drastic changes in the coolant flow regime, and severe core damage due to partial overheating.

Those defects occured at Biblis A and B, Stade, Unterweser, and GKN-1 (Neckarwestheim) in the F.R.G., Borsselle in the Netherlands, and Gösgen/Switzerland. It is notable that the severity of the problem appears to have been underestimated for several years. At first, only defective Inconel bolts were replaced by austenitic steel bolts. Defects kept occuring, and only in 1986 (possibly in connection with the "Chernobyl-shock") a general replacement of all Inconel bolts was begun. It is scheduled to be completed within the next few years (Hillrichs, 1987).

Failure of the Reactor Trip System in French PWRs

From 1980 - 1985, failures of the emergency shutdown system were observed in 7 French PWRs during testing. Two incidents resulted from poor contact at the shunt trip coil; once an intruded piece of metal blocked the trip mechanism; once the

detectable through normal inspection methods and may not become evident during leak-rate tests (which in the United States are conducted at ambient temperature and 115 percent of design pressure). Yet, they can become very significant when the containment is stressed well beyond its design limits.

Degradation of Materials in the Reactor Coolant System Boundary

Preservation of the integrity of the reactor coolant system (RCS) is one of the highest priorities of reactor safety. Many possible failure modes of the RCS boundary -- such as failure of the pressure vessel -- are outside the design basis, even though the materials in that boundary face a severe environment. Cycles of pressure and temperature, high neutron flux, mechanical shock and vibration, and corrosive environments each pose their special challenge.

Operating experience in the United States has shown that RCS boundary materials may be unexpectedly degraded by these challenges. The examples mentioned here are of defects which were identified before a major failure occurred, but they illustrate the difficulty of predicting the nature and likelihood of failure modes.

First, consider the case of failures in PWR steam generator tubes. Such failures are potentially significant because they can cause a loss of coolant which initiates a core melt accident, and because they can create a direct path from the core region to the outside atmosphere. It is therefore disturbing that significant tube degradation has been observed at many plants, and tubes have failed in service. On 25 January 1982, a tube rupture occurred at the Ginna plant (a 490 MWe PWR) leading to a small release of radioactivity and the declaration of a Site Area Emergency (NRC, 1982a). In response to this and other events, plant licensees have paid increasing attention to tube degradation. However, it may be difficult to detect the full extent of degradation through routine inspections. For example, in April 1985 the licensee of Millstone Unit 2 (an 870 MWe PWR) used a new chemical cleaning process to remove accumulated sludge from the secondary side of steam generator tubes. This revealed extensive thinning of tubes, with some defects exceeding 40 percent of wall thickness. Yet, eddy current testing conducted prior to the chemical cleaning had predicted much less extensive damage (Ryan, 1985b).

A second example is the faster-than-anticipated embrittlement of reactor pressure vessels as a result of exposure to neutron flux. Current concern is greatest for older vessels which have a high copper content of welds in high-flux regions of the vessel. The problem has been known for some time (eg, Marston, 1980) but has been highlighted by recognition of the significant likelihood of "pressurized thermal shock" events (eg, Phung, 1983). In such events, the vessel is subjected to a rapid temperature transient while at high pressure. Attempts have been made to estimate the probability of vessel failure following hypothesized events of this kind (eg, Simonen, 1986) but, even if such analytic methods were to be perfected, there

concrete containments -- both reinforced and prestressed -- which are the most common containment type in the United States and elsewhere. Clearly, the strength of a concrete containment will depend heavily on the care taken in its construction. For example, the strength of a reinforced concrete containment depends on the integrity of long reinforcing bars with multiple splices -- these bars are only as strong as the weakest splice. Voids in concrete, which are particularly likely where concentrations of reinforcing steel (and stress) are high, can substantially weaken the containment. In addition, the geometry of the actual containment may not be exactly as specified. For example, out-of-roundness of the containment cylinder can occur, causing local stress intensification and instability. Such asymmetry could arise during construction, or subsequently due to factors such as creep distortion caused by long-term insolation on one side of the structure (Gittus, 1982).

Also, experience with reinforced and prestressed concrete structures in a variety of non-nuclear applications shows many problems with corrosion of steel reinforcing bars and tendons (Gittus, 1982). Although this problem is recognized and guarded against for reactor containments, it is impossible to guarantee totally that corrosion has not occurred.

An NRC-sponsored review of detected defects in concrete structures at US nuclear plants shows a variety of problems, as summarized in figure 15.1. Of these problems, five could -- if not identified and corrected -- have had serious consequences. All five instances were related to concrete containments and involved two dome delaminations, voids under tendon bearing plates, tendon anchor head failures, and a breakdown in quality control and construction management (Naus, 1986).

Figure 15.2 shows the extent of dome delamination identified at Turkey Point Unit 3 (a 666 MWe PWR) during construction. This problem was revealed during tensioning of tendons in the containment dome, when sheathing filler was observed to leak from a crack in the dome surface and a bulge developed elsewhere in that surface. Extensive repairs were necessary.

In another example, two anchor heads for vertical prestressing tendons were found fractured at Farley Unit 2 (an 829 MWe PWR) in January 1985, and numerous tendon wires were broken near the fractured anchor heads. This failure was detected about 8 years after the tendons were stressed, and it is speculated that the breakages occurred during a minor seismic event in October 1984 (Hudgins, 1985). Further examination using magnetic particle testing revealed cracks in 18 other anchor heads at Farley Unit 2 and 6 anchor heads at Farley Unit 1 (each unit has about 100 vertical tendons). Laboratory tests have indicated that the cause of the anchor head failures was stress corrosion cracking, exacerbated by the presence of moisture and impurities (Naus, 1986).

Although these defects were detected, there is no basis for assuming that all comparable defects have been detected. Containment defects such as these may not always be readily

Table 2.3: Comparison of core damage frequencies due to internal initiators (from NUREG-1150 Grand Gulf, RSSMAP Grand Gulf, and IDCOR Grand Gulf)

Event Type	Core Damage Frequency (per reactor year)		
	NUREG-1150 Grand Gulf	RSSMAP Grand Gulf*	IDCOR Grand Gulf**
Station Blackout	2.8×10^{-5}	1.3×10^{-6}	3.4×10^{-7}
ATWS	1.8×10^{-7}	5.4×10^{-6}	6.7×10^{-6}
Transients with Loss of Long-Term Heat Removal	$<1 \times 10^{-6}$	1.8×10^{-5}	1.9×10^{-7}
Transients with Loss of All Injection	$<1 \times 10^{-6}$	2.2×10^{-6}	1.0×10^{-6}
LOCA*** with Loss of Long-Term Heat Removal	$<1 \times 10^{-6}$	9.9×10^{-6}	1×10^{-6}
LOCA*** with Failure of All Injection	$<1 \times 10^{-6}$	7.7×10^{-7}	1×10^{-6}
Total Core Damage Frequency	2.8×10^{-5}	3.6×10^{-5}	8.3×10^{-6}

*From Appendix D, Grand Gulf RSSMAP report (Ref. 3.12).
**From Table 5-11, IDCOR Task 21.1 Report (Ref. 3.7).
***Includes stuck-open relief valves.

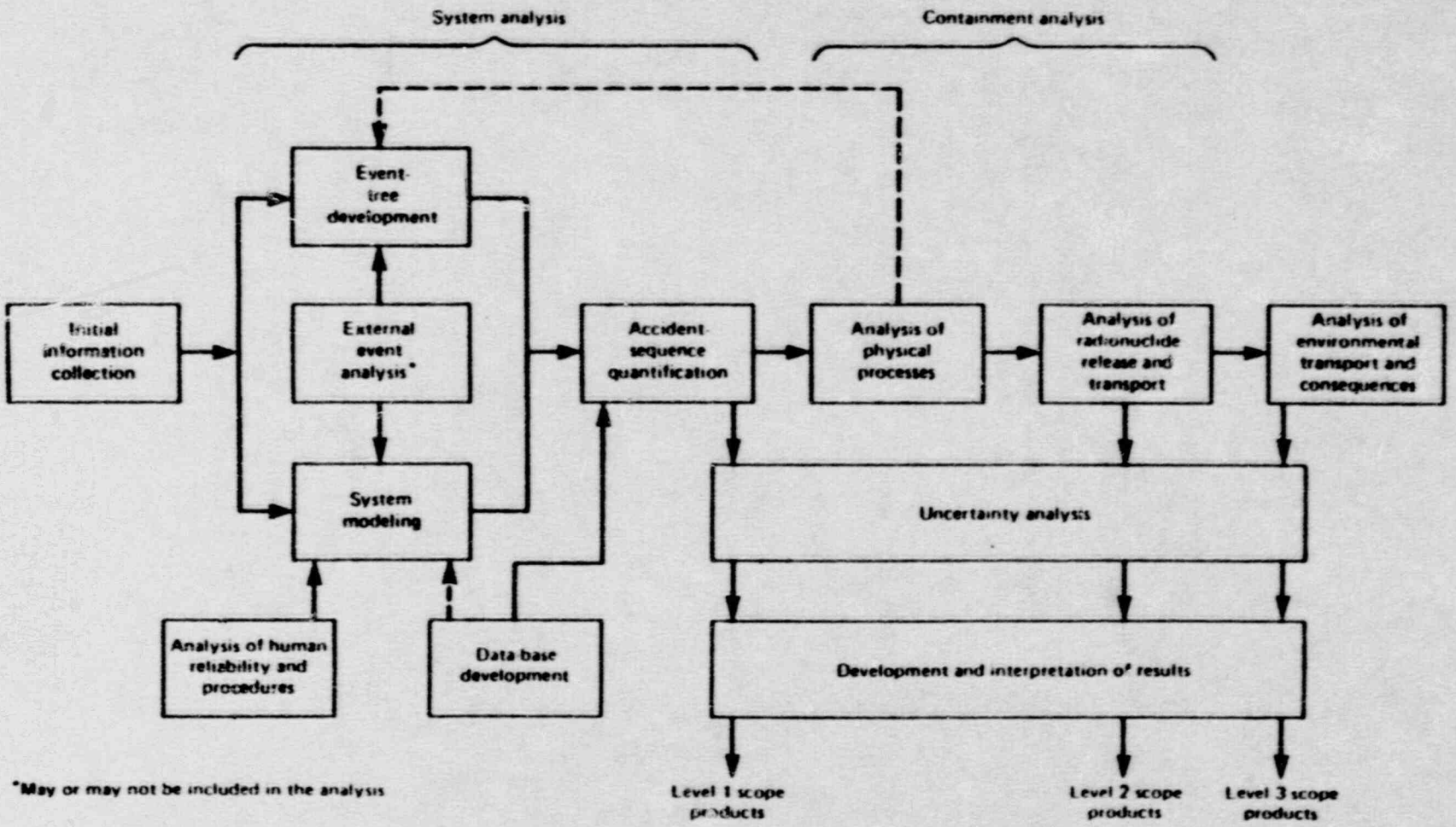


Fig. 2.1: Risk-assessment procedure
(NRC, 1982b)

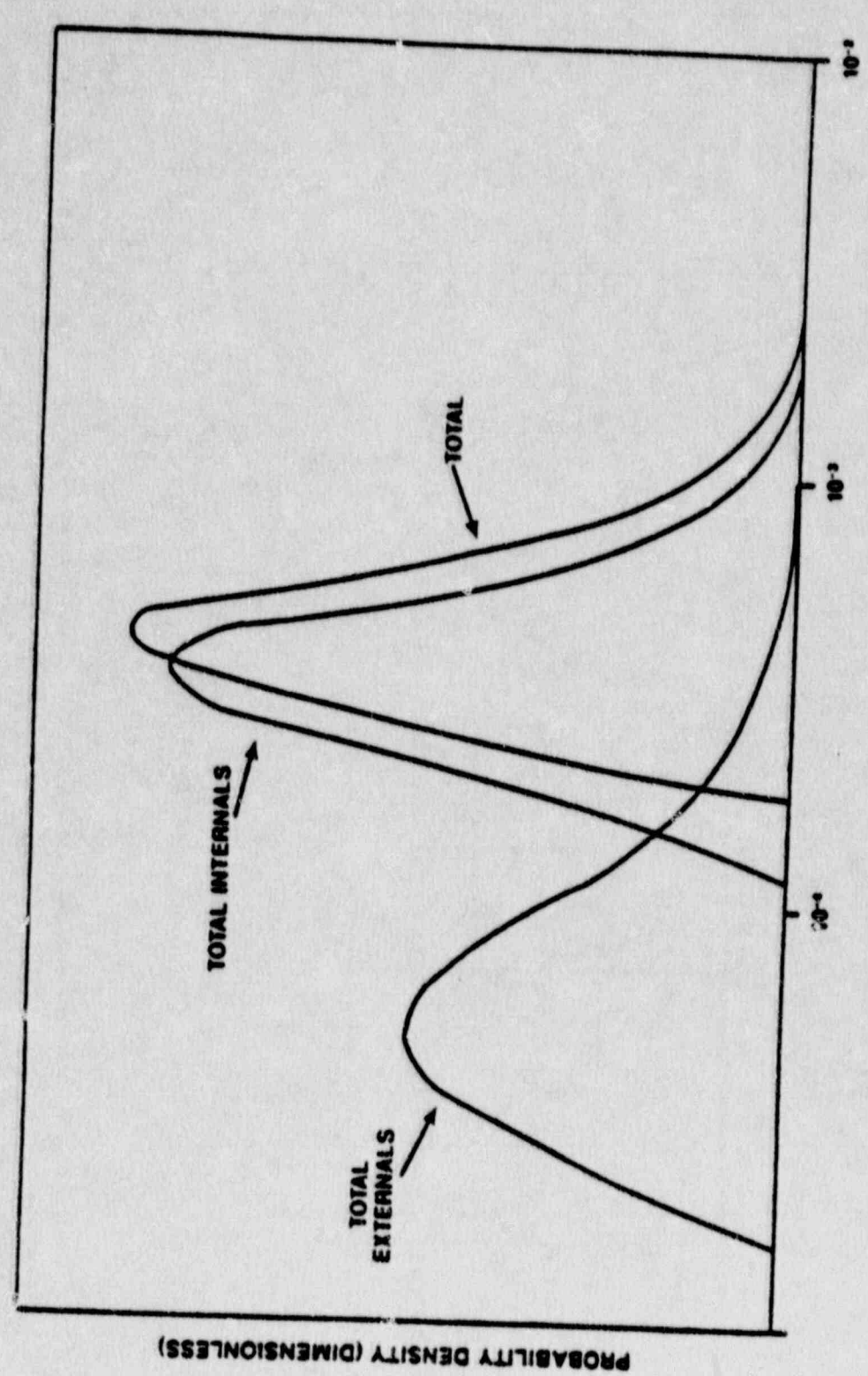
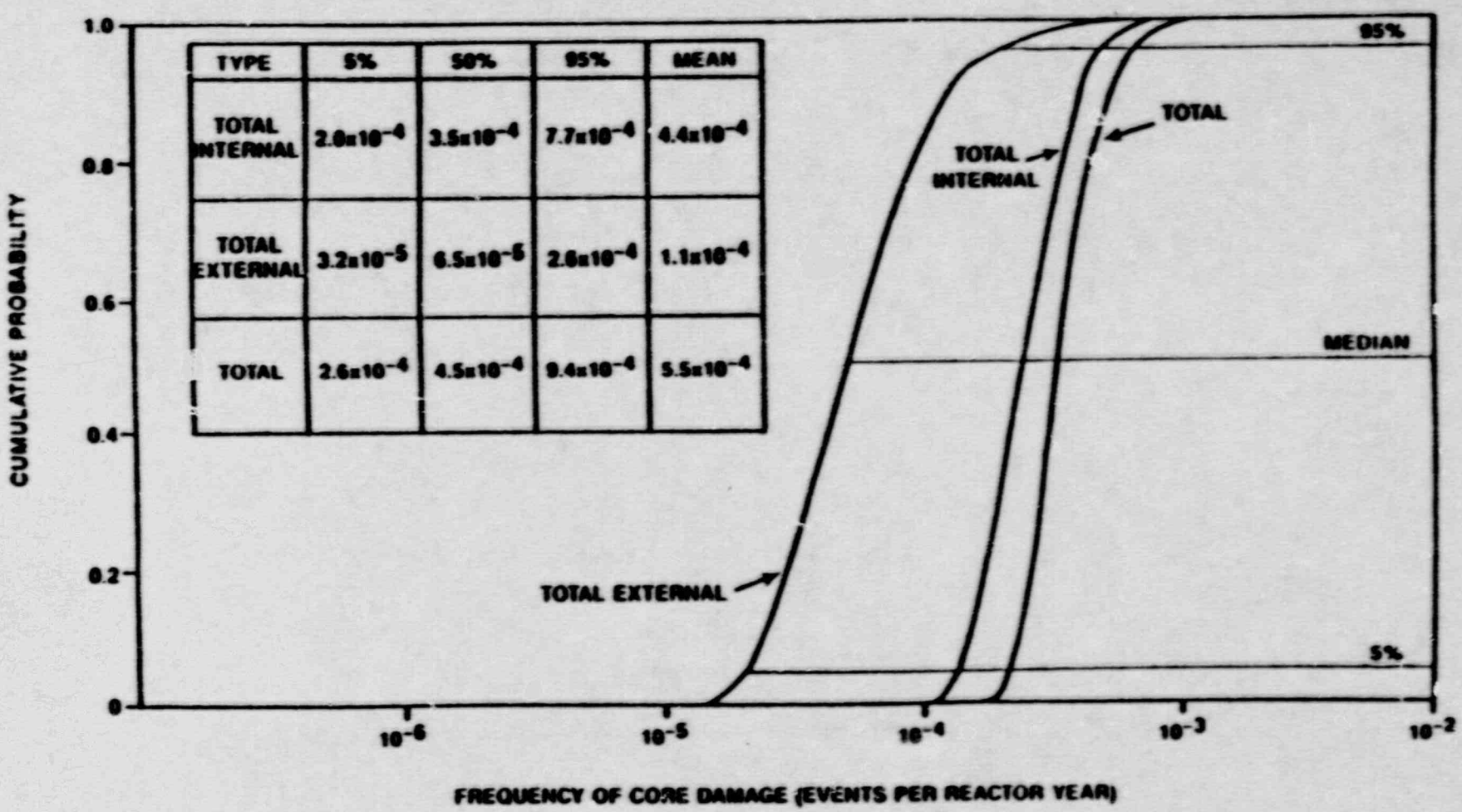


Fig. 2.2: TMI-1 PRA PROBABILITY OF CORE DAMAGE FREQUENCY DISTRIBUTIONS (PROBABILITY DENSITY FORMAT)

(PLG, 1987)



TYPE	5%	50%	95%	MEAN
TOTAL INTERNAL	2.8×10^{-4}	3.5×10^{-4}	7.7×10^{-4}	4.4×10^{-4}
TOTAL EXTERNAL	3.2×10^{-5}	6.5×10^{-5}	2.8×10^{-4}	1.1×10^{-4}
TOTAL	2.6×10^{-4}	4.5×10^{-4}	9.4×10^{-4}	5.5×10^{-4}

Fig. 2.3: TMI-1 PRA PROBABILITY OF CORE DAMAGE FREQUENCY DISTRIBUTIONS (CUMULATIVE PROBABILITY FORMAT)

(PLG, 1987)

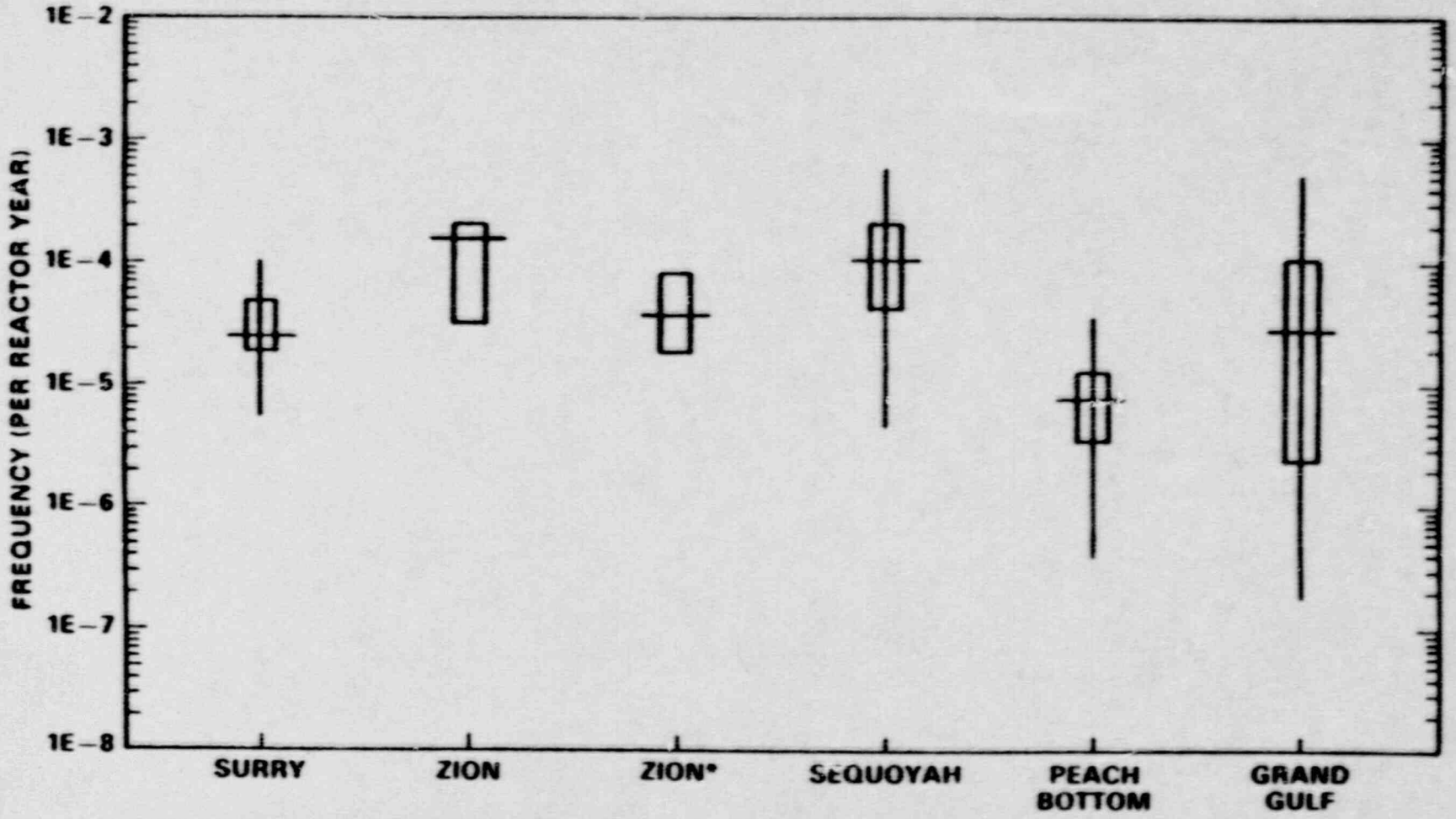


Fig. 2.4: Comparison of severe core damage frequencies (NUREG-1150, 1987)

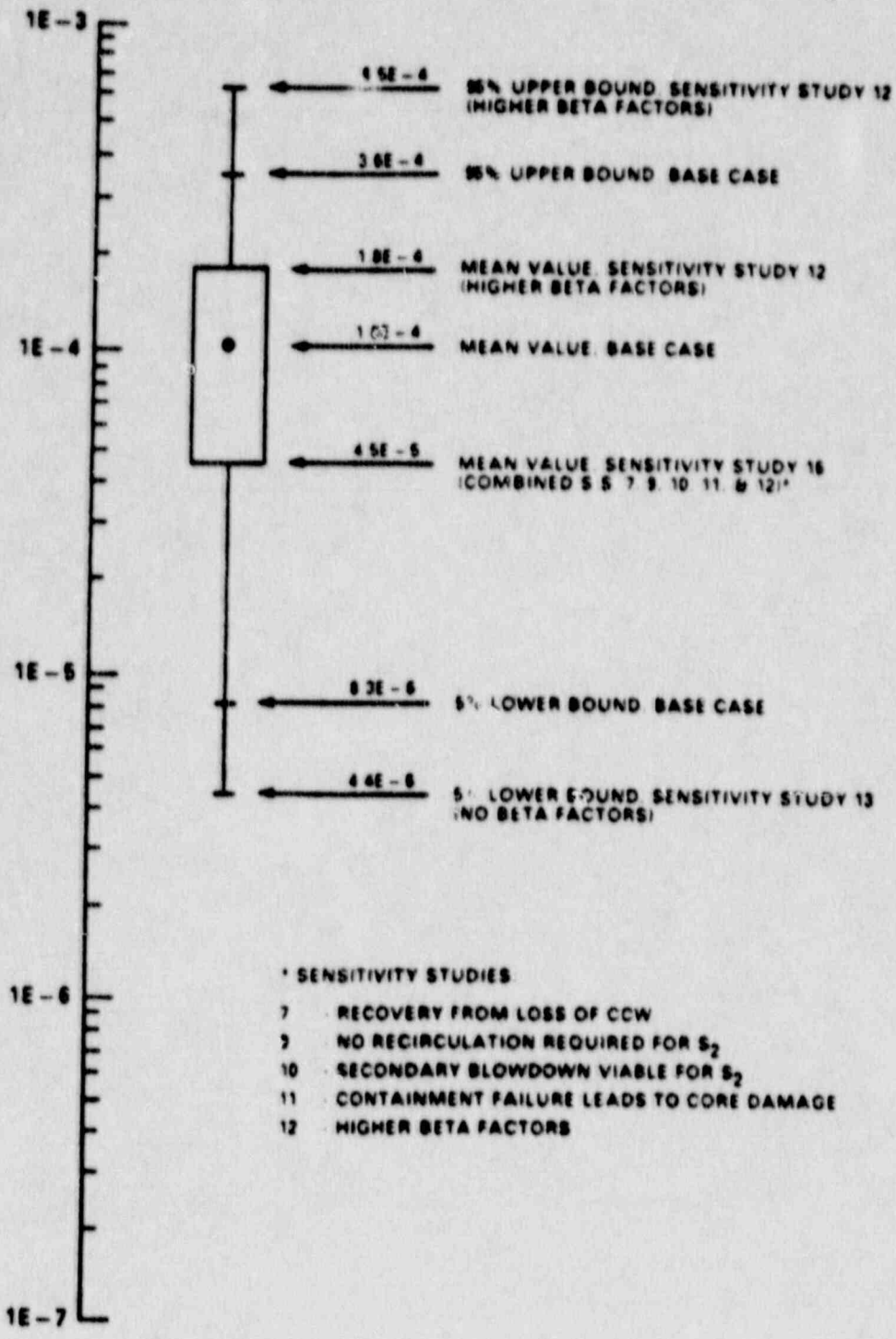


Fig. 2.5: "Box-and-whisker" display of uncertainties for core damage frequency at Sequoyah

(NUREG-1150, 1987)

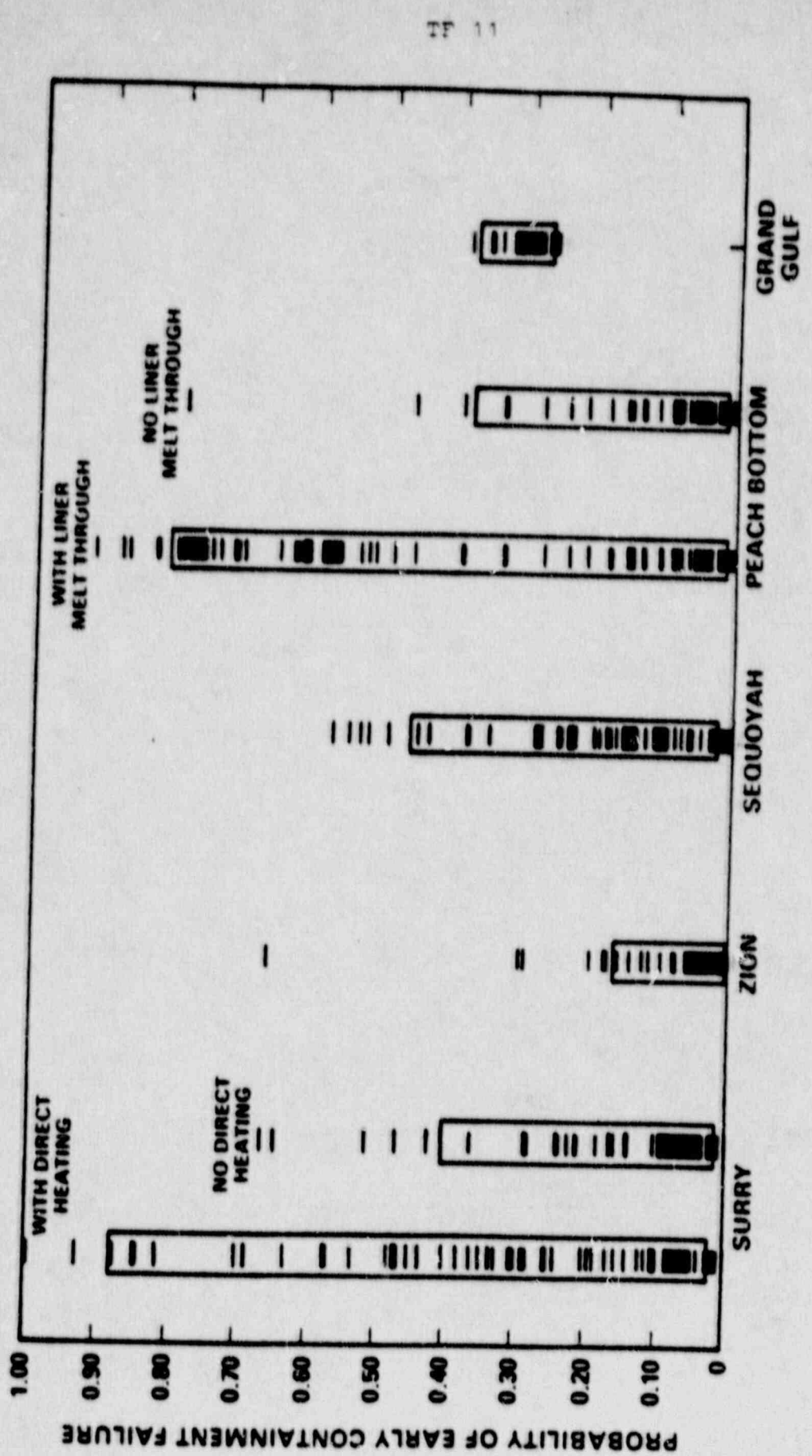
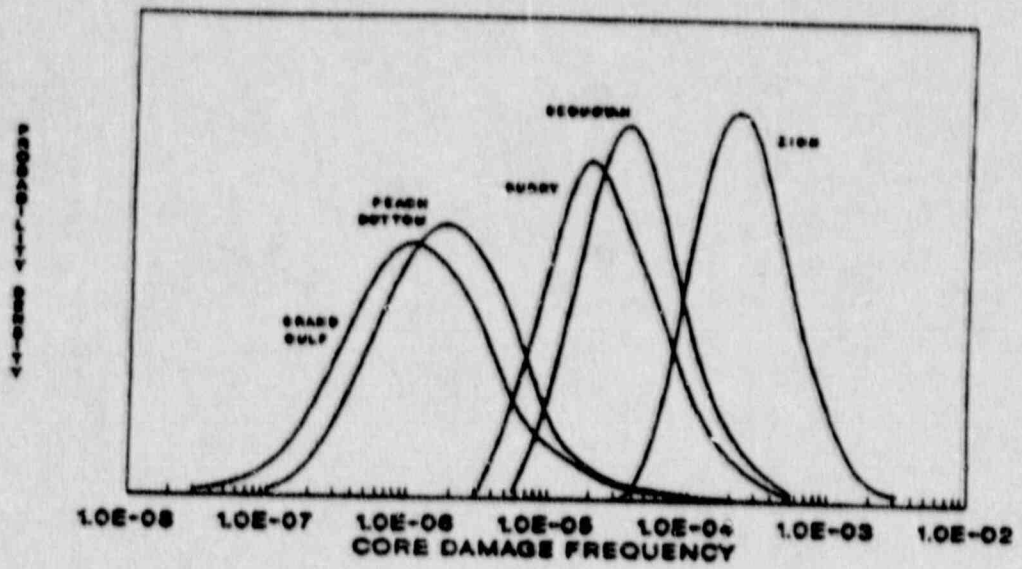
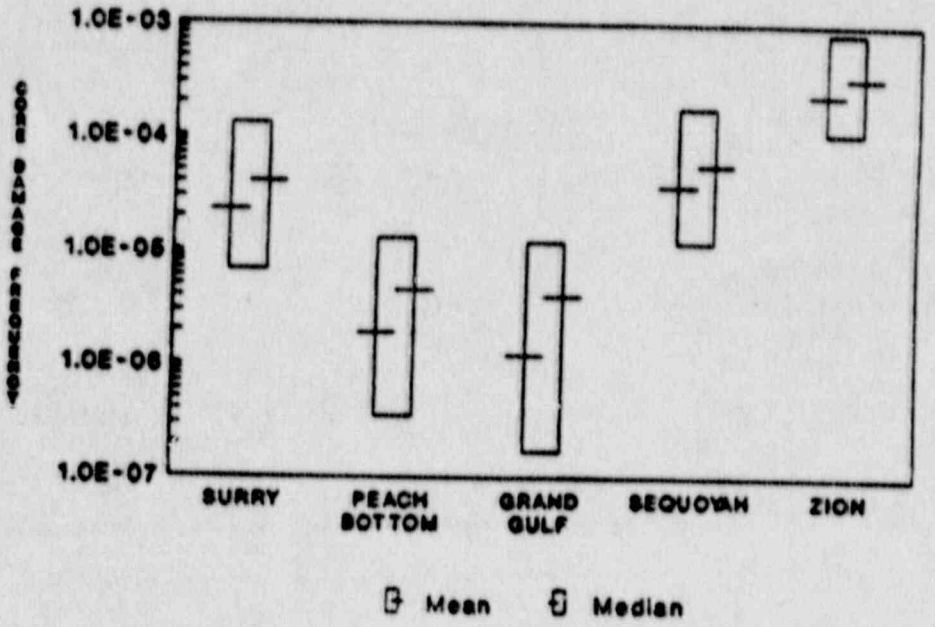


Fig. 2.6: Comparison of early containment failure probabilities (NUREG-1150, 1987)

Figure 2.7 (NUREG-1150/2, 1989):

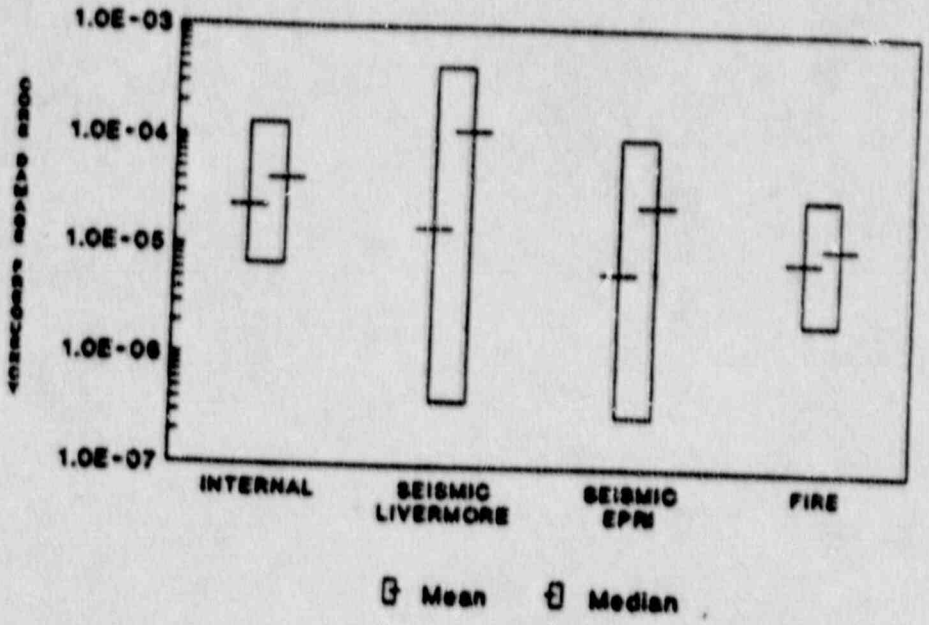


(a) Internal core damage frequency distributions

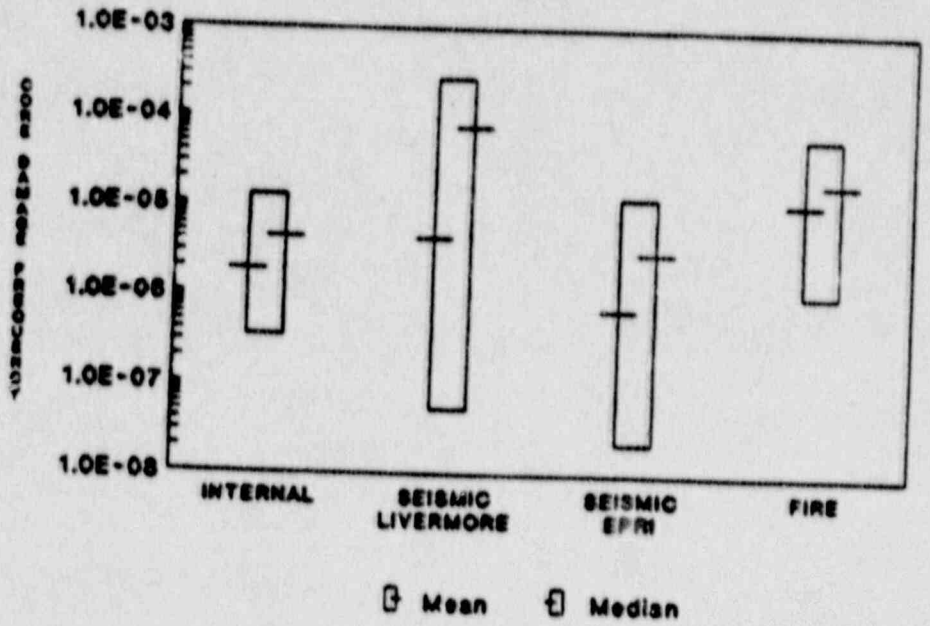


(b) Internal core damage frequency ranges (5th and 95th percentiles)

Figure 2.8 (NUREG-1150/2, 1989):



(a) Surry external events, core damage frequency ranges (5th and 95th percentiles)



(b) Peach Bottom external events, core damage frequency ranges (5th and 95th percentiles)

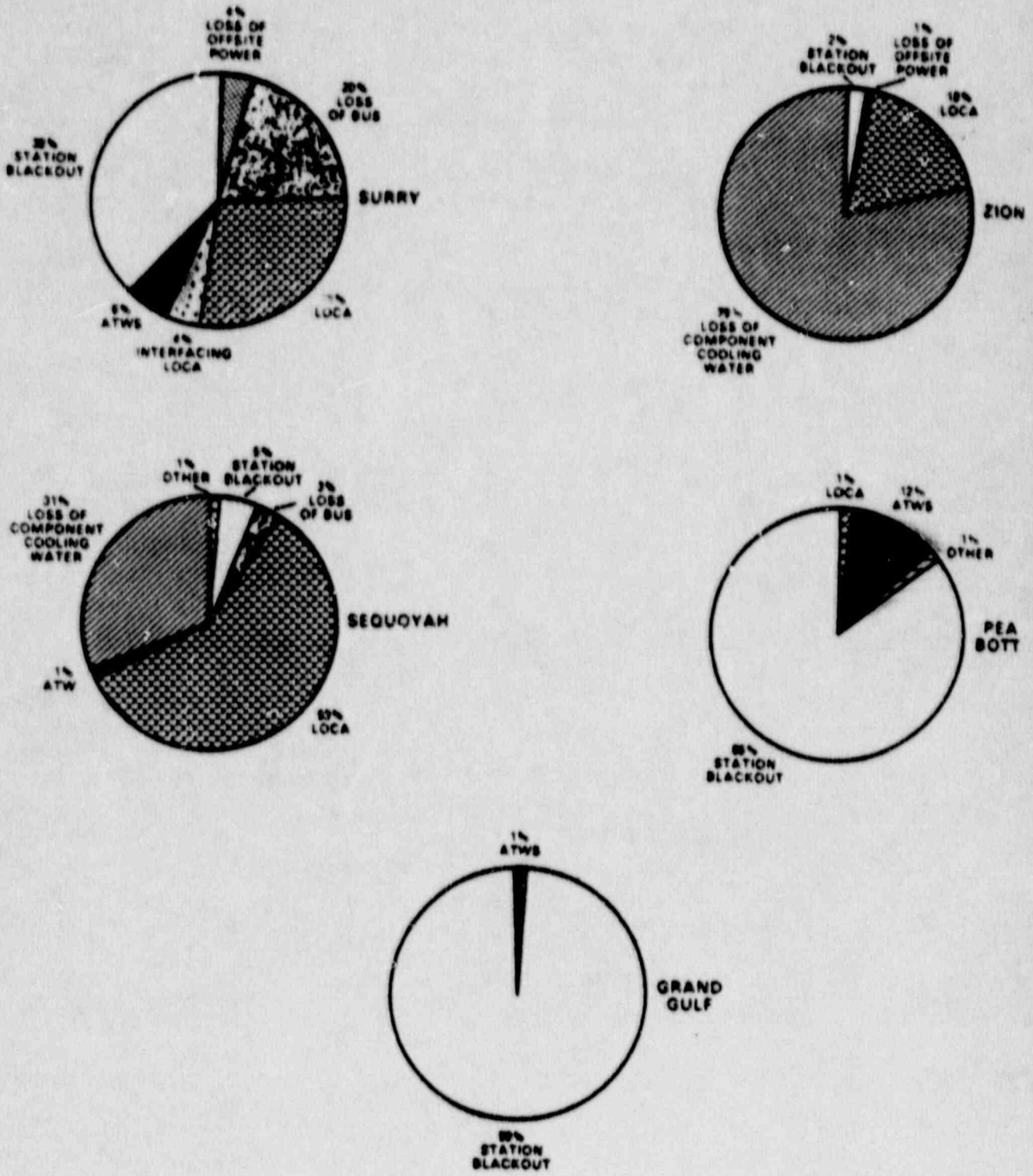


Fig. 2.9: Principal contributors to core damage frequency
(NUREG-1150, 1987)

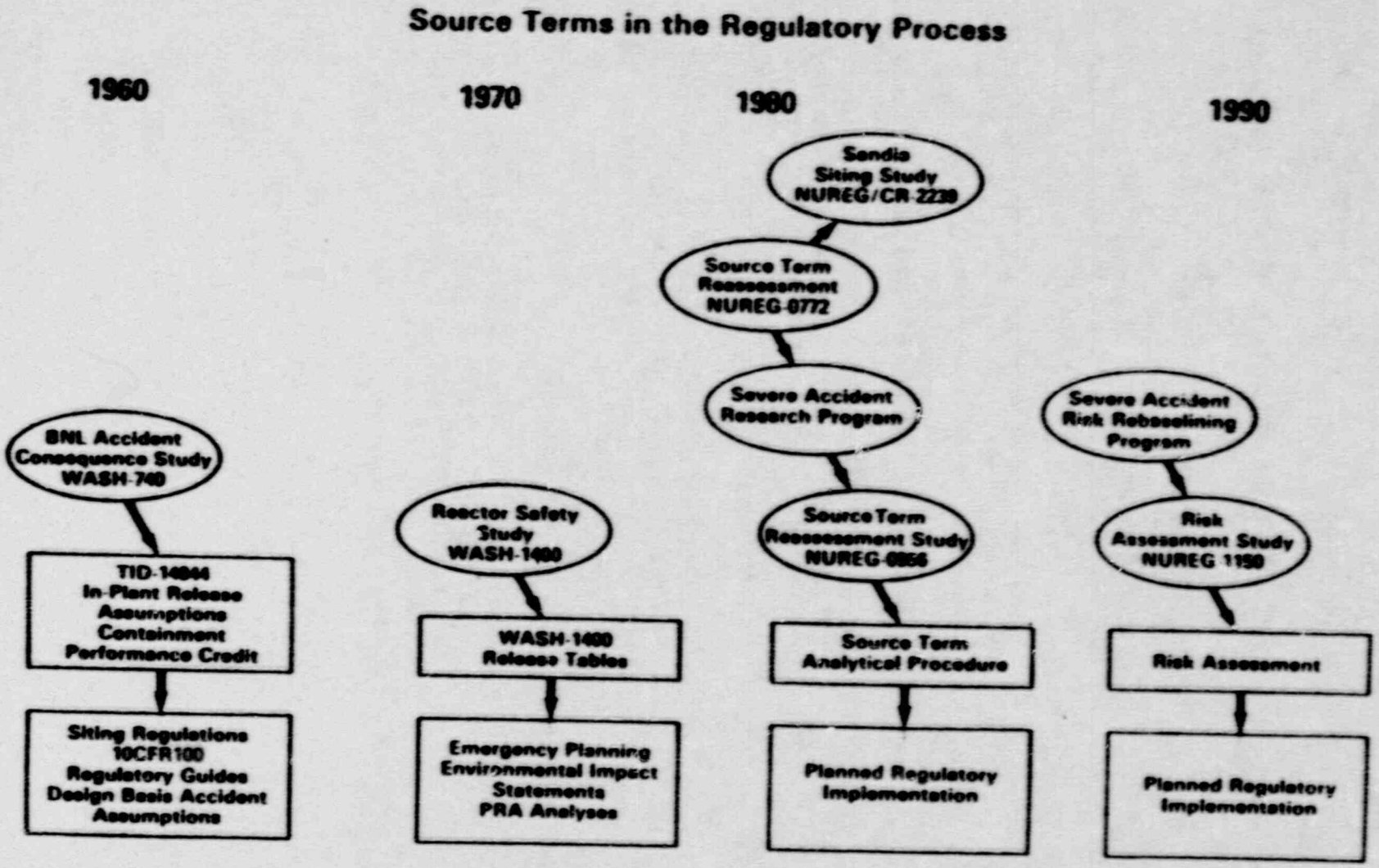


Fig. 2.10: History of severe accident assessment and its relationship to regulatory processes (Silberberg, 1986)

Fig. 2.11: Source: NRC, 1986b

NRC's Safety Goals for Operation of Nuclear Power Plants

- **Qualitative Safety Goals:**

  (1) Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

  (2) Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

- **Quantitative Objectives Used to Gauge Achievement of the Safety Goals:**

  (1) The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the US population are generally exposed.

  (2) The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

- **General Performance Guideline:**

  Consistent with the traditional defense-in-depth approach and the accident mitigation philosophy requiring reliable performance of containment systems, the overall mean frequency of a large release of radioactive materials to the environment from a reactor accident should be less than 1 in 1,000,000 per year of reactor operation.

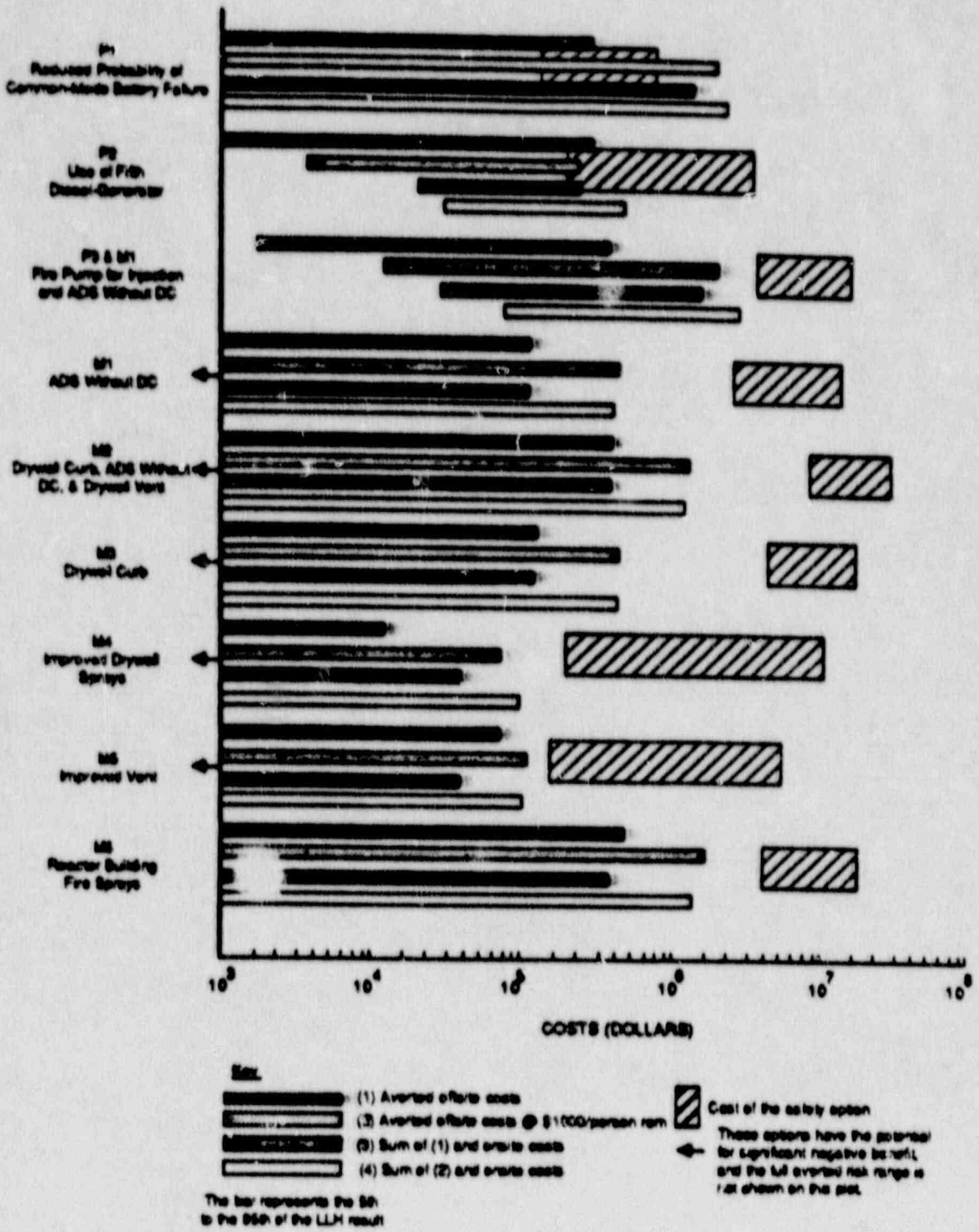


Fig. 2.12: Comparison of costs and benefits (monetized averted risks) for preventive and mitigative options -- Peach Bottom (NUREG-1150, 1987)

Table 3.1: Summary of ASP findings to date (Minarick, 1988)

Period	Frequency of events (per reactor-year)	
	With P (core damage) $>10^{-3}$	With P (core damage) $>10^{-4}$
1969–1979	0.039	0.15
1980–1981	0.045	0.12
1984–1986	0.022	0.13

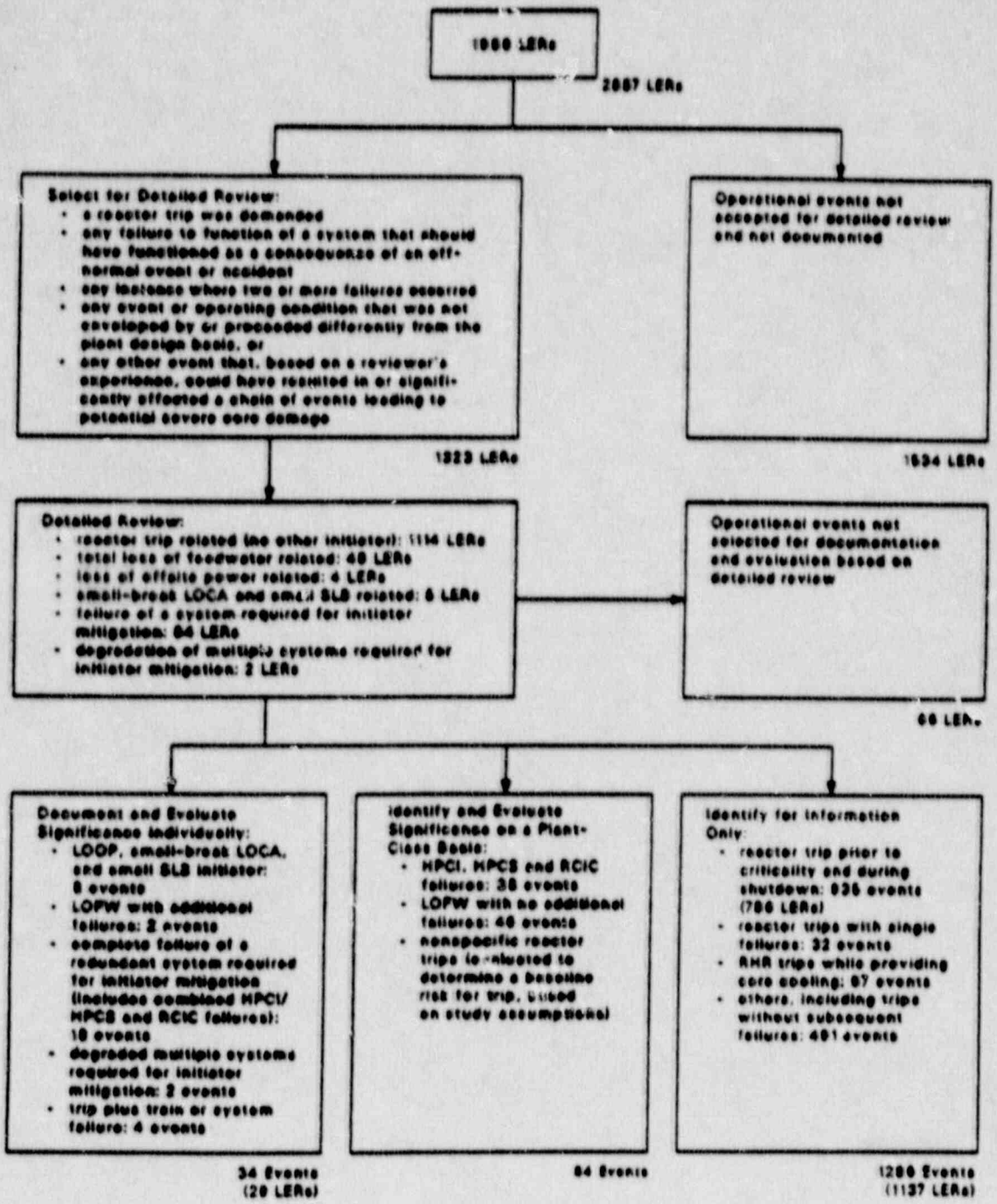


Fig. 3.1: Operational review process for 1986 (Minarick , 1988)

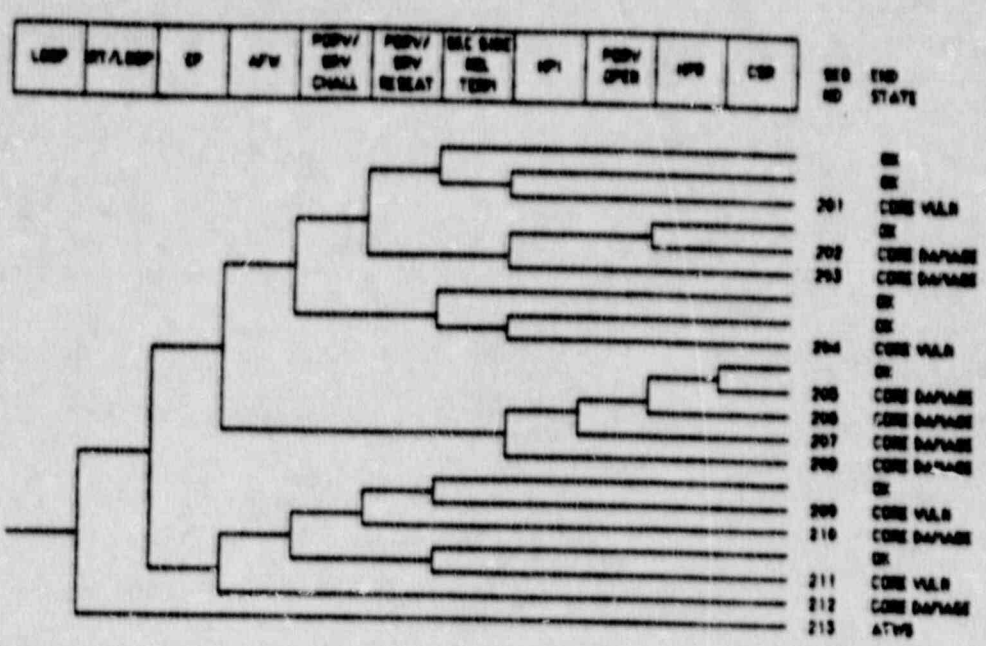


Fig. 3.2: PWR Class G loss-of-offsite-power event tree. (Minarick, 1986)

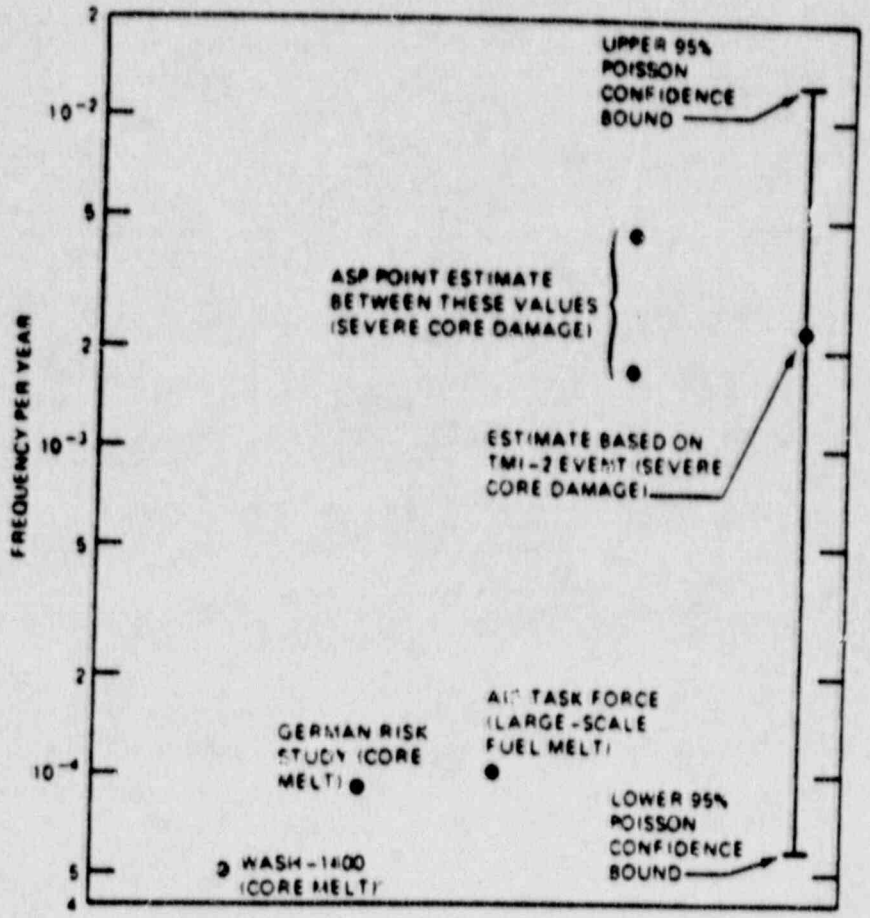


Fig. 3.3: Comparison of ASP results for 1969 - 1979 with other core damage estimates (Minarick, 1982)

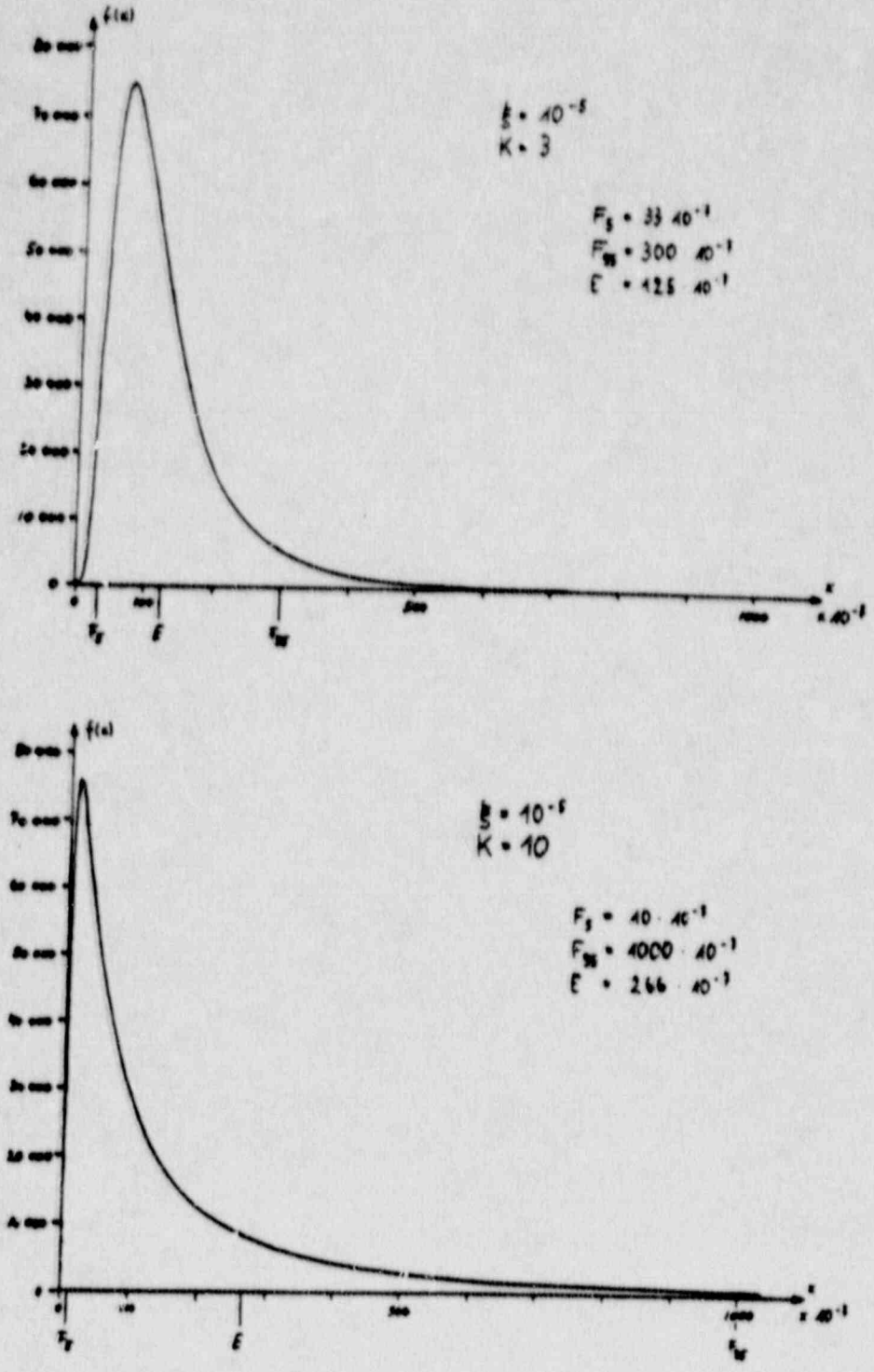


Fig. 5.1: Proability density function of the lognormal distribution

$$f(x) = \frac{1}{\sqrt{2\pi}} \frac{1}{\sigma x} \exp\left[- \frac{(\ln x - \ln \tilde{x})^2}{2\sigma^2} \right]$$

$\tilde{x}$ = median
E = expectation value
K = variation value
P = %-fractile

K = exp (1.6449 σ)
$F_5 = \tilde{x} / K$
$F_{95} = \tilde{x} \cdot K$
E = $\tilde{x} \exp(\sigma^2)$

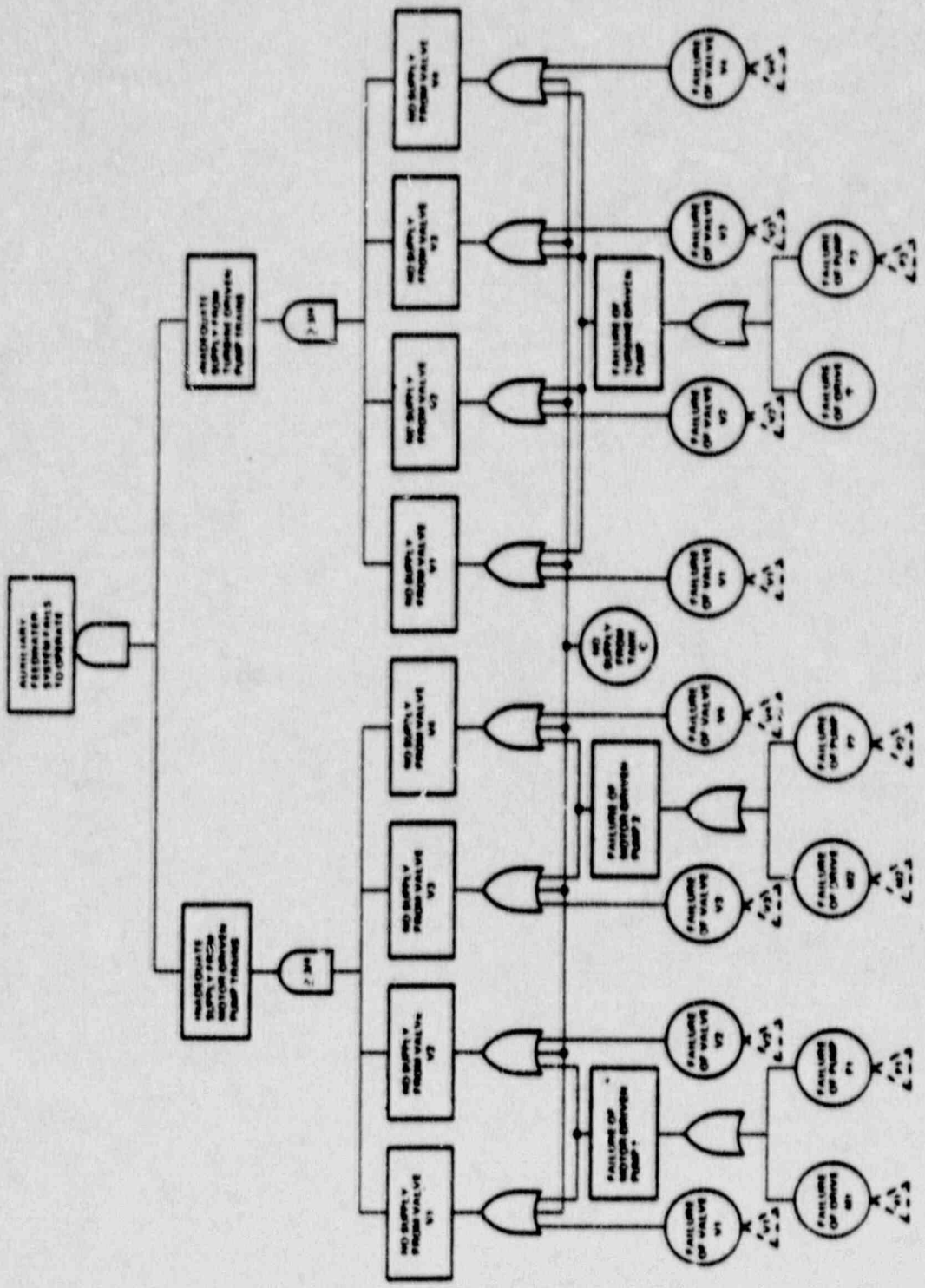


Fig. 6.1: The fault tree from draft NUREG-1150 (1987),

Table 7.1

Types of Dependent Failures Encountered in PRA (Fleming, 1983)

Dependent Failure type	Characteristics	Subtype	Example
Common Cause Initiating event	Causes a plant transient and increases unavailability of one or more systems	Physical Interaction Human Interaction	Earthquake Maintenance Error shorting out Instrument Bus
Intersystem Dependency	Causes a dependency in joint failure probability of two or more systems	Functional dependency Shared-equipment dependency Physical Interaction Human Interaction	Coolant charging fails because component cooling fails Pump fails due to electric power unavailability Fire causes loss of equipment in two systems Operator error causes loss of two systems
Intercomponent Dependency	Causes a dependency in joint failure probability of two or more components	Functional dependency Shared-equipment dependency Physical Interaction Human Interaction	Battery loses charge after it is run beyond capacity Recirculation pump fails because same pump fails during injection mode Fire causes loss of redundant pumps Design error present in redundant pump controls

Table 7.2

Treatment of Common Cause Events in selected PRAs (Fleming, 1986), NUREG-1150 and German Risk Study supplemented

PRA	Year completed	Method used for Subcomponent level Common Cause Failure Analysis
Reactor Safety Study	1975	"Square root" method used in selected cases
[illegible] AIPA Study	1976	Beta factor method used for all redundant active components; parameters quantified from LER and and GCR operating experience
Zion PRA	1978	Beta factor method used for selected components; parameters quantified judgmentally
German Risk Study	1979	Improved "Square root" method used for Human Interaction; CCF-Data assessed for selected systems, when German operating experience available
IREP PRAs		CCF not modeled or reflected in quantification
RINGHALS 1	1981	C-factor method used for most redundant active components; parameters quantified with plant-specific data
Seabrook PRA	1983	Multiple Greek Letter, δ-Factor and their variations used for all redundant active and some diverse components; parameters estimated from 500 years of U.S. operating experience data
Diesel PRA	1984	CCF not modeled; cutoff probabilities used and arbitrary sensitivities calculated
NUREG-1150	1987	δ-Factor method

Table 7.3

Results of different models for unavailability of AFW-System (frequency per demand) (Fleming, 1986); Authors' calculations for β=0.1 and Indep. Models

BPM	MGL	APM	β-Fact.	β=0.1	Indep.
$1.0*10^{-3}$	$8.2*10^{-4}$	$1.1*10^{-3}$	$1.3*10^{-3}$	$5.0*10^{-4}$	$4.0*10^{-4}$

Table 7.4

Data base for Diesel Generator Case (Hirschberg, 1985)

- 50 groups of four diesel generators (DGs); 200 DG-units
- Two operating years for each group
- Test interval T = 2 weeks = 336 h; all four DGs were started simultaneously when tested
- Real demands: 0.5 per operating year and DG-group
- 2600 tests of DG-groups, 50 real demands (2650 DG-group starts, which correspons to 10600 DG-unit starts
- 256 single failures (246 at tests, 10 at demands)
- 31 double failures (29 at tests and 2 at demands), whereof 13 independent and 18 CCFs
- 3 triple failures (3 at tests and 0 at demands), whereof one corresponds to 3 independent single failures, one is a combination of a double CCF and an independent failure, and one is a triple CCF
- No quadruple failures

Table 7.5

Results of different models for Diesel Generator Case (frequency per demand) (Hirschberg, 1985); Authors' calculations for MGL-FL Model

	DATA*)	MGL*)	B-Fact	BFR	MDFF	MGL-FL**)
2 of 4 1)	$1.32*10^{-2}$	$1.28*10^{-2}$	$8.22*10^{-3}$	$7.50*10^{-3}$	$2.63*10^{-3}$	$1.14*10^{-2}$
3 of 4 2)	$1.51*10^{-3}$	$1.26*10^{-3}$	$3.85*10^{-3}$	$3.68*10^{-4}$	$2.48*10^{-3}$	$8.74*10^{-4}$
4 of 4	$3.77*10^{-4}$	$3.99*10^{-4}$	$3.85*10^{-3}$	$6.86*10^{-6}$	$9.94*10^{-5}$	$8.55*10^{-5}$

*) upper bound approximation for quadruple failure

**) calculated according Bayesian approach (Fleming, 1986) no quadruple failure assumed

1) 2 of 4 means failure of 2, or 3, or 4 components

2) 3 of 4 means failure of 3, or 4 components

Table 7.6

Effect of Data Screening on Data base
(Hennings, 1985)

Standby pumps			
	failure of components	number of counted events	frequency per plant's operating hour
not fault tree specific Marshall-Olkin-Model	2 of 4	5	$1.3*10^{-6}$
	3 of 4	0	$1.5*10^{-7}$
	4 of 4	1	$4.8*10^{-6}$
fault tree specific Marshall-Olkin-Model	2 of 4	0	$1.6*10^{-7}$
	3 of 4	0	$1.5*10^{-7}$
	4 of 4	0	$2.0*10^{-6}$

Motor Operated Valves			
	failure of components	number of counted events	frequency per plant's operating hour
not fault tree specific; Marshall-Olkin-Model	2 of 4	20	$1.1*10^{-6}$
	3 of 4	3	$2.6*10^{-7}$
	4 of 4	0	$1.2*10^{-6}$
fault tree specific; Marshall-Olkin-Model	2 of 4	11	$6.0*10^{-7}$
	3 of 4	0	$4.8*10^{-6}$
	4 of 4	0	$1.2*10^{-6}$

Figure 7.1

Common Cause Contributions according to NUREG-1150
for different plants

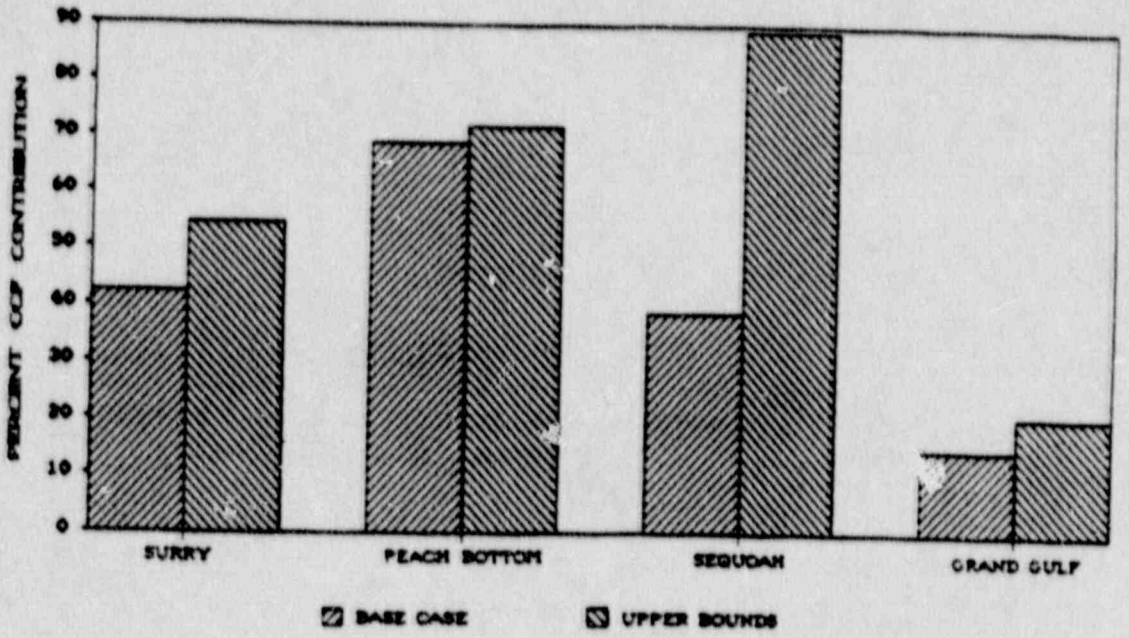


Figure 7.2

Simplified schematic of major components of the example AFW-System (Fleming, 1986)

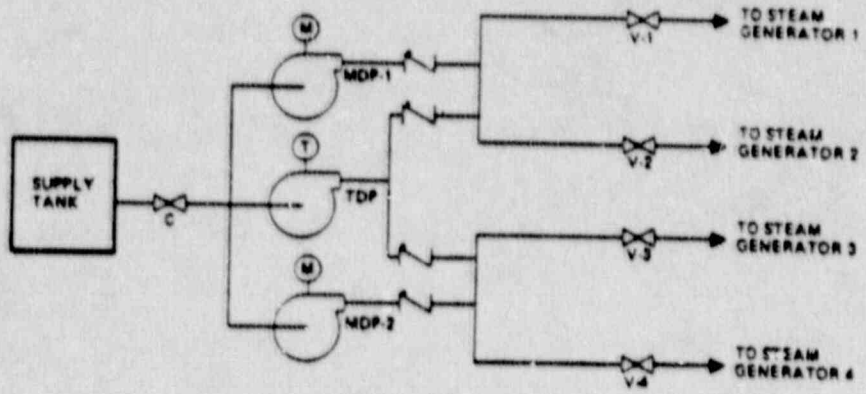


Figure 7.3

Reliability block diagram of example AFW-System (Fleming, 1986)

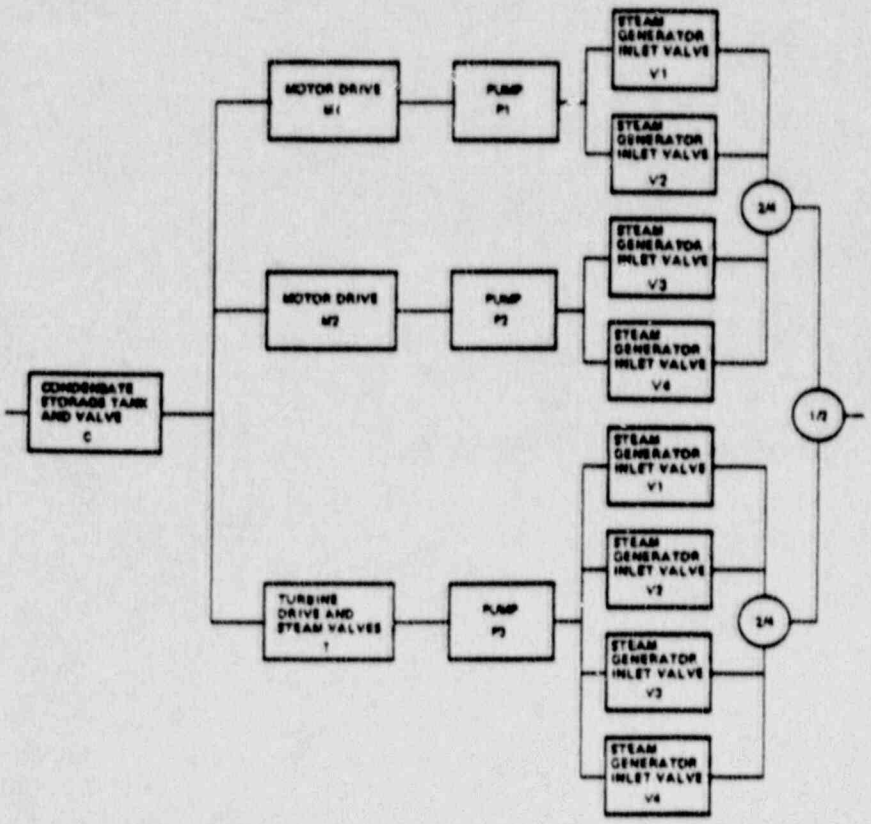
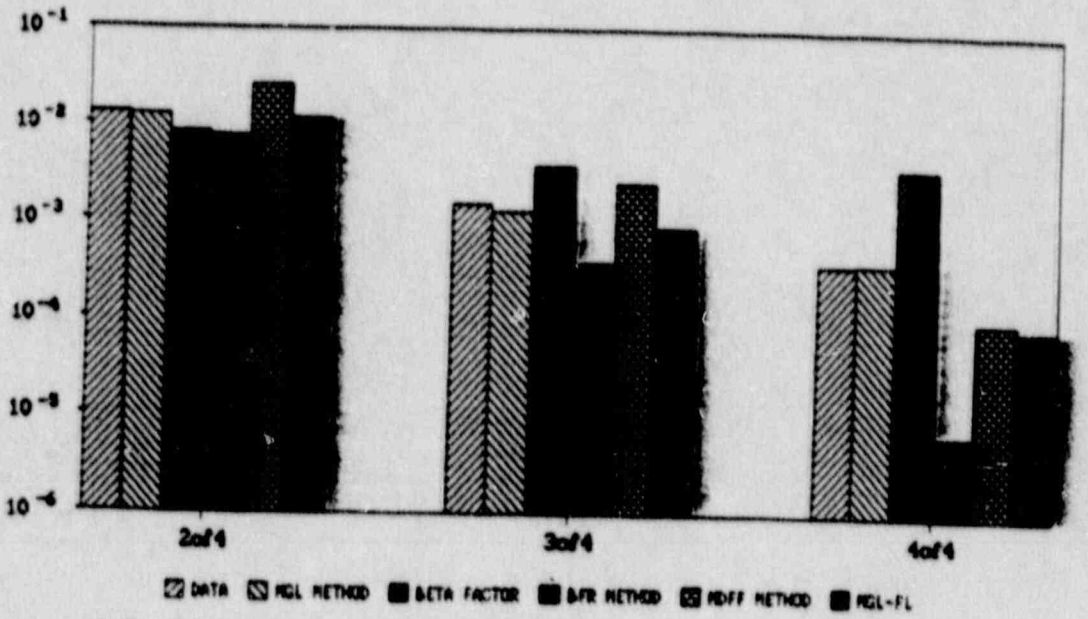


Figure 7.4

Results of Diesel Generator Case for different Models



MGL-FL: Multiple Greek Letter according to Bayesian Procedure of <Fleming 86>

Figure 7.5

General common cause fault subtree for Component A in a common cause group of N components (Fleming, 1986)

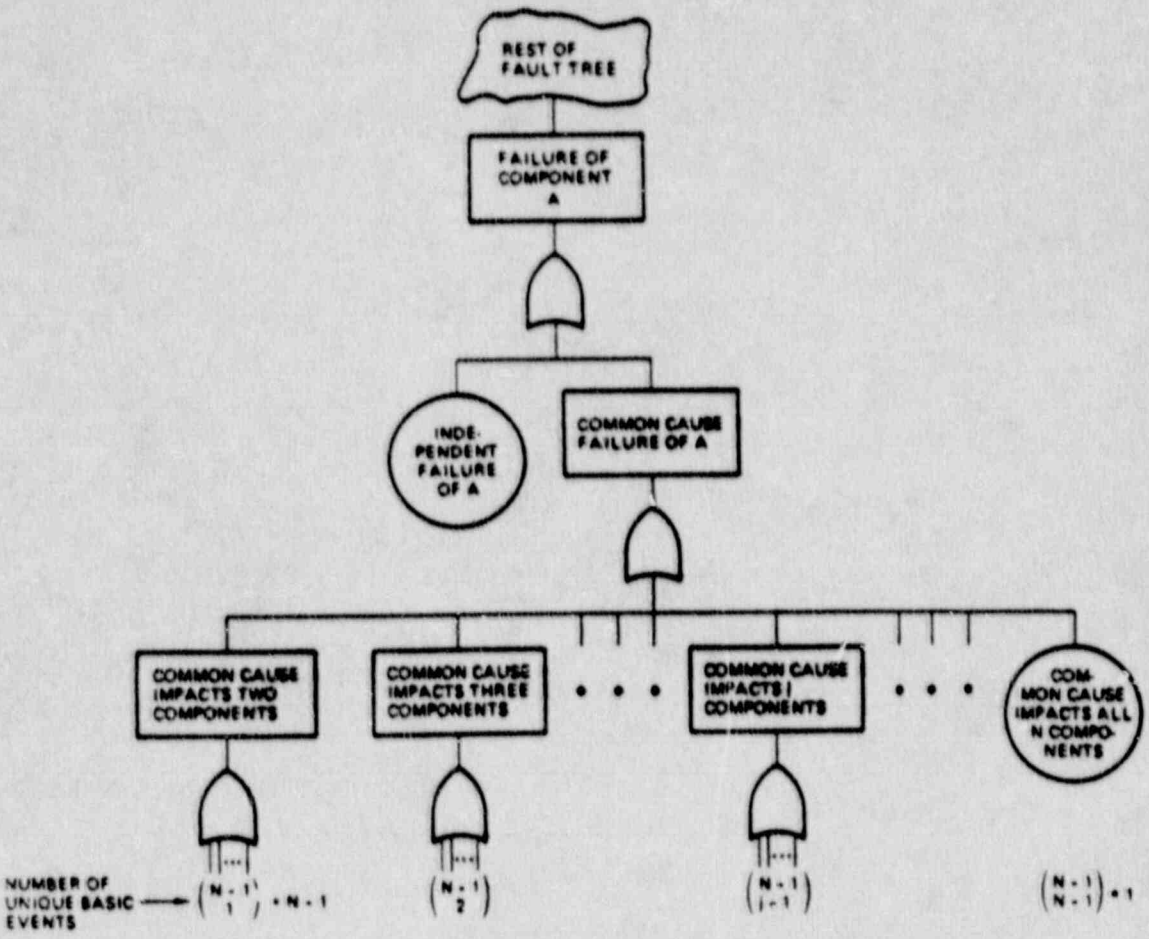


Figure 7.6

Results of different teams for unavailability of AFW-System of a German PWR (Poucet, 1987)

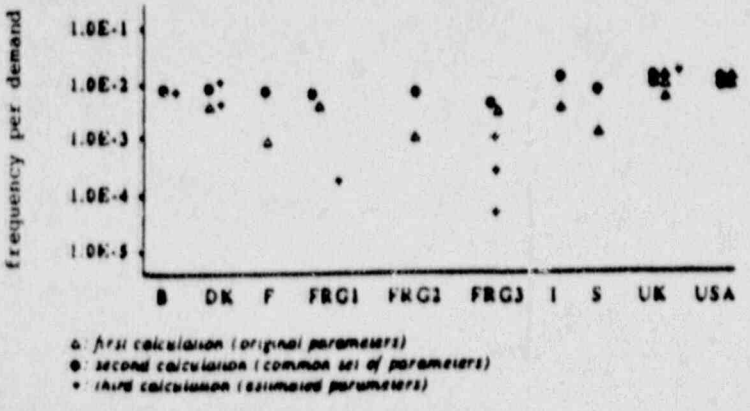


TABLE 8.1 (Röbke, 1973): Error sources of general working accidents

*(1)	50 %	- unsufficient attention
*(2)	30 %	- violation of safety rules (intentional)
	15 %	- violation of safety rules (unintentional)
	9 %	- overloading of phsiological functions
	8 %	- lack of skill
*(3)	5 %	- uncontrolled reactions to sudden incidents
*(4)	3 %	- lack of communication

* - relevant for nuclear power plants

(1) - due to boring and monotone working conditions

(2) - risk increasing motivation may be due to possible increase of wages, laziness or desire to show off

(3) - the main task of operators is to react to sudden incidents

(4) - team work and communication is essential in the control room

Note: multiple reasons are possible

Table 8.2: Number of Records for Each Personnel Category

Personnel	Totals by Personnel
Shift Supervisor	13
Shift Technical Advisor	1
Reactor Operator	1539
Auxiliary Operator	8
Maintenance Mechanic	211
I&C Technician	191
Engineers	3
Contractor Personnel	6
Plant Management	4
TOTAL	1976

Table 8.3: Number of Records for Each Accident Situation

Situation	Totals by Accident Situation
Loss of Coolant Accident (LOCA)	492
LOCA with Other Transient	6
Station Blackout	14
Loss of Off-site Power (LOSP)	71
Degraded Power Conditions	40
Anticipated Transient w/o Scram	12
Reactor Trip	22
Turbine Trip	19
Loss of Feedwater	28
Steam Generator Tube Rupture	58
Main Steam Isol. Valve Closure	4
Unclassified*	126

*Based on information in PRA, these accidents could not be classified under other categories.

Table 8.4: Number of Records for Each Action

Actions	Totals by Action
Testing	269
Operating	950
Monitoring	74
Inspecting	83
Checking	93
Deciding	53
Managing	3
Communicating	19
Calibrating	182
Responding	21
Maintaining	229
TOTALS	1976

Table 8.5: Number of Systems

Systems	Total by System
Air	2
Condensate	53
Containment (CS)	170
Electrical Distribution	22
Emergency Core Cooling (ECCS)	523
Emergency Power (EPS)	66
Engineering Safety Features (ESFS)	7
Hoodwater	213
Fire Protection (FP)	2
Instrumentation and Control (I&C)	149
Generator	22
Reactor Coolant (RCS)	69
Turbine	13
Water	113

Reference for tables 8.2 - 8.5: Ryan, 1985a.

Table 8.6: "Rule of thumb" for basic error quantification (Pope, 1986)

Classification of error type	Typical Error Probability
Processes involving creative thinking, unfamiliar operations, where time is short, high stress	0.1 - 1.0
Errors of omission where dependence is on situation cues and memory	0.01
Errors of commission such as operating wrong button, reading wrong dial etc.	0.001
Errors in regularly performed, commonplace tasks	0.0001
Extraordinary errors for which it is difficult to conceive how they might occur; stress free, with powerful cues.	0.00001

TABLE 8.7 (Hannaman, 1985a): Desirable features for a HRA model

- include quantification of crew success probability as a function of time.
- consider different types of cognitive processing, i.e., skill, rule and knowledge
- identify relationship of the model to factors influencing the non-success probability, such as
  - plant design features affecting man-machine interface
  - operator training and experience levels
  - operator stress
  - misdiagnosis
  - recovery
  - system time window for action
- be comparable to the highest degree possible with existing data from plant experience, simulator data or expert judgement
- be simple to implement/use
- help generate insights and understanding about the potential for operators to cope with the situations identified in PRA studies
- be compatible with and complement current PRA analysis techniques
- be scrutable, verifiable and repeatable

Table II, continued

United States (continued)

6.	Dec. 3, 1979 Quad City Reactors, IL (operational 1972)	Two valves verified open at 8am, with switches separated by six feet, were discovered closed at midnight. It was inferred that the mispositionings resulted from a deliberate act by knowledgeable plant employee(s).
7.	Feb. 1980 Browns Ferry Reactor, AL (operational)	During an investigation of several unexplained reactor trips, in which intentional malfeasance was suspected, 8 employees were suspended. The wife of one later appeared at the site asking to see the plant supervisor; a routine search discovered that she was carrying a pistol and a knife.
8.	Sept. 10, 1980 Salem Reactor, NJ (operational 1977)	Following a reactor trip and initiation of auxiliary feedwater flow, an anonymous caller warned of problems with a tank that adds necessary chemicals to auxiliary feedwater. The tank was discovered to be contaminated with sodium (500ppm) and chloride (1000ppm). Sabotage considered probable.
9.	June 6, 1981 Beaver Valley 1 Reactor, PA (operational 1977)	A manual valve on the High Head Safety Injection (HHSI) pumps' common suction line was found shut at 1 am and immediately reopened. The valve had been verified open 8 hours earlier. The chain and padlock that normally secured the valve in the open position could not be found. On the morning of June 5 similar locks and chains were discovered missing from 3 auxiliary feedwater pumps' manual suction isolation valves, although these valves were in their proper positions. According to the Nuclear Regulatory Commission (NRC) these events constituted "a major degradation of essential safety-related equipment designed to mitigate the consequences of a major occurrence such as a loss of coolant accident." An NRC source said that whoever closed the valve "knew exactly where to go and what to do."

Table II, continued

United States (continued)

10. Aug. 18, 1981 Nine Mile Point 1 Reactor, NY (operational 1969)	Two diesel generators found inoperable due to intentional tampering. The NRC judged that this constituted major degradation of the on-site back-up power supply, but not a major reduction in the protection of public safety.
11. Dec. 1, 1981 Perry Reactor, OH (70% complete)	Handful of metal filings found in the SCRAM discharge volume piping during the initial system check-out.
12. May 14, 1982 Brunswick 2 Reactor, NJ (operational 1975)	During a shutdown period, 12 in-core neutron detector tube guides were found to be bent. A deliberate act is suspected. In the event of an overpower transient or analogous occurrence, this would have represented "a major degradation of essential safety-related equipment...had the condition not been detected prior to start-up of the unit" (NRC).
13. 1982 Salem Reactors, NJ (operational 1977 and 1981)	On May 28 a steam generator feedwater pump tripped while the plant was operating at 100% power. An isolation valve and a vent valve were found mispositioned. The utility concluded these were deliberate acts to trip the plant. Labor union contract negotiations were in progress. Aug. 9 and 16, and Sept. 3: On these dates various incidents occurred in which intentional malfeasance was suspected. It was eventually judged that one incident probably represented an accident, while the other two may have resulted from deliberate acts. In no instance, according to the NRC, was there a major reduction in the degree of protection of public safety.
14. Nov. 18, 1982 Maine Yankee Reactor (operational 1972)	During refueling a cupful of metal chips, 2 bolts and 2 nuts were discovered inside the oil reservoir of a lube oil pump for the No. 1 Reactor Coolant Pump. No debris had been detected during an inspection two days earlier

Table III Miscellaneous Events at Nuclear Power Reactor Sites, Including Sabotage Threats, Indications of Security Lapses, and Indications of Tactical or Technical Sophistication on the Part of Antinuclear Activists or Potential Saboteurs (List is incomplete)

Canada		
1.	June 2, 1979 Darlington Reactors (under construction)	While other demonstrators penetrated the modestly guarded construction site by tunneling under or climbing over the fence, 5 members of Greenpeace dramatized their opposition to nuclear power by parachuting onto the site.
Federal Republic of Germany		
2.	June 1975 Biblis A Reactor (operational March 1975)	As a demonstration of lax security, a German politician carried a Panzer-faust bazooka past guards and detectors and presented the weapon to the plant's director.
Italy		
3.		There has been a report of a terrorist group (Red Brigade) document urging attacks on Italian nuclear power plants to exploit antinuclear sentiments.
United Kingdom		
4.	1966-1975 Facilities of British Nuclear Fuels, Ltd. and U.K. Atomic Energy Authority	23 threats and hoaxes received by staff. (Does not include threats to nuclear stations run by the Central Electricity Generating Board).
5.	1972 and ?	Scottish nationalists threatened on several occasions to sabotage an English nuclear power station.

Table III, continued

United Kingdom (continued)

6.	July 1980	20 members of the Bath Antinuclear Group halted a train carrying radioactive waste from Gloucester Sharpness for burial at sea. The protestors stopped the train by standing on a ten-foot high scaffolding that they had erected across the at dawn. 7 protestors arrested, and police called in heavy machinery to clear the track.

United States

7.	1977-June 1982 United States	During this period a total of 131 persons were reported fired from their jobs at nuclear power plant sites, or denied future access to the sites, owing to possession, consumption, or sale of marijuana or other drugs. Several examples: (a) On Nov. 8, 1979 at the operating Trojan nuclear plant in Oregon, 13 persons were arrested or fired as a result of an investigation into alleged use and dealing of marijuana and amphetamines. Of the 13, 8 were guards, 2 were former guards, and one had been a watchman. (b) On Dec. 9, 1981 at the operating Surry reactors in Virginia, 18 security personnel resigned or were fired for using marijuana off-site or reporting to work under its influence. (c) On Feb. 4, 1982 at the Shearon Harris nuclear plants under construction in North Carolina, a quality assurance weld inspector was fired due to drug use. Weld defects were found in seismic hangers that he had inspected. (d) On Feb. 5, 1982 at the operating Zion reactors in Illinois, a security force supervisor and a security force training coordinator were suspended owing to indications of drug and/or alcohol use both on and off site.

Table III, continued

United States (continued)

		(e) On Feb. 11, 1982 at the operating Turkey Point reactors in Florida, seven security officers, three workers and one concessionaire were denied future access to the site as a result of an investigation into illegal drug use.
8.	1976-June 30, 1982 United States	During this period there were more than 360 bomb threats received at reactors (operating or under construction).
9.	April 19, 1977 Fort St. Vrain Reactor, CO (operational 1979)	An NRC inspector who was not recognized gained access to the vital areas of the plant without a security challenge.
10.	Jan. 1978 Dow TRIGA Reactor, MI	Two NRC inspectors entered the reactor building through an unlocked rear door and proceeded through the control room into the reactor room. The inspectors had neither registered with the building receptionist nor were they badged as visitors. Their presence was not challenged although they had been seen by at least five persons.
11.	July 22, 1979 Salem Reactors, NJ (1 unit operational; 1 under construction)	An exit search of a suitcase carried by a contract employee who had been on site for eleven and one-half hours was found to contain a loaded .357 magnum revolver.
12.	1980	A communiqué was received by a newspaper in Bogota, Columbia stating that armed action would be taken in the United States if any military action were taken to end the occupation of the Dominican Embassy in Bogota, then under terrorist siege. The announcement was issued jointly by the Columbian 19 April Movement, the Dominican 14 June Movement, and the Armed Forces for the Liberation of Puerto Rico. The communiqué said: "You must remember, U.S. gentlemen, that you have never experienced war in your vitals and that you have many nuclear reactors."

Table III, continued

United States (continued)

13. May 1980 Seabrook Reactor, NH (under construction)	During attempted occupation of the site, state troopers, National Guardsmen and police used Mace, pepper gas, clubs and water hoses to repel an estimated 1800 antinuclear demonstrators.
14. Sept. 3, 1980 St. Lucie Reactor, FL (operational 1976)	A news reporter with a camera gained unauthorized access to the nuclear plant control room during an emergency drill.
15. Sept. 1981 Diablo Canyon Reactor, CA (completed but not yet operating)	The Abalone Alliance staged a two-week long anti-nuclear demonstration at the plant site. More than 1800 demonstrators, who were attempting to prevent workers from entering the site to load fuel into the reactor, were arrested.
16. Dec. 9, 1981 Monticello Reactor, MI (operational 1971)	Two security officers discovered sleeping at their gatehouse posts, 6am.