NEA/CSNI/R(92)18

RESTRICTED

OECD
NEA

STATE OF THE ART OF LEVEL-1 PSA METHODOLOGY

*A Report Prepared by a Task Force
of Principal Working Group N° 5
of the NEA Committee of the Safety
of Nuclear Installations (CSNI)*

Editor

Mr. R.K. Virolainen

January 1993

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS (CSNI)
OCDE NUCLEAR ENERGY AGENCY
Le Seine Saint-Germain - 12, boulevard des Iles
92130 Issy-les-Moulineaux, France

CSNI

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers who have responsibilities for nuclear safety. The Committee was set up in 1973 to develop and co-ordinate the Nuclear Energy Agency's work in nuclear safety matters, replacing the former Committee on Reactor Safety Technology (CREST) with its more limited scope.

The Committee's purpose is to foster international co-operation in nuclear safety amongst the OECD Member countries. This is done in a number of ways. Full use is made of the traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences. Some of these arrangements are of immediate benefit to Member countries, for example by improving the data base available to national regulatory authorities and to the scientific community at large. Other questions may be taken up by the Committee itself with the aim of achieving an international consensus wherever possible. The traditional approach to co-operation is reinforced by the creation of co-operative (international) research projects, such as PISC (Programmes for the Inspection of Steel Components), OECD/LOFT (Loss-of-Fluid Test), Halden, the TMI-2 Sample Examination Programme and the TMI-2 Vessel Investigation Project, and by the organisation of international standard problem exercises, for testing the performance of computer codes, test methods, etc. used in safety assessments. These exercises are now being conducted in most sectors of the nuclear safety programme.

Increasing attention is devoted to the collection, analysis and dissemination of information on safety-related operating experience in nuclear power plants; CSNI operates an international mechanism for exchanging reports on nuclear power plant incidents (NEA-IRS).

The greater part of the CSNI co-operative programme is concerned with safety technology for water reactors. The principal areas covered are operating experience and the human factor, reactor system response during abnormal transients and accidents, accident prevention and control, various aspects of primary circuit integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, severe accidents, and accident management. The Committee also studies the safety of the fuel cycle, and conducts surveys of reactor safety research programmes.

FOREWORD

In October 1989, the Principal Working Group on risk assessment (PWG 5) discussed the most problematic areas of Level-1 PSA. Several PSA methods were still evaluated to be in question such as analysis of dependencies, human errors, time-dependent phenomena, external events and analysis of uncertainties. Due to this discussion PWG 5 outlined the contents of a new Task, "State-of-the-Art of Level 1 PSA Methodology". Because of the broad expertise needed, the task force was divided into five subgroups reflecting the aforementioned topics.

A general objective of the group was to make a review of the use and maturity of the respective methods and to take a glance at the foreseeable future making remarks on the challenges of expected evolution of methodology and the direction to go. In order to provide support to the Task Force, a Workshop on "Special Issues of Level 1 PSA" was jointly organised by OECD and Bundesministerium für Umwelt, Naturschutz und Reactorsicherheit (BMU) in Cologne, May 27.-29.1991.

This state-of-the-art report, finalized in autumn 1992 for CSNI review is to provide insights into the maturity of Level 1 PSA methods for the parties who use or intend to use PSA for management and regulation of nuclear power plants. As well this report is to give incentives to research institutes to explore the solutions for some unresolved issues still existing in level 1 PSA methodology.

Task force activities

Editor of the report was R.K. Virolainen. The task force members contributing to various subtasks were:

Subtask 1: Dependent Failures

U. Hauptmanns, task leader	(FRG)
U. Pulkkinen	(Finland)
J.K. Vaurio	(Finland)
R.K. Virolainen	(Finland)
S. Hirschberg	(IAEA)
J.M. Jehee	(Netherlands)
G. Parry	(U.S.)
H. Paula	(U.S.)

Subtask 2: Human Errors

J. Mertens, task leader	(FRG)
F.W. Iven	(FRG)
J.-M. Lanore	(France)

Subtask 3: Time-Dependent Phenomena

J.-M. Lanore, task leader	(France)
U. Pulkkinen	(Finland)

Subtask 4: External Events

C. Zaffiro, task leader	(Italy)
E. Iaccarino	(Italy)
A. Pugliese	(Italy)
K. Abe	(Japan)
O. Keski-Rahkonen	(Finland)
U. Pulkkinen	(Finland)
R.K. Virolainen	(Finland)
S. Vuori	(Finland)
J. Murphy	(U.S.)

Subtask 5: Uncertainties

U. Pulkkinen, task leader	(Finland)
R.K. Virolainen	(Finland)
E. Hofer	(FRG)
N. Holloway	(UK)

CONTENTS

INTRODUCTORY REMARKS

This document reports on the State-of-the-Art of Level 1 PSA methodology focusing on some topics still being in question such as

- Dependent Failures with Emphasis on Common Cause Failures (CCF)
- Human Errors
- Time-Dependent Phenomena
- External Events
- Uncertainty

Most of the topics in Task 9 are well established issues. The analysis of time-dependent phenomena, however, is a topic which is not fully developed in present PSA studies. Therefore this subject calls for major developments also on a basic level.

Dependent Failures with Emphasis on Common Cause Failures

At present most of the different types of dependencies can be modelled explicity in a satisfactory way. This can be done primarily by use of standard event tree and fault tree based approaches to represent the functional and shared-equipment dependencies. In addition, supporting methods (for example walk- and think-through analysis), and computerized tools are available to improve the completeness of the analysis. Thus, many computer tools have options where attributes can be set for dependency factors e.g. common support systems, common rooms, common maintenance, same types of components, similar environmental circumstances and so forth, whichever can be recognized as potentially causing dependencies between components.

In contrast, the analysis of subtle statistical and probabilistic correlations is still in question. Statistical and probabilistic correlations are e.g. hidden shortcomings in components often inherited from past actions affecting the components such as design, manufacture, installation, leading e.g. to wrong tolerances, wrong materials, flaws in materials, different environmental sensitivities and several others, unforeseeable failure causes which usually need harsh circumstances to be realized as failure. Hidden shortcomings (often called trigger event) may expose the components to failures and if correlation is strong (coupling mechanism exist), it can increase the failure rate of several components simultaneously.

From a practical point of view, common cause failure (CCF) events represent those potentially significant intercomponent dependencies which are not explicitly represented in the logical model on the plant. Thus, the CCF methods in common use raise several questions such as how to assign correlation between CCF parameters in uncertainty analysis, how to analyse high redundancy structures (e.g. safety relief systems in BWRs) and how to credit physical separation of trains. Last but not least problem is the interpretation of sparse data in distinguishing between potential and real CCFs.

An inevitable problem is also that CCFs are highly plant specific and adequate analysis would require the use of plant specific parameters, which is difficult due to the sparse data base.

There are few preferences on how the practitioners typically deal with dependent and CCFs:

- Majority of practitioners is in favor of using a combination of explicit and parametric methods (IEEE/ANS PRA Procedures Guide NUREG/CR-2300, IAEA Guidelines for PSA, NUREG-1150).

- Minority of practitioners prefers of using methods where dependent failures are explicitly treated in fault trees without applying special CCF methods other than qualitative screening of CCFs (IREP and NREP PSA procedures Guides and IPE)

A unique solution between the aformentioned procedures is to use explicit fault tree analysis of dependent failures supported by worldwide direct CCF estimates for systems as given in report EPRI-NP 3967 or a simple system unvailability cut-off. A procedure of this kind is used in a Finnish PSA and in a UK PSA as well.

Human Errors

Analysis of human errors is still an unresolved issue in PSA. This is due to sparse data available for Human Reliability Analysis (HRA) as well as due to difficulty to cover different types of human errors by existing methods.

There is a consensus that human errors can be divided into three categories such as

- errors prior to an accident e.g. in maintenance, calibration, testing
- errors causing an accident initiator e.g. human error results in transient
- errors in response to an accident initiator e.g. misdiagnosis of accident initiator or response needed, errors in response action.

The first two categories of human errors can to a certain extent be supported by plant specific data but human actions during accident situations remain as the most difficult topic for analysis.

An inherent issue in human performance is its ambiguity. Human interactions provide both beneficial and detrimental contributions to safety. Detrimental actions typically increase the unavailability of plant systems or result in an initiating event. The beneficial actions such as correct diagnosis of initiating event and implementation of recovery of systems decrease the potential to accidents.

A methodological difficulty of human error analysis is inherited from the special nature of human mind. As far as the assumption can be made that human errors are only slips or errors in following correct procedures, the present methods cover the possible errors made. If other types of errors (errors of commission) are included, no well established methods are available.

The available PRA Procedures guides recommend the use of methods as follows

- SHARP is a framework for a systematic treatment of man-machine interactions. It can be used in conjunction with different methods. SHARP procedure with various HRA methods is recommended by NREP Guide, NUREG/CR-2815 and IAEA guidelines.
- ASEP HRA method is used in NUREG-1150
- THERP method is recommended by IEEE/ANS Guide, NUREG/CR-2300 and IREP Guide, NUREG/CR-2728

An interesting approach amongst the HRA methods are those most based on expert judgement. SLIM-MAUD is an example of these methods. It makes use of both expert judgement and simulator based time reliability curves (TRC). Expert judgement is mentioned briefly in the context of HRA in NREP, EWAT, IAEA PRA guidelines and IPE. Expert judgement is mentioned in SHARP Procedure as well.

The contemporary human error analysis suffers from two main unresolved issues; sparse data base on all human activities and shortage of methods for dealing with errors of commission. The sparse data on human activities such as diagnosis errors and other human actions during accident sequence can to some extent be replaced by using full-scale plant specific simulator. In contrast, the treatment of non-procedural operator measures is still at early development phase.

Time-Dependent Phenomena

Time-dependent phenomena are an evolutionary topic in PSA. Only a few time dependent phenomena are modeled in PSA studies in a detailed way. One example of such a detailed modeling is time dependent success criteria in long term accident sequences (French PSAs). Several time dependent phenomena such as aging of components, time dependent unavailabilities (test intervals, latent failures, repair), time dependencies of accident sequences (time dependent succes criteria, time dependent operator actions, time dependent physical phenomena) are usually treated in averaged or conservative way in PSAs. The question how good the approximation represented by the averages is, remains open.

In some US PSA studies time dependency of emergency diesel generator mission unavailability from the recovery of offsite power is considered by an integrated way (e.g. Zion PSA). In Loviisa PSA study, a trend analysis (aging, learning) of failure rates has been made. Without saying that the examples given above are unique, it is evident that the contemporary PSA procedures do not favor of using time dependent models especially in the context of accident sequence modeling. This is evidently due to the model complexity and time consuming calculation routines which make the time dependent models rather less attractive.

A major incentive to the introduction of time dependent models in PSA studies is the extension of PSA towards short term decision making in real time. In order to deal with increasing or decreasing trends of phenomena e.g. time delays existing for recoveries and competition between degrading system function and decreasing residual heat production, more sophisticated models may be needed.

External Events

Subgroup, external events, of accident initiators has frequently given a significant contribution to NPP risk. Typical external events such as seismic events, fires and flooding (external, internal) are vital parts of recent PSA studies. All these accident initiators are of a clearly distinct nature as compared with internal initiators. External events are predecessors of accident initiators rather than initiating events themselves. This makes the analysis of external hazards different from that of internal events.

The contribution of external events to risk is separately site and plant specific. Quite large contributions of external risks to older plants are plausible and closely argued because of the vulnerable or non-existing physical protection and separation in older designs. In new designs, however, component qualification, adequate physical separation and risk averse lay-out are expected to stand harsh environments and to diminish the risk of external events significantly.

An inherent methodological feature of contemporary methods is large uncertainty. Statistical uncertainties of the results are in range 100 to 1000, expressed in terms of error factor. Large uncertainties involved in external risks estimates present difficulties in combining these results with those of internal events.

The methodological maturity of external event analysis is still partly poor. Especially the fire development analysis needs improvements. A number of fire development analysis models are available and development of several new models is underway. Multicompartment calculation codes are not yet well validated. Therefore, great care should be taken to understand the underlying fire phenomena when using these models for systems composed of complicated or big compartments. When properly used these programs offer even now an invaluable tool for fire development assessment.

The intensive model development associated e.g. with recent HDR fire experiment programme in Germany, give quite promising possibilities for future fire simulation of reactor containment buildings containing real fire loads found in nuclear reactors, such as pump oils and electrical cables. Although much development work is still needed, it is clear that already in the near future there are available validated fire simulation models running on personal computers or workstations, which can be used for quantitative fire risk estimation and mitigation of critical points of nuclear installations.

Uncertainty analysis

Uncertainty analysis in PSA is to give a realistic picture of credibility of analysis usually containing a number of uncertain features such as reliability data, modelling assumptions e.g. success criteria, systems interactions, dependent failures and CCFs and expert judgment. The uncertainty in reliability data reflects on the one hand stochastic variability and on the other hand lack of knowledge. The modelling uncertainty reflects the inability to deal with all phenomena, failure mechanisms or accident possibilities in the model.

The technical complexity is a decisive point for incompleteness issue. In practice, however, the crucial issue seems not to be only the complexity but the inadequate design and lack of physical protection and isolation between vital safety systems, support systems and redundancies and lack of diversity which makes the modelling of the plant difficult. If the design based physical protection of components, separation between systems and trains and diversity of components are adequately provided, it implies that several reasons for dependencies, interactions and CCFs are cut down and, to a large extent, systems and trains are independent of each other. This facilitates the modelling and lessens the exposure of PSA to incompleteness.

Even though probabilistic uncertainty analysis is well-known and by and large mature part of PSA, it still contains some less discussed issues. For some analysis approaches problems arise as dependencies are concerned. Dependencies between minimal cut sets are a problem for analytical methods (e.g. moment propagation and Discrete Probability Distribution methods). Dependencies between components raise a question of correlation between parameters of CCF methods. Pooling of plant specific data makes that a common failure rate distribution has to be used for parallel identical components which may sometimes extend the uncertainty of systems reliability estimate significantly.

1. Dependent Failures with emphasis on common cause failures

1.1. Introduction

In fault and event tree analyses dependent failures have to be treated in addition to independent failures in order for meaningful results to be produced. The effect of dependent failures is especially grave if they affect redundant components and occur within a small interval of time so that the failed states exist simultaneously. The following six types of dependent failures may be distinguished:

(1) Shared equipment dependencies where one system is a support system for others or a component is shared by several systems/subsystems. Failure of the support system leads directly to complete or partial failure of all the supported systems.

(2) Functional dependencies where the operation or non-operation of a system affects the ability of another system to be operated and may therefore cause its unavailability (e.g. where a low pressure injection system cannot be used unless the reactor is depressurized first).

(3) Common cause initiators where the availability of support or mitigating systems is affected by an initiating event. This includes major energetic external events but also equipment-related transients.

(4) Physical interaction failures where the environmental effects caused by a failure (e.g. after a pipe break) cause other systems to fail.

(5) Human interaction dependencies where an operator error affects the operation of more than one system or component.

(6) Common cause failures where two or more identical or similar components fail at the same time because of some common cause not covered by explicit modelling of the types of dependencies given above. Common cause failures may, for example, be due to design errors or deficiencies, lack of quality control in manufacturing or installation, procedural errors during operation or maintenance, environmental effects such as excessive temperature.

The first four categories of dependent failures should be modelled and taken into account explicitly in fault tree analyses /1-1/. This has been common practice in recent PSA studies /1-2/ - /1-4/. Similarly multiple failures due to clearly identifiable human errors, such as for example errors in calibrating several redundant measuring devices should be modelled explicitly in the fault tree.

The following two examples addressing point 1 and 4 are meant to underline this.The fault tree of Fig. 1.1 concerns the failure of two parallel pipes. Apart from a spontaneous failure of pipe 1 (basic event x_1) there exists the possibility of a spontaneous failure of pipes 2 (basic event x_2) such that it ruptures pipe 1 (event x_3).

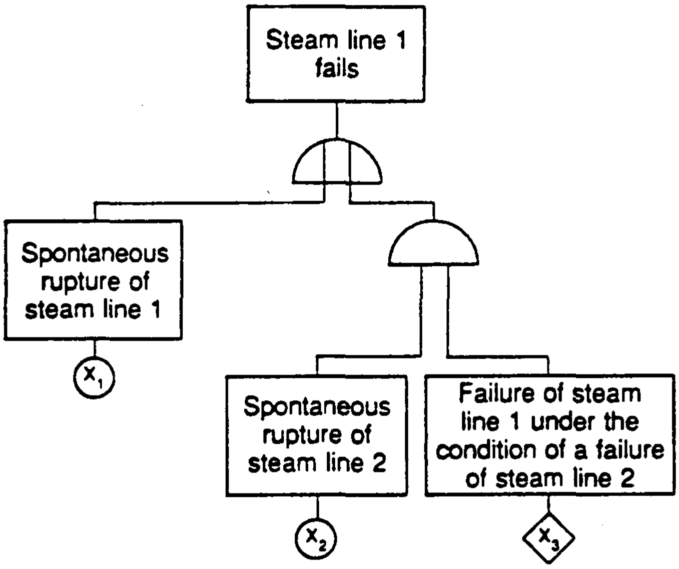

Steam line 1 fails
Spontaneous rupture of steam line 1
x_1
Spontaneous rupture of steam line 2
x_2
Failure of steam line 1 under the condition of a failure of steam line 2
x_3

Fig. 1.1: Fault tree for a secondary failure

The dependence of the failure of pipe 1 on the rupture of pipe 2 is described by the conditional probability for the occurrence of the event x_3. This will p.e. be obtained from relevant model calculations, in the present case from the field of structural mechanics and thermal hydraulics.

Fig. 1.2 shows the modelling of a functional dependence. It concerns the failure of two redundant valves. Their failure may be brought about by a simultaneous failure of both valves or of both actuating signals or the failure of the 380 V supply which they have in common (basic event x_3)

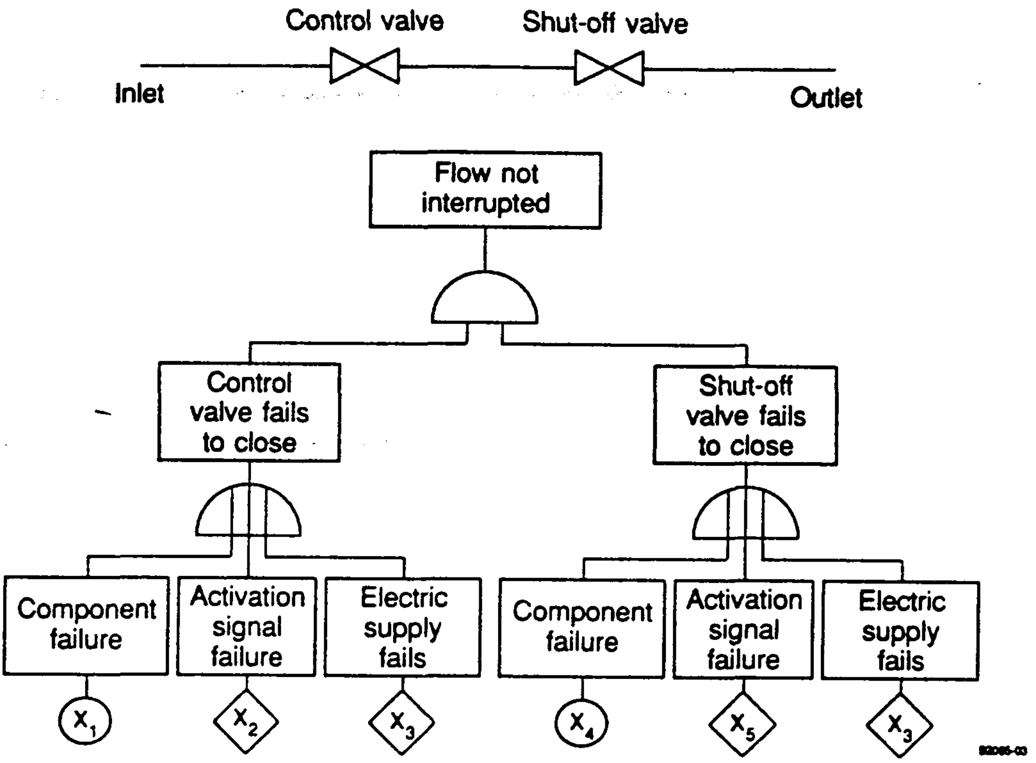


Fig.1.2: Fault tree for a shared equipment dependence

In this case probabilities are assigned on the basis of the relevant failure rates for independent failures.

Common cause (CC) failures are introduced as basic events into the fault tree in addition to the basic events reflecting independent failures. Their importance is underlined by the fact that, depending on the PSA study considered, the calculated core-damage frequency would be reduced by 20% to 60% if there were no common cause failures /1-5/.

Common cause failures are generally quantified employing parametric models. Such models, which serve to interpret operational experience on dependent failures, are dealt with in Section 1.4.

Occasionally different categories from the above mentioned ones are used. In /1-6/ for example, functional dependencies were included together with common cause failures in the β-factor which is the characteristic parameter of the Beta Factor Model (cf. Section 1.4.2).

Evidently, the delimitation of failures which is adopted, influences both the fault tree model and the interpretation of the observed operational experience.

The division of dependent failures into the categories mentioned leads to a more complex fault tree model than would result if several of these categories were pooled and jointly treated with a parametric model.

This increase in fault tree complexity should, however, not represent a major problem with present-day computer programs for fault tree evaluation.

Although explicit modelling should go as far as explained there may be cases in which it is considered too much of an effort and therefore the analyst may decide to include several of the categories of dependent failures in the parameteric model. Another reason for doing this may be the type of data available, which in some cases may contain events which should, in principle, be modelled explicitly. It must be assured, however, that the pooling process takes into account the specific conditions of the component location in order to avoid mistakes.

Modelling of common cause failures is a complex task composed of several steps as can be seen from Fig. 1.3. However, recent Benchmark Exercises coordinated by the JRC Ispra /1-8/ and those carried out in Nordic countries /1-9/ contributed to the solution of a number of problems in identification, modelling and quantification of CCF events. Based on these experiences and those from current PSAs a procedural framework for CCF analysis was developed /1-7/. This was followed by application of the cause-coupling method to demonstrate a systematic approach towards analysis of defences against CCFs (cf. Section 1.3.2 and /1-10/). The IAEA published a procedure for conducting CCF analysis /1-11/, which in a concise form combines the frameworks of references /1-7/ and /1-10/, and in addition addresses some pitfalls. The IAEA is presently developing a structured example application of this procedure /1-12/.

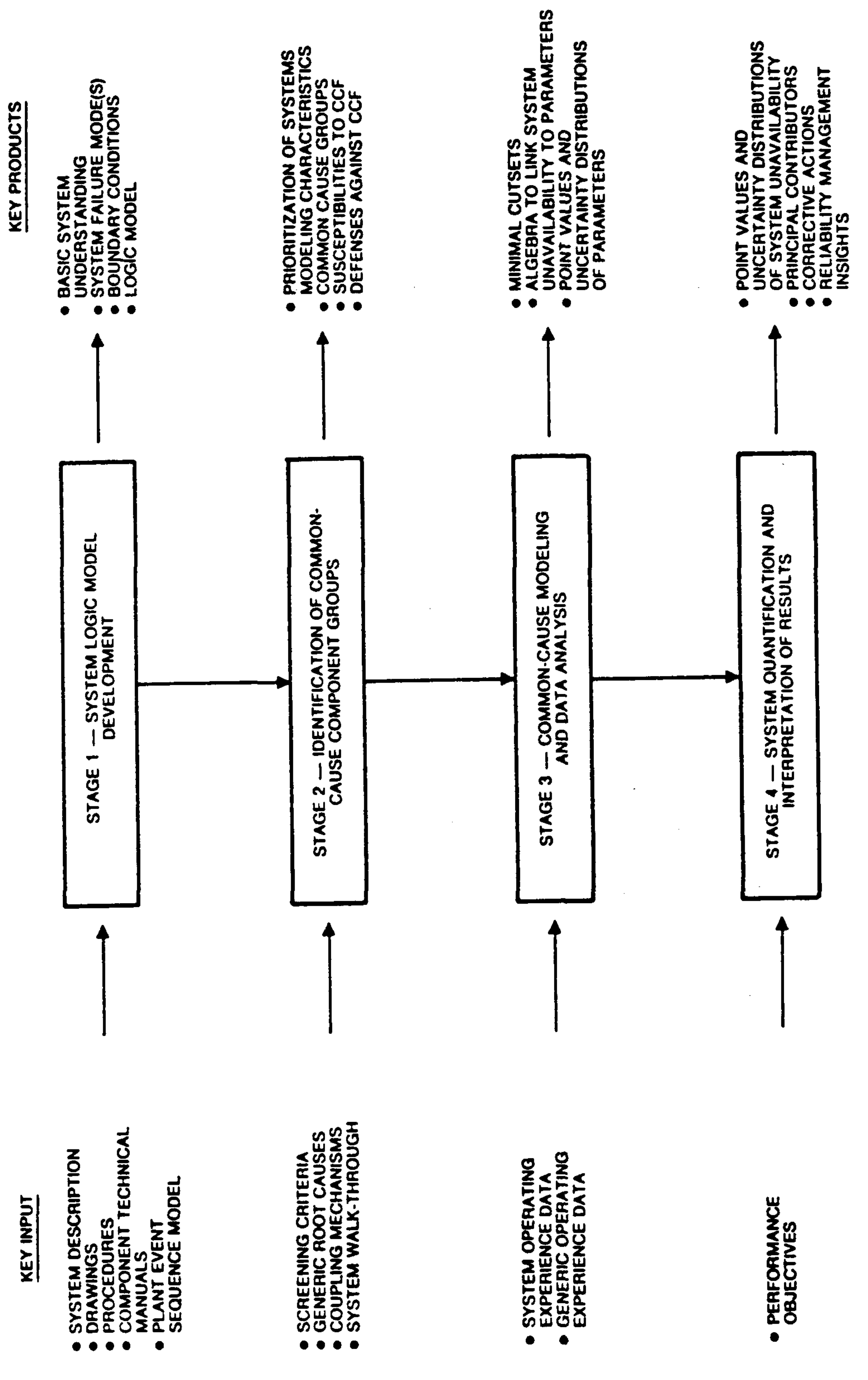

KEY INPUT
• SYSTEM DESCRIPTION
• DRAWINGS
• PROCEDURES
• COMPONENT TECHNICAL MANUALS
• PLANT EVENT SEQUENCE MODEL
STAGE 1 — SYSTEM LOGIC MODEL DEVELOPMENT
KEY PRODUCTS
• BASIC SYSTEM UNDERSTANDING
• SYSTEM FAILURE MODE(S)
• BOUNDARY CONDITIONS
• LOGIC MODEL
• SCREENING CRITERIA
• GENERIC ROOT CAUSES
• COUPLING MECHANISMS
• SYSTEM WALK-THROUGH
STAGE 2 — IDENTIFICATION OF COMMON-CAUSE COMPONENT GROUPS
• PRIORITIZATION OF SYSTEMS MODELING CHARACTERISTICS
• COMMON CAUSE GROUPS
• SUSCEPTIBILITIES TO CCF
• DEFENSES AGAINST CCF
• SYSTEM OPERATING EXPERIENCE DATA
• GENERIC OPERATING EXPERIENCE DATA
STAGE 3 — COMMON-CAUSE MODELING AND DATA ANALYSIS
• MINIMAL CUTSETS
• ALGEBRA TO LINK SYSTEM UNAVAILABILITY TO PARAMETERS
• POINT VALUES AND UNCERTAINTY DISTRIBUTIONS OF PARAMETERS
• PERFORMANCE OBJECTIVES
STAGE 4 — SYSTEM QUANTIFICATION AND INTERPRETATION OF RESULTS
• POINT VALUES AND UNCERTAINTY DISTRIBUTIONS OF SYSTEM UNAVAILABILITY
• PRINCIPAL CONTRIBUTORS
• CORRECTIVE ACTIONS
• RELIABILITY MANAGEMENT INSIGHTS

Fig. 1.3: Stages of the framework, key input, and procedures of a CCF analysis (from /1-7/)

1.2. Guidance on desired characteristics and interpretation of data

1.2.1. Characteristics

The probabilities of the simultaneous failure of a high number of redundant components, e.g. 3-out-of-4 or 4-out-of-4 are of special importance for fault tree analysis because they are likely to make the system function in question fail. The simultaneous failure of fewer redundancies, on the other hand, would frequently require an additional independent failure to occur in order to cause a failure of the system function.

The probability of the simultaneous failure of a high number of redundant components can, in general, not be estimated directly from operating experience because such failures are hardly ever observed in the system under consideration or in any other similar system. A zero-failure statistics evaluation, which despite the low degree of confidence to be placed in the result would often be used in such a case, is not recommendable because it might lead to unrealistically bad results. This is due to the fact that the period of observation of reactor operation is generally too short, especially since the number of systems to be considered similar to the one under investigation tends to be small.

Operating experience with failures due to a common cause can frequently not be applied directly to the plant under investigation because

- after the occurrence of a common cause event its cause is discovered and removed with a certain probability so that its recurrence becomes less probable,
- operating experience in the plant under investigation is normally not sufficient; therefore failures have to be included which occurred in systems of other plants which are different from the ones under investigation,
- frequently the failures which occurred affected different numbers of redundancies from those to be assessed.

Because of these differences with respect to the case under analysis events may be taken into account for assessing CC probabilities only on the basis of engineering judgement.This judgement refers to whether and in what way an observed failure may be applied to the system under investigation.

In addition, it must often be decided with what probability an observed failure may lead to a different failure combination (e.g. observed 2-out-of-3, to be assessed 4-out-of-4). Single failures have to be taken into account as well, if their underlying damage mechanism is characteristic of CC failures. This could be the case, for example, if one component of a redundant group has failed and the other components of the group are affected by the same failure mechanism although they have not yet failed.

The analysis of observed common cause failures shows that they are mostly due to specific properties of the affected equipment. For example, corrosion may only occur if there is a contact between certain types of materials or if the surrounding medium has specific chemical properties. In general, the conditions under which the observed common cause failure occurred do not or no longer apply to the system under analysis so that such a failure cannot occur in the same way. If strict criteria for the relevance of observed common cause events for a specific analysis are applied, most observations cannot be taken into account. Since they must be taken into account all the same given the dearth of occurrences the question of where to draw the line between events to be included and those which are not be included arises. If an event is to be counted the following conditions must be met:

- the technical systems where the failure was observed must have sufficient resemblance with those of the analysis;
- similar failure mechanisms to those observed must not be impossible in the analysed system nor should they be so unlikely that their inclusion would obviously be a mistake.

The likelihood of an erroneous judgement should be kept small by deciding, whether or not the criteria are met at the level of equipment or component where similarities are more likely than at system level.

In judging whether an observed failure mechanism is to be taken into account for the system under consideration it is useful to distinguish between its immediate and its root causes. Examples for immediate causes are corrosion, pipe blockage, trapped gas volumes in pipes filled with liquids or falsely calibrated measuring devices. The corresponding generic causes may be design flaws, inappropriate supervision of operation or inadequate maintenance. For example, the root cause of a failure due to corrosion might be the choice of an inappropriate material or of incompatible materials or the use of inadequate lubricants in maintenance. An observed failure is to be taken into account if its immediate cause e.g. corrosion is of relevance for the system under investigation even if the root cause e.g. wrong choice of material is considered not to apply. It is not to be counted if the immediate cause may be excluded with high probability.

The valuation depends on the individual case, and the judgement involved allows a margin of interpretation. The following examples may serve for clarification:

- in pipes transporting boric acid of a concentration of 20,000 ppm pipe blockages due to crystallization occurred even cross sections were large. In systems working with pure water or boric acid of less concentration a blockage of large cross sections may be excluded whilst blockage of pipes with small cross sections is to be expected;
- an event with false positioning of valves without position indicators should not be counted when analysing valves with a position controller and an indication in the control room;
- accumulation of gas in pumps during stand-still has occurred for different underlying causes. Such events should be accounted for although the origin of the gas may not apply for the system under consideration;
- if an observed failure mechanism has been excluded for the case under investigation it is recommended to check whether it can be used for assessing similar equipment. This proceeds if this equipment can fail in the same way as the components to be analysed. For example, if a pump fails in a system with a common oil circuit because of a lack of oil this would be counted as a functional dependency and not as a common cause failure. If, on the other hand, an observed cause could apply to a system of separate oil circuits, e.g. the formation of sludges, such an event would have to be considered as a common cause failure.

The judgements to be made by the analyst are supported if the underlying data satisfy certain characteristics, as, for example, exposed in /1-12/. The key features identified there are described briefly below. It should be recognized that many of the characteristics are also essential for estimating single failure event probabilities. The ideal data base would:

a) Describe the component involved in terms of its engineering characteristics. This is useful for the CCF analyst to identify the events that meet his needs.

b) Record the operational history of each component in terms of the times associated with periods of operation, dates of demands (surveillance tests or real), and of event reports (failures or maintenance), etc. In order to estimate the reliability parameters of most of the simple PSA models, it is necessary to have a record of the exposure of the components in terms of number of demands (including successful demands), time in stand-by, time in operation, etc. It is also necessary to have a record of the number of events which have occurred and which have been associated with failure or unavailability of each component, and the total time the components have been unavailable. In this context, it is important to note the operational status of the plant at the time of the events. Some failures are only likely to occur in certain operational conditions (It should be noted that if the Alpha-Factor Model (cf. Section 1.4.5), or any other similar, failure-ratio based, parametric model such as the MGL model (cf. Section 1.4.3) is to be used, the requirement to have records of the exposure can be relaxed).

c) Contain a sufficiently detailed description of each event in terms of the states of the components of interest (i.e. failure mode) and the impact on the functionality of the system of which they are a part. Each event in the data base has the potential for contributing to a PSA basic event which can be a failure in a particular failure mode or an unavailability due to the component being in maintenance (either preventive or corrective). In order to make the association with a specific basic event, it is necessary to be able to distinguish between different degrees of degradation or failure. A commonly used classification is: a catastrophic failure is one which prevents the component from performing its mission; a degraded failure is such that the component can perform its mission, but at a less than optimum performance level; and an incipient failure is such that there is no significant degradation in performance but there are indications of a developing fault. References to other, similar failures are also helpful.

d) Provide the number and status of redundant components associated with the components involved in a failure event. In particular, specify when more than one component is failed. This may be done explicitly or by cross-referencing other reports. This is often not done when the raw data is contained in a maintenance or component reliability data base, and the analyst should always be careful to look for temporal correlations.

e) Provide a clear extensive presentation describing the chain of events which led to the failure, a determination of a root cause, and an assessment of the inadequacy of the defences. In /1-13/ a root cause is defined as "the most basic reason for an effect, which, if corrected, will prevent recurrence." This definition is most appropriate because prevention (as well as preventing similar occurrences at other plants) is one of the goals in ensuring reliable nuclear power operation.

Determining the root cause is not always straightforward, and there will often be an element of uncertainty regarding the root cause of an event. Additionally, a number of causes may have contributed to an event, and it may be difficult, and possibly misleading, to select one of the contributing causes as the root cause for the event. Thus, it is often necessary to present some discussion of a number of causes which have or may have contributed to a failure occurrence.

In /1-10/ (cf. Section 1.3.2) the concepts of trigger events (events which initiate the transition to the failed state), and conditioning events (events which set the stage for failure but do not by themselves cause failure) are introduced as a means for describing events and focusing attention on the essential sub-events which led to failure. It is also pointed out that the root cause may be identified with the trigger event or a conditioning event depending on the defensive strategy the plant adopts. Different plants will often select different approaches for preventing recurrence of a failure event. These defensive strategies differ because the plants may have different management philosophies, technical expertise, maintenance and surveillance approaches, and priorities in allocating budget and resources. As a result, the plants will attribute different root causes to a failure.

In /1-10/ the importance of identifying coupling factors is also pointed out. For failures to become multiple failures from the same cause, the conditions have to be conducive for the trigger event and/or the conditioning events to affect all the components simultaneously. The meaning of simultaneity in this context is that failures occur close enough in time to lead to the inability of redundant components to perform the mission required of the redundant system of which they are a part. It is convenient to define a set of coupling factors. A coupling factor is a characteristic of a group of components or piece parts which identifies them as susceptible to the same causal mechanisms of failure. Such factors include similarity in design, location, environment, mission and operational, maintenance, and test procedures. These, in some references, have been referred to as examples of a coupling mechanism, but because they really identify a potential for common susceptibility, it is preferable to think of these factors as factors which help define a potential common cause component group. Defences against common cause failures can act by effectively decoupling components as well as by preventing the root cause.

It is important to present details about all factors that contribute to failure events so that an analyst can make a better assessment of how, and how well, other plants are protected against these occurrences.

f) Include a presentation of the method of discovery of the failure. The description of how a component failure was detected can be used to assess and/or design defences against the identified failure. It is important to know whether detection was a result of a test or of a demand.

The presentation of the method of discovery becomes even more valuable when details are included regarding tests or other surveillance techniques which failed to detect the condition. Knowing why a certain defence failed at one plant can help an analyst make a better assessment of the quality of the defence at his plant.

g) Include a presentation of the corrective actions. This is another source of informaton about defences against CFFs. It provides additional perspective on the utility's perception of what was the root cause, and gives insight into its defensive strategy.

h) Include information on the scheduling of inspection testing and maintenance activities for redundant components. The approach used to schedule these activities for redundant components (e.g. staggered versus simultaneous testing) can further improve their effectiveness against CFFs. As pointed out in reference /1-7/, the estimates for common cause failure model parameters may be different if the data are from plants with staggered versus non-staggered testing schedules. This information also provides a means of assessing the maximum latent time for the CCF.

i) Include a presentation of selected aspects of inspection, testing and maintenance activities, that may differ from practices at other plants. This is useful in that these activities play a major role in component reliability. Since all nuclear power plants have some kind of inspection, testing, and maintenance activities that may differ from practices at other plants. This information would allow analysts to make a better assessment of how well other plants are protected against the reported occurences.

1.2.2. Interpretation

The use of generic CCF data is an unavoidable issue in plant specific PSA. The process of interpreting generic data for plant specific applications can and partly has to be performed in different ways because recognition, analysis and interpretation of CCF data are to some extent associated with the CCF model used. Even though the CCF root cause analysis /1-13/ serves, in principle, as a conveyance to all CCF models, the statistical variables needed are different for each model which requires further analysis. This is due to the different underlying nature of the models.

Parametric models (β-family) (cf. /1-14/ and Section 1.4.2) are based on the ratios between dependent and independent failure rates. The shock rates resulting e.g. from environmental impact are necessary for shock models (cf. /1-15/ and Section 1.4.6 and 1.4.7). The correlation models (cf. Section 1.4.10) need the statistical correlation information explicitly or implicitly from the data, because the correlation models accomodate the dependency in a statistical correlation coefficient and/or in the increased failure rates.

In most cases the failures of redundant components cannot be shown to be dependent because of primary causes, but common hidden factors lead to a common tendency of the components to fail. The further light thrown on these causes by more thorough analysis is often associated with large uncertainties which can be misleading when deciding on the implementation of CCF defence measures /1-15/. The tendency of components to fail is interpreted in different ways in different CCF models even though the basic classification and analysis of dependent failures would be quite similar /1-7/, /1-10/, /1-14/, /1-16/ and /1-33/. It is proposed in /1-17/ that the poor quality or deterioration of components sometimes make them deviate from the nominal component reliability significantly due to e.g. design, manufacture or installation errors and environmental causes which decrease the system reliability just like CCFs.

The interpretation of data for parametric models is straightforward and focuses on the search for simultaneously or almost simultaneously occurring multiple failures. In this context the interpretation of dependencies is also extended to potential CCFs by searching for degraded components with similar root causes as the observed CCFs. The share of degraded components are taken into account by weight factors in order to account for the effect of these failures on system unavailability. It is evident that the introduction of degraded components in that way will have advantages and drawbacks. On one hand, it tends to extend and supplement the CCF information and to complement the effect of CCFs. On the other hand, assignment of weights is based on subjective judgement and introduces new uncertainty contributions that are difficult to assess.

Shock models, such as the BFR model (cf. Section 1.4.6), contain parameters like the omega factor (lethal shock parameter) as well as conditional probabilities and nonlethal shock rates. Shock models, therefore, can in principle deal with the degraded potential failures in a more consistent way than the beta family. Consequently, these underlying features of shock models also make the data interpretation more difficult than that of the beta family.

A logical consequence of the internal structure of shock models is that the interpretation of data is not necessarily focused as thoroughly on the qualitative event analysis of component failures as in the case of the beta family. The statistical structure of shock models tends to account for all kinds of dependencies which potentially lead to single or multiple failure. Further, an additional important analysis step in the shock models is the interpretation of shocks and shock rates from the data. This implies that much subjective judgement has to be used in order to get the necessary parameters.

In the correlation models the dependency between components is interpreted as a statistical variable that ranges from complete independence to complete dependence. This underlying feature makes a clear distinction between parametric CCF models and correlation models. The BFR model is an example of an approach between those models.

The data interpretation for correlation methods e.g. the model proposed in Section 1.4.10 is not based on the qualitative recognition of root causes of components and multiple failures but on the variance of the identical components unavailabilities and the correlation (dependency) of the unavailabilities of parallel components. The correlation model utilizes the generic (industry wide) data for use in a specific plant. The data interpretation and the use of discrete probabilities like those of the BFR model makes some newer models /1-18/, /1-19/ to resemble the BFR model.

It is evident that both the data interpretation and the choise of the CCF model itself have consequences for the unavailability calculations and results. A comparison of different CCF models /1-20/ shows that using the same basic data and the same interpretation of data for different models the unavailability estimates deviate fairly much in simple parallel 2-out-of-2 structures. The comparison included the Beta-Factor Model, the BFR-model, Hartung's correlation model, the complete dependency model ($E(X_1X_2) = E(X^2)$), and the direct estimation model (prior moment matching method). The extensive data base for Diesel Generators (LERs 1976-78) /1-21/ was used as well as the basic interpretation of data, (distinction between independent and dependent failures and determination of multiple failures given there). Approximately 40 Diesel Generator systems were involved and they represent a very good data base, which produced an excellent Diesel Generator system unavailability distribution for comparing different methods.

The comparison indicated that the expected value of the correlation model and the direct estimate were the best match. The Beta-Factor Model introduced a slight underestimate and the BFR model a quite clear underestimate which is not much bigger than the estimate resulting from the independence assumption. The most conservative estimate was given by the simple correlation method ($A = E(X^2)$), which corresponds with the complete dependence of parallel DGs.

The comparison indicated that not even the robust analysis and interpretation of data alone can solve all CCF issues.The CCF model should be able to deal with and distinguish between the different kinds of common causes such as shocks (lethal and nonlethal) and also weaker dependencies (physical, statistical) because the correlation between component failures may have quite a remarkable effect on the unavailability of systems. The interpretation of these correlations is CCF model specific and depends on the structure of the model.

A significant problem with CCF data interpretation is the so called mapping-up procedure which is used to extend the scarce CCF data by judgement. This is done for example, by extrapolating the rate of multiple 3 out of 3 failures up to 4 out of 4 failures because such failures are rare. This is a common procedure in PSA and can strongly affect the value obtained for the unavailability of systems.

A corresponding interpretation issue is always present in PSA due to the unavoidable use of an industry wide CCF data base, which means that CCF data of dissimilar plants are used in plant specific PSAs.

1.3. Qualitative Considerations

1.3.1. Qualitative Common Cause Analysis /1-22/

In the step of qualitative common cause analysis a search is made for common attributes of components and mechanisms of failure that can lead to potential common cause failures. Analysts in the past have relied on a variety of factors, including engineering insight, obvious signs of dependence, and the perceived effectiveness of certain defences, to identify component groups for common cause analysis.

This process can be enhanced by developing a checklist of such key attributes as design, location, operation, etc., for which the analyst can assess the degree of similarity of the various components. A partial list of such attributes is the following:

- *component type* (e.g. motor-operated valve), including any special design or construction characteristics (e.g. component size, material, etc.)
- *component use:* system isolation, flow modulation, parameter sensing, motive force, etc.
- *component manufacturer*

- *component internal conditions* (e.g. absolute or differential pressure range, temperature range, normal flow rate, chemistry parameter range, power requirements, etc.)
- *component boundaries and system interfaces* (e.g. common discharge header, interlocks, etc.)
- *component location name and/or location code*
- *component external environmental conditions* (e.g. temperature range, humidity range, barometric pressure range, atmospheric particulate content and concentration, etc.)
- *component initial conditions* (e.g. normally closed, normally open, energized, etc.) and *operating characteristics* (e.g. normally running, stand-by, etc.)
- *component testing procedures and characteristics* (e.g. test interval, test configuration or line-up, effect of test of system operation, etc.)
- *component maintenance procedures and characteristics* (e.g. planned, preventive maintenance frequency, maintenance configuration or line-up, effect of maintenance on system operation, etc.)

The above list or a similar one is simply a tool to help account for factors affecting component interdependence and to readily identify the presence of identical redundant components. It provides a method of documenting the qualitative analysis required to support the selection of common cause groups. Based on experience in performing these evaluations and in analysing US operating experience data, additional guidance can be provided in the assignment of component groups. The most important guidelines follow.

- When identical, functionally non-diverse, and active components are used to provide redundancy, these components should always be assigned to a common cause group, one group for each set of identical redundant components. In general, as long as common cause groups of identical active components are identified, the assumption of independence among diverse components is a good one and is supported by operating experience data.
- When diverse redundant components have piece parts that are identically redundant, the components should not be assumed to be fully independent. For exam-

ple, pumps can be identical except for their drivers. One approach in this case is to break down the component boundaries and identify the common piece parts as a common cause component group.

- In systems reliability analysis, it is frequently assumed that certain passive components can be omitted, based on the argument that active components usually dominate system unavailability. In applying this principle to common cause analysis, care must be exercised to not exclude such important events as debris blockage of redundant-pump strainers, etc.

Susceptibility of a group of components to common cause failures not only depends on their degree of similarity to such attributes as those listed here but also on the existence or lack of defensive measures against common cause and the degree of their effectiveness.

Although much work is needed to determine the relation between various root causes, coupling mechanisms, and defensive tactics, valuable insight can be gained by considering, in a qualitative fashion, the effectiveness of some broad categories of defences for various general groups of causes. Such an analysis can be useful in the evaluation of common cause event data for plant-specific applications. As an example, physical separation of redundant equipment may reduce the chance of simultaneous failure of the equipment due to some environmental effects. In this case the defence acts to weaken the coupling mechanism. Other tactics may be effective at reducing the likelihood of root causes resulting in independent failures as well as common cause failures. Thus it can be argued that a complete treatment of common cause failures should not be performed indepentently of an analysis of the independent failures, but rather the treatment of all failures should be integrated.

A structured and systematic way for identifying and classifying groups of components for common cause analysis in larger and more complex problems is known as the generic cause method. This methodology begins with the identification of a wide range of postulated causes of CCF events, and searches for common susceptibility of groups of components to such causes. Several computer codes are available to support this type of analysis.

1.3.2. The Cause-Coupling-Defence View of Common Cause Failures

To understand common cause failures it is essential to understand how components can fail and why more than one component can be simultaneously susceptible to the same failure cause. In /1-10/ the causal picture adopted consisted of a root cause, a means by which the root cause is more likely to impact a number of components simultaneously (the coupling), and the failure of the defences against such multiple failures. The description of the failure in terms of a single root cause is, in reality, too simplistic. If we are interested only in single failures, it may be quite adequate to identify that a pump failed because of high humidity. However, since we are interested in a detailed understanding of the potential for multiple failures, we need to identify further why the humidity was high and how it affected the pump. This understanding opens the doors to different methods of defence against multiple failures.

When viewed from the point of view of defences in particular, it is useful to think of different types of common-cause failure events. Firstly, consider causes of failure. While a "root cause" of failure taken, for example, from one of the root-cause classification schemes, may provide a characterization of the ultimate condition which led to the failure, it does not in itself necessarily provide a full understanding of why the failure occurred. To understand the characteristics of the failure the following concepts are helpful. A conditioning event predisposes a component to failure but does not itself cause failure. For example, failing to provide adequate protection against high humidity conditions a component to increased chance of failure given a high humidity condition occurs. A trigger event activates a failure; an example related to the above would be an event which leads to high humidity. A trigger event may be an event internal or external to the component it affects. An event which leads to high humidity in a room and a subsequent failure would be an external trigger event. An internal event which caused a short circuit in a component would be an example of an internal trigger event. It is not always necessary nor even possible to uniquely define a conditioning event and a trigger event for every type of failure. Conceptually, it is useful, however, to focus on identifying the immediate cause (trigger) and on those factors (conditioning events) which leave the component in question susceptible to the trigger.

Another useful concept in discussing failures, and particularly defences against them, is the speed of the failure mechanisms. This is a measure of the time between the occurrence of the trigger event and the occurrence of the actual failure. For the case of impulsive (i.e., fast acting) triggers, such as missiles, the time scale is small. On the other hand, the time scale for the development of degradation to the point of failure for the persistent (i.e., slow acting) triggers such as aging may be large. This is important from the point of view of detection. Defects which develop slowly with evidence of degradation have a greater chance of being discovered before they result in failure.

For failures to become multiple failures, the conditions have to be conducive to the trigger event and the conditioning event affecting all the components simultaneously. The first step in discussing this is the identification of coupling factors. A coupling factor is a property of a group of components or piece parts that makes them potentially susceptible to the same cause of failure. Such factors include similarities in design, environment, maintenance and test procedures. To understand how common cause failures can arise it is important to understand how this common susceptibility is enhanced or activated, resulting in multiple failures. It must also be kept in mind that the coupling factors are different for different causes, conditioning events, and trigger events. The strength of the coupling is the important factor. Empirically it can be measured by the time between successive failures of the redundant components relative to their individual mean-time between failures (MTBF). A strong coupling means that the redundant component failures are virtually certain to occur almost simultaneously. A weak coupling means only that there is an increased chance of simultaneous failure over the chance of purely independent failures. The strength of the coupling is a function of the probability and trigger events affect the redundant components simultaneously.

In /1-10/ a classification for defensive tactics is proposed that can be used to minimize the effects of CCFs. Defences against CCF can be effective in many different ways. For example, they can prevent the cause. An example would be to protect motor control centers (MCCs) against humidity by sealing them (not sealing the MCCs is a conditioning event). This is equivalent to hardening the component, and the defence acts against the conditioning event. Another example is the training of maintenance staff to assure correct interpretation of procedures. This prevents potential trigger events due to misapplication of procedures. A defence can also decouple failures by effectively decreasing the similarity of components or the environments to which they are exposed and thereby prevent a particular type of root cause from affecting all components simultaneously. This allows more opportunity for detecting failures before they appear in all components of the group. However, using dissimilar components must be approached with caution, since additional failure modes could be introduced. The key to successful mitigation of potential common cause failures is to understand how the defences can fail. With this information, defences which will prevent failures can usually be develop.

1.3.2.1. A Cause-Defence Methodology for CCF Analysis

Based on the discussion in the last section, it is clear that CCFs can be prevented or mitigated by design and procedural defences. From this it follows that reliability and safety analyses that properly address CCF events can aid in designing defences to prevent or mitigate the occurrence of these events. The cause-defence methodology is a CCF analysis technique that explicitly accounts for plant-specific defences to reduce the likelihood of CCF events at nuclear power plants (NPP).

The objective of the cause-defence methodology is to extend the state of the art of plant-specific analysis by providing enough detail in reliability and safety analysis to (1) establish and assess plant-specific defence alternatives against CCF and (2) improve the accuracy of plant-specific CCF analyses. This is accomplished by developing matrices that show the qualitative and quantitative impact of different plant-specific defences on different categories of causes and the degree of coupling associated with CCF events. The work to-date has identified categories of potential root causes, the associated coupling factors, possible defences, and characteristics of the matrices. Separate matrices are developed for defences which act primarily against the cause itself (and hence reduce independent failure frequencies), and for those which act to decouple failures in the common cause group defined by the coupling factors. Some example matrices have also been developed, including one which shows the impact of defences on selected causes of battery failure. The causes of failure, such as internal faults, are listed down the left side of the matrix. Across the top, selected defences, such as inspection and testing, are listed. At the intersection of each cause and defence, the impact of the defence on the cause or coupling is specified. Depending on the type of matrix, the impact can be qualitative (e.g., weak defence or strong defence) or quantitative (a numerical value which indicates the strength of the defence). The items in the matrix can be broken down so the analysis can be done in as much detail as necessary. Once developed and reviewed, the matrices may be used by analysts to perform comprehensive analyses of CCFs for any NPP. The matrices will also be useful to power plant designers, inspectors, and operators. Example qualitative matrices are given in Tables 1.1 and 1.2.

The initial results from the development of the cause-defence methodology have shown that the cause-defence matrices must be fairly detailed to allow for CCF analyses that truly account for design features, and operational and maintenance policies. Therefore, the matrices should be developed for each component type and should account for design variations as well as the way the equipment is tested, maintained, and operated. The cause-defence matrices must be developed by experienced CCF analysts, and reviewed by experts in design, operation, and maintenance of NPP equipment. The matrices will then reflect the consensus of the people involved in developing and reviewing them, which is particularly desirable in areas where data are sparse. While their use as a qualitative tool is relatively straightforward, the basis of the quantitative matrices is not yet developed. One problem to be resolved is the development and interpretation of a reference set of quantitative data to be used along with the matrices. This set of data should contain reference CCF unavailability contributions for each cause considered in the matrices. The entries in the matrices could then be used, when constructed for a particular plant, to modify the reference data and generate the specialized estimates.

The development of the reference data, however, is complicated by the fact that the generic data currently available were collected from plants that had many of the defences considered in the cause-defence matrices, but the generic data bases often do not provide enough information to identify what defences existed at each plant and how well those defences were implemented. Thus, probability estimates that are derived directly from generic data cannot be used as reference data; some judgment will have to be used in developing reference data from the available generic data.

1.3.2.2. A Procedure for a CCF Review Based on Defences

This section discusses the possibility of developing a procedure for performing a review of nuclear power plant design and operations that is focused on identifying potential common-cause failure mechanisms. The overall philosophy proposed is to structure the review according to a generic class of defences against equipment un-

Table 1.1: Assumed impact of selected defences against root causes of diesel generator failures

	Selected Defenses Against Root Causes											
	General Administrative/Procedural Controls				Specific Maintenance/Operation Practices				Design Features			
Selected Failure Mechanisms for Diesel Generators	Configuration Control	Maintenance Procedures	Operating Procedures	Test Procedures	Governor Overhaul	Drain Water and Sediment from Fuel Tanks	Corrosion Inhibitor in Coolant	Service Water Chemistry Control	Air Dryers on Air Start Compressors	Dust Covers with Seals on Relay Cabinets	Fuel Tank Drains	Room Coolers
Corrosion products in air start system	-	o	-	o	-	-	-	-	■	-	-	-
Dust on relay contacts	-	o	-	o	-	-	-	-	-	■	-	-
Governor out of adjustment	-	o	-	o	■	-	-	-	-	-	-	-
Water/sediment in fuel	-	o	-	■	-	■	-	-	-	-	■	-
Corrosion in jacket cooling system	-	o	-	-	-	-	■	-	-	-	-	-
Improper lineup of cooling water valves	■	o	-	o	-	-	-	-	-	-	-	-
Aquatic organisms in service water	-	■	■	-	-	-	-	■	-	-	-	-
High room temperature	-	o	-	-	-	-	-	-	-	-	-	■
Improper lube oil pressure trip setpoint	-	o	-	o	-	-	-	-	-	-	-	-
Air start system valved out	■	o	-	o	-	-	-	-	-	-	-	-
Fuel supply valves left closed	■	o	-	o	-	-	-	-	-	-	-	-
Fuel line blockage	-	-	-	o	-	-	-	-	-	-	-	-
Air start receiver leakage	-	-	-	-	-	-	-	-	o	-	-	-
Corrective maintenance on wrong diesel generator	■	■			-	-	-	-	-	-	-	-

a solid square (■) represents a strong defense, an open circle (o) represents a relatively weak defense, and a dash (-) represents no defense.

Table 1.2: Assumed impact of selected defences against coupling associated with diesel generator failures

Selected Failure Mechanisms for Diesel Generators	Selected Defences Against Coupling						
	Diversity			Barrier		Testing and Maintenance Policy	
	Functional	Equipment	Staff	Spatial Separation	Removal of Cross-ties (or Implementation of Administrative Controls)	Staggered Testing	Staggered Maintenance
Corrosion products in air start system	■	·	·	·	·	·	○
Dust on relay contacts	·	·	·	○	·	○	○
Governor out of adjustment	·	○	○	·	·	·	○
Water/sediment in fuel	■	·	·	·	○	·	·
Corrosion in jacket cooling system	■	·	·	·	·	·	·
Improper lineup of cooling water valves	■	·	■	○	·	■	■
Aquatic organisms in service water	■	·	·	○	○	·	○
High room temperature	·	·	·	○	·	·	·
Improper lube oil pressure trip setpoint	■	■	■	○	·	■	■
Air start system valved out	■	·	■	○	·	■	■
Fuel supply valves left closed	■	·	■	○	·	■	■
Fuel line blockage	■	·	■	·	·	·	·
Air start receiver leakage	■	·	·	·	■	·	·
Corrective maintenance on wrong diesel generator	■	○	■	○	·	○	·

availability. These defences can be argued to be present in some form or other at all plants. Since it is the role of defences in inhibiting the CCFs that is of primary interest here, however, the objective of the review is to identify particular weaknesses in the application of these defences that could allow simultaneous multiple failures.

The reason for attacking the problem from the point of view of the defences is that it can be argued that a good defence can prevent a whole class of common-cause failures for many types of components, irrespective of the details of the failure mechanisms. Thus identification of the existence of particular strengths in the defences can lead to increased assurance that certain types of CCFs are unlikely to occur. The identification of weaknesses leads to an identification of the type of mechanisms for which a more detailed analysis is warranted. The first level of the review, therefore, is a high level screening analysis.

Because of the emphasis on common cause failures, a major requirement for a review is that it should provide a means to assess the adequacy of the defensive strategy being applied at a plant, as a means of maintaining independence between redundant components with respect to the occurrence of failure causes. However, it should not be forgotten that an equally good strategy is to prevent CCFs by preventing the failure mechanisms themselves. Thus a review of the defensive strategy that is focused on the assurance of a low probability of common cause failures cannot be divorced from one that is designed to minimize unavailability or maximize reliability of individual components.

In order to structure the review, it is necessary first to identity how each tactic can help prevent CCFs. This can be used to define a requirement, or set of requirements, for the successful implementation of that tactic. Further, it will help to define the information that will be necessary to assess the quality of the implementation. An essential part of the review process will be the establishment of methods for determining the significance of any observed weaknesses. It is at this stage that an appreciation of individual failure mechanisms becomes more important.

As an example of the approach, consider the role of barriers as a defensive tactic.

Definition of requirements

Barriers are effective as defences against common cause failures resulting from environmental or external agents if they:

(1) create separate environments for redundant components and therefore reduce the susceptibility of components to a single trigger event which affects the quality of the environment;

(2) shield some or all of the components from potential trigger events.

The barriers may separate redundant components, separate the trigger source from one or more components, or be local, at the component, and thus relate to the quality of the effectiveness of component design against prevailing or abnormal environmental conditions. Barriers are primarily designed to protect against internal or external environmental disturbances which are harmful to the components; (the internal environment is the fluid for fluid systems, the electrical current for electrical systems. A barrier for the fluid systems can be the provision of a separate water supply, for example. A fuse or protective relay acts as a barrier in an electrical system). The specific characteristics of the barriers are different for different classes of environmental disturbances.

Review guidelines

For the purpose of the review it is initially sufficient to identify the potential types of environmental disturbances and their impact domain, which will generally depend on the type of environmental disturbance. The disturbance type can be equated to the proximate cause, which is the agent causing failure, e.g., humidity, smoke. Thus a review of the effectiveness of barriers should include identification of the type, location, and purpose of barriers, the type of disturbance to which a barrier is impermeable, the quality of its installation, and the quality of administrative controls that maintain its integrity, coupled with an identification of potential sources for trigger events for the various environmental disturbances, in terms of their location and severity. It should be noted that barriers are not the only defences against environmental disturbances. Surveillance tests, monitoring, and preventive maintenance can also be effective against those agents whose effects result in a measurable degradation of performance.

A review process for identifying potential locations of concern has been developed for dealing with fires and floods. It can be adapted to cover other types of environmental disturbances by following the steps below for each disturbance in turn:

(1) Identify the location of the components of interest.

(2) Identify the piece parts of the components that are susceptible to each disturbance.

(3) Identify the locations of the barriers against the disturbance and divide the plant into nominally independent zones.

(4) Identify potential sources of significant environmental disturbances.

(5) Identify those zones that contain more than one component, or vulnerable piece parts of more than one component, and a source or sources.

(6) Identify potential pathways between zones containing components or vulnerable piece parts, and/or sources via penetration/connections, or defective barriers.

The process identifies the zones, or groups of zones, on a qualitative basis and does not require a detailed analysis of the specific failure mechanisms. This constitutes a coarse screening analysis. It may be refined further, following again the examples of fire and flood analysis.

The adequacy of a design with barriers that have allowed a zone identified in step (5) to contain vulnerable piece parts of more than one redundant component and a potential source of a trigger event has to be assessed against the likelihood of the occurrence of the trigger affecting the component group. This type of analysis is done routinely in fire and flood risk analysis. The factors taken into account include the relative locations of the source(s) and the vulnerable component piece parts, the magnitude of the disturbance (as a function of frequency), the potential for propagation of the disturbance, and the possibility of early detection and mitigation of the disturbance, and is thus dependent on a more detailed assessment of failure mechanisms.

For the groups of zones identified in step (6) the primary review should be directed towards establishing the adequacy of the barrier, as its existence implies that it is believed to be necessary. The barrier has to be investigated for its design adequacy, its installation, and the adequacy of, and adherence to, the administrative controls designed to maintain the integrity of the barrier.

The example discussed above is relatively well developed conceptually, because such a procedure has been used in PRAs to model the effects of fires and floods. Development of detailed guidelines for other defences will require substantial effort. It is relatively straightforward to define general requirements for, and general characteristics of, a good defensive strategy, which can be used as a tool for screening analysis, but developing guidelines for a more detailed analysis is more complicated. For example, setting criteria for the measurement of the quality of training or the clarity of procedures is not a trivial task. In addition, the qualities of the defences are not independent. For example, the quality of the preventive maintenance programme can be influenced by that of the ISI programme and the quality of the training programme by that of the procedures review. It is clear that the establishment of the guidelines and their application in a review will be multi-disciplinary and involve design engineers, operating staff, and human factors specialists.

Nevertheless, the idea of basing a review on the analysis of the quality of the defensive strategy seems to be an approach that has considerable merit, particularly as a complement to a review against historically occurring events. It is of particular value because it approaches the problem from a different direction, thus increasing the scope of the review. The increased appreciation of the role of defences provides input to the cause-defence matrices introduced in the previous sub-section and is also important for improving the quantification of CCF probabilities.

1.4. Short overview of Common Cause Models

In the following, an overview of some of the more frequently used models for calculating the probability of a common cause failure is given. Most of the models serve to cast the information contained in the observed common cause failures into a set of parameters. Usually two classes of models are distinguished:

- shock models

and

- non-shock models

The shock models recognize two failure mechanisms:

(1) failures due to random independent causes of single component failures and

(2) failures of one or more components due to common cause shocks which impact the system at a certain frequency.

In shock models the frequency of the second type of failure is developed as the product of the frequency of shocks and the conditional probability of failure of components, given the occurrence of shocks. They imply a model assumption on the conditional probability of the number of components which fail as a result of a common cause shock. The non-shock models, on the othe hand, serve to estimate common cause probabilities without an underlying failure model being postulated, i.e. they estimate the basic event probabilities directly.

The models are outlined below. The mathematical details, especially of the parameter estimation, may be found in the literature cited. In particular, the following models are addressed:

(1) Basic Parameter Model

(2) Beta Factor Model

(3) Multiple Greek Letter (MGL) Model

(4) Multiple Dependent Failure Fraction (MDFF) Model

(5) Alpha-Factor Model

(6) Binomial Failure Rate (BFR) Model

(7) Multinomial Failure Rate (MFR) Model

(8) Stochastic Reliability Analysis (SRA) Model

(9) System Failure Rate Model (SFRM)

(10) Correlation Model

(11) Extended Common Load Model

(12) Modified Beta Approach

(13) Partial Beta Factor Method

(14) Distributed Failure Probability Model

(15) Random Probability Shock (RPS) Model

Their relationship is shown in the diagram of Fig. 1.4.

The first five models are of the non-shock type, the sixth and the seventh model are examples of shock models. Details on both classical and Bayesian parameter estimation for models (1) - (3) and (4) and (6) and the corresponding uncertainty analyses may be found in reference /1-7/, as well as an explanation of the procedures to be used for accounting for the fact that observed data may stem from systems which have a different number of redundancies from the one under analysis (up and down mapping). These are required for some of the models, e.g. (1), (3) and (5) whilst in other models differences in redundancy are accomodated by the model itself, e.g. (6) or (11). An overview of the parameter estimation results for models (1) - (3), (4) and (6) is given in Table 1.3. Details on the remaining models are given in the references cited.

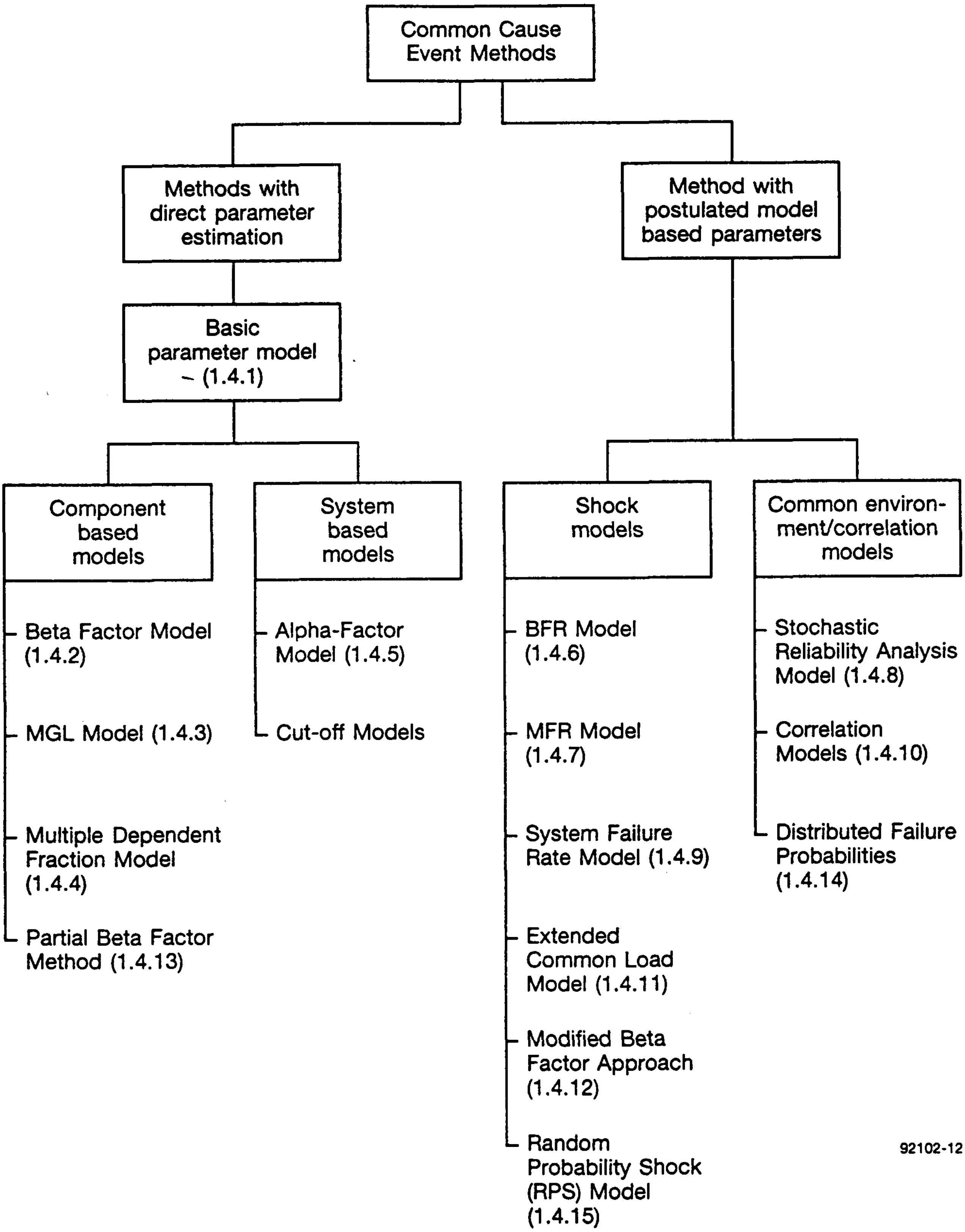

Common Cause Event Methods
Methods with direct parameter estimation
Method with postulated model based parameters
Basic parameter model – (1.4.1)
Component based models
System based models
Shock models
Common environment/correlation models
Beta Factor Model (1.4.2)
MGL Model (1.4.3)
Multiple Dependent Fraction Model (1.4.4)
Partial Beta Factor Method (1.4.13)
Alpha-Factor Model (1.4.5)
Cut-off Models
BFR Model (1.4.6)
MFR Model (1.4.7)
System Failure Rate Model (1.4.9)
Extended Common Load Model (1.4.11)
Modified Beta Factor Approach (1.4.12)
Random Probability Shock (RPS) Model (1.4.15)
Stochastic Reliability Analysis Model (1.4.8)
Correlation Models (1.4.10)
Distributed Failure Probabilities (1.4.14)
92102-12

Fig. 1.4: Assignment of common cause models to different classes

(The corresponding Section is indicated in parentheses).

Table 1.3: Key characteristics of the parametric models (from /1-7/)

ESTIMATION APPROACH			MODEL	MODEL PARAMETERS*	GENERAL FORM FOR MULTIPLE COMPONENT FAILURE FREQUENCY
NONSHOCK MODELS	DIRECT		BASIC PARAMETER	$Q_1, Q_2, \ldots, Q_m$	$Q_k = Q_k \quad k = 1, 2, \ldots, m$
	INDIRECT	SINGLE PARAMETER	BETA FACTOR	Q_t, β	$Q_k = \begin{cases} (1-\beta) Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta Q_t & k = m \end{cases}$
		MULTIPARAMETER	MULTIPLE GREEK LETTERS	$Q_t, \underbrace{\beta, \gamma, \delta, \ldots}$ m - 1 PARAMETERS	$Q_k = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{i=1}^{k} \rho_i \right) (1 - \rho_{k+1}) Q_t$ $\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \ldots, \rho_{m+1} = 0$
			ALPHA FACTOR	$Q_t, \alpha_1, \alpha_2, \ldots, \alpha_m$	$Q_k = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \quad k = 1, \ldots, m$ $\alpha_t \equiv \sum_{k=1}^{m} k \alpha_k$
SHOCK MODELS			BINOMIAL FAILURE RATE	Q_1, μ, ρ, w	$Q_k = \begin{cases} \mu \rho^k (1-\rho)^{m-k} & k \neq m \\ \mu \rho^m + w & k = m \end{cases}$

1.4.1. The Basic Parameter Model

The basic parameter model /1-14/ is based on the straightforward definition of the probabilities of the common cause basic events. Taking $q_k^{(m)}$ as the probability of the event of a failure of a specified component in a system of m redundant components susceptible to common cause failures,

$$q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} q_k^{(m)} \tag{1.1}$$

gives the total failure probability of both common cause and chance failures of a component of the common cause group. The binomial term

$$\binom{m-1}{k-1} = \frac{(m-1)!}{(m-k)!(k-1)!} \qquad (1.2)$$

represents the number of ways in which a specified component can fail together with (k-1) other components of the system consisting of m components altogether. Eq. (1.1) implies that the individual probabilities $q_k^{(m)}$, $q_j^{(m)}$ are defined as being mutually exclusive for all k and j. The observed failures of 2, 3, ... components due to common cause serve to estimate the probabilities $q_k^{(m)}$ by dividing them by the number of demands. If the probabilities $q_k^{(m)}$ are replaced by failure rates the number of observed failures must be divided by the relevant time of exposure for the rates to be estimated. Both frequentist and Bayesian parameter estimation including the treatment of uncertainties are presented in /1-7/.

1.4.2. The Beta Factor Model

The Beta Factor Model /1-22/ is a single parameter model, because it is based on calculating one additonal parameter to the total failure probability. This parameter represents the ratio between the common cause failure probability and the total failure probability. If q_t is the total probability of failure of a component (both chance and common cause failures)

$$q_1 = q_t \cdot \beta \qquad (1.3)$$

is the probability of a common cause failure. The model was developed for 1-out-of 2 systems and gives conservative results if applied to systems with higher redundancies provided that all observed events with multiple failures have been taken into account in estimating the parameter. The model has been extensively used in PSA studies, e.g. in /1-23/, /1-24/.

1.4.3. Multiple Greek Letter (MGL) Model

The Multiple Greek Letter Model /1-25/ is an extension of the Beta Factor Model which takes into account explicitly higher redundancies. The MGL parameters consist of the total failure probability, q_t, which includes the effects of all independent and common cause contributions to the failure of the component in question, and several conditional failure probabilities. The latter describe the probabilities of a double, triple, or quadruple failure given that a failure has occurred.

In particular we have:

q_t: total failure probability of the component in question due to all independent and common cause events;

β: conditional probability that the cause of a component failure will be shared by one or more additional components given that a specific component of the redundant system has failed;

γ: conditional probability that the cause of a component failure which is shared by one ore more components will be shared by two or more additional components, given that two specific components have failed;

δ: conditional probability that the cause of a component failure which is shared by two or more components will be shared by three or more additional components, given that three specific components have failed.

It should be noted that in using the MGL model parameters may have to be estimated on the basis of zero failures if no event affecting the number of redundancies implied by the parameter in question has been observed. This may well be the case for parameters γ and δ because triple and quadruple failures are usually rare. A remedy would then be the Bayesian approach, which in addition allows the parameter uncertainties to be treated. Details are given in /1-7/.

The model has been used extensively in the International Common Cause Failure Reliability Benchmark Exercise /1-8/.

1.4.4. Multiple Dependent Failure Fraction (MDFF) Model

Multiple Dependent Failure Fraction (MDFF) model /1-26/ is a generalization of the beta factor method. The original formulation of the model was later modified /1-27/ to account for some missing transition rates.

MDFF defines a new parameter - the fraction of n-tiple failures, to make it possible to distinguish between different failure multiplicities. General solutions for the MDFF method can be obtained using the state equations of a Markov model for a case with arbitrary number of identical parallel units and no repair. In /1-26/ a set of solutions is provided for a four train system.

1.4.5. Alpha-Factor Model

Rigorous estimators for the Beta-Factor and the MGL model parameters are fairly difficult to obtain, as explained in reference /1-7/. In order to overcome this difficulty the Alpha-Factor Model /1-28/ was developed. The corresponding model parameters are estimated from system-failure data and not from component-failure data, as is the case with the previously treated model.

The Alpha-Factor Model is based on the use of the total component failure probability, q^t, and the parameter α, defined as /1-28/

$$\alpha_k{}^{(m)} = \frac{\binom{m}{k} q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} q_k^{(m)}} \tag{1.4}$$

In eq. (1.4) $q_k{}^{(m)}$ is the probability of failure of k specific components in a group of m components potentially subject to common cause failures, and the denominator represents the sum of all failure events. The basic event probabilities are given by

$$q_k^{(m)} = \frac{m}{\binom{m}{k}} \frac{\alpha_k^{(m)}}{\alpha_t} \cdot q_t \tag{1.5}$$

where $\alpha_t = \sum_{k=1}^{m} k \cdot \alpha_k^{(m)}$ and $q_t = \sum_{k=1}^{m} \binom{n-1}{k-1} q_k^{(m)}$.

Both the frequentist and the Bayesian approach including the treatment of parameter uncertainties are developed, as explained in /1-7/.

1.4.6. Binomial Failure Rate (BFR) Model

As mentioned before, in the Binomial Failure Rate Model /1-16/ two types of failures are considered:

(1) independent failures.

(2) failures caused by shocks which can result in the failure of any number of components.

Furthermore, two types of shocks are distinguished: lethal and non-lethal. When a non-lethal shock occurs, each component within the redundant group under consideration is assumed to have a constant and independent probability of failure. The name of this model arises from the fact that the probability of the number of components failed as a consequence of a non-lethal shock is assumed to be given by a binomial distribution. Additionally, lethal shocks are provided for which make all the components the analysed group fail.

The model may be used to include single failures considered as potential common cause failures in the process of parameter estimation (cf. /1-7/). Both frequentist and Bayesian methods of parameter estimations including the treatment of uncertainties are available (cf. /1-7/).

1.4.7. Multinomial Failure Rate (MFR) Model

MFR model /1-29/ belongs to the class of shock models. It treats the dependence between the components in two levels: stochastic dependence and state-of-knowledge dependence. As the basis for parameter estimation the MFR model uses numbers of events rather than numbers of component failures. In that respect it is similar to the alpha factor model (cf. Section 1.4.5) as opposed to the MGL model.

For the stochastic part the MFR model employs the independent failure rate of the components, the shock rate for failures that may fail more than one component and failure fractions representing conditional probabilities of failures with specific multiplicities. In order to include some of the correlations between the parameters, beta and Dirichlet distributions have been assigned to the parameters /1-29/.

1.4.8. The Stochastic Reliability Analysis (SRA) Model

This model starts from the assumption that failure-rate data is prepared from observations of inhomogeneous populations and is based on decomposing the failure behaviour into so-called shells, three of which are generally considered sufficient. These shells represent homogeneous sub-populations of the original inhomogeneous total population characterized by different failure behaviour. The basic idea of the SRA model is that "non-lethal" dependencies are not a result of "common causes" but of dissimilar failure behaviour, i.e. of an inhomogeneous population. In addition "lethal dependencies" are considered.

The event "k specific components out of m redundant components are in failed state" is then described by the equation.

$$p_{K/m} = a_o\, p_0\, \delta_{\kappa,m} + a_1\, p_1^{\,k} (1-p_1)^{\,m-k} + a_2\, p_2^{\,k} (1-p_2)^{m-k} \qquad (1.6)$$

where coefficient 0,1,2 represent the three shells (sub-populations) and with $\delta_{\kappa\kappa} = 1$, if m = k and 0 otherwise.

The following types of behaviour are reflected by the coefficients of the eq. (1.6):

- normal ("generic") failure behaviour with a weight of a_2. This type of behaviour reflects independent failures with a failure probability p_2;
- outliers, e.g. due to design flaws or extreme operating conditions. Weight a_1, typically within the range of a few percent, is attached to this category which describes independent failures with an increased failure probability p_1;
- physical coupling leading to the failure of all redundancies. If with weight a_0 the conditions of totally dependent failures are fulfilled, the conditional failure probabiltiy of this sub-population amounts to 1 ("lethal shock").

The model parameters are determined as follows:

If sufficient measures of defence against common cause failures such as

- low degree of intermeshing,
- strict spatial separation of redundant equipment,

- staggered testing (personal diversity).

are given, a_0 is considered to be in the range of 10^{-4} - 10^{-7}. The parameters describing outliers are assumed to be $a_1 = 0.05$ and $p_1 = 10\ p_2$. This proportion of outliers results from the knowledge that "additions" of approx. 5 % cause the maximum dependency effect (for usual degrees of redundancy and orders of magnitude for failure frequencies). This choice of values is claimed to correspond roughly to the experience with collected data; p is the unavailability of the component type in question and p_2 is calculated from it according to the relation $p_2 = p/1{,}45$; p is obtained from

$$p = \frac{\lambda_t \theta}{2} \qquad (1.7)$$

In eq. (1.7) λ_t is the total observed failure rate and θ the mean time between functional tests.

Further details may be found in references /1-18/ and /1-30/. Procedures for taking into account uncertainties are under development.

1.4.9. System Failure Rate Model (SFRM)

The System Failure Rate Model (SFRM) is based on the direct estimation of the system failure rates λ_c from generic data sources for different systems and component types. In /1-31/ estimates for (n-1) -out-of-n systems (i.e. systems with success criterion such that any two or more failures fail the system) are given. If three or more failures are needed to fail the system, the system failure rate estimate λ_c is taken to be one half ot these values.

For a normally operating system the system failure rate λ_c as such is the initiating event rate contribution of the common cause failures. For standby safety systems the main quantity of interest is not the failure rate but the unavailability of the system. And this depends not only on λ_c but also on the residence time of a failure. If all n redundant trains are tested simultaneously (or consecutively, in practice) then the average residence time of a CCF is one half of the test interval T, and the system unavailability due to CCF is

$$u_s=\lambda_c T/2 \tag{1.8}$$

In case of staggered testing all n trains are not tested consecutively but with a time shift of T/n with respect to each other. The interval between two tests of any particular train is T. Any failure discovered in a test is immediately repaired. Thus, the system failure of an m-out-of-n-system is removed after m repairs. This means that the average residance time of the system failure is (m-1/2)T/n. The system unavailability due to CCF is then

$$u_s=\lambda_c T\ (m-1/2)/n. \tag{1.9}$$

This is usually smaller than the value obtained from eq. (1.8).

The system unavailability can be further reduced by setting an additional rule to test all redundant trains whenever a failure is observed in any train. In such a case the CCF average residence time is T/(2n), and the system unavailability is

$$u_s=\lambda_c T/(2n). \tag{1.10}$$

An inherent assumption in the SFRM is that partial system failure events do not contribute significantly to the system unavailability (because two or more such events must coincide before a system fails). This simplifies the system modelling considerably. Further details on how to combine plant-specific an generic data, and on how to calculate the uncertainty distribution of λ_c can be found in /1-32/.

1.4.10. Correlation Models

When the failure probabilities x and y of two components are distributed variables, the simultaneous failure probability has the expectation value

$$E(X\,Y) = E(X) \cdot E(Y) + r\sigma(X)\,\sigma(Y), \tag{1.11}$$

where $E(\cdot)$ is the mean value and $\sigma(\cdot)$ the standard deviation of the argument variable and r is the correlation coefficient between X and Y. The second term is the contribution of dependent or correlated failures. The effect of r has been demonstrated for typical n-redundant systems in case of identically distributed variables [E(X) = E(Y), $\delta(X) = \sigma(Y)$] and typical values of $\sigma(X)/E(X)$ /1-32/.

As a further specialization of this line of thought one can assume that parallel redundant components are completely identical (Y = X, r = 1) so that the average probability of simultaneous failure of r components is $E(X^r)$, and the probability of exactly r failures out of n components has the expectation value

$$P_{r/n} = \frac{n!}{r!(n-r)!}\int_0^1 x^r (1-x)^{n-r} f(x)\,dx \qquad (1.12)$$

In this Distributed Failure Probability (DFP) model /1-18/ the density function f(x) can be written as

$$f(x) = \sum_j p_j f_j(x), \qquad (1.13)$$

where p_j is the probability of "environment j" and $f_j(x)$ is the (conditional) density of the component failure probability in environment j. These can be defined on the basis of observations:

$$f_j(x) = \frac{(n_j+1)!}{r_j!(n_j-r_j)!} x^{r_j} (1-x)^{n_j-r_j} \qquad (1.14)$$

where r_j is the number of component failures in n_j demands in environment j, and

$$p_j = \frac{s_j+1}{\sum_j s_j+m}\cdot \qquad (1.15)$$

where m is the number of different environments, each of which occurred s_j times in the data base. Each failure multiplicity defines a different "environment", and the BFR model and the SRA model can be obtained as special cases of this approach /1-33/.

1.4.11. Extended Common Load Model

Many systems in nuclear power plants have redundancy levels higher than the usual two or four redundant trains. Examples of such a system are the reactor safety/relief valves of BWR plants.

According to /1-34/ the methods like MGL Model (cf. Section 1.4.3), Alpha-Factor Model (cf. Section 1.4.5) and the Binomial Failure Rate (BFR) Model (cf. Section 1.4.6) may encounter difficulties when the structures have more than four redundant components. The Alpha-Factor and MGL models require new parameters for each failure multiplicity and the parameters are not invariant with respect to the total number of redundant components in the system. In the binominal failure rate model the high order failure probabilities are dominated by the lethal shocks, which provide a rather inflexible cut-off model, if it is deemed necessary to include them. Furthermore, the MGL and Alpha-Factor models are based on a low level cause-event model, which causes difficulties in the minimal cut set treatment. In order to overcome the above problems in the CCF modelling of highly redundant systems the approach described below was introduced which was applied in the analysis of safety relief valves of the Finnish TVO PSA, and more recently in the CCF analysis of safety relief values of the Nordic BWR plants (cf. /1-35/, /1-36/).

The model is based on so called common load model (CLM) in which the probability that k specific components fail is written in the form

$$psg(k) = P(k\text{ specific components fail}) = \int_{-\infty}^{\infty} f_s(x)F_R(x)^k dx \qquad (1.16)$$

where $f_s(x)$ is the probability density function of common stress to which the redundant components are subjected and $F_R(x)$ is the cumulative probability distribution of the resistances of the components. The probability of eq. (1.16) is called sub-group failure probability (SGFP). From the eq. (1.16) we can see that the resistances of the components are assumed to be independent identically distributed random variables and that the stress is common to all components, which can also be seen from Figure 1.5.

In the parametrization of the basic version of CLM with normally or log-normally distributed stresses and resistances only two parameters are needed

P_1 = total single failure probability

$$c = \text{correlation coefficient} = \frac{1}{1+\left(\frac{d_R}{d_s}\right)^2} \in [0,1], \qquad (1.17)$$

where d_R and d_s are the standard deviations of the stress and resistance distributions. It should be noted that P_1 and psg(1) are equal.

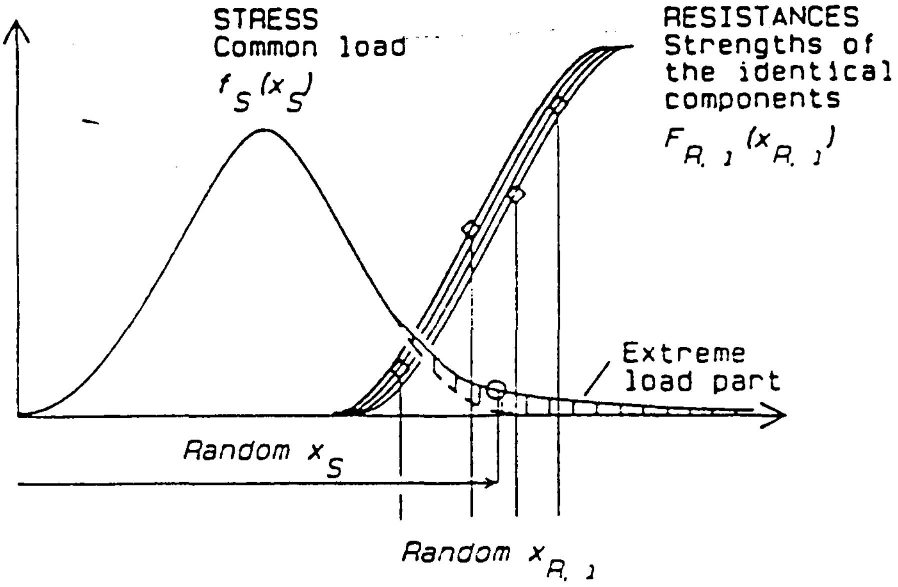


Figure 1.5: Basic concepts in the extreme common load model

In the case of very high redundancy levels a new version of the CLM approach was applied /1-34/. In this so called extented CLM the distribution of the common stress is assumed to have two components, the base load and the extreme load parts. The extreme load component can be interpreted to describe environmental shocks, latent design faults, systematic maintenance errors or their combinations. This can be parametrized with four quantities:

p_{tot} = total single failure probability;

p_{xtr} = extreme load part as contribution to the single failure probability;

c_{co} = correlation coefficient of the base load part;

c_{cx} = correlation coefficient of the extreme load part.

p_{tot} equals to P_1 in eq. (1.17) and psg(1) defined in eq. (1.16). The above parametrization is chosen among various possibilities by trial-and-error in order to find a practical solution. Alternative parametrizations could be developed also to describe more general dependency structures.

The treatment of highly redundant structures requires the definition of some group failure probability concepts. The basic entity is the subgroup failure probability SGFP defined in eq. (1.16). If the CCF-groups are assumed to be homogeneous, the SGFPs are invariant with respect to the group size, i. e.

$$\text{psg}(k/n) = P(k \text{ specific components fail/CCF group } n) = \text{psg}(k) \qquad (1.18)$$

The failure dependencies are modelled via SGFPs and the other structural entities are easily constructed. The success criteria can be interpreted also via the equivalent failure criteria and the total failure probability of the structure is of the form

$$\text{pts}(k/n) = P(k \text{ or more out of } n \text{ fail}). \qquad (1.19)$$

The probabilities psg(k) and pts(k/n) can be evaluated by applying simple transformation by algorithms. For that purpose one has to apply the exclusive subgroup failure probabilities

$$\text{pgs}(k/n) = P(\text{the specific } k \text{ out of } n \text{ components fail, the other } n - k \text{ survive}$$

The probabilities peg(k/n) and pts(k/n) are related to psg(·) s by

$$\text{peg}(k/n)=\sum_{m=k}^{n} (-1)^{n-k}\binom{n-k}{m-k}\text{psg}(m) \qquad (1.20)$$

and

$$\text{pts}(k/n)=\sum_{m=k}^{n} \binom{n}{m}\text{peg}(m/n). \qquad (1.21)$$

the above equations together with eq. (1.16) are sufficient for evaluating the failure probabilities of any order.

The estimation of parameters can be performed, for example, by calculating first the estimate for the total single failure probability and then searching the other parameters with the maximum likelihood method. In /1-35/ experiments with Bayesian estimation were also made. Independently of the estimation method careful qualitative study and interpretation of operational experience is required. In /1-36/ the estimation of parameters in the case of safety relief valves in the Finnish TVO PSA is shown.

1.4.12. Modified Beta Factor Approach

The approach was used, for example, in /1-4/ and is based on the Beta Factor Method (cf. Section 1.4.2).

In order to cover cases of redundancy of a factor of more than 2, the Beta Factor Method was extended by using factors β_k^n , representing the proportion of common modes affecting k components with redundancy of a factor of n.

Using the parameters of the BFR model (cf. Section 1.4.6), it is possible to calculate the β_k^n set using the three basic values which are: β_2^2, β_3^3, β_4^4.

It can be stated that:

$$\beta_2^2 = \frac{\mu p^2+\omega}{\lambda}$$

$$\beta_3^3 = \frac{\mu p^3+\omega}{\lambda} \tag{1.22}$$

$$\beta_4^4 = \frac{\mu p^4+\omega}{\lambda}$$

where μ is the shock rate for non-lethal shocks, p the probability of component failure, given that a non-lethal shock has occurred, and ω the occurrence rate of lethal shocks; λ is the failure rate, for all modes, of the component in question, and hence the value found in data bases.

A lethal shock causes the failure of all redundant components, a non-lethal shock causes the failure of one component with a conditional probability p.

The above formulae were used ot derive the values of parameters and p, μ and ω.

It is then possible to calculate, for each type of component, values of:

β_{K}^{n} where k ≤ n, such that: $\beta_{k}^{n} = \frac{\mu p^{k}(1-p)^{n-k}}{\lambda}$ corresponding to the failure of k specific components in a set of n.

1.4.13. Partial Beta Factor Method

The basic format of all the partial β factor models is that the multiple failure group is assessed against a series of features (such as segregation, complexity, design) against some form of criteria. A partial β factor is then assigned for each feature. The partial factors are then combined to form a β factor for that multiple failure group.

Within this framework there are three main methods which are seen commonly although variations on these are appearing. The original partial β factor /1-37/ was based on a scheme in which 19 factors were assessed and then multiplied to give an overall β factor. The second version /1-38/, used in the European CCF Reliability Benchmark Exercise during the 1980's, extended the first method by including a further division based on the failure cause. The third version /1-39/ is more simple, being based on only 8 factors which are added to give an overall value for β.

1.4.14. Distributed Failure Probability

An entirely different and more detailed approach which has had only limited usage in the UK so far, is that based on dividing the data into "environments". The only form of this applied thus far in the UK is the DFP Method /1-40/, although other related approaches from other areas of Europe have been acknowledged. In DFP these environments may be variously defined, but should have the feature of being independent of one another. Within an environment the failure rate is "enhanced" but the components are considered to be independent. The result is a model in which the probability of a multi-train system failure can be estimated from data which has failures of only one or two trains.

The method can be difficult to apply and only really has advantages over more simple approaches in cases where high levels of redundancy are being considered.

1.4.15. Random Probability Shock (RPS) Model

This model is an extension of the BFR model in that it allows for various degrees of dependence in the outcomes of a shock. In this sense it is in contrast with the β-Factor Model, which assumes complete dependence of multiple failures following a shock and the BFR-Model which implies the same failure probability for all shocks (naturally excluding lethal shocks). In the RPS model the binomial parameter p of the BFR model is assumed to a be Beta distributed random variable. Its random variation would describe, for example, differing degrees of vibration from shock to shock in case vibrations were the cause of the CCF. The procedure encompasses the β- and BFR models as extreme cases. Its parameters may be estimated from observed data, as is shown in /1-41/.

1.5. Valuation of different models

There is no generally preferred procedure for the evaluation of common cause failures. However, there is consensus, that in cases where a sufficient number of common cause failures for the component to be assessed covering the entire range of redundancies has been observed, models directly based on experience such as the basic parameter, Beta-Factor or MGL models should be used. This is not the usual case, which is characterized by the dearth of observations and it is not infrequent that the failure of higher numbers of redundancies has not been observed at all. In such cases Bayesian methods may be used. However, this may lead to overly conservative results in cases where no failures have been observed, because the period of observation was too short.

Models in which the total failure rate is multiplied by factors such as the MGL model should only be applied if the factors have been derived from the same data base as the total failure rate. If this is not done and "generic" MGL factors are used this may lead to different failure rates for common cause failures depending on the total failure rate for the plant under the investigation. This implies that the same common cause experience would lead to different results, depending on the indepent failure rate of the components in question, an undesirable property.

Models making use of an intrinsic mechanism of extrapolation such as the BFR model are preferred by some analysts if for some degree of redundancy no failures have been observed. Although it may not be guaranteed that the failure rates thus obtained are correct they are at least consistent within the context of the model.

If owing to a lack of plant-specific data, information on occurences in other plants has to be used for the CC-analysis, models which add a common cause part to the independent failure rate are to be preferred to models of the multiplicative type, as mentioned before.

Given the uncertainties of CC-analysis a model should be accompanied by a formalism to consistently treat parameter uncertainties. If the original events are known their relevance for the case under consideration should be assessed by using impact vectors (cf. /1-42/) with assigned subjective probabilities. These probabilities should reflect the uncertainty in the interpretation of the observed degree of failure and of the application of events from other plants to the plant under investigation. They are fixed by engineering judgement.

1.6. Recommendations and outlook

Despite the large number of parametric models available, which impose different requirements on event data, the principal drawback of common cause analysis is the paucity of data. Since this will remain true in the future as well, given the circumstances that common cause failures are rare events, data from different sources will always have to be pooled in order to arrive at a number of events acceptable for statistical analysis. This implies that unified criteria should be applied in order to make the different sources of data comparable. In addition, detailed descriptions of the relevant systems of different types of plants should be made available as a support of the engineering judgement which will always have to exercised in common cause analysis.

The different mechanisms for common cause events should be identified, the cause-defence approach seems to be a step in the right direction.

The possibility of contributions forming inter-system CCFs should be considered in the analyses and methods for coping with CCF in systems with extremely high levels of redundancy such as BWR safety and relief valves should be developed and adequately validated.

A framework for the engineering judgement involved should be created and made available, if possible, in the form of a computer-aided system.

References

/1-1/ Mosleh, A:
Dependent Failure Analysis
Reliability Engineering and Systems Safety 34 (1991) 243-248

/1-2/ Severe Accident Risks. An Assessment for five US Nuclear Power Plants.
NUREG-1150, Vols. 1 and 2, June 1989

/1-3/ Der Bundesminister für Forschung und Technologie (Hrsg.),
Deutsche Risikostudie Kernkraftwerke - Phase B, Köln 1990
(English Summary: German Risk Study Nuclear Power Plants, Phase B, GRS-74, Köln 1990)

/1-4/ Etude Probabiliste de Sûreté d'une tranche du Centre de Production Nucléaire de Paluel (1300 MWe),
Rapport de Synthèse, ESP 1300, Mai 1990

/1-5/ Werner, W.:
Results of Recent Risk Studies in France, Germany, Japan, Sweden and the United States
to be published

/1-6/ HTGR Accident Initiation and Progression Analysis Status Report. GA-A-13617 (October 1975)

/1-7/ Mosleh, A. et al.:
Procedures for Treating Common Cause Failures in Safety and Reliability Studies
NUREG/CR-4780; EPRI NP-5613; Vol. 1 (January 1988)
Vol. 2 (January 1989)

/1-8/ Poucet, A; Amendola, A. and P.C. Cacciabue:
Summary of the Common Cause Failure Reliability Benchmark Exercise
JRC Report, EUR-14054, 1987

/1-9/ Hirschberg, S. (Ed.):
NKA-project "Risk Analysis" (RAS-470)
Summary Report on Common Cause Failure Data Benchmark Exercise,
Nordic Liaison Committee for Atomic Energy, June 1987

/1-10/ Paula, H.M. and G.W. Parry:
A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures
NUREG/CR-5460 / SAND 89-2368 (March 1990)

/1-11/ International Atomic Energy Agency (IAEA)
Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment,
IAEA-TECDOC-648, Vienna, Austria, 1992

/1-12/ Example Application of a Structured Procedure for Estimating Common Cause Failure Probabilities
IAEA TECDOC (to be published in 1993)

/1-13/ Gano, D.L.:
Root Cause and How to Find it.
Nuclear News Vol. 30, No. 10, August 1987, 39-43

/1-14/ Fleming, K.N., A. Mosleh and D.L. Acey:
Classification and Analysis of Reactor Operating Experience Involving Dependent Events,
Report EPRI-NP-3967, Electric Power Research Institute, June 1985

/1-15/ Paula, H.M.:
Data Base Features that are needed to support Common-Cause Analysis and Prevention: An Analysts Perspective
Nuclear Safety, Vol. 31, No. 2, April - June 1990

/1-16/ Atwood, C.L.:
Estimation for the Binomial Failure Rate Common Cause Model,
NUREG/CR-1401, March 1980

/1-17/ Virolainen, R.K.:
On Common Cause Failures, Statistical Dependence and Calculation of Uncertainty; Disagreement in Interpretation of Data,
Nuclear Engineering and Design 77, 103-108, 1984

/1-18/ Dörre, P.:
Basic Aspects of Stochastic Reliability Analysis for Redundancy Systems
Siemens AG (KWU) Offenbach, F.R.G.

/1-19/ Hughes, R.P.:
A New Approach to Common Cause Failure,
Reliability Engineering 17 (1987) 211-236

/1-20/ Virolainen, R.K. and A. Buslik:
On Common Cause Failure Methods Dealing with Dependent Failures; A Comparative Application to US Diesel Generator Data based on licensee Event Report
International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, 24-25 February 1985, USA

/1-21/ Atwood, C.L.:
Common Cause Fault Rates for Diesel Generators: Estimates based on licensee Event Reports at US Commercial NPPS 1976-1978, NUREG/CR-2099, May 1982

/1-22/ Fleming, K.N.:
A Reliability Model for Common Mode Failure in Redundant Safety Systems
Proceedings of the Sixth Annual Pittsburgh Conference on Modelling and Simulations
GA-A 13284, April 23-25, 1975

/1-23/ HTGR Accident Initiation and Progression Analysis, Status Report,
GA-A 13617, I-VII General Atomic Company, 1975-1976

/1-24/ Severe Accident Risks. An Assessment for five US Nuclear Power Plants
NUREG-1150, Vols. 1 and 2, June 1989

/1-25/ Fleming, K.N. and A. M. Kalinowski:
An Extension of the Beta Factor Method to Systems with High Levels of Redundancy,
PLG-0289, June 1983

/1-26/ Stamatelatos, M.G.:
Improved Method for Evaluating Common-Cause Failure Probabilities,
Trans. Am. Nucl. Soc., Vol. 43, pp. 474 - 475, 1982

/1-27/ Hirschberg, S.:
Comparision of Methods for Quantitative Analysis of Common Cause Failures
- A Case Study, Proceedings of PSA'85, International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications,
San Francisco, California, U.S.A., February 24 - March 1, 1985

/1-28/ Mosleh, A. and N.O. Siu:
A Multi-Parameter, Event-Based Common-Cause Failure Model
Proceedings of the Ninth International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, 1987

/1-29/ Apostolakis, G. and P. Moieni:
The Foundations of Models of Dependence in Probabilistic Safety Assessment, Reliability Engineering, Vol. 18, pp. 177 - 195, 1987

/1-30/ Feigel, A. and J. Wenzel:
PSA Convoy-Influence and Modelling of Common Cause Failures
in : Proceedings of the OECD/BMU-Workshop on Special Issues of Level 1 PSA
Cologne, F.R.G., May 27 - 29, 1991

/1-31/ Vaurio, J.K.:
A Procedure for Common Cause Failure Assessment,
Proc. PSA' 91, IAEA-SM-321/46, Vienna, Austria, 3-7 June 1991

/1-32/ Hartung, J.A.:
A Statistical Correlation Model and Proposed General Statement of Theory for Common Cause Failures
Proc. Intl. ANS/ENS Topical Mtg. on Probabilistic Risk Assessment, Port Chester, New York, September 20-24, 1981

/1-33/ Hughes, R.P.:
A Framework for Dependent Failure Analysis,
Reliability Engng. and System Safety 24 (1989) 139-149

/1-34/ Mankamo, T., Kosonen, M.,
Depent failure modeling in highly redundant structures - Application to BWR safety valves
Reliability Engieering and Systems Safety 1992, 35, 235-244.

/1-35/ Mankamo, T., Björe, S., Erixon, S., Johansson, G., and M. Kosonen:
CCF analysis of high redundancy systems, safety/relief valve data analysis and reference BWR application.
Int. Symposiom on the Use of PSA for Operational Safety, PSA '91
IAEA-SM-321/47

/1-36/ Mankamo, T.,
Extended common load model, a tool for dependent failure modeling in highly redundant structures.
Avaplan Oy, Espoo, Finnland, 30 March 1990

/1-37/ SRD Dependent Failures Procedures Guide
SRD 418 March 1987

/1-38/ Johnson, B.D. and J. Crackett:
Common Cause Failure Reliability Benchmark Exercise
SRD R383 and GD/PE-N/I329 (CEGB) August 1985.

/1-39/ Numerical Values for Beta Factor Common Cause Failure Evaluation
RRA/7692
ANS Proceedings of Reliability '87

/1-40/ Hughes, R.P.:
The Distributed Failure Probability Method for Dependent Failure Analysis.
PSA '89 Int. Topical Meeting on Probability, Reliability, and Safety Assessment.
April 2. - 7.1989, Pittsburg, Penn. USA

/1-41/ Hokstad, P.:
A Shock Model for Common-Cause Failures,
Reliability Engineering and System Safety, Vol. 23, pp. 127 - 145, 1988

/1-42/ Siu, N. and A. Mosleh:
Treating Data Uncertainties in Common-Cause Failure Analysis
Nuclear Technology, 84, 265-281, March 1989

Annex A: Data Sources in different countries

A

A.1. Belgium

In Belgium a thorough analysis of significant events is being performed in the framework of activities called "feedback of experience". This analysis covers significant events in foreign as well as in Belgian nuclear power plants.

For a systematic analysis of significant events, the CANIS databank has been created at AIB-Vinçotte Nuclear. It includes the ARIANE data bank which permits to make a search of those records labeled with "CMF". In this way it is possible to identify (potential) CMF-events having occurred in Belgian nuclear power plants.

It must be emphasized that this system can only be used as a descriptive source of information on these events. It cannot be used for quantifcation of CMF probabilities or parameters, since the number of independent failures or the number of demands is not registered.

An example of an ARIANE-record, treating a potential CMF-event, is given Table A1.

The data bank can be characterized as follows:

- the information concerns PWR;
- the records describing (potential) CMFs are coded with "CMF";
- an informal type of quality control is used (for the ARIANE data bank events from a large range of internationally available documents are selected on a subjective basis). No "source" documents are produced for the data bank;
- full text description of events is available (see example below);
- the information from the data bank is available on request (the same restrictions as for the IRS apply cf. Section A.12).

Table A1: Example from the ARIANE data bank

```
*************************************************
*ARIANE RECORD No.    972 : INFORMATION 2 *
*************************************************

Plant: DOEL_3

Initial Date: 870125          Time:
Final   Date:                 Time:

=================================================
TITLE:
======
Unexpected DG trip on low oil pressure. Warm start
not considered in design.

SUMMARY
=======
  Discovered during the yearly LOOP loading
sequence. Potential CMF. Same problem during a
hot start slow test, at CNT2, in March 91.
  This low lubricating oil pressure trip was
added after a March 1983 seizure due to lack of
lubrication.
  The initial oil temperature influences:
 *the oil pressure build-up speed during startup
of the DG
 *the oil pressure at equilibrium.

  The qualification tests had been done so far
from cold conditions.

  See also a MAC GUIRE 2 8min loss of essential
power due to a "false" low lube oil pressure
signal, on 880624 (air or sediment in the
instrument lines).
  Sporadic failures to start occurred at the "0"
ZION DG on 900301 because of a "sensed" low lube
oil pressure. An air pocket was trapped in the
turbocharger filter unit.

CORRECTIVE ACTIONS.

  Delay changed from 6 to 15 sec, for all similar
DGs.
  Blackout sequence testing after the endurance
test.
  Monitoring of the pressure parameter during
future periodic tests.
  ZION required that the filter housings be
vented when maintenance is performed.

LESSONS LEARNED.

  Importance of a well considered design review.
  Priority trips should rely on reliable
instrumentation. Reviewed in the Decennal Topic
7-3.1.

*************************************************
DOCUMENT LIST
=============
 87.08.20 IRS          755
 88.09.01 LER          111 (88-014)
 90.05.31 LER          215 (90-008)
 88.10.31 NPE          XI.A.1030

*************************************************
```

A.2. Canada

Component Data System - Description

Ontario Hydro operates a comprehensive component fault data system for its eighteen operating CANDU reactors. The failure history of essentially all components are recorded, reviewed and input into a data base called CORDS. Approximately 2,200 failure events per unit are entered into the database each year. For ten reactors this data base has been operational since January 1, 1990; four more were included in July 1991 and the remaining four in November 1991. All components have a unique identifying code which is consistent with field and PSA use. Text descriptions of the events are available in electronic format but the extent of description varies. The quality of the data is assured by the use of well-trained, dedicated staff to input data and through auditing by other staff. The CORDS data base has restricted access.

Component Data System-Analysis

The Ontario Hydro component fault data base will be used to help identify common cause failures. This will be done by conducting computer searches of failure records of components in similar component groups to identify instances where two or more components in the same group have been unavailable within a short period of time due to the same failure mode or mechanism. If potential common cause failures have been identified in this manner a root cause analysis will be performed and if apppropriate, like components in broader component groups will also be considered. The purpose of this root cause analysis is to identify corrective actions to eliminate or reduce the likelihood of future common cause failures.

A.3. Finland

Reliability Data Collection at Loviisa NPS in Finland

The data bank contains information on WWER-440 pressurised water reactor plants.

Raw data on failures which occurred during operation of the plant since 1977 have been collected using plant records, work orders and requests, control room log-books and test records. This work is continuing now with an on-line data collection system.

The special data collection form of Figure A1 was used to gather all relevant information about events. A multiplicity of failure entering, detection and exit mechanism is taken into account to enable both base case quantifications and time-dependent calculations. Some of the important items are: Item A indicates the failure detection method like alarm, shift inspection, periodic testing, scheduled maintenance, on demand etc. Item B indicates the effect of an event on the operation of the equipment like "prevented", "did not prevent but repair prevented". These items concem also stand-by operation of the equipment. Item C indicates the likely time of occurrence of the failure like "immediately before detection", after previous test", "during previous test" or "before previous test". Full text descriptions are available as special reports for safety significant events.

A computer program for making logic checks and searching failure data in various ways is available. In addition to any item or combination of items in the form, component type, manufacturer and room identification can be used as search criteria. Searches can also be made for a particular time interval, for a specific component, a group of components or a sub-system. Potential common cause failures (based on overlapping unavailability times) can be searched for and the number of occurrences of each item in the failure data search is added up.

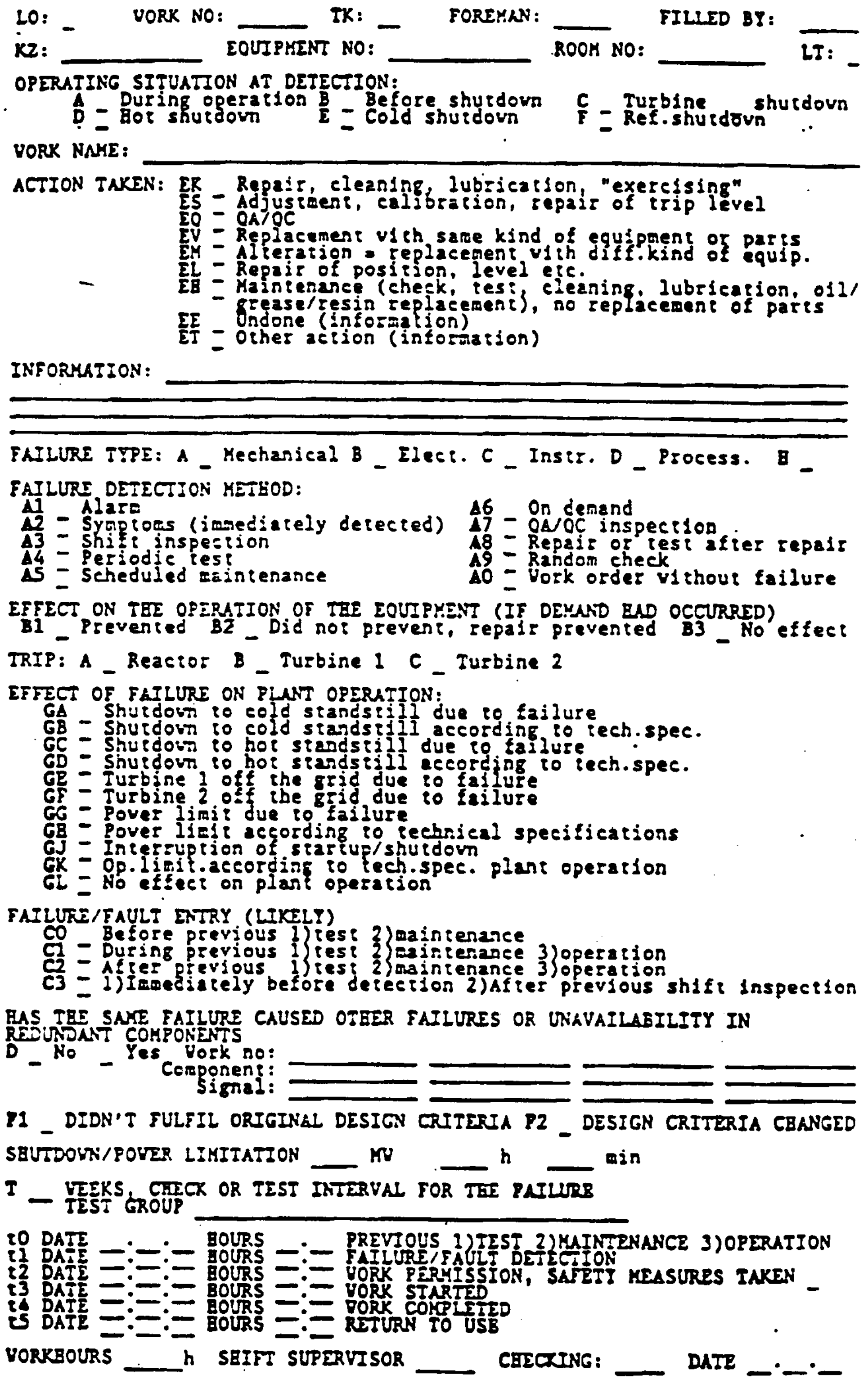
The following methods are used for quality control:

(1) The program makes logic checks of the answers given on the data collection form. (For example, if the failure detection method is A1 or A2, the time of the occurrence of the failure might not be C0, detection A4 might not be consistent with entry C3, etc.).

(2) Entries made by foremen and shift supervisors are verified by a dedicated specialist for all events conceming components covered by technical specifications.

(3) Before any parameters (failure rates) are used in a PSA, they are compared with generic data available (IAEA, NRC, EPRI etc.).

Equations for all possible combinations of answers to the items in the data collection form were developed to obtain failure rates and unavailability parameters /A-1/ needed in basic quantification and in time-dependent calculations. A computer program was



LO: _ VORK NO: _____ TK: __ FOREMAN: _____ FILLED BY: _____

KZ: __________ EQUIPMENT NO: __________ ROOM NO: ________ LT: _

OPERATING SITUATION AT DETECTION:
A _ During operation B _ Before shutdown C _ Turbine shutdovn
D _ Hot shutdovn E _ Cold shutdovn F _ Ref.shutdövn

VORK NAME: ______________________________

ACTION TAKEN: EK _ Repair, cleaning, lubrication, "exercising"
ES _ Adjustment, calibration, repair of trip level
EQ _ QA/QC
EV _ Replacement vith same kind of equipment or parts
EM _ Alteration = replacement vith diff.kind of equip.
EL _ Repair of position, level etc.
EH _ Maintenance (check, test, cleaning, lubrication, oil/ grease/resin replacement), no replacement of parts
EE _ Undone (information)
ET _ Other action (information)

INFORMATION: ______________________________

FAILURE TYPE: A _ Mechanical B _ Elect. C _ Instr. D _ Process. H _

FAILURE DETECTION METHOD:
A1 _ Alarm A6 _ On demand
A2 _ Symptoms (immediately detected) A7 _ QA/QC inspection
A3 _ Shift inspection A8 _ Repair or test after repair
A4 _ Periodic test A9 _ Random check
A5 _ Scheduled maintenance A0 _ Vork order vithout failure

EFFECT ON THE OPERATION OF THE EQUIPMENT (IF DEMAND HAD OCCURRED)
B1 _ Prevented B2 _ Did not prevent, repair prevented B3 _ No effect

TRIP: A _ Reactor B _ Turbine 1 C _ Turbine 2

EFFECT OF FAILURE ON PLANT OPERATION:
GA _ Shutdovn to cold standstill due to failure
GB _ Shutdovn to cold standstill according to tech.spec.
GC _ Shutdovn to hot standstill due to failure
GD _ Shutdovn to hot standstill according to tech.spec.
GE _ Turbine 1 off the grid due to failure
GF _ Turbine 2 off the grid due to failure
GG _ Pover limit due to failure
GH _ Pover limit according to technical specifications
GJ _ Interruption of startup/shutdovn
GK _ Op.limit.according to tech.spec. plant operation
GL _ No effect on plant operation

FAILURE/FAULT ENTRY (LIKELY)
C0 _ Before previous 1)test 2)maintenance
C1 _ During previous 1)test 2)maintenance 3)operation
C2 _ After previous 1)test 2)maintenance 3)operation
C3 _ 1)Immediately before detection 2)After previous shift inspection

HAS THE SAME FAILURE CAUSED OTHER FAILURES OR UNAVAILABILITY IN REDUNDANT COMPONENTS
D _ No _ Yes Vork no: ________ ________ ________ ________
Component: ________ ________ ________ ________
Signal: ________ ________ ________ ________

F1 _ DIDN'T FULFIL ORIGINAL DESIGN CRITERIA F2 _ DESIGN CRITERIA CHANGED

SHUTDOVN/POVER LIMITATION ____ MV ____ h ____ min

T __ VEEKS, CHECK OR TEST INTERVAL FOR THE FAILURE
TEST GROUP ______________________

t0 DATE _._._ HOURS _._ PREVIOUS 1)TEST 2)MAINTENANCE 3)OPERATION
t1 DATE _._._ HOURS _._ FAILURE/FAULT DETECTION
t2 DATE _._._ HOURS _._ VORK PERMISSION, SAFETY MEASURES TAKEN _
t3 DATE _._._ HOURS _._ VORK STARTED
t4 DATE _._._ HOURS _._ VORK COMPLETED
t5 DATE _._._ HOURS _._ RETURN TO USE

VORKHOURS ____h SHIFT SUPERVISOR ____ CHECKING: ____ DATE _._._

Figure A1: Data collection form of the Loviisa reliability data collection

is available to estimate the parameters. The program reads the coded failure data from the file and tests if the failure process is time-independent. If the failure rate is not constant, a trend analysis is performed and up-to-date reliability parameters are estimated. Component-specific failure rates and unavailabilities on demand, repair rates and finally the unavailability values for selected failure modes with their uncertainty distributions can be calculated. A special robust empirical Bayes method is used for parameter estimation (/A-2/ - /A-5/). It yields parameters for individual components as well as for groups of identical components.

The mean values of the unavailability are transferred into the fault tree program input file after comparison with generic data. Distributions are also estimated for all parameters.

More detailed information can be found on the data collection and handling in /A-1/, on the reliability parameter estimation in /A-1/, /A-2/, on the special empirical Bayes estimation method in /A-1/ - /A-5/, and on the reliability parameter estimation in the case of increasing or decreasing failure rates in /A-6/ - /A-9/.

Information from the data base is currently available for outside users only on a case-by-case basis, normally on commercial terms.

A.4. France

With view of obtaining a large amount of data national data banks were made use of as much as possible in France: hence the S.R.D.F. (Reliability Data Collection System) and F.E. (Event File) banks were analysed along with the file of statistical data on the operation of the French nuclear power plants.

It was deemed necessary to complete these studies by on-site surveys in order to account for practical aspects and thereby render the study more realistic.

Finally, some foreign data bases were used to supplement and compare some particular data.

This approach at 3 levels - local, national, international - is described below.

A.4.1. Local Level

A.4.1.1. Method

- The surveys and case histories on site provided insight into real-life operations and identified further specific data. Also local analysis of plant operation showed the need to include a number of events that had not been identified initially in the reliability studies of systems or sequences.

  Operating and reliability data were obtained, in particular on equipment for which generic data was not available or on equipment for which on-site operating experience indicated that actual data would differ notably from the corresponding generic data.

  In the very particular case of limited experience feedback, aggregating methods of the Bayes type were used in order to take into account different types of information concerning components of the same kind, to improve the validity of the data.

  In addition, several annual shut-downs for refuelling of different types were the subject of special monitoring.

  A general flowsheet illustrating the different phases of water levels and movements of water in the primary system was derived.

A.4.1.2. Tools

All the local systems were used for data collection. Automatic analysis programs were developed to facilitate the extraction of relevant data.

Three important local files were particularly valuable:

- Data files based on information from the plant unit computer that permanently records plant operations. Any change of state of a component or any variation of an analogous quantity is stored and processed by a software tool.
- Data files concerning items of equipment withdrawn from service, created by means of a software tool: AIC (computer assisted plant isolation) and recording the history of all maintenance operations.

- A local history file recording data on malfunctions noted in the operation of an equipment and containing a request for servicing to correct the malfunction.

These computer or automatic systems were complemented in specific cases by studies of the operating reports of the unit shifts and of the safety engineers and by discussions with the operating and maintenance personnel.

A.4.2. National Level

At national level data acquisition was mainly from data banks: S.R.D.F. (Reliability Data Collection System) and F.E. (Event File).

The statistical data file was used to acquire plant unit operating data, availability and production coefficients.

A.4.2.1. S.R.D.F.

- **File Description**

Approximately 500 electrical and mechanical items of equipment have been monitored per plant unit (pumps, valves, diesel generators, motors, transformers etc.) since the S.R.D.F. was first set up at the Fessenheim plant site in 1978. Failure data is acquired locally in the form of a descriptive file containing a brief description of the fault, the failure mode and its severity as well as the consequences for the plant unit. In addition, operating parameters are recorded regularly for each item of equipment. Data management and processing are carried out at national level on a mainframe computer which can be accessed from different terminals.

On the average, the data bank receives over a hundred files per year and per plant unit (about 20,000 files by the end of 1988).

Due to the specific nature of the electronic equipment used in control/monitoring of the 1,300 MWe plant units, a special monitoring system was developed, the S.R.D.F.A (about 5,000 files by the end of 1988).

- **Methodology followed**

Apart from the data bank on control and instrumentation equipment which is controlled at mainframe level, the raw data are not systematically analysed at central level before processing.

This means that the consistency, homogeneity and representativeness of data conceming all the descriptive aspects of a failure collected under routine operating conditions, had to be ensured before they were incorporated in EPS-1300 study /A-10/.

A centralized control of the files by engineers with good operating experience ensured that the data obtained were consistent and realistic by reducing the margin for interpretation related to personal judgment and by applying strict criteria with respect to critical failures in terms of safety.

The study of about 5,000 failure records was complemented by an analysis to identify common cause failures.

Most of the reliability data were prepared in this way over an observation period lasting generally from 1978 to 1986 approximately, depending on the progressive installation of the S.R.D.F. system on the different sites.

A.4.2.2. Event file

- **File description**

The data collected for the F.E. mainly concern operating incidents (shut-downs, reduction in output, departure from technical specifications), incidents conceming nuclear safety and the environment and incidents due to human factors.

This data bank was set up in 1978. Events are acquired at local level in the form of a descriptive event file containing a brief description of the event, its origin and nature, as well as the unit state and the operating data.

Data management and processing are performed at national level on a mainframe computer. Interrogation-analysis sessions are possible from each terminal.

By the end of 1988 the file contained some 20,000 records.

- **Methodology followed:**

A large number of file records (approximately 5,000) were analysed in detail in order to:

- complete the S.R.D.F. reliability data in some cases by analysing the events in relation to their consequences rather than in relation to their causes,
- provide operating data,
- complete and validate the quantification of the operating profile,
- permit the quantification of a great number of initiating events.

A.4.3. International Level

A.4.3.1. Tools used

- Data acquisiton was complemented by consulting certain foreign data banks. Two of them deserve being mentioned, in particular:
  - NPRDS: (Nuclear Plant Reliability Data System). This American data bank managed by the INPO (Institute of Nuclear Power Operation) is the equivalent of the S.R.D.F.,
  - the "Incident File" concerning foreign nuclear plants constituted by EDF's Research Directorate (DER)
    This file contained over 20,000 operating events at the end of 1987 representing an experience feedback equivalent to 500 reactor years.

A.4.3.2. Methodology

In some particular cases the analysis of the aforementioned data bases provided data that were not monitored elsewhere, for instance the frequency of initiating events of the pipe break type. More generally, they provided experience feedback on a worldwide scale for comparison and validation of certain data.

Data quality assurance relies on:

- elaboration of a user guide making it possible to carry out a logical analysis and to ensure consistency between all the plants,
- site collection supervised by a person at each 2 unit plant, responsible for checking information,
- national checking under sampling for the whole data except for 1,300 MWe data concerning electronic components for which checking is systematic,
- control of the application: monitoring and deciding the main developments in order to improve the quality of application.

A.4.3.3. Application

Using the aforementioned methodology and data bases $\beta_k^n (n = 2 \text{ to } 4)$ factors according to the method outlined in Section 1.4.12 were estimated for the following equipment.

- sensors and instrumentation,
- check valves,
- contactors and circuit breakers,
- reactor trip breakers,
- pumps,
- steam isolation valves,
- motor-operated valves,
- pneumatically-operated valves.

For equipment for which experience feedback was insufficient, the values were estimated either by analogy with the preceding components or using engineering judgment, with allowance for the values used in probabilisitc safety studies in other countries.

A.5. Germany

The data bank for licensee event reports BEVOR maintained at GRS on request of the Federal Ministry for Environment, Nature Protection, and Reactor Safety (BMU) contains reports on licensee events of safety relevance. Its objective is to support the supervision of the safety of the nuclear power plants in operation. The systematic evaluation of licensee events permits one to detect possible deficiencies at an early stage, to prevent the recurrence of similar failures in other power stations and to improve plant safety.

The notification of the licensee events is based on unified reporting criteria and reporting formats for the entire FRG. The criteria refer to the types of events to be notified. The reporting form contains a full text description of the event and a classification by means of codes. The report is then processed by storing the information in a data bank which contains, in particular, details on

- event sequence
- way of discovery
- effects
- causes
- technical equipment affected by the event
- remedies
- provisions against repetition
- radioactive emissions
- radiological effects
- classification of the event

In order to facilitate the selection of potential common cause events there is a code called "component and system failures due to a common cause". Search according to this code serves to give a rough selection of potential common cause events. A more profound analysis would require, however, to select events applying various codes like component type, systems involved etc.

The data bank has been used in conjunction with the data bank IRS (cf. Section A.13) and information from plant specific reliability data acquisition projects to prepare common cause data for the German Risk Study /A-11/.

The information contained in the BEVOR data bank is confidential.

A.6. Japan [1]

In Japan there are two incident data bases for commercial nuclear power plants: the data base developed by the Nuclear Power Engineering Center (NUPEC) for the Ministry of International Trade and Industry (MITI), which is the regulatory body for commercial power plants, and the data base developed by the Central Research Institute of Electric Power Industry (CRIEPI) for the electric utilities. Short descriptions of these two data bases are given below.

A.6.1. Incident Data bases of NUPEC

A.6.1.1. Outline

The objective for NUPEC to develop an incident data base was mainly to provide information on similar incidents whenever an incident occurred and to perform a statistical analysis of incidents and failures. This database contains all incident reports submitted to MITI after 1966, when the first commercial power plant in Japan, Tokai 1, started operation. These reports to MITI are required by law and MITI notifications to the utilities. All commercial nuclear power plants in Japan, including PWR, BWR, and Gas-Cooled Reactors, are covered by this data base. Further information on this data base is given in /A-12/.

[1] Acknowledgement
This material was prepared based on information from Mr. M. Hada of the Nuclear Power Engineeering Center and Mr. I. Tanaka of the Central Research Institute of Electric Power Industry. The author would like to acknowledge their co-operation.

A.6.1.2. Coding

The incident data stored in the data base have keywords for information retrieval, which are classified according to the data items shown in Table A.2. In addition to the keywords, the database containing the following types of data:

(1) Description in natural language: Descriptions of situation and cause of incident (Operation management card).

(2) Data on optical disk system: Incident reports (Operation management card and detailed incident reports, etc.).

Information can be retrieved using either keyword search or word matching based on natural language descriptors.

All descriptors in this database, including the keywords, are in Japanese.

Table A.2: Input Data Items (Keywords) of NUPEC's Incident/Failure Data Base

1)	Identification number
2)	Power station and unit names
3)	Incident name
4)	Date of incident occurrence (discovery)
5)	Plant status
6)	Description of incident/failure
7)	Name of failed system/train/component/part
8)	Reactor trip signal
9)	Cause of incident/failure
10)	Countermeasures to prevent recurrence
11)	Effects (on reactor power and safety)
12)	Way of discovery
13)	Plant down time due to the incident
14)	Others

A.6.1.3. Quality control of the data base

The incident reports submitted to MITI are prepared based on reporting criteria specified in laws or regulatory notifications. These reports are used as direct input to the data base; additional quality control of the contents of these reports is not performed by the data-base management.

A.6.1.4. Information which can be obtained from the data base

In addition to the incident reports which can be retrieved by keyword search or word matching, various forms of summary tables can be compiled by the data-base management system on a computer. A list of computer output items is given below.

(1) List of incident/failure names (for use in searching similar incidents).

(2) Description of incident/failure.

(3) Number of incident/failure reports (for different failure locations).

(4) Number of incident/failure reports (for different causes).

(5) Number of incident/failure reports (for different combinations of failure location, cause and reactor type).

(6) Frequency of occurrence of incident/failure (in the form of graphs).

(7) Number of incident/failure reports (for different systems).

(8) Relative frequency of occurrence of incident/failure (for different combinations of systems and causes).

(9) Number of incident/failure reports (for different trains, components, and parts) (in the form of graphs).

(10)Average number of incident reports per year (in the form of graphs).

(11)Summary table of numbers of incident/failure reports.

A.6.1.5. Availability of data sources to outside organizations

The data base was developed for the government organization and cannot be accessed by other organizations. The detailed reports stored in the optical disk system also cannot be accessed by other organizations. Important incidents in this data base are reported to the OECD/NEA as a Japanese contribution to the Incident Reporting System (IRS) (cf. Section A.12).

A.6.2. Incident data base of CRIEPI

A6.2.1. Outline

The objective of CRIEPI in developing an incident data base was to provide a common data base for the electric utilities in Japan. The data base includes all incidents and failures reported to MITI after 1966. It covers all commercial power plants in Japan and contains information on PWR, BWR and Gas-Cooled Reactors.

A.6.2.2. Coding

For each of the original incident reports received from the utilities an abstract is made and included in the data base.

Incident descriptions are coded to allow data retrieval by keyword searching or word matching.

(a) Searching by keywords.

A set of keywords is assigned to each incident report. Table A.3 shows the items of keywords used in this data base. The data-base user will search for incidents with certain attributes by giving a combination of keywords selected from such items.

(b) Searching by word matching.

The data base user specifies a string of characters (part of a sentence) in the original incident descriptions. Then the data-base management system will retrieve incident data that contain the same character string.

All descriptions in this data base, including keywords, are in Japanese.

A.6.2.3. Quality control of the data base

The assignment of keywords for data searching were decided upon after a discussion by the keyword review committee organized by CRIEPI.

A.6.2.4. Information that can be obtained from the data base

In addition to the incident descriptions that can be retrieved by keyword searching or word matching, various forms of summary tables can be made by the data base management system on a computer. A list of computer output items is given below:

(1) Number of incidents/failures at different units.

(2) Number of incidents/failures for different reactor types.

(3) Number of incidents/failures for different systems.

(4) Number of incidents/failures for different trains.

(5) Number of incidents/failures for different components.

(6) Number of incidents/failures for different parts.

(7) Number of incidents/failures for different causes.

(8) Number of incidents/failures for different severity classes of effects on power generation.

(9) Number of incidents/failures for different durations of plant down time.

A.6.2.5. Availability of data sources to outside organizations

Japanese utilities have on-line access to the data base. However, the access to this data base is restricted to the utilities.

Table A.3: Data Items (Keywords) of CRIEPI's Incident/Failure Data Base

1)	Identification number
2)	Company name
3)	Unit name
4)	Reactor type
5)	Reactor vendor
6)	Date of incident
7)	Date of reporting
8)	Component failure
9)	Plant status at time of discovery
10)	Reactor power at time of discovery
11)	Reactor trip signal
12)	Effect on reactor power
13)	Effect on reactor safety
14)	Effect on health and radiological protection
15)	Plant down time due to the incident
16)	System
17)	Train
18)	Component
19)	Parts
20)	Cause of incident
21)	Description of incident
22)	Operation status of the system or component at the time of discovery
23)	Ways of discovery
24)	Counter-measures to prevent recurrence

A.7. The Netherlands

A.7.1. General

Plant specific data sets exist for both NPPs in the Netherlands.

Borssele is a 2 loop 477 MWe Siemens/KWU PWR with bunkered primary and secondary emergency supply systems as a special feature. Operation started in 1973.

Dodewaard is a 60 MWe G.E. BWR with a pre-Mark 1 containment (2 suppression pool vessels), natural circulation (no recirculation pumps) and isolation condenser as special features. Building began in 1965 and operation started at the end of 1968.

To assess common cause failures use has been made of generic data sources (/A-13/, /A-14/, /A-15/ and /A-16/).

A.7.2. Experience of common cause failures

Borssele experienced twice a common cause event. In 1984, during the transient following the loss of main coolant water, secondary relief valves had electrical problems and did not operate properly. The pressure reached 91 bar, but the safety valves (setpoint 88 bar) did not open. The cause of this CCF was corrosion on the chrome-plated pistons of the pilot valves. Both safety valves are equipped with three redundant pilot valves. The root cause was probably chlorine contamination of valve internals from maintenance activities. Both an administrative control of all potentially corrosive chemicals used for maintenance work and a design change (each safety valve has been substituted by ten smaller safety valves) were taken as corrective actions.

In 1990, during refuelling outage and unloaded core, a heavy storm accompanied by an extremely high tide, washed floating dirt into the circulating inlet station. The mesh filters were clogged. Due to the suction of the main coolant water pumps of the coal-fired plant (both NPP and Coal-Fired Power Plant draw main coolant water and service water from the same inlet station in the Schelde river), a protection by-pass opened and dirt was sucked into the service water system of the NPP Borssele. This common cause event could have led to the loss of the ultimate heat sink - including 3--out-of-4 Diesel Generators - if the station had been on power. However, the bunkered systems should have kept the plant in hot stand-by if needed. The root causes were: extreme weather conditions, not timely tripping of the pumps of the coal-fired power plant, and pressure difference measurement of filters not available. As a consequence of the event, the instrumentation of the inlet station was changed. Also the bunkered system will be improved for cold shut-down requirements. Additionally, an extremely low tide is practically excluded as a common cause initiator, because of an extensive dredging programme of the inlet channel.

A.7.3. Dependent failures in the PSA for Borssele and Dodewaard

A.7.3.1. Borssele

- **Generalities**

In the Borssele PSA three types of dependent failures were analysed:

(1) Common-cause initiator dependencies.

(2) Inter-system dependencies.

(3) Inter-component dependencies.

For the types 2 and 3, four subcategories were defined:

(1) Functional dependencies.

(2) Shared equipment dependencies.

(3) Physical interaction.

(4) Human interactions.

Dependencies which could be specifically identified and quantified were modelled explicitly in the event and fault trees.

Dependencies which could not be modelled explicitly were included in the study in two ways:

In the first place, dependent failures arising from phenomena interactions and unforeseen design interactions (subtle interactions) were analysed by reviewing the applicability of subtle interactions found in past PSAs to Borssele and secondly by the modelling of common cause failures to account for the sum of inter-component dependencies not modelled explicitly in the fault tree models.

Lastly, as part of the systems modelling task, a review of actuation, control and component protection was performed. This review was conducted to determine whether any dependencies exist between components within each system or between systems which could potentially result in a significantly lower availiability than expected. This review included the following:

(1) Component dependencies on actuation signals.

(2) Actuation signal dependencies on sensors/transmitters.

(3) Component protective trips.

(4) Permissive signals required for operation.

(5) Presence/absence of conditions required for automatic operation.

The significant dependencies identified during this review were explicitly modelled in the fault tree models.

- **Common Cause Initiating Event Dependencies**

Common cause initiating events were modelled as part of the Borssele event tree analysis; e.g. Loss of Off-site Power .

- **Functional Dependencies**

Functional dependencies were also treated in the construction of event trees.

- **Shared System Dependencies**

Shared system dependencies were identified and modelled during the fault-tree modelling task accounting for dependencies of plant systems on the successful operation of other plant systems. An example of such a dependency is that of the emergency diesel generators on the auxiliary and emergency cooling water system. Dependency matrices were developed in the system modelling task to define such shared-system dependencies. In the development of system-level fault trees, specific failure events were included to account for the dependency of each portion (train) of a front-line system on a portion of a support system.

- **Physical Interactions**

Physical interactions like fires and floods were treated explicitly in the PSA.

- **Subtle Interactions**

A list of subtle interactions was developed based on nuclear plant operating experience. PSA analyses were examined with respect to the specific Borssele design to determine whether or not similar interactions exist at Borssele, e.g. issues investigated were:

Diesel generator load sequence failures, sneak circuits, bus switching problems, pump room cooling, steam binding of emergency feedwater pumps due to leaking main feedwater valves, inadvertent isolation of all feed flow to steam generators, cross-tied pumps discharge check valve failures, main/emergency feedwater commonalities, turbine driven pump failure due to water carry-over, etc.

- **Common Cause Failure Analysis**

The method applied for CCF analysis was taken from /A-13/. It consists of four steps:

(1) System logic model development.

(2) Identification of common cause component groups.

(3) Common cause modelling and data analysis.

(4) System quantification and interpretation of results.

The qualitative screening included the identification of attributes such as design, location, modes of operation and operational history for various components in order to identify factors that might be affected by component interdependence. The types of equipment judged to be important for the Borssele PSA are the following:

- Valves (motor-operated and air-operated).
- Pumps (motor-driven and turbine-driven, failure to start).

- Diesel generators.
- Major electrical breakers.
- Batteries.
- Check valves (F.T.O. and F.T.C. for selected combinations).

A quantitative assessment of CCF component groups was performed in conjunction with a qualitative assessment to screen out insignificant CCF groups by inserting events into the system fault trees which represent the common cause failure events. The fault trees were then quantified to assess the relative importance of each common cause group, using conservative values for the common cause failure events. Common cause events found to be insignificant relative to others were removed from the fault trees.

For historical reasons and because of the availability of parameter estimates, the Multiple-Greek-Letter Method (cf. Section 1.4.3) was used as basis for the Borssele PSA. CCF parameter data sources used were /A-13/ , /A-14/ and /A-15/.

In reviewing 5 years of plant operating experience, no CCFs were found to be applicable. Although the plant had experienced several CCFs, e.g. CCF of multiple steam generator safety relief valves and CCFs of the auxiliary and emergency feedwater system pumps, these CCFs were not found to be applicable any more, because of modifications and design changes since then. Nevertheless, special attention was given to these systems and systems with similar components.

A.7.3.2. Dodewaard

- **Data Analysis**

For Dodewaard an extensive task to derive plant specific data was undertaken. Approximately 20,000 maintenance work records were reviewed. Also monthly and yearly operating reports were reviewed covering a time window of approximately 20 years. The following components were reviewed:

(1) Emergency Condenser	pipe, valves, condenser tubes
(2) Automatic Depressurization System	valves
(3) Low Pressure Coolant Injection	pumps, valves
(4) Closed Cooling Water	pumps, valves, heat exchangers
(5) Steam and Feedwater System	pumps, valves
(6) Instrument Air System	compressors, valves
(7) Control Rod Drive System	pumps
(8) Suppression Pool Cooling System	pumps, valves, heat exchangers
(9) Electrical Distribution System	diesel, load circuit breakers, motor generator sets, transformers, turbo-generator
(10)Direct Current System	batteries, inverters,
(11)Service Water	pumps, valves, heat exchangers, strainers

The maintenance work records were classified in four categories:

(1) Catastrophic failure.

(2) Degraded failure.

(3) Incipient failure.

(4) Not applicable.

The demands due to isolation requirements for repair of other components and the total number of demands per group of components due to the applicable tests performed within the data window were calculated for the estimated times of exposure. All the information was put together in data sheets, where for each component and failure mode, the total number of catastrophic failures (numerator) is listed together with the total time of exposure (denominator). The latter is divided into different categories: tests, repairs, isolation, operation, calender hours (used for these basic events when the failure mode can occur at virtually any time), reactor hours.

Maintenance outage times were determined by interviewing the plant operators.

The following generic assumptions were made:

a) For normally operating systems, the exposures due to repairs and isolations were neglected. The contribution of such terms are negligible compared with the total operating history of these systems.

b) To estimate the exposures due to repairs (only for stand-by systems), two demands for each failure mode were assumed after each repair requiring operational check. Fifteen minutes of operation and one start were assumed for those components with a time failure rate.

For components for which no or very little data were found, generic data were used from Science Application International Corporation (SAIC) sources.

- **Common cause failure analysis**

For the Dodewaard PSA generic common-cause data are used as given in /A-15/. The Alpha-Factor Method (cf. Section 1.4.5) was used as method for the Dodewaard PSA. The impact vector approach was used to address plant-specific features. In the Dodewaard PSA, CCF events were screened for their risk significance using the Beta-Factor Model (cf. Section 1.4.2). The generic screening β-factors were taken from /A-13/. The events to be modelled in the fault trees are derived according to the methods described in /A-13/. The common cause groups are defined in the systems analysis task.

- **Quality Control**

For both PSAs (Borssele and Dodewaard) quality assurance was provided by a Q.A. effort of the contractors (Siemens/NUS for the Borssele PSA and SAIC for the Dodewaard PSA). Besides this effort both the utilities together with KEMA had an extensive and detailed review process of the drafted PSA tasks. This review included the data collection tasks. Last but not least IAEA IPERS reviews took place for both the PSAs.

A.8. Spain

There are no data banks in Spain providing information for common cause failure analysis. However, a data bank system on abnormal events and component failures in Spanish Nuclear Power Plants is under development. One of its principal purposes is the acquisition of reliability data to be used in probabilistic safety assessments.

The component data bank system basically stores information about component design and operational characteristics, operating hours or demands, as well as component failure descriptions. It is structured in a way which allows an efficient classification and retrieval of information. Therefore, many of the data fields are related to component failure aspects, such as failure mode, failure cause or repair type, are carefully encoded. Full text descriptions are also provided. One of these fields is used to establish a relationship between maintenance records whenever they deal with failures which are linked by their causes in some way. This can provide a hint for a detailed common cause analysis.

The topics on which information is requested are:

- **Type of reactor**

All the Spanish Nuclear Power Plants in commercial operation are included in the data bank system. They comprise 9 reactors, from which 7 are PWR and 2 BWR. The designers of the PWR are Westinghouse (6) and Siemens Kraftwerk Union (1), whilst the designer of the two BWR is General Electric.

- **Coding**

The structure and coding of the data bank system was based in the beginning on those of the "Component Event Data Bank (CEDB)" from the Joint Research Centre at Ispra, in order to ensure a good degree of compatibility when interchanging information with the CEDB. Later on, the data bank was modified in a way which satisfies better the Spanish needs and objectives. The essential information encoded in the component failure records are the way of failure detection, the failure effects, the failure mode, the corrective and administrative actions performed, the failure causes, the reactor status at the time of failure and during repair, and start-up restrictions.

- **Type of quality control used**

There is a qualified team belonging to the maintenance department in each nuclear plant that generates and supplies the data to the data-bank system. These teams have been instructed about the data bank goals and the way to analise and encode the plant information. The control and management of the data-bank system is done by UNESA (the association of Spanish electricity companies) and a consultant firm. They take care of quality control of the data supplied by the utilities and hold periodical meetings with them thus ensuring homogeneity of the analysis criteria.

- **Full text description of the events**

Besides the encoded information of the failure records, which is necessary for an efficient data classification, a full text description of the events and the maintenance carried out is provided for. The length of these descriptions is unrestricted.

- **Data access**

The data-bank system is managed by UNESA and can be freely accessed by the nuclear utilities and the "Consejo de Seguridad Nuclear", the Spanish Nuclear Regulatory Commission. Access to the data-bank system by any other organisation is only possible with the authorization of UNESA.

At present, the data bank mostly contains information on mechanical and electrical equipment of safety related systems. An extension to instrumentation and control equipment is planned for the future. At present, the system keeps track of all the necessary information about a total of 6,659 component since approximately the beginning of 1989.

On the other hand, a dependent failure analysis is performed as part of the probabilistic safety assessments that the Spanish nuclear utilities are carrying out. In these analyses the plant operating experience is examined from the viewpoint of common cause failures; some occurrences have been identified.

A.9. Sweden

An overview of the reliability information systems in the Nordic countries is given in Table A4.

Table A4: Overview of the reliability information systems in the Nordic countries

CASE Database or information system	Trip reports	LER	Maintenance hist.	Tech. data	Failure statistics	Int. events	Dose measurements	Trend analyses	
STAGBAS2 (SKI)	x	x			x				x
ERF (KSU)	x	x			x		x		
TVO failure reporting system						x			
ATV						x			
Information system in B1/B2 (BIS)			x	x				x	
Information system in 01, 02, 03 (OAS)			x	x				x	
Information system in F1, F2, F3 (KIF)			x	x				x	
Information system in R1, R2, R3,R4 (RIS)			x	x				x	
Information system in Lovisa 1,2 (LOTI)			x	x				x	x

The search and classification of CCF-data is a very time-consuming process. Neither the Swedish (nor Finnish) data bases listed in Table A4 are geared towards classifying and identifying CCFs. The analyst has to draw data from many sources and search for data with unique CCF attributes in order to be able to find e.g. precursors.

The analyst also has to find relevant operating and background data like operating hours, hours of stand-by, number of activations. The data have therefore to be treated statistically and carefully examined with respect to correctness and consistency.

In Sweden the best sources for CCF information are the LERs (Licensee Event Reports) stored in the data base STAGBAS2, maintained by the Regulatory Body SKI and the failure reports stored in the ATV-data base. CCF events are rare. To estimate CCF parameters, especially for highly redundant systems is a matter of deep analysis and requires the sophisticated mathematical tools. These are available in Sweden. At present, there are CCF projects ongoing on highly redundant systems in Sweden, sponsored by the SKI.

A.9.1. The Scandinavian Nuclear Power Reliability Data System (ATV)

In accordance with a government decision, probabilistic safety assessment (PSA) studies are to be performed, and regularly updated for each of the Swedish nuclear power plants.

Long before the initiation of the first of these PSA studies and in order to enhance their quality, the Swedish nuclear utilities realized the importance of disposing of an accurate and reliable data base for failure probabilities for all major safety related components.

Coordinated by the Nuclear Safety Board of the Swedish Utilities (KSU) and with the participation of all Swedish nuclear power utilities, the Swedish Nuclear Power Inspectorate (SKI), ABB-Atom and Studsvik, a project started in 1981 for developing such a data base. In 1982 the first version of the so-called "T-book" was published, a comprehensive, user-oriented data handbook for use in current and future Swedish PSA studies.

The "T-Book" has been developed on the basis of appropriate statistics from the ATV-system, the information of which was complemented, when pertinent, with information gained from a review of the Swedish LERs. Whenever statistically feasible the "T-Book" contains plant-specific failure data (failure to start/open on demand, failure to run, repair times etc.) for pumps, valves, diesel engines, instrumentation etc. which mainly belong to safety systems. Distributions are provided, based on the use of the

Gamma-prior-distribution for failure rates and a Beta-prior-distribution for failure probabilities per demand.

The updated second edition of the "T-Book" (in English) was released at the beginning of 1985. After consolidating the methods and the extent of the T-Book by the experience with the first two editions, the future updating will be an integral part of the ATV-system.

A.9.2. Quality assurance

The most important factor for a reliability data system is to assure good quality of the input data. When creating the ATV-system the following factors promoting good quality of the data were considered:

- Voluntary co-operation by the utilities for defining the requirements and development of the system.
- Failure and engineering reports based on and integrated with the local maintenance routines and information systems.
- Input of failure reports (in flexible ways) checked by a control program, errors can quickly be corrected via local terminals.
- Fast and easy feedback of data to the reporting stations.
- A user's manual defining the characteristics and the treatment of the system.
- Designated persons responsible for the different activities according to the instructions.
- A central secretariat responsible for the running adminstration and follow-up.
- Common working group for the follow-up and evaluation of the system function.
- Education of and information to all parties involved.

After completion of the system some activities were initiated for improving the quality of the input information, viz.:

- Publication of an ATV-pamphlet
- Quantitative and qualitative analyses of the input information

At present the quantitative analyses of the failure reporting are updated every year. These analyses have shown an upward trend in the coverage of the reported failures to the ATV-system. The coverage has increased from about 50 % in year 1976 to about 80 - 99 % in year 1980 - 89. Small fluctuations can be seen among different units.

In order to improve the quality of the input information all failure reports from each unit have been studied during a certain time period. This work has shown the weaknesses both in the reporting of each unit and in the ATV-system. Looking at the details, the most important failure data code (failure mode) proved to be very reliable. Only six percent was judged to be faulty. The main result of this study shows the need for more information of the plant personnel about the use and the necessity of the ATV-system.

A.9.3. The T-Book Version 3

The third Swedish edition of the T-book was published in 1992. It contains values based on failure information up to 1987 for all units reporting to the ATV-system. This is equivalent to a total of 108 reactor years. An English version of the book is available as well.

The main objective of the T-book is to provide reliability data for the unavailability computations which are performed for each component that is considered in the PSA of nuclear power plants. As the use of PSA is steadily growing in the daily safety work at the NPP and at SKI, there will be a corresponding rise in the need for good quality reliability data. A new feature of great interest is the application of the $q_0 + \lambda t$ model, where q_0 is derivided from failures occurring on demand while λ represents failures during the stand-by time. This model is applicable to component groups where several test intervals are represented in the operational data.

A.9.4. The STAGBAS2 Database at SKI

All licensee event reports (LER) and reactor trip reports (SS) occurred in Sweden are stored in the STAGBAS2 database. Today the database contains about 5,500 reports. The data base contains information on a wide spectrum of incidents ranging from less significant effects on safety systems or components to important common cause failure events. The STAGBAS2 data is, however, not a quantitative failure data

data base, such as the ATV database. The LERs and SSs reports are more concentrated on violations of the Technical Specifications and occurrences during power operation.

A.10. United Kingdom

A.10.1. Different Approaches to Dependent Failures

Over the past 20 years the importance of dependent failure analysis in probabilistic assessments has become widely recognised in the UK. The current position is that there are many differences of detail in the approaches used by different analysts/companies, but it is possible to group the methods used by their more general features.

The most simple classification which can be made is based on the level at which the system is considered. The majority of the approaches taken in UK PSAs can be allocated to one of two groups:

(1) System Level Assessment.

(2) Component Level Assessment.

The first group includes methods which consider the system as a whole and estimate a dependent failure probability of the system directly, over-riding any estimate based on methods, such as Fault Tree Analysis (FTA) which do not consider dependencies. Such an assessment does not use any detailed component-level analysis.

The second group covers the methods which consider the effect of dependencies within the identified "Multiple Failure Groups" (MFGs) and then allow the ordinary assessment tools (usually Fault Tree Analysis (FTA)), to incorporate the dependent failures effect into the system failure model. In the latter case the most simple MFGs are of course groups of identical redundancy components.

A.10.2. Graded Levels of Detail

In many cases, probabilistic assessments follow a graded structure in which an initial set of fairly conservative "screening" values would be applied, at either the system or component level, in order to identify or confirm those dependency issues which are likely to appear prominently in the final results of the assessment. A second stage of dependent failures assessment in which resources are focused on these prominent areas and more detailed analysis is carried out.

In some cases, the screening assessment may be a simple set of system level estimates, with the key areas being analysed using a component-level approach.

A.10.3. Methods

A.10.3.1. System Level

Nearly all system-level assessments in the UK can be referred to as "Cut-Off' models (also referred to as System Reliability Cut-Off or CMF Cut-Off), since they all result in an estimate of the maximum reliability which may be claimed for a given system. Thereafter, they differ only in how the numerical value of the Cut-Off is obtained, and the level of detail in the assessment. A number of common applications are noted below.

- **Simple Cut-Off Chart/Table**

A chart, usually similar to that seen in /A-17/ - /A-19/, is used to quickly estimate system unavailability on demand based on the level of redundancy/diversity in the system. e.g. Simple Redundancy 10^{-2} - 10^{-4}, Diverse Trains 10^{-5}. A very similar approach using a "check-list" is also common. A table is formed which expresses a limited number (5 to 12) of system features which should be present for a given probability of system failure. The criteria focus on the general features seen in the chart approach, but also consider elements such as segregation, inspection etc.

- **More Detailed Cut-Off Charts and Tables**

Both of the above approaches are often refined for more detailed analysis, by adding studies of engineering aspects of the system which either improve of detract from the defences against dependent failures. A structure for doing this was contained in the original report from which the most common chart was drawn /A-17/, although this is not often applied in detail.

- **Cut-Off Generated Directly from Data**

In the Sizewell B Fault Analysis a representative cross-section of the key system cut-offs were of generated directly from studies of data for similar plant types in the USA. The database was large enough to estimate unavailabilities in the region of 10^{-4} per demand and failure rates while running of 10^{-5}/hr. Event data was studied in depth and assessed for its likely impact, should the events have occurred on the systems in the plant for which the fault analysis was being carried out. In this way a reliability for the key systems was generated based on operational experience. For the majority of UK PSAs such a study would not be possible due to the limited amount of data.

A.10.4. Component Level Approaches

Many UK PSAs apply some form of component level assessment of dependent failures, the most common method still being some sort of β factor (cf. Section 1.4.2), even when the systems contain more than two trains of equipment. The Multiple-Greek-Letter Model (cf. Section 4.3) is not seen very often in the UK. Analysts seem to prefer the use of partial β factor models (cf. Section 1.4.3) with some form of interpretation of the sub-factors to allow for failure of more than 2 trains. These are discussed below, as is the extent of use of other more complex models.

A.10.4.1. Beta-Factor Models

The most simple usage of this well known approach is the screening of a system by applying β factors within fault trees wherever redundant components or trains of components are modelled. In such a case a universal β factor is often applied in the first stage of analysis, for the same purposes as the broad cut-offs in A.10.3.1 above. The most common value used at this level is $\beta = 0.\ 1$, although some groups use $\beta = 0.2$.

Beyond this screening assessment a number of approaches are taken.

- **Beta Generated from Data**

The ability to generate β factors from plant-specific data is rare, but β factors from similar plants or component types are occasionally used. However, such a transference of data is not as common as the use of the partial β factor method described in Section 1.4.13.

A.10.5. Beyond Methods

When very low system failure probabilities are being assessed (perhaps those in the 10^{-5} - 10^{-6} region), the attention of UK PSAs is often focused on the qualitative assessment of the systems. One of the methods of Sections 1.4.2, 1.4.13 or 1.4.14 may be applied as a basis for the analysis, but the level to which the quality of the defences against dependent failures in the design becomes as important as the numerical output of one model or another. The principles of triggers or causes of failure and potential coupling mechanisms may be discussed, perhaps alongside a study of the precursor data if available.

A.10.6. Summary

In general, UK PSAs utilize one or more of the methods described in Sections 1.4.2, 1.4.13 and 1.4.14 to incorporate a numerical estimate of the effect of dependent failures into the fault tree analysis. The numerical values used will usually be obtained as an autonomous study within the PSA.

In terms of development, there are several places in which consolidation is taking place, with reports being produced to provide clear guidance to analysts who are not dependent failures specialists, on the most appropriate usage of the models described above and described more fully in Section 1.4. Further development of the DFP meapthod (cf. Section 1.4.14) is being considered for specific projects where it would be appropriate.

A.11. USA

Due to the scarcety of common cause events and the limited experience of individual plants, data on common cause events from general industry experience and a variety of other sources is needed to make statistical inferences about the frequencies of the common cause events. However, due to the fact that there is a significant variability in the U.S., especially with regard to the coupling mechanisms and defences against common cause events, the U.S. industry experience is not, in most cases, directly applicable to the specific plant being analysed (although much of it may be indirectly applicable). Also, and perhaps equally important, the analysis boundary conditions that dictate what category of components and causes should be analysed requires careful review and screening of events to ensure consistency of the data base with the assumptions of the system model and its boundary conditions.

The significance of this step cannot be overemphasized. An important conclusion of the Common-Cause Failure Reliability Benchmark Exercise /A-20/ is that the most important source of uncertainty and variation in the numerical results is data interpretation. Thus, careful attention and documentation must be given to this step.

The existing data sources generally fall into one of the following categories:

- Generic Raw-Data Compilations
- Plant-Specific Raw-Data Records
- Generically Classified Event Data and Estimated Parameters

Typical data sources within the above categories are briefly described in the following.

A.11.1. Generic raw-data compilations

- **Licensee Event Report (LER) System**

This source is a compilation of "safety significant" event reports submitted to the U.S. Nuclear Regulatory Commission (USNRC) by nuclear power plant licensees in accordance with the U.S. government regulations. Various summaries of the LERs are published by different organizations. For instance, summaries of all reported events sorted by plant name are published by Oak Ridge National Laboratory. In addition, the USNRC has published a compilation of one-line summaries of events involving several categories of components. These are:

- Diesel Generators /A-21/
- Pumps /A-22/
- Valves /A-23/
- Selected Instrumentation and Control Components /A-24/

- Primary Containment Penetrations /A-25/
- Control Rods and Drive Mechanisms /A-26/

These reports also provide statistical analyses of the data and give estimates of component failure rates, but an attempt is made to obtain estimates for the parameters of dependent failure models.

- **Nuclear Power Experience (NPE)**

This source is an LER-based compilation of event reports supplemented by information from other sources. It includes a large number of LERs and is updated monthly /A-27/. NPE is available on a subscription basis only.

Both sources, LER and NPE, provide information about abnormal occurrences, but are not particularly designed to be used as data bases for model-parameter estimation. Nevertheless, they are often the only sources of data available to the analyst. The event reports should be reviewed and classified to extract information about the parameters of interest. The degree of usefulness of the LER and NPE data sources for the purpose of estimating dependent-failure parameters depends on the type of model being used. For instance, either of the two sources forms a sufficient basis for estimating the parameters of the Multiple-Greek-Letter (MGL) (cf. Section 1.4.3) and Alpha-Factor Methods (cf. Section 1.4.5) , whereas additional information, such as system success data, is needed to estimate Binomial-Failure-Rate (BFR) (cf. Section 1.4.6) parameters. Furthermore, under the present LER reporting rules, single component failures, in general, are not recorded. Consistent recording of single and multiple failure events is required for most parameter estimates.

A.11.2. Plant-specific raw data records

For a plant-specific analysis, the most applicable sources of data are the plant records, such as operator log-books and maintenance request records. Review of the plant-specific records can provide a much more accurate account of failure as well as success data compared with generic raw data sources, but this depends on the quality of the plant record-keeping activity and on such a factor as how well the root causes of various events have been pinpointed. The statistical significance of plant-specific data, however, is a direct function of the number of years of operation of the plant, and, as mentioned before, for plants with even a few years of operating history, the plant-specific data alone will, in general, be insufficient for a common cause analysis.

Once the raw data (event reports) are collected, a review and classification of the events to identify where each event fits in a set of predifined categories is required which describes the type of the event, its cause(s), and its impact; e.g., number of components failed. For this purpose, a data classification approach, such as the one developed for EPRI /A-28/ is needed.

A.11.3. Data sources specifically developed for dependent failure analysis

Results of systematic efforts directly aimed at extracting qualitative as well as quantitative information about dependent failures can be found in the following reports:

- Pumps /A-29/
- Valves /A-30/
- Instrumentation and Control assemblies /A-31/
- Pumps, Valves, Diesel Generators, and Breakers /A-32/

The first three of the above reports provide the result of event classification and parameter estimation for the BFR (cf. Section 1.4.6) and Beta-Factor Models (cf. Section 1.4.2).

The EPRI-dependent events data classification study /A-32/ presents the results of applying EPRI's detailed and systematic approach /A-28/ for classifying events on a large number of NPE events for the purpose of identifying common-cause events.

A.12. OECD

A.12.1. Presentation

The OECD/NEA is an institution that focuses on co-ordinating the co-operation among the nuclear regulatory authorities of the Member Countries by offering agreed-upon services in the fields of operating experience, human factors, severe accidents, probabilistic risk assessment, and data processing, to name but a few. One tool that members agreed is indispensable in identifying weaknesses and in validating design assumptions is that of feedback of experience related to operation and human factors. It was on this basis that the NEA has established in 1980 an Incident Reporting System (IRS) with the broad objectives of:

> "... collection and dissemination of sufficiently detailed information on incidents of safety significance in nuclear power plants, as soon as practicable, and feedback of appropriate conclusions from such incidents."

The NEA-IRS thus conceived, satisfies the following basic steps, essential in the process of "learning from experience":

(a) accurate reporting (to the appropriate organizational units), classification and documentation of failures, malfunctions and other operational problems;

(b) analysis of the data thus accumulated to determine the most effective means of alleviating failures, mitigating failure consequences and preventing accidents through the identification of precursors;

(c) implementing recommendations which arise from the data analysis;

(d) exchanging information on various topics and issues, at national and international level.

A.12.2. System evolution and modus operandi

Within the framework of the NEA-IRS, the organization coordinates distinct activities such as reporting and report handling, software and data management and data utilization.

A.12.3. Reporting and report handling

An "IRS-Co-ordinator" is designated by the regulatory body of each of the thirteen participating countries. When an event occurs which is considered "reportable" according to certain criteria, the appropriate Co-ordinator forwards a report to the System Co-ordinator at the NEA Secretariat in Paris. This report contains, at a minimum, the following information in a standardized format:

(a) Plant name, unit number and licensee

(b) Date of occurrence

(c) Type of reactor and manufacturer

(d) Authorized electrical power output

(e) Date of first commercial operation

(f) Power level at the time of the event

(g) Event details, classified according to standard codes:

- Reporting category
- Plant status
- Systems affected
- Components affected
- Observed causes
- Root causes
- Effect on operation
- Consequences
- Type of failure

(h) Short and long term actions taken

(i) Lessons leamt and significance of the event

(j) Abstract of the event

Each IRS report received at the NEA Secretariat is subject to the following treatment:

(a) The classification codes, abstract and report contents are checked to ensure:

- consistency with others and with the general guidelines, and
- homogeneity in reporting quantity and quality.

(b) Copies of the report are disseminated to all the national NEA-IRS co-ordinators (who in tum distribute the information to appropriate organizations in their respective countries).

(c) The report is filed

(d) Follow-up reports, produced by the originating country, are also treated in a similar fashion

A.12.4. Software and data management

The rigorous quality control process currently in use ensures that, amongst other things, data is classified and stored consistently, and retrieval is adequate.

Incident-related data, notably the abstracts and all the classification codes (referred to later as Standard Codified Abstracts - SCA) are stored in a data base residing at the Oak Ridge Data Bank in the United States. This central data base performs the dual function of administrative controls (keeping track of corrections, follow-up reports, etc.) as well as the source of raw material for studies. Access to the information by authorized users can be effected via diskettes regularly updated or by posing the query to the Secretariat.

Program development and/or modifications are also carried out as required, as well as routine software maintenance.

A.12.5. Data utilization

Data stored in the NEA-IRS data base are used for:

- Single event assessment: this constitutes the first "basic element" of data use. As event reports are disseminated, recipients examine the information contained in the individual reports for applicability to any of the nuclear installations in their respective countries.
- Analysis of groups of events: the "second level" of data utilization is the identification of groups of events that represent similar failures or event sequences.
- Generic studies, questionnaires and task forces: Data stored in the NEA-IRS data base is scanned periodically by members, as well as by the Secretariat, to identify issues that may warrant conducting generic studies, holding specialist meetings, forming task forces, or any combination thereof.
- Precursors: Perhaps one of the most important goals of learning from experience is to have the ability to identify potentially serious failures or event sequences, such that preventive measures can be taken before such occurrences should materialize.
- Feedback to specialist fields: In addition to the applications in the human factor domain referred to above, IRS data will now be used for the feedback of operational experience to other specialized areas such as radiological protection, thermal-hydraulic transients and material properties.

A.12.6. Data availability

Unless otherwise specified by Member Countries, IRS reports and relevant activities such as CSNI reports, are classified as "restricted". Within the framework of the NEA publication policy, this classification means that the use and distribution of these documents is at the discretion of the designated recipient in each participating country. These recipients will only use and/or distribute the documents in their respective countries for official purposes.

References

Annex A

/A-1/ Jänkälä, K.E., J.K. Vaurio, U.M. Vuorio:
Plant Specific Reliability and Human Data Analysis for Safety Assessment
Int. Conf. on Nuclear Power Performance and Safety, Vienna, 28 Sept. - 2 Oct. 1987
IAEA-ČN-48/78 Nuclear Power Performance and Safety, Vol. 4: Safety Technology, pp. 135 - 151

/A-2/ Jänkälä, K.E. and J.K. Vaurio:
Empirical Bayes Data Analysis for Plant Specific Safety Assessment
Int. Topical Conf. on Probabilistic Safety Assessment and Risk Management
Zürich, Switzerland, Aug. 31 - Sept. 4, 1987
Verlag TÜV Rheinland, Köln 1987, Vol. 1, pp. 281 - 286

/A-3/ Vaurio, J.K. and G. Linden:
On Robust Methods for Failure Rate Estimation
Reliability Engineering 14 (1986) 123 - 132

/A-4/ Vaurio, J.K. and K. Jänkälä:
Comparison of Methods for Estimating Failure Probabilities
The 7th SRE-Symposium, Espoo, Finland, Oct. 14 - 16, 1986
Society of Reliability Engineers, Scandinavian Chapter

/A-5/ Vaurio, J.K.:
On Analytic Empirical Bayes Estimation of Failure Rates
Risk Analysis 7(1987) 329 - 338

/A-6/ Jänkälä, K.E. and J.K. Vaurio:
Component Aging and Reliability Trends in Loviisa Nuclear Power Plant
PSA'89 - Int. Topical Meeting: Probability , Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2 - 7, 1989, Vol. 2, pp. 919 - 928

/A-7/ Vaurio, J.K.:
Learning Curve Estimation Techniques for Nuclear Industry
Proc. Intl. Conf. Numerical Methods in Nuclear Engineering, CNS/ANS, 1983 Sept. 6 - 9, Montreal, Canada

/A-8/ Vaurio, J.K., J. Isaksson and U. Linden:
Studies with a New Risk Reduction Model,
in L.A. Cox Jr. and P.F. Ricci (Eds.) New Risks
Plenum Press, 1990

/A-9/ Vaurio, J.K.:
Learning from Nuclear Accident Experience
Risk Analysis, 4, 2 (1984) 103 - 115

/A-10/ Etude Probabiliste de Sûreté d'une tranche du Centre de Production Nucléaire de Paluel (1300 MWe),
Rapport de Synthèse, ESP 1300, Mai 1990

/4-11/ Der Bundesminister für Forschung und Technologie (Hrsg.),
Deutsche Risikostudie Kernkraftwerke - Phase B, Köln 1990
(English Summary: German Risk Study Nuclear Power Plants, Phase B, GRS-74, Köln 1990)

/A-12/ Harima, M. and M. Hada:
The Domestic Incident Reporting System Management and Consideration on Implementation of the Lessons Learnt, Proceedings of the Seminar on the Use of Unusual Event Reports for Improving Nuclear Power Plant Safety, Vienna, Austria, 14-18 May 1990, IAEA-SR-169/33.

/A-13/ Mosleh, A. et al.:
Procedures for Treating Common Cause Failures in Safety and Reliability Studies
NUREG/CR 4780; EPRI NP-5613; Vol. 1 (January 1988)
Vol. 2 (January 1989)

/A-14/ Ishack, G.:
The Incident Reporting System of the OECD Nuclear Energy Agency (July 1988)
(Notes for the International Course on the Safety of PWR Power Plants)

/A-15/ Fleming, K.N. and A. Mosleh:
Classification and Analysis of Reactor Operating Experience Involving Dependent Events
EPRI NP-3967, June 1985

/A-16/ Analysis of Core Damage Frequency: Internal Events: Methodology,
NUREG/CR-4550, Vol. 1 January 1990 Rev. 1, US-NRC

/A-17/ Defences Against Common-Mode Failures in Redundancy Systems
SRD 19, January 1981

/A-18/ SRD Dependent Failures Procedures Guide
SRD 418 March 1987

/A-19/ Johnston, B.D. and C. Cracket:
Common Cause Failure Reliability Benchmark Exercise
SRD R383 and GD/PE-N/I329 (CEGB) August 1985.

/A-20/ Poucet, A., A. Amendola and P.C. Cacciabue:
Summary of the Common Cause Failure Reliability Benchmark Exercise
Joint Research Centre Report
PER 1133/86, Ispra, Italy, April 1986

/A-21/ Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants
January 1, 1976 to December 31, 1978
NUREG/CR-1362, EGG-EA-5092, March 1980

/A-22/ Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants
January 1, 1972 to April 30, 1978
NUREG/CR-1205, EGG-EA-5044, January 1982

/A-23/ Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants
January 1, 1976 to December 31, 1987
NUREG/CR-1363, EGG-EA-5125, October 1982

/A-24/ Miller, C.F., W.H. Hubble, M. Trojovsky, and S.R. Brown:
Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U.S. Commercial Nuclear Power Plants
NUREG/CR-1363, EGG-EA-5816, Rev. 1, October 1982

/A-25/ Sams, D.W., and M. Trojosky:
Data Summaries of Licensee Event Reports of Primary Containment Penetrations at U.S. Commercial Nuclear Power Plants
January 1, 1972 to December 31, 1978
NUREG/CR-1730, EGG-EA-5/88

/A-26/ Hubble, W.H. and C.F. Miller:
Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U.S. Commercial Nuclear Power Plants,
January 1, 1972 to April 30, 1978
NUREG/CR-1331, EGG-EA-5079

/A-27/ Stoller, S.M.:
Nuclear Power Experience, updated monthly

/A-28/ A Study of Common Cause Failures - Phase II:
A Comprehensive Classification System for Component Fault Analysis
EPRI NP-3837, May 1985

/A-29/ Atwood, C.L.:
Common Cause Fault Rates for Pumps
NUREG/CR-2098, EPRI-685-DOC-01, EGG-EA-5289

/A-30/ Atwood, C.L and J.A. Steverson:
Common Cause Fault Rates for Valves
Estimate Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants
NUREG/CR-2770, EGG-EA-5485, February 1983

/A-31/ Meachum, T.R. and C.L. Atwood:
Common Cause Fault Rates for Instrumentation and Control Assemblies
NUREG/CR-3289, EPRI-685-DOC-6, EGG-2258, May 1973

/A-32/ Fleming, K.N. and A. Mosleh:
Classification and Analysis of Reactor Operating Experience Involving Dependent Events,
Electric Power Research Institute, EPRI NP-3967, February 1985

2. HUMAN ERRORS

2.1 INTRODUCTION

The influence of human factors on the reliability and safety of Nuclear Power Plants (NPPs) in particular and of complex industrial systems in general is widely recognized. Due to the severe accidents which have occured some years ago in several industrial and transportation sectors like TMI, Chernobyl, the Bhopal chemical plant, the Challenger shuttle or the Zeebrügge-Dover ferry-boat, the public and also the scientific communities believe that human errors play a significant part in risk and they regard human factors important. Thus severe accidents are viewed to result from simultaneous or sequential occurance of a number of equipment failures and human errors.

After TMI and Chernobyl a lot of studies and research work were focused on the improvement of the man-machine interface to mitigate operator errors. Besides great efforts have been made to improve the understanding of the behaviour of operators during severe accidents. Particular attention was paid to understand knowledge based operator actions, such as problem solving or decision making. Special exertion is made to develop models for qualitative and quantitative description of these operator actions /Pe81/, /Wo81, Wo82/.

Due to the lack of validity of human error probability data, also called "hard data", a lot of research projects concentrate on gaining hard data. Hence the evaluation of Licencee Event Reports (LERs) as well as full-scale simulator experiments are investigated to determine Human Error Probabilities (HEPs).

2.2 INFLUENCE OF HUMAN ERRORS ON THE SAFETY OF NUCLEAR POWER PLANTS (NPPS)

Several possible human error types could influence the safety of an NPP. It is convenient to divide these errors in two categories:

- human errors during the design and construction of NPPs
- human errors during the operation of NPPs

I. Human errors during the design and construction of NPPs

An NPP is a very complex system and a lot of physicists and engineers work together to design and construct such a giant factory. Accordingly several human errors can happen during such a project. These errors can be more or less dominant to plant safety but usually they play a minor part in Human Reliability Analysis (HRA).

II. Human errors during the operation of NPPs

During the operation of NPPs a lot of human errors may occur. Most of these human errors are not very important and so the plant state will not be changed and the NPP safety will not be jeopardized. For HRA it is decisive to determine those human errors that are dominant to NPP risk or could influence the safety. These human errors can be categorised as

- errors before initiating event e.g. errors made during surveillance test and maintenance of stand-by components and calibration action (latent failure)
- operator errors that initiate unwanted events (transients)
- operator errors as an incorrect accident control action.

Errors before initiating event (latent operators errors)

Operator actions made during surveillance, test or maintenance of stand-by components should improve the availability of the system. The benefits of testing and maintenance are modelled by the selection of repair times and by test intervals. Usually these actions are done in time constrain so that failures sometimes happen. Thus it is obvious that this kind of human mistakes have to be taken into consideration in HRAs.

Operator errors that initiate unwanted events.

An example of an initiating event caused by human actions is a plant trip following a mistake in testing procedures. External human actions such as sabotage are usually not considered.

Operator errors during accident.

This operator behaviour consists of actions that do not mitigate or even aggravate the accident situation. To identify this type of error a cooperation between human reliability and system analyst is very important. These can be actions where

1) the operator's image of the plant differs from the actual state and thus the operator performs the wrong actions for the event (incorrect diagnosis), or
2) the operator diagnose the event correctly but fails to perform the correct action or chooses a non optimal or a wrong strategy (delayed actions)

Another possibility to classify operator action is the distinction between planned and unplanned actions. Planned operator actions are trained. Operators follow explicit procedures or stored rules. These actions are usually automated or will be executed in familiar situations. Unplanned operator actions usually happen in unfamiliar circumstances. Either operators have no proper procedures for correct reactions or they intentionally ignore procedures because of an internal conflict between competitive benefits such as loss of money versus safety aspects.

2.3 INFLUENCING FACTORS ON HUMAN RELIABILITY

There are many factors that influence the human behaviour during human performances in a complex man-machine system like a Nuclear Power Plant. In modelling operator performances for HRA, it is necessary to consider those factors that have most effect on the performance. These factors are called Performance Shaping Factors (PSFs). Examples are ergonomic design, written procedures or instructions, signals or annunciators, stress, personnel redundancy and dependence.

PSF Stress

One of the most influential and most important PSFs is the stress. Stress can be defined as an operator response to a stressor. There are psychological and physiological stressors. The distinction is often arbitrary. Psychological stressors include e.g. task speed, monotonous work, threats from supervisors or emergency situations. Physiological stressors include e.g. fatigue, constriction of movement or heat effects (high temperature) and so on.

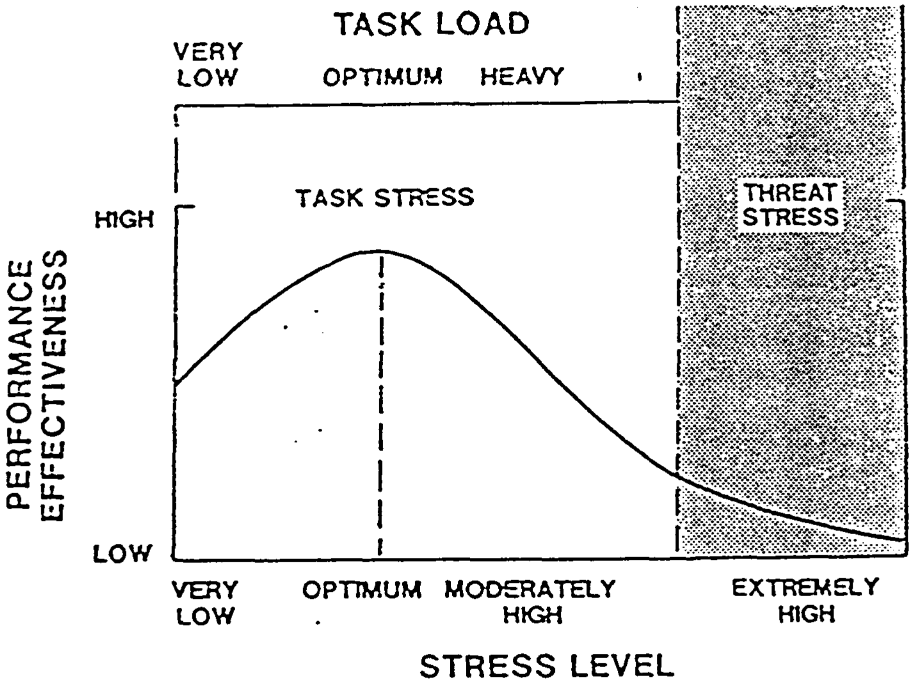


Fig. 2.3.1: Hypothetical relationship between performance and stress with task stress and threat stress division /Sw83/

The classical stress curve (Fig. 2.3.1) indicates that performance follows a curvilinear relationship with stress, from very low to extremely high.

The characteristic of a very low stress level is that there is not enough stimulation to keep the operator alert. His state of arousal is below normal. He has vigilance problems (e.g. night-lookouts on ships, boring task jobs where usually nothing happens). A person's effectiveness declines very rapidly under such conditions.

The optimum stress level is characterized by an active interaction between the operator and his environment.

Moderately high stress level situations arise for persons, when they have to perform tasks which are close to their possible capacity or exceed it. They have to operate under a heavy tasks load.

Extremely high stress level includes an emotional component: the feeling of threat. This situation occurs after a misdiagnosis i.e. that the system does not respond by the way the operator had to expect, considering the actions he has taken. Accordingly the operator feels that he has lost control of the system.

PSF Dependence

A major problem is the estimation on how the probability of error or success on one task may be related to error or success on some other tasks. If tasks are not independent, that means if the second task is influenced in any way by the former task, the dependence must be considered to determine a realistic human error probability.

Dependences can occur between and within people. Dependences between people are fairly common, for example, one operator restores a valve and a other operator checks the accuracy of the restoration. Dependence can also occur between different tasks performed by the same operator, for example when one person restores two adjacent valves or switches.

The degree of dependence among operator actions ranges along a continuum from negative dependence through independence (zero dependence) to positive dependence. Negative dependence implies a negative relationship between tasks, e.g. error on the first task reduces the probability of error on the second task or success on the first task increases the probability of error on the second task.

Positive dependence implies a positive relationship between tasks i.e. success on the first task increases the probability of success on the second task and error on the first task increases the probability of error on the second task.

PSF Personnel Redundancy

If an operator performs a task and makes a mistake a second operator who checks the task would detect the error and correct it. This is an important factor and it should be considered in HRA's. But the use of the recovery factor 'operator redundancy' contains difficulties in assessing and quantifying it correctly. It is decisive to determine the dependence between the operator and the controller. This has a great influence on the error probability e.g. if the controller believes that the operator's work is reliable he tends to assume that the operator's performance will be correct. This assumption or expectancy reduces the controller's effectiveness. He may miss an operator's error because he does not expect it. If on the other hand the operator who is being checked is relatively inexperienced, the controller may take extra care because he has doubts about the reliability of the operator. This would result in a lower error probability for the controllers.

- Training

Generally the PSF training will not be explicitly considered in HRA. However-it is very important that NPP personnel take part in authentic full scale simulator training course. Usually the training of operators includes a training simulator practice on how to respond to transients, LOCAs and other abnormal events. This training is very valuable, but such initial practice is not sufficient to maintain the operator's skills in coping with unusual events.

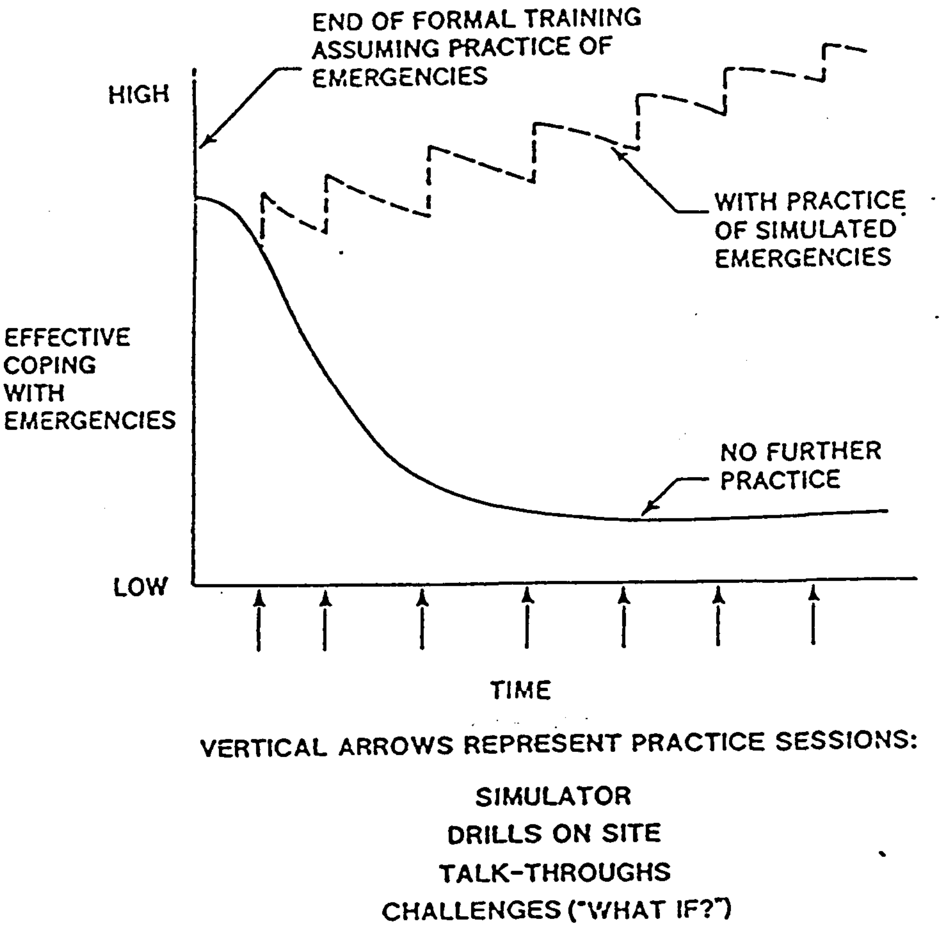


Fig. 2.3.2: Effects of more or less practice on maintenance of emergency skills /Sw83/

An operator needs to have sufficient continuing practice in safety-related tasks for adequate implementation of skills of these tasks. A curve in Fig. 2.3.2 reflects the ability of operator to cope with emergencies (1) in the absence of practice after the initial operator training (the solid line) compared with (2) periodic practice (the dotted line) /Sw83/.

- Quality of Emergency Operating Procedures (EOPs)

Emergency Operating Procedures deal with the recognition and mitigation of abnormal operating conditions during an accident. They can be event-oriented or symptom-oriented. The quality of EOPs have significant effect on the probability of correct performance. Thus EOPs should be assessed in a HRA.

- Quality of control room design

The PSF quality of control room design is very important and has a dominant influence to operator error probability. Several methods consider this factor explicitely because of its importance. In new NPP control rooms there are computer programs or expert systems which promote operators during an accident. These programs can be very helpful if they are absolutely correct. If not, they can confuse NPP personnel and aggravate the emergency situation. The reliable testing of software is still an unresolved issue.

2.4 GENERAL DESCRIPTION OF OPERATOR RELIABILITY

The first systematic studies for human reliability attempted to develop a database of HEPs derived from experimental studies in the context of nuclear weapons development /Me64/, /Sw64/. These and other early reliability methodologies were dominated by the mechanistic view of human performance known as Behaviourism. Behaviourism concentrates exclusively on the observable aspects of human performance in terms of the stimuli received by an individual and responses that he reacts on the basis of these stimuli. Behaviourism compares the human to a black box. It is not important, what happens inside the black box, behaviourism observes only the external factors. These factors, called Performance Shaping Factors (PSFs), could influence the success or failure probability of human actions. The Behaviourist view of the human fits well with the models applied in most systems reliability assessments. Usually such analyses have concentrated on the probability that the operator will perform a required function in an abnormal situation. This probability is then put into fault or event trees in the same way as a hardware component failure probability.

Because the Behaviourism approach allows only to evaluate <u>what kind</u> of human errors occur but not <u>why</u> they occur other methodologies were required. Jens Rasmussen developed a cognitive psychology model, based on the psychological theory /Ra83/. Cognitive psychology replaced the idea of the human as a passive component responding to stimuli with a much more dynamic model of the individual as a goal directed processor of information /Ra85/.

Rasmussen distinguished human behaviour in three classes, skill-based, rule-based and knowledge-based behaviour (Fig. 2.4.1). These are three levels of cognitive control which basically depend on the degree of familiarity of the environment and the nature of the information used for each level.

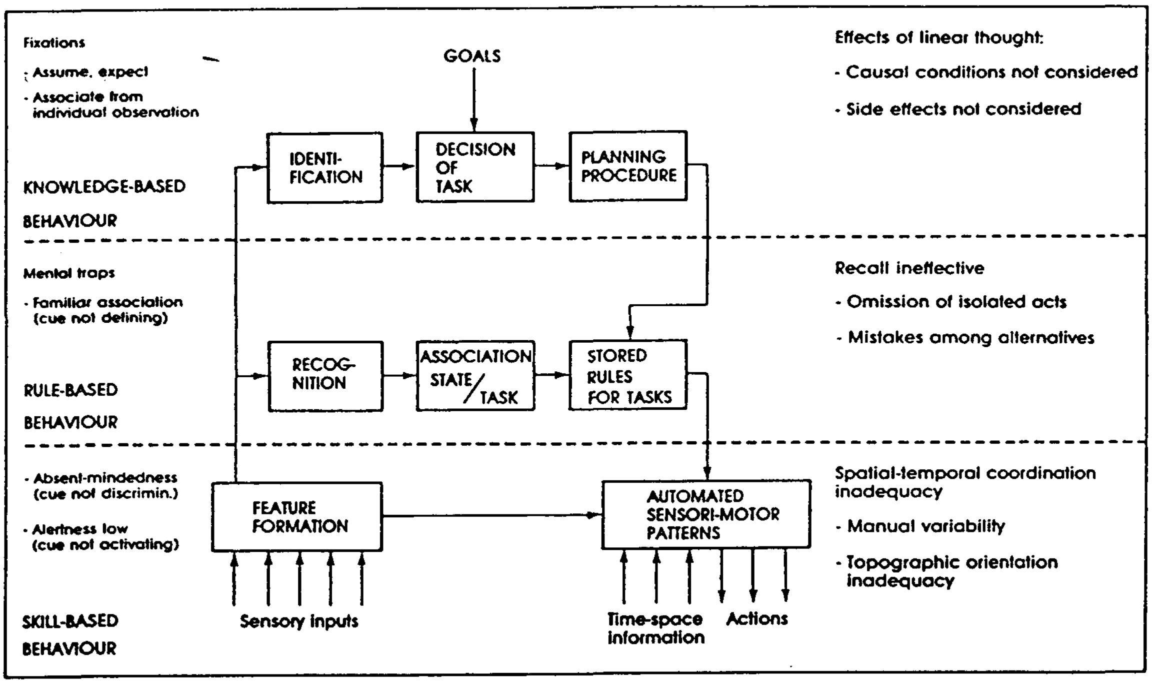

Fixations
- Assume, expect
- Associate from individual observation
GOALS
Effects of linear thought:
- Causal conditions not considered
- Side effects not considered
IDENTI-FICATION
DECISION OF TASK
PLANNING PROCEDURE
KNOWLEDGE-BASED BEHAVIOUR
Mental traps
- Familiar association (cue not defining)
Recall ineffective
- Omission of isolated acts
- Mistakes among alternatives
RECOG-NITION
ASSOCIATION STATE/TASK
STORED RULES FOR TASKS
RULE-BASED BEHAVIOUR
- Absent-mindedness (cue not discrimin.)
- Alertness low (cue not activating)
FEATURE FORMATION
AUTOMATED SENSORI-MOTOR PATTERNS
Spatial-temporal coordination inadequacy
- Manual variability
- Topographic orientation inadequacy
SKILL-BASED BEHAVIOUR
Sensory inputs
Time-space information
Actions

Fig. 2.4.1: Schematic illustration of different cognitive levels of internal control of human behaviour /Ra83/

Skill-based behaviour

The skill-based behaviour represents sensor-motorical performance during activities which take place without conscious control. These are smooth, automated and highly integrated patterns of behaviour. The experienced operator will recognize the pattern of symptoms or alarms as a familiar pattern for which a simple preprogrammed action is available and he will directly execute the action.

Rule-based behaviour

Rule-based behaviour typically occurs in a familiar situation and involves stored rules or procedures. The operator does not recognize a pattern of indications and this will normally initiate a process of scanning and information collection. This leads usually to the selection of an approriate procedure (either formalized as an explicit plant procedure or from the operator's memory), which will be executed to achieve the desired result.

Knowledge-based behaviour

Knowledge-based behaviour happens in unfamiliar circumstances. There are no rules or specific procedures, that the operator can use. He has to solve problems, to make decisions and formulate new hypotheses based on engineering principles.

2.5 HUMAN RELIABILITY ANALYSIS (HRA) METHODS

This part provides a review and evaluation of the major technique that are currently published for qualifying (SHARP) and quantifying operator errors. These techniques can be classified in four groups.

I. Systematic Human Action Reliability Procedure (SHARP)

II. Time Dependent Methods

- methods based primarily on the PSF time
  - Operator Action Tree (OAT) Model
  - Human Cognitive Reliability (HCR) Model

III. Expert Estimation Methods

- operator mistakes are quantified with structured expert judgement
  - Direct Numerical Estimation (DNE)
  - Paired Comparison (PC)
  - Socio Technical Assessment of Human Reliability Method (STAHR)
  - Success Likelihood Index Method (SLIM)
  - Confusion Matrix (CM)

IV. Simulator and Decomposition Methods

- methods simulate operator actions or decompose operator actions
  - Maintenance Personnel Performance Simulation Model (MAPPS)
  - Technic Empirica Stima Errori Operatori (TESEO)
  - Technique of Human Error Rate Prediction (THERP)
  - Accident Sequence Evaluation Programm (ASEP)

- Human Error Assessment and Reduction Technique (HEART)

There still exists other HRA methods like AIPA (/F175/), MSFM (/Sa81/), SAINT (/Wo78/, Me82/), PSALOT/IVO (Va87), VISHN (/Po88/).

Because these methods were seldom used in PRA they were not considered in this report. Nevertheless the relevant documents about model description and application were cited if somebody is interested in getting information about these methods.

2.5.1 Systematic Human Action Reliability Procedure

The Systematic Human Action Reliability Procedure (SHARP), developed by Hannaman and Spurgin / Ha84 /,is not a method for quantifying human failures. It is a framework for systematically incorporating man-machine interactions into PRAs. The object of the framework is to help in defining types of interactions that are important to risk analysis and to enable the analyst to incorporate them into the system analysis task. Furthermore it is easier to review an analysis. SHARP is divided into seven steps (Fig. 2.5.1)

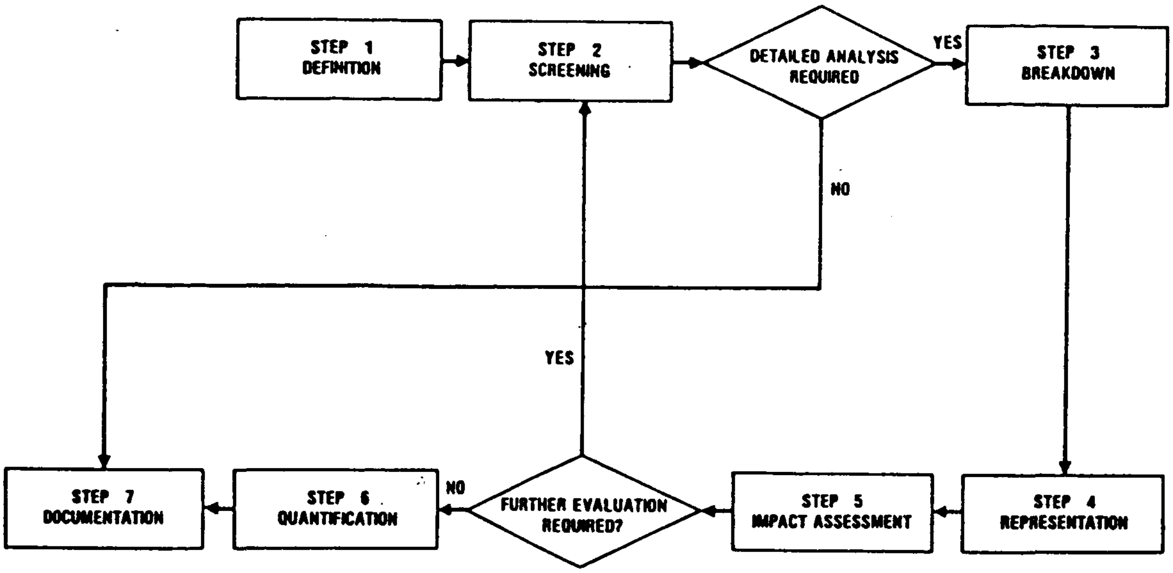


Fig. 2.5.1: Steps in the SHARP framework /Ha87/

1. Definition

The basic logic trees developed by the systems analysts from the functional description of the plant are enhanced in order to fully describe human interactions, i.e. to ensure that all different types of human interactions are adequately considered in the study.

2. Screening

The logic trees, enriched with human interactions, are screened to select only the most important human interaction for further analysis.

3. Breakdown

Each key interaction is subdivided into tasks and subtasks, in order to define influence factors (PSFs) necessary for a complete modelling.

4. Representation

These interactions are explicitly modelled to include the possible options that the operator may choose. In this way, it is possible to identify additional significant human actions that have an impact on the system logic trees.

5. Impact Assessment

The system logic trees are modelled in order to explore the impact of significant human actions identified on the preceding step.

6. Quantification

The human actions are quantified for incorporating them into the PRA, including the evaluation of uncertainties associated with data.

7. Documentation

The results are documented in order to include all the necessary information for assessment to be further used and applied.

2.5.2 TIME DEPENDENT METHODS

2.5.2.1 Operator Action Tree Model

The Operator Action Tree method (OAT) /Wr82/ is for basic representation of the sequence of actions needed to accomplish a function or task. In its representation OAT focuses on diagnosis and decision making actions of the NPP crew (knowledge-based behaviour). Other operator actions (skill- or rule-based actions) are not so dominant. If the operators have made the correct decisions, there are often many ways of overcoming these response errors.

The OAT method is based on the premise that human behaviour in response to an event can be described in three phases of activity:

1. observing the event
2. thinking about it
3. responding to it

The basic operator action tree (Fig. 2.5.2) is based on the potential for error in each of the three activities. The OAT method assumes that errors occurring during the third phase, carrying out the necessary operator action (skill- and rule-based behaviour) are not of the dominant concern.

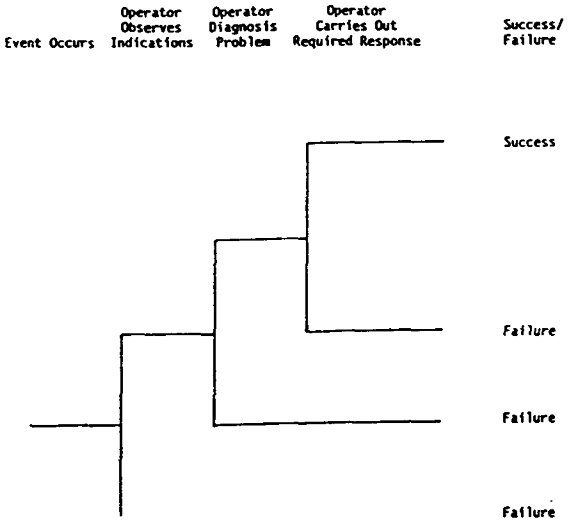

Event Occurs
Operator Observes Indications
Operator Diagnosis Problem
Operator Carries Out Required Response
Success/ Failure
Success
Failure
Failure
Failure

Fig. 2.5.2: Example of a Basic Operator Action Tree /Wr82/

The OAT developers propose a time reliability curve, which is based only on expert judgement (Fig. 2.5.3). The dominant PSF is the remain time t, for diagnosing the accident.

The time available to operators to make a diagnosis is referred to as the thinking interval. The thinking interval T_t is defined as:

$$T_t = T_o - T_i - T_a$$

where T_o is the overall time from the initiation of an accident sequence to the point by which actions have to be completed, T_i is the time after initiation at which appropriate indications or other cues are given, and T_a is the time taken to implement the actions decided on.

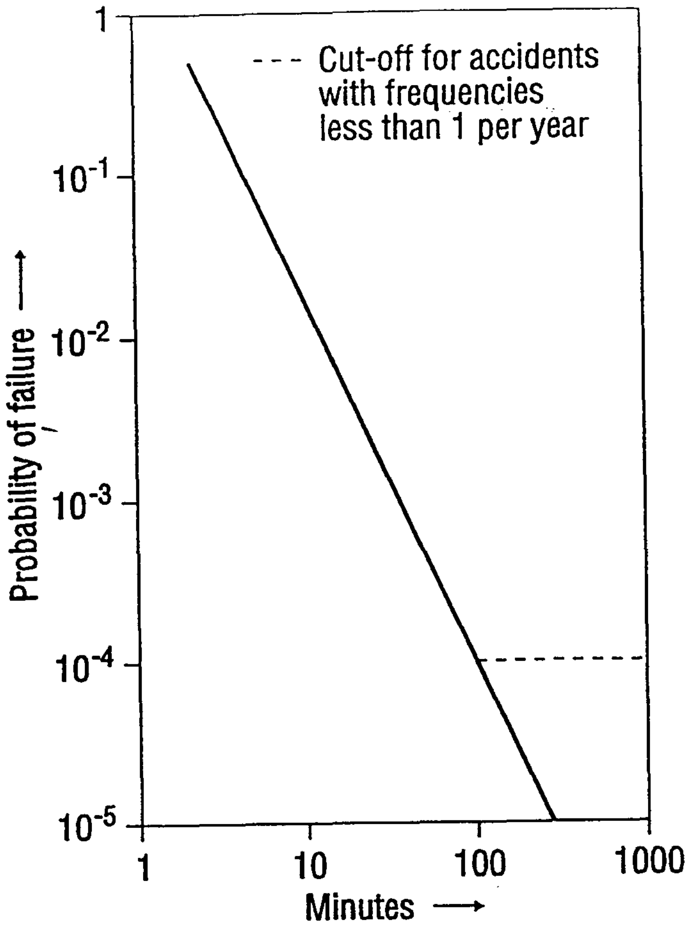


Fig. 2.5.3: Time Reliability Correlation /Wr82/

2.5.2.2 The Human Cognitive Reliability Model

The Human Cognitive Reliability model (HCR) /Ha84a/, /Ha84b/, /Ha87/ was developed by the NUS Corporation on a research project sponsored by the Electric Power Research Institute (EPRI). The HCR technique represents a time reliability correlation approach based on data obtained from a nuclear power plant simulator (La Salle BWR simulator). Other time reliability models like OAT are based only on expert judgement. Because of that, a proposal was made in NUREG/CR 0400 to develop a time reliability model based on 'hard data'.

The technique applies to the quantification of operating nuclear power plant crews actions during an accident and to the assessment of non-response probability, using one of a set of three time-reliability correlations. The three curves are based on J. Rasmussen's cognitive behaviour model, /Ra83/. Rasmussen divided the behaviour of the operator in three cognitive processes:

1. skill-based behaviour
2. rule-based behaviour
3. knowledge-based behaviour

To determine the kind of operator behaviour, Hannaman presents a logic tree (Fig. 2.5.4). These correlations relate to the probability of non-response of a normalized time for the task. The normalized time consists of the relationship between the time window t and the median response time of the crew $T_{1/2}$ to perform the required tasks. The NPP crew must determine and implement the correct response to the transient within time, before a significant irreversible change in plant state occurs. The median time $T_{1/2,nom}$ has to be obtained from simulator measurements, task analyses or expert judgement. The median response time of the crew can be modified with several PSFs (experience level of the crew=K_1, stress level = K_2, control room design = K_3 Fig. 2.5.5, Fig. 2.5.6).

$$T_{1/2} = T_{1/2}, \text{nom} \cdot (1+K_1)\cdot(1+K_2)\cdot(1+K_3)$$

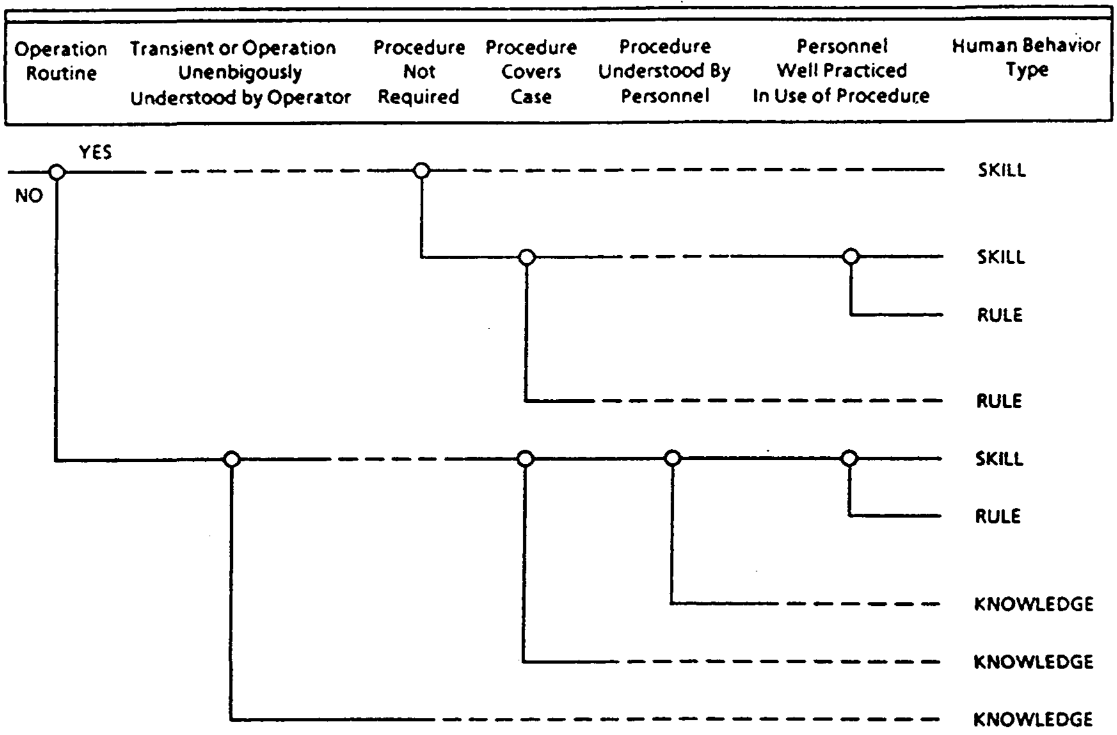
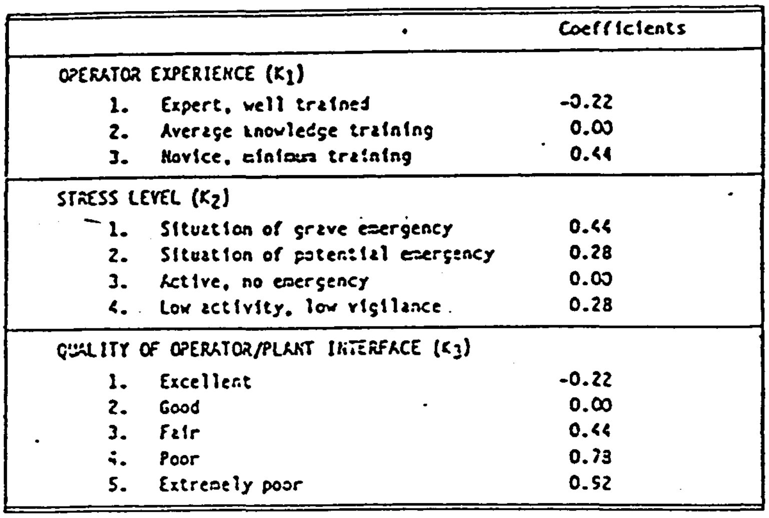
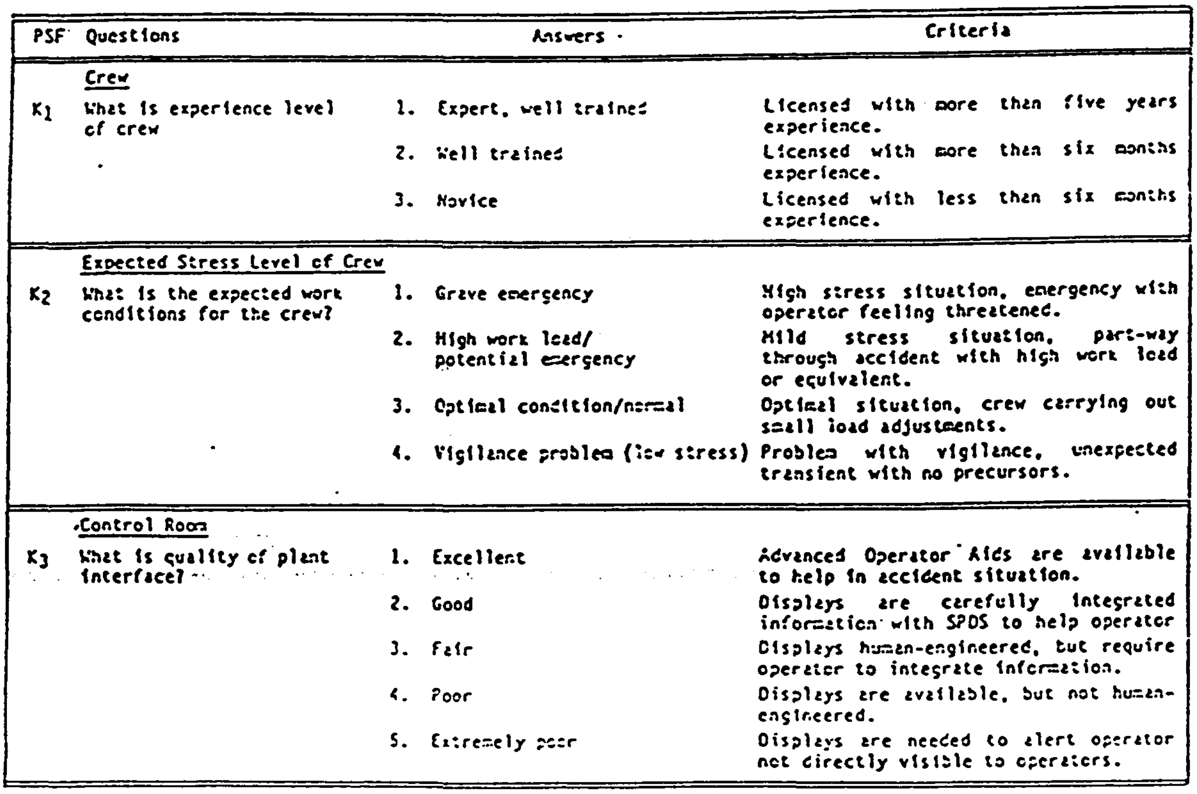


Fig. 2.5.4: Logic Tree to Aid in Selection of Expected Operator Behaviour Type /Ha84/



	Coefficients
OPERATOR EXPERIENCE (K_1)	
1. Expert, well trained	-0.22
2. Average knowledge training	0.00
3. Novice, minimum training	0.44
STRESS LEVEL (K_2)	
1. Situation of grave emergency	0.44
2. Situation of potential emergency	0.28
3. Active, no emergency	0.00
4. Low activity, low vigilance	0.28
QUALITY OF OPERATOR/PLANT INTERFACE (K_3)	
1. Excellent	-0.22
2. Good	0.00
3. Fair	0.44
4. Poor	0.78
5. Extremely poor	0.92

Fig. 2.5.5: HCR PSFs and related coefficients /Ha85/



PSF	Questions	Answers	Criteria
	Crew		
K_1	What is experience level of crew	1. Expert, well trained	Licensed with more than five years experience.
		2. Well trained	Licensed with more than six months experience.
		3. Novice	Licensed with less than six months experience.
	Expected Stress Level of Crew		
K_2	What is the expected work conditions for the crew?	1. Grave emergency	High stress situation, emergency with operator feeling threatened.
		2. High work load/ potential emergency	Mild stress situation, part-way through accident with high work load or equivalent.
		3. Optimal condition/normal	Optimal situation, crew carrying out small load adjustments.
		4. Vigilance problem (low stress)	Problem with vigilance, unexpected transient with no precursors.
	Control Room		
K_3	What is quality of plant interface?	1. Excellent	Advanced Operator Aids are available to help in accident situation.
		2. Good	Displays are carefully integrated information with SPDS to help operator
		3. Fair	Displays human-engineered, but require operator to integrate information.
		4. Poor	Displays are available, but not human-engineered.
		5. Extremely poor	Displays are needed to alert operator not directly visible to operators.

Fig. 2.5.6: Questions and Criteria for determining PSFs /Ha85/

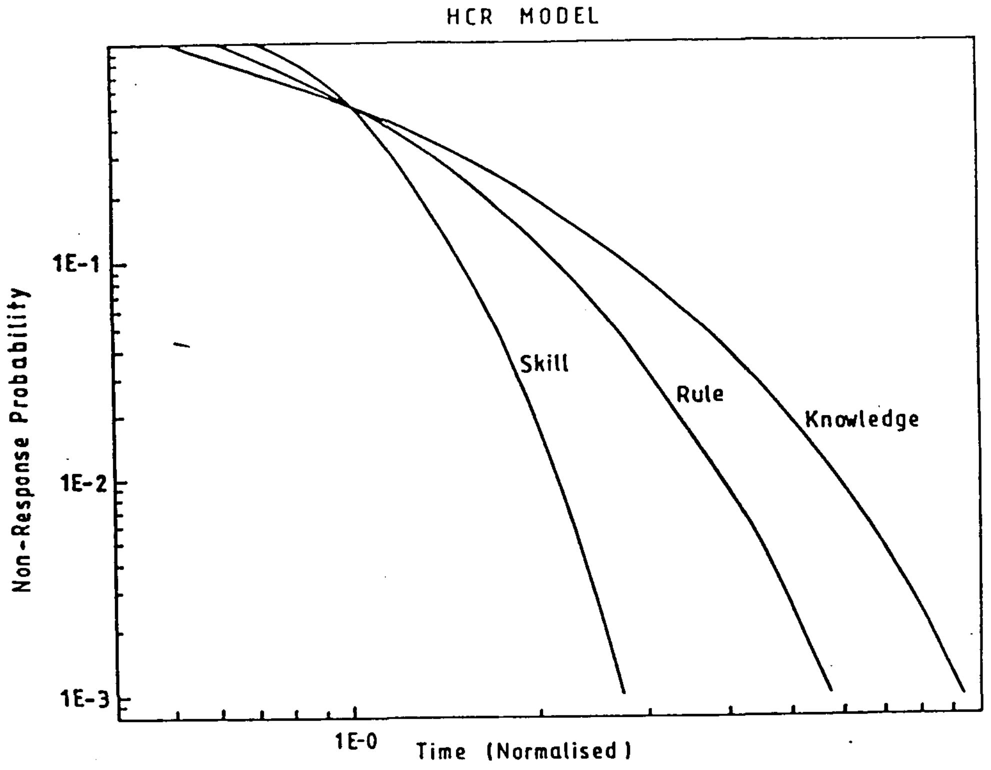


Fig. 2.5.7: Normalized crew non-response curves for Skill, Rule-, and Knowledge-based behaviour /Ha85/

2.5.3.1 Direct Numerical Estimation

The Direct Numerical Estimation (DNE) developed by Seaver and Stillwell is /Se82/ based on the suggestion that experts estimate HEPs on the basis of their knowledge and experience. The reason for using expert judgement in human reliability assessment is that there exists little if any relevant human error probability data, whereas there exist experts who have much experience and appropriate knowledge that can be translated into quantitative estimates of probability of occurrence of an event.

There are two forms of DNE, group and single expert method. Most analyses have used the group method, if enough experts are available, because it is seldom the case that a single expert has sufficient relevant information and expertise to accurately estimate human reliability. Four well-known group methods for direct numerical estimation are:

- Aggregated individual method

  Experts do not meet, but make estimates individually. Estimates are combined statistically by taking the geometric mean of the individual estimates.

- Delphi method

  Experts make individual assessment but they can review and reassess their individual estimates on the basis of the other experts estimates, which are shown to everyone. The revised data are then statistically combined as above.

- Nominal Group Technique

  This technique is similar to the Delphi method, except that some limited discussion is allowed between experts for clarification purposes only.

- Consensus Group Technique

  Each member contributes to the discussion, but the group must reach an estimate which all members of the group agree upon.

2.5.3.2 The Paired Comparisons Technique

The Paired Comparisons technique (PC) /Bl66/, /Se83/ is a structured expert judgement method for quantifying human error probabilities. This technique does not require experts to make direct quantitative assessments like the direct numerical estimate method. Rather the experts are asked to compare a set of pairs of tasks for which human error probabilities are demanded, and for each pair the expert must decide which has the highest likelihood of error.

PC is a scaling technique based on the idea, that it is easier for experts to make simple comparative judgements than absolute judgements. In other words, it is easier to say, based on expert judgement, that for example "a car crash is more likely than a plane crash" as a car crash will occur every x minutes and a plane crash will occur every y days".

The technique elicits these comparative judgements from a number of experts and develops a scaling of the tasks in terms of their relative likelihoods of error. At least two tasks with known HEPs are necessary to calibrate this scaling, based on a logarithmic transformation to derive the overall HEPs.

2.5.3.3 The Socio-Technical Assessment of Human Reliability Method

The Socio-Technical Assessment of Human Reliability (STAHR) method /Ph85/ consists of a technical and a social component. The technical component takes the form of an Influence Diagram (Fig. 2.5.8), a graphical representation of the effects of various performance shaping factors on the probability of success in a situation. The influence diagram demonstrates the network of causes and effects that link the factors to the outcome of the situation. It is a logic model of a situation's underlying influences.

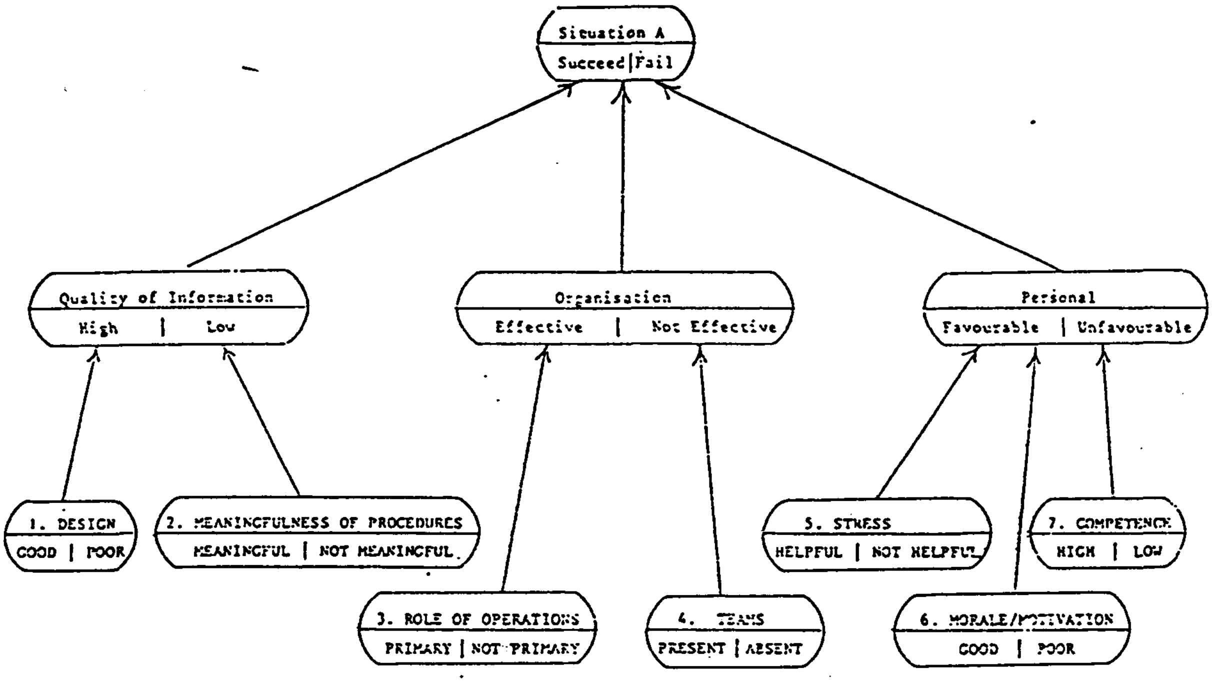


Fig. 2.5.8: The STAHR Influence Diagram /Ph89/

The social component of STAHR consists of the elicitation by group consensus of expert judgements of the conditional probabilities of various factors shown in the influence diagram as well as of their respective weights of evidence.

The STAHR approach does not offer probability data, but it does provide a method for obtaining and combining probability estimates. The major steps of the STAHR procedure are to describe the relevant conditions, define the target event, assess the weights of evidence, assess the interactions and the conditional probabilities, then calculate the target-event probability, compare the results of the analysis to holistic judgements, and perform and report on a sensitivity analysis.

2.5.3.4 The Success Likelihood Index Method

The initial development of the Success Likelihood Index Method (SLIM) for quantifying human failures was carried out by D.E. Embrey at al. /Em84a/ /Em84b/. SLIM utilizes decision analysis techniques and its basic premise is that human error probabilities depend on the combined effects of Performance Shaping Factors (PSFs) such as stress, training, quality of procedures, available time to perform a task etc. A systematic approach is used to identify these PSFs for a specific set of tasks. The tasks are then evaluated on the PSFs, and the relative importance (weights) of the PSFs are derived by structured expert judgements. From these evaluations, a Success Likelihood Index (SLI) is derived for each task.

For calibrating these SLIs at least two reference tasks with known error probabilities and known SLIs are necessary in order to transform the derived SLIs to HEPs.

Beside the SLIM method Embrey et al. developed a software program called SLIM-MAUD (Multi- Attribute Utility Decomposition) and SLIM-SARAH (Systematic Approach to the Reliability Assessment of Human) for a support use of the technique.

2.5.3.5 The Confusion Matrix

The confusion matrix technique is used to estimate the probability of initiating-event misdiagnosis. Actions taken during an event sequence to supplement automatic system response are of major concern. Actions that fall outside the response envelope, such as errors made in test and maintenance activities, are included in the systems analysis, but are not modeled explicitly in a confusion matrix.

This technique distinguishes between the initiating events that are similar in appearance to the operators. To construct a confusion matrix, these events are listed on the vertical and horizontal axes of the matrix. Expert opinion is used to rank each initiator in the order in which they would most likely be confused with actual events by considering the similarity of symptoms and how frequently they occur. Once the ranking is completed, probabilities are assigned for each misdiagnosis. The probabilities are then modified to reflect the quality of the control room design and of operator training.

2.5.4 SIMULATOR AND DECOMPOSITION METHODS

2.5.4.1 Maintenance Personnel Performance Simulation model

The Maintenance Performance Simulation (MAPPS) model is a computer simulation model developed by Siegel et al. /Si84a/ /Si84b/. MAPPS provides a tool for identifying required insights relative to Nuclear Power Plants maintenance. A principal focus of the model is to produce maintenance-oriented human performance reliability data for PRA purposes.

This software program incorporates recovery factors such as the effect of rest and checks enforced by quality-control policies. It includes several performance shaping factors that can influence the personnel performance reliability such as environmental (noise, temperature, radiation level etc.), motivational and organisational factors, in other words a lot of physical and psychological variables. The analyst can vary systematically in any combination a variety of conditions.

2.5.4.2 The TESEO Method

The TESEO method (Tecnic Empirica Stima Errori Operatori) was developed by Bello and Colombari /Be80/ at the ENI Research Group, Italy. It was intended to be applied primarily to the analysis of human reliability in process industries. The model predicts human reliabilty as a function of five performance shaping factors which are assumed to be the major influence of operator performance in any situations being considered.

The TESEO model describes a operator's error probability called HEP as a multiplicative function of five factors:

1. type of activity to be carried out (K_1)
   (from simple routine to not routine)

2. time available to carry out this activity (K_2)
   (also called the temporary stress factor)

3. human operator's characteristics (K_3)
   (from expert to poorly trained)

4. operator's emotional state (K_4)
   (from grave emergency to normal situation)

5. environmental ergonomics characteristics (K_5)
   (ergonomic design of the plant)

The value of these five factors can be extracted from special tables or functions, that are based only on expert judgement.

The HEP for a given tasks is then calculated as

$$HEP = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \cdot K_5$$

Whenever the result of the multiplication is more than or equals to 1, it is assumed that HEP = 1.

2.5.4.3 Technique for Human Error Rate Prediction (THERP)/ Handbook

The most used decomposition method is the Technique for Human Error Rate Prediction (THERP) developed from A.D. Swain and H.E. Guttmann. The key document, called the Handbook, was published 1983 /Sw83/. A short version of THERP is called the Accident Sequence Evaluation Program (ASEP) /Sw87/. The method has been developed and applied primarily in the nuclear power industry, particularly in the context of Probabilistic Risk

Assessments (PRA) of nuclear power plants. However, it is also used to evaluate the degradation of a man-machine system. The method which uses the conventional reliability technology, is subdivided in the following steps:

1. Define the system failures of interest
2. List and analyse the related human operations, and identify human errors and human error recovery modes
3. Estimate the relevant error probabilities
4. Estimate the effects of human error on the system failure events
5. Recommend changes to the system and recalculate the system failure probabilities

1. Define the system failures of interest

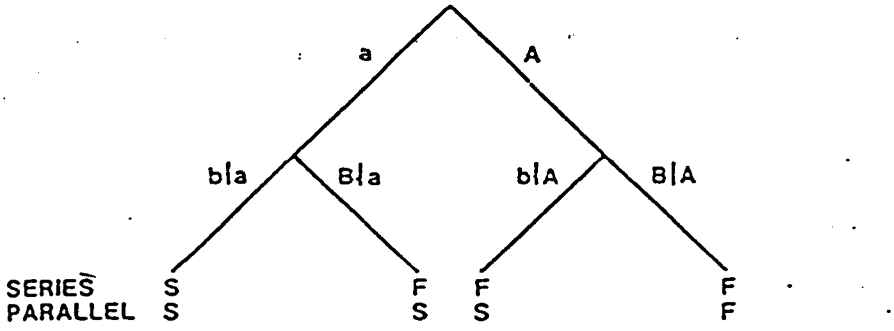
Estimate these system failures that may be influenced by human errors. In case of a risk assessment, estimate these human errors, that have a dominant contribution to the total risk. Human operations with little impact on the risk don't require detailed analysis.

2. List and analyse the related human operations

After estimating the main system failures and human errors, a detailed task analysis and human error analysis is necessary. The task analysis should record every task step and all information used by operators for performing the task. For each task step identified in the task analysis, the analyst must decide what errors could occur. Furthermore opportunities for recovery of human error should also be identified. The consideration of error recovery is important, because it may reduce the overall human error probability for a task.

In order to describe and analyse these human operations and errors, THERP uses the Human Reliability Analysis (HRA) event tree as a basic tool. HRA event trees are a graphical description of the procedural steps in a task, set out in a logical framework. Each node in the tree is a binary decision point (task step successful or task step fail) so that every HRA event tree is compatible with the event tree methodology used in risk analysis. Therefore, if all subtasks in a particular task are described within a HRA event tree and if the probability of success of each task step is known, the entire reliability of the task can be calculated and combined with a event tree.

The basic form of HRA tree is shown in Fig. 2.5.9. The task is decomposed into elementary task steps for which Human Error Probabilities (HEPs) are available. The decompositional approach is very similar to the engineering risk assessment of hardware components.



TASK "A" = THE FIRST TASK
TASK "B" = THE SECOND TASK
a = PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK "A"
A = PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK "A"
b|a = PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK "B" GIVEN a
B|a = PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK "B" GIVEN a
b|A = PROBABILITY OF SUCCESSFUL PERFORMANCE OF TASK "B" GIVEN A
B|A = PROBABILITY OF UNSUCCESSFUL PERFORMANCE OF TASK "B" GIVEN A

FOR THE SERIES SYSTEM:

$Pr[S] = a(b|a)$

$Pr[F] = 1 - a(b|a) = a(B|a) + A(b|A) + A(B|A)$

FOR THE PARALLEL SYSTEM:

$Pr[S] = 1 - A(B|A) = a(b|c) + a(B|a) + A(b|A)$

$Pr[F] = A(B|A)$

Fig. 2.5.9: Human Reliability Analysis event tree for series and parallel systems /SW83/

3. Estimate the relevant error probabilities

HEP is required for every failure branch in the HRA event tree for calculating the entire human error probability. These HEPs can be derived from:

- the THERP/Handbook databank
- simulator results
- data derived from recorded incidents (LERs)
- expert judgement data

However, the primary data source used is the THERP databank itself. The databank in THERP/Handbook Chapter 20 consists of:

- data tables containing HEPs and associated Error Factors (EF)
- performance models, explaining how to modify the data in the data tables for changes in PSFs
- guidelines on how to convert independent (basic) HEPs into conditional HEPs

4. Estimate the effects of error on the system failure events

The next step involves the incorporation of the HRA into the overall analysis, to determine the human contribution to failure. In a PRA this would mean that the HEPs are put into the system fault and event trees for evaluating the frequencies of undesired events (system failures).

5. Recommend changes to the system and recalculate the system failure probabilities

After finnishing step four and evaluating the weak points in man-machine system, a sensitivity analysis can be performed to determine, how the system availability can be improved by reduction of human error probabilities.

2.5.4.4 Accident Sequence Evaluation Program (ASEP)

The Accident Sequence Evaluation Program (ASEP) /Sw87/ is a shortened version of the THERP/Handbook. It requires less expenditure of time and other resources and incorporates many simplifications of human performance models. It was recognized that the full THERP/Handbook does require considerable manpower on the part of a team of experts including a human reliability specialist, system analyst and plant personnel. The simplification of THERP is done at a cost of greater conservatism in estimated HEPs.

The ASEP technique offers rule-based procedures to help and to lead the analyst during the human reliability analysis. The procedures are divided into pre-accident and post-accident tasks. Pre-accident tasks are those, which, if performed incorrectly, could result in the unavailability of necessary systems or components. Post-accident tasks are those which are done to return the plant's systems to a safe condition.

The ASEP pre- and post-accident HRA procedures are further divided into procedures for screening and nominal HRAs. A nominal HRA is applied to those human tasks that survive the screening analysis. The screening analysis uses conservative, i.e. pessimistic estimates of HEPs and PSFs, while the nominal HRA uses more realistic values, but still conservative compared with a THERP HRA.

2.5.4.5 Human Error Assessment and Reduction Technique (HEART)

The Human Error Assessment and Reduction Technique /Wi85/, /Wi88/ offers nine nominal Human Unreliability Values that can be modified with 38 PSFs, called Error Producing Conditions (EPC) . These factors consider particular environmental and ergonomic aspects, that have an influence on operator reliability. The human error probability is calculated as a function of the product of those EPC factors identified for a particular task.

First the assessor should decide what the likely nominal range of human unreliability might be in relation to types of tasks that have to be quantified. After choosing a generic task with the associated unreliability value the assessor can modify this value under consideration of all EPC factors that are present during task execution. Williams offers 38 factors, that may have more or less influence on a successful operator task performance.

To calculate the effect of the error producing conditions the assessor has to estimate what proportion of any given error-producing condition might exist and has to multiply the nominal human unreliability value by appropriate proportions of the chosen EPC factors.

2.6 EVALUATION CRITERIA FOR QUANTITATIVE HRA METHODS

Due to the great number of different HRA methods it is necessary to compare these methods in order to be able to present advantages and disadvantages of each technique. This helps the user to decide which technique is best for his purposes to assess human reliability. Accordingly the purpose of chapter 2.6 is to describe some criteria which are useful to provide guidance for evaluating the HRA methods. A more detailed HRA evaluation offers /Sw89/, /Hu88/, /Sw83/.

The major criteria for HRA method evaluation are

- usefulness/completeness
- validity/accuracy
- ease of use
- acceptability.

Each criterion includes several subcriteria. These subcriteria serve to define a criterion more closely and provide the possibility of a more detailed assessment of a technique where particular criteria are deemed to be of major importance. It should be mentioned that it is not possible to provide infallible guidance on criteria.

Usefulness/Completeness

An important question is to what extent specific subcriteria in HRA methods are useful. It should be examined whether the HRA method allow sensitivity analyses and thus deliver qualitative information. It is important to gain such information and insights for providing recommendations so that the plant safety can be improved. To get deeper insight in the system a sensitive analysis should be performed. The results of such an analysis could offer improvements in the design of equipment, written procedures, man-machine interfaces, operator training and other socio-technical and organizational factors that can affect the personnel impact on plant risk or effectiveness.

It should be possible to assess types of operator behaviour with the HRA method.

The traditional i.e. older HRA methods have been concentrated primarily on simple proceduralized tasks. Usually they allowed to assess skill-based and rule-based operator behaviour. However, there is an increasing tendency to consider diagnostic and decision-making-errors and thus to handle all types of operator performances described by J. Rasmussen.

Furthermore the HRA method should allow the assessment of all kind of operator tasks including test, and maintenance tasks done under normal conditions (pre-accident conditions) as well as diagnostic tasks (post-accident conditions).

Validity/Accuracy

Validity/Accuracy refers to the degree to which the assessment of operator error probability is sufficiently accurate for PRA purposes. It should be examined which kind of data was used to develop the method and whether the method is based on empirical data such as operational experience or Licencee Event Reports (LERs). The most desirable data source, data from operational experience and LERs, has not yielded very much because of inadequate, less detailed event descriptions which influence the factors and which conditions caused the error. The reporting system needs to include facilities for collecting the detailed background information for example the operator's intention, experience, similarity of the task to another task etc. Some methods are based on data generated from full scale training simulators. But because of the very high simulator costs data collected from simulator investigation are rare.

Ease of use

One criterion for selecting methods is the ease of use of HRA techniques. It should be mentioned how much analysts are necessary for assessing operator errors and if they need special training for an effective application of the HRA methods. Do they need additional equipment such as computer programs to calculate HEPs and Uncertainty Bounds. How much time is necessary to learn the application of the HRA method. A further question is the data requirements that are necessary to use the methods.

Acceptability

Acceptability is defined as the extent to which PRA and HRA practitioners, utilities, regulatory authorities and experts in human behaviour technology accept the method and its outputs. Techniques which have been often applied in PRAs or PSAs are likely to be rated as the most acceptable by assessors.

2.7 EVALUATION OF HRA METHODS

In chapter 2.7 each of the HRA methods described in 2.5 are evaluated according to the criteria explained in 2.6 including the main advantages and disadvantages of each technique. It should be mentioned that it is not possible to provide infallible guidance or proposals. Most methods are based on expert judgement because of lack on human reliability data.

OAT

Usefulness/Completeness

OAT concentrates only on knowledge-based operator behaviour during an accident (post-accident tasks). Thus skill- and rule-based operator actions cannot be assessed. Furthermore it is not possible to make a sensitivity analysis. Only the PSF's time and stress can be considered. The uncertainty bounds can be calculated with the proposed Error Factor 10. In practice the OAT method is already old-fashioned.

Validity/Accuracy

OAT time correlation curves are based on expert judgement. This means that the calculated HEPs are subjective because the modell developers did not use "hard data".

Ease of use

The OAT method is easy to use. After determining the time-parameter the calculation of HEPs will follow very quickly. Extensive training for applying the technique is not necessary and only few analysts are needed to take part in estimating the parameters.

Acceptability

The acceptability of OAT is quite low. After the development of the Human Cognitive Reliability curves analysts prefer it or Swain's diagnostic model to OAT if they use time reliability curves for quantifying operator actions

DNE

Usefulness/Completeness

Similar to the PC method DNE is not particularly useful for generating qualitative recommendations to improve the plant design and thus the operator reliability. It has no sensitivity analysis capability. If knowledgable experts apply this method it can be used for almost any application area i.e. pre-accident and post-accident operator quantification. It is possible to estimate all kinds of operator behaviour with it whereas PSF's are not explicitly integrated into the technique. The determination of Uncertainty Bounds should be gained in the same way as the estimation of HEPs.

Validity/Accuracy

Especially the direct numerical estimation depends on the knowledge of experts who judge human errors. Accordingly the application of this method needs experts with different backgrounds like system engineers, ergonomics, NPP operators and their supervisors. It is also important to use a method which allows the interaction between the assessors so that realistic data can be gained. The degree of feedback that the analysts receive influence the results dominantly.

Ease of use

The DNE method has relatively high resource requirements due to its use of multiple experts (in Comer et al. /Co84/ 19 judges took part). It could be a problem to bring the judges together. Otherwise the technique is fairly easy to use but it is important to have an experienced group leader who coordinates the work and finds a group consensus.

Acceptability

The acceptability of DNE to assessors is relatively low. The method is one of the first HRA techniques developed. In the last published PRA the DNE method was not used.

Paired Comparison

Usefulness/Completeness

The PC method is not particularly useful for generating sensitive analysis to propose recommendations for operator reliability. It can be used for evaluating pre- and post-accident human action. Skill-, rule- and knowledge-based operator behaviour can be assessed. The PSFs are considered to compare different operator tasks. The estimation of the Uncertainty Bounds are derived in the course of use of the method.

Validity/Accuracy

The validity of this method depends mainly on the knowledge of the assessors, when they make individual paired comparisons and the necessary calibration HEPs. So this method is highly subjective. These calibration HEPs allow to convert the relative paired comparison scale values to human error probabilities. But it is a problem to find suitable calibration HEPs.

Ease of use

PC requires a large number of experts. However, the bigger is the number of tasks to be evaluated, the smaller is the number of experts needed to achieve good accuracy. If these judges have to assess many operator actions e.g. more than 20, the prework is very time consuming because of the large number of actions which have to be compared. The method is easy to use and usually experts do not require extensive training for the PC application.

Acceptability

PC is a well established technique based on a good deal of scientific research which enhances its acceptability. It has been reviewed by independent experts (Swain, Humphreys, Comer et al.) and designed useful for PRA studies. However, in the last published PSAs or PRA the PC technique was not applied.

SLIM

Usefulness/Completeness

SLIM allows to assess every kind of operator behaviour and errors. Skill-based as well as rule- and knowledge-based operator tasks can be included in the human reliability analysis. The assessor is able to consider every influence factor. It is possible to quantify test, maintenance and accident operator tasks with this method.

When using the SLIM method experts have the possibility to include a wide range of factors in the analysis which affect the operator reliability. With structured expert estimation (ratings and weightings of PSFs) SLIM elicits the influence of every factor for quantifying the operator task.

Thus SLIM is a method for every kind of operator analysis, which enables a sensitive analysis to find weak points in ergonomic plant design, procedures and to offer improvements that mitigate the risk.

Validity/Accuracy

Uncertainty Bounds cannot be obtained with SLIM-Maud. As indicated in Embrey et al (1984a) the Uncertainty Bounds can be derived by using other methods. One problem is the determination of the calibration factors, that are necessary to calculate operator error probabilities. The probabilities depend dominantly on these calibration factors. These two factors are difficult to obtain. Often these factors are missing so that either experts have to estimate them or handbook data has to be used. In that case the estimation of the HEPs is not based on hard data.

Ease of use

As other expert judgement methods SLIM requires a lot of experts too. They also need training to use the method. Especially if expert assess with MAUD software, analysts will require training to get deeper insight into the system and to learn how to apply it effectively.

Acceptability

SLIM-Maud has been used in several PRAs and PSAs which were published during the last years /Ko86, Re91/. Next to these publications SLIM was also applied during the human factor Benchmark Exercise /Po88/. This indicates a high acceptability.

STAHR

Usefulness/Completeness

The STAHR method can be used to generate qualitative recommendations. It has considerable sensitivity analysis capability and is applicable to a wide range of situations. Pre-accident operator tasks as well as post-accident operator tasks can be quantified with it. STAHR is the only method that considers interdependences between the PSFs. The other methods estimate the influence of every PSF on the operator task separately. The Influence Diagram includes 10 PSFs whereas three PSF take into consideration the dependence of PSFs. STAHR allows to estimate skill-, rule- and knowledge-based operator behaviour. Uncertainty bounds derivation has not been demonstrated by the STAHR methodology.

Validity/Accuracy

The theoretical validity of STAHR is ambivalent. The positive aspect is the capability to consider interdependences between PSFs. Unfortunately no consistent theory exists to consider the interdependencies between PSFs and in this sense the STAHR model is speculative. But the HEP calculation approach requires theoretical justification and mathematical evaluation. The numerical accuracy of the STAHR method has not been determined. It is based strongly on the subjective opinions of the assessors.

Ease of use

STAHR requires a high level of resources in terms of time and personnel to develop and quantify the Influence Diagram. Especially the calculation is time-consuming. To use the method some training is necessary.

Acceptability

The acceptability is not very high. It was applied in only a few safety analyses. Nevertheless it should be mention that STAHR is the only expert judgement technique that does not need calibration and considers dependences between PSFs.

HCR Method

Usefulness/Completeness

The HCR Method is intended for the estimation of the crew-non-response probability. It has little use in derivation of error reduction strategies and of gaining deeper qualitative information. However sensitivity analyses varying time and training, stress and quality of the information interface may be performed easily. The approach could be used in other situations where time dependent actions are crucial to success.

The HCR correlation allows to categorize skill-, rule-, and knowledge-based operator behaviour. HCR concentrates only on post accident crew behaviour. Thus no pre-accident operator action can be quantified.

Validity/Accuracy

The dominant Performance Shaping Factor is time. Thus for long time operator actions, i.e. actions where operators have a lot of time to react, HCR methods offer unrealistic low probabilities. If the parameter time is unambiguous and the determination of cognitive operator behaviour is unequivocal the convergent validity is very good. A more detailed description for cognitive operator behaviour estimation would be helpful for HRA analysts. The numerical accuracy and consistency of the HCR correlation has not been determined. Especially probabilities lower than 10^{-2} are difficult to validate because of the necessary simulator data. EPRI and EdF sponsored simulator tests to promote a research project for comparing HCR correlation with this new data. HCR correlation concentrates on crew non-response probability estimation. If there are other possible operator errors like selection of a non-avaliable alternative or misdiagnosis' it should be combined with other HRA techniques. Other investigations show that there could be two additional HCR curves, one between the skill- and rule-based curve and another between the rule- and knowledge-based curve.

Some revision work has been performed under the ORE program /Sp90/. It was realized that the HCR correlation was not appropriate to fit experimental data. Therefore a special type of time reliability correlation, called the HCR/ORE correlation has been proposed /Pr91/ to "use response time data for the evaluation of the probability of failure to initiate timely action".

However, the HCR method is one of the few technique which is not only based on expert judgement but on simulator data.

Ease of use

The HCR method is easy to use. Analysts who assess operator actions with the technique do not need excessive training. Only the derivation of the time parameter could become a problem, for example the treatment of two operator actions within one time window.

Vestrucci et al. /Ve91/ offer a method to calculate the overall success probability given the total time window. After determining all PSFs and the cognitive operator behaviour the calculation can be done very quickly.

Acceptability

The acceptabtlity of the HCR method is good. It is being used by a number of utilities in the USA for PRA purpose or to analyse simulator tests. During the ISPRA Human Factor Benchmark almost all used the HCR technique in combination with THERP/ Handbook, because the possibility for quick operator error assessment is recognized by a lot of analysts.

CM

Usefulness/Completeness

The Confusion Matrix method concentrates on the aspect of misdiagnosing an accident. Thus only knowledge-based operator behaviour can be assessed. It is not possible to elaborate emergency procedure improvements. But the method can serve to offer proposals for better ergonomic plant design. No formal procedure is provided to take into consideration the relevant PSFs. As demonstrated in the Oconee PRA CM can be used to estimate Uncertainty Bounds.

Validity/Accuracy

As the other expert judgement methods CM is based only on the knowledge and the experience of the analysts who apply the technique. But for instance in /Oc64/ the weightings used by the analysts to modify the basic HEPs are not justified; the general idea of CM is sound, but the manner in which the expert judgements were used is based only on unsubstantiated assumptions.

Ease of Use

It is not easy to use the CM method, especially if analyst would like to derive HEPs. The Oconee PRA showed that though qualified assessors took part the judgement were difficult to make.

Acceptability

The CM method has been used at least in three PRAs /Oc64, Pi83, Va91/. But in Seabrook PRA it was applied for qualitative purpose only, not for estimating HEPs. The idea that possible misdiagnosis has to be considered in PRA is accepted but the quantitative estimation of operator errors with CM is not yet accepted.

MAPPS

Usefulness/Completeness

MAPPS computer simulation program was originally designed for assessing pre-accident maintenance operator tasks. It considers skill-, rule- and knowledge-based operator behaviour. The user has to consider nine PSFs. MAPPS allows to calculate Uncertainty Bounds too.

Validity/Accuracy

Most of the data that are implemented in the computer code are based on expert judgement. It seems that for a lot of HRA analysts the HEPs calculated with MAPPS are accurate enough to use these HEPs as anchor points for other methods like SLIM (see Ispra HE-benchmark).

Ease of Use

In spite of the users guide on the use of MAPPS computer program it is not easy to use. That was obvious during Ispra benchmark where some difficulties were experienced by users. They rated it low in ease of use.

Acceptability

In spite of some disadvantages the acceptability is moderate. This was showed in Ispra benchmark where MAPPS were used by nine teams. Most teams applied MAPPS only for pre-accident operator tasks.

TESEO

Usefulness/Completeness

The TESEO method allows to assess any type of pre-accident as well as post-accident tasks. It considers five PSFs. But there is no description on how to calculate Uncertainty Bounds. Any kind of operator behaviour can be considered though there are no explicit distinction between skill-, rule- and knowledge-based operator behaviour.

Validity/Accuracy

The numerical accuracy and consistency of TESEO have not been assessed. The equations for calculating the five parameters are based dominantly on expert judgement.

Ease of Use

To use TESEO it does not need much training. It is easy to use. The method is very simple and quick to apply.

Acceptability

The acceptability of TESEO method is very low because of the lack of evidence for its theoretical validity. There has been little published use of this technique.

THERP

Usefulness/Completeness

THERP/Handbook is a method which allows to assess pre-accident and post-accident operator actions. Using the HRA tree technique every event sequence can be decomposed in single operator actions and then be determined with data tables in the Handbook. For considering PSFs the Handbook offers several models like stress model, dependence model to modify the HEPs found in the tables. With this decomposition technique sensitive operator action analysis is possible to gain qualitative information. The Handbook offers also a model for calculating Uncertainty Bounds. The terms skill-, rule- and knowledge-based behaviour are not used in THERP but these categories of behaviour are implicitely considered.

Validity/Accuracy

A lot of data in the THERP/Handbook tables are derived from real world tests from similar systems for example routine tasks in the manufacturing of weapons. This type of behaviour can be classified as skill- and rule-based. Furthermore data from simulator tests were used to gain HEPs. But the diagnostic models, presented in the THERP/Handbook for assessing knowledge-based operator actions in accident situations are based only on expert judgement. It seems that the nominal HEPs from Swain's diagnosis model are too optimistic /Sw89, p. 3-28/.

Ease of Use

The user of this method needs some training in THERP/Handbook to apply it correctly. The best way to learn the technique is to attend a Swain's HRA course, to read the entire Handbook and then to work through the examples in Chapter 21 of the Handbook. With the Handbook search scheme and the instructions in Chapter 20 THERP/Handbook is easy to use.

Acceptability

The acceptability of THERP/Handbook is very high. In almost every PRA which was published during the last years, THERP was used. Also during Ispra HE-benchmark every team assessed pre-accident and post-accident operator action with this method.

ASEP

ASEP method is a short version of the THERP/Handbook. A difference between the methods is that ASEP offers a step by step procedure for assessing operator tasks. The use of ASEP procedure means more quick but more conservative results in HRA.

HEART

Usefulness/Completeness

HEART has some sensitivity analysis capability. It is possible to estimate all kind of operator behaviour. Pre-accident operator tasks as well as post-accident operator tasks can be calculated with this method. It includes more than 30 PSFs which can be considered for quantifying HEPS. Furthermore HEART presents Uncertainty Bounds for every HEP.

Validity/Accuracy

As mentioned above HEART offers a lot of parameters for determining operator errors but the underlying database are not published. As most of other methods HEART does not consider interactions between different PSFs. Thus it requires justification from an empirical viewpoint.

Ease of Use

HEART is relatively easy to apply and uses minimal resources. Personnel and time resource requirements are low but some training is required to calculate HEPs with the method.

Acceptability

HEART is one of the newest technique considered. It has been applied several times. Also during HE-Ispra benchmark two teams used this method for calculating HEPs.

2.8 PRESENT STATE OF HRA

The principle objective of HRA application in PSA for Nuclear Power Plants is to assess human contribution to core damage frequency. An adequate treatment of human interactions is a key to the understanding of accident sequences and their relative importance in overall risk.

For example table 2.8.1 shows human contributions to core damage frequencies calculated in five studies /Hi90/ (the results quoted from the Sizewell B PSA should be taken as preliminary /Wh92/).

Human contributions to core damage frequencies

Plant	Core Damage Frequency	Impact of Human Errors	Impact of Recovery
Oconee	$2.5 \cdot 10^{-4}$ (mean; modified plant)	4 %	75 %
Seabrook	$2.3 \cdot 10^{-4}$ (mean for a single unit)	30-50 % (estimate)	not clear, evidently significant
Calvert Cliffs	$1.3 \cdot 10^{-4}$ (mean)	12 %	90 % (order of magnitude)
Biblis	$9.0 \cdot 10^{-5}$ (mean)	63-69 % (with other failures)	not documented
Sizewell	$1.0 \cdot 10^{-6}$ (median)	1.4 %	not documented

Table 2.8.1: Human contributions to core damage

A significant result of a recent probabilistic safety assessment of 900 MW(e) pressurized water reactors /La91/ was the important contribution (more than 30 %) of non-power states to the total probability of core damage. In the most important accident sequences, core damage is avoided only by operator intervention due to the lack of automatic systems to deal with these situations. The impact of human factor was therefore of great importance, and "the probabilities of human error have been estimated using to the greatest possible extent real experience and tests on simulators".

In the framework of the EPS 1300 project (PSA of the Paluel Power Plant) HRA methods were used which combine a "highly systematized analysis approach with a large data base on simulator tests"/Mo91/.
The results illustrated the important role of operators in the recovery of accidents. They also demonstrate that "the success of the recovery efforts strongly depends on the extent to which operators grasp the situation and understand the procedure". As an outcome of the EPS 1300 project improvements of training, organization and man-machine interface have been proposed to develop the operators' ability to understand accident phenomena and procedures.

The probabilistic safety studies carried out for the NUREG-1150 program /Nu90/ found that "human interactions are extremely important contributors to the safety of nuclear plants". The ability of operators to activate alternative systems for accident control or to recover failed functions is emphasized.

"Symptomatic emergency procedures" are recognized to reduce the number of diagnosis errors and provide clear direction for accident mitigation.
The human error contribution to core damage frequency for PWRs in the case of LOCA, was relatively high. Although error probabilities for these events (in the course of transfering the emergency core cooling system pumps suction to the containment sump) are comparable to other human errors, the impact of human errors is significant, because alternative systems or actions are not available to recover from this error. Potential human errors that occur during testing or maintenance prior to the accident were generally found to be important.
Human error probabilities for ATWS events were generally lower for both BWRs and PWRs than in previous PRA studies. In all cases, this resulted from the increased training on ATWS events and increased awareness on the actions required in ATWS events.

Sensitivity studies carried out by varying the human error probabilities can provide valuable insights into the role of the human in plant risk and suggest on how to reduce plant risks /Pa91/.

An important concept in HRA is the SHARP procedure for incorporating human reliability analysis results into a PSA framework.

The methods most frequently used for a formal HRA are ASEP, HCR, OATS, SLIM and the THERP/handbook.

Level-1 Probabilistic Safety Analysis Guidelines /Je90/ recommend and prefer following methods

PRA Procedure Guide /PR83/

The focus is on the THERP method which is extensively described; the briefly described OAT method is mentioned as an alternative.

IREP PSA Procedures Guide /JR83/

The THERP method, which was used in the IREP analyses, is briefly described.

NREP PSA Procedures Guide /PS85/

The general SHARP procedure is outlined, and an overview is given of the various HRA methods.

The NUREG-1150 study and supporting documents /NU90/

The ASEP HRA method, which was used in the 1150 analyses, is briefly described.

Electrowatt PSA Procedures Guide /EW87/

The SHARP procedure and THERP method are recommended as a useful basis. The guide states what is to be included at a minimum in the HRA, with respect to the scope and products.

IAEA PSA Procedures Guide /IA89a/

The general SHARP procedure is outlined as an example. A separate HRA guide on the usefulness and applicability of various methods will be published in the future.

Individual Plant Examination IPE /IP90/

- The reporting guidelines require listing the considered types of human errors, the time available for recovery actions, and the screening criteria for human errors.
- Important human recovery actions for which greater credit than 1 error in 10 is claimed, should be discussed.
- In performing the IPEs frequent usage of simulator data for predicting HEPs is to be expected.

At the present time, fully adequate methods for HRA have not yet been performed. In the course of quantifying human actions in PSA, the operator is mostly regarded as part of the system, comparable to a system component. The corresponding failure mode is 'error of omission'. The critical disadvantage of this engineering approach is the lack of appreciation of the internal human mechanisms, for example reasoning, associating and memory that govern human behaviour. This behaviour is characterized by a substantially larger variability and complexity, and the description in terms of reliability parameters is difficult /HW91/. Properties of human mind described above are often associated with so called "errors of commission" which are mostly not included in PSA.

Experts on human behaviour therefore agree that often such actions or elements of actions can be described sufficiently by reliability parameters which refer to skill- or rule-based behaviour. The use of any such view of human behaviour, however, is "limited to those control scenarios that can be thought about in enough detail ahead of time so that they can be rendered in tree form. This is indeed a PSA limitation which does not only apply to human error models. In this sense, the technique cannot 'create' situations that may have been unanticipated" /Ba82/.

Regarding the assumption that human errors are only slips or errors in following correct procedures, the present methods cover in principle the possible errors made.

But strictly spoken there is no PSA-relevant area concerning human factors for which the methods are established and validated, compared for instance with the methodology of fault trees. In respect of both the qualitative and quantitative assessment of operator actions, the identification of possible human errors in the course of planned actions seems to be relatively practicable.

In comparison with the identification of such error-likely situations the quantification of operator error frequencies is less validated. The large number of operator models reflects of methodological deficiencies, and additionally there is a lack of sufficiently validated reliability data regarding to operator actions.

As already mentioned, suitable methods and data are available for 'skill-based' and 'rule-based' behaviour, which is typically needed to perform planned actions. However, the applicability to deal with the methods knowledge-based behaviour of unplanned actions is limited. So-called cognitive models refer to the great complexity and variability of human behaviour, which can provide both beneficial and detrimental contributions to safety, particular if decisions have to be made in new and complicated situations. It is questioned whether an improvement will be possible using such cognitive models.

Even if suitable models are available to identify and quantify operator errors, an essential problem lies in the subjectivity of the analysts using these models. The related uncertainty margings are in the same order of magnitude as those caused by the applications of different models, as the Ispra Human Factors Reliability Benchmark Exercise /PO88/ has shown. This exercise has illustrated that problems linked with human reliability analysis are much greater than those in system analysis. The main reason is the large impact of dependency mechanisms caused by human behaviour. The insights received from this benchmark indicate that the priority is not the development of models but rather the validation of existing models in order to limit the impact of subjectivity. Therefore a systematic and objective evaluation of operator actions is desirable. There is a need for systematic and reproducible methods for identifying human actions in a PRA, especially in the field of cognitive actions /OE89/.

"Despite the present limitations of HRA, it still represents a very useful tool for designing complex systems and for assessing the human-induced risks of such systems to the public. HRA provides a formal, analytical method to identify the potential for important human errors, i.e. the identification of error-likely situations. Even if one has doubts about the accuracy of individual estimated HEPs, HRA provides a determination of the relative importance of error-likely situations for the system criteria of interest" /SW90/.

2.9 DATA

There is a general agreement that one essential problem concerning HRA is the scarcity of data on human performance that can be used to estimate human error probabilities for tasks. From a questionaire, prepared by CSNI-PWG 5 and addressed to human reliability specialists, the following results can be derived /OE89/.

- Operating experience has been used for assessing human reliability in PSA's. The most frequently mentioned category of human action were the most often indicated is test and maintenance activities; the next one was the response time.

- The most frequent use is the qualitative one indicated in almost all cases.

- The main sources of information are special inquiries and - more and more - incident reports with specific reporting systems related to human factor aspects.

- For quantification purposes, simulator observations are often presented as an important source of data.

Furthermore the results show clearly what are the important informations needed for assessing human reliability in PSA's: Use of procedure, timing of the incident and recovery process.

The following source categories to derive human reliability probabilities for HRA's are listed up in /IA89b/:

1. Nuclear power plants;

2. Dynamic simulators of NPP's;

3. Process industries;

4. Other industries and in military activities that are psychologically similar to NPP tasks;

5. Experiments and field studies using real-world tasks of interest, e.g., experimental comparisons of measurement techniques in an industrial setting, performance records of industrial workers, etc.;

6. Experiments using artifical tasks, e.g., typical university psycholcgy studies, which have limited application to real-word tasks and

7. Expert opinion.

Several data banks have been derived by using such sources. The most widely used data bank is the set of tables of estimated HEP's in the Handbook /SW83/, with its underlying taxonomy in the "search scheme" in Chapter 20 of that document. A recent addition to the body of data banks consists of the tables of HEP's in the Accident Sequence Evaluation Program HRA Procedure /SW87/.

A research program has been funded by NRC to develop the conceptual framework and implementation procedures for a human reliability data bank that would support the incorporation of HRA into nuclear power plant PRA's.

Some of the features that make this data bank attractive and feasible are as follows /Sa87/:

1. Incoming data are screened to ensure they meet the minimum criteria (e.g., quantitative HEPs and error rates).
2. Administrative reviews and procedures are set up to minimize erroneous categorization of incoming data.
3. The data bank is set up to receive field, simulator, laboratory, and analytic data.
4. PSF informations is "tagged" to the data.
5. Rules and procedures are established for data combination and aggregation.
6. Three different specificity levels offer flexibility in accommodating data of differing levels of task analysis detail.
7. The data bank user has a set of procedures to help him in finding the appropriate data of interest.
8. A data clearinghouse is established to provide additional information and assistance to the data bank users.

"The human reliability data bank, if implemented, will have the primary purpose of supporting nuclear power PRA activities. If it is successful, the scope of its uses may be widened to support human reliability activities applicable to other industries as well" /Sa87/.

One issue of the EDF/EPRI collaborative program on operator reliability experiments is to establish an appropriate data base for HRA /Jo88/. Under the EPRI ONE project, data collection is made mainly during plant crews simulator retraining sessions by observer teams collecting times to success for crews performing particular human interactions. Among other things the data was utilized to test correlation in the HCR model.

The purpose of the EDF HRA activity is to study the operator's behaviour under simulated incident or accident conditions as realistic as possible, and therefore data collection never occur during retraining sessions, but during specially organized tests.

The data situation regarding HRA in general can be characterized as follows /IA89b/:

"There is a paucity of plant-specific error relative frequencies on which to base estimates of time-dependent and time-independent HEP's. There is a growing base of such data from NPP training simulators, which will be very useful for HRA's. Nevertheless, it is still the case that judgement of experts is necessary in performing an HRA. This judgement will be much more reliable if actuarial data on the tasks of interest are available to aid the judgement process. Extrapolation from highly relevant data should nearly always provide better estimates of HEP's and performance times than judgement based even on superior expertise."

"It now appears that it is very difficult to perform a realistic HRA in a PSA without simulator data. One should therefore use them as much as possible. This is why the Electric Power Research Institute and Electricité de France, for instance, are carrying out an extensive program of simulator tests. Hundreds of tests have already been made and are presently being analyzed. These tests provide qualitative and quantitative data of the utmost importance for PSA applications. But they also provide information which can be directly used by man-machine interface designers and by trainers. They are a very valuable way to acquire a good knowledge of what the operators really do, which is very often different from what designers expect them to do. Simulator data, however, certainly differ from field data, because of the many "biases" that can be reduced, but never fully suppressed. It is therefore very important to carry out studies for calibrating simulator data with field data."

2.10 CONCLUSIONS

Human reliability analysis (HRA) is considered as an important task within a PSA, because human errors contribute significantly to accidents as is reflected by accident statistics.

Regarding to PSA application, human errors are normally divided into three categories: errors prior to an accident (maintenance, calibration, testing), errors as accident initiating events and errors in response to an event (accident control).

The two first kinds of human errors are normally included in system fault trees and reliability data, whereas human actions during accidents create particular PSA problems.

The typical methodological difficulties of HRA originate from the human behaviour characterized by large variability and complexity.

There are several models available for human reliability analysis (HRA); mainly concerning skill-based and rule-based actions which have been used in PSA/PRA. Such HRA methods provide useful techniques to idendify the potential for important human errors and to design complex systems considering human factors.

In view of the quantification of human error probabilities the uncertainties are still extensive, and the possibilities to consider all relevant aspects of human behaviour (especially the cognitive and psychological aspects) are under discussion.

To compensate the lack of operating experience on human errors in accident control attempts are made to use expert judgement and simulator experiments.

In conclusion only few cautious recommendations can be given as regards to the appropriate practices for the use HRA methods in current PSA. The evaluation of HRA methods in chapter 2.7 by four qualitative indicator (usefulness/completeness; validity/ accuracy; ease of use; acceptability) showed that the application of THERP can well be recommended, preferably supplemented by preceding application of SHARP and ASEP for incorporation of man-machine interactions into PSA and for screening analysis. In comparison with other HRA methods THERP achieved good proportional qualifications for all aforementioned indicators measuring the applicability of the methods. In addition to THERP also HCR method copes well with other HRA methods. An advantage of HCR is its easy applicability of utilizing simulator experiments for PSA purposes.

The methods which are mainly based on expert judgements suffer still partly from difficulties to calibrate the expert judgement to real world data and simulator data. This make them so far less useful to practical PSA work than the aformentioned methods. It is, however, quite a general tendency that the expert judgements methods become more and more important if more sophisticated features of human behaviour need to be taken into consideration in PSA.

The following recommendations for future research on HRA can be derived

- Errors of commission are assessed only to some extent in PSA. There is a need for progress with special respect to knowledge based actions. Studies are needed in the field of cognitive behaviour under accident conditions. Models should be developed to identify errors, error-likely situations and possibilities to act in an unscheduled way. Classification systems and descriptions should be given in such a way that designers can use them to develop improvements.

- To collect data from operating experiences, structured collection schemes should be used. Another need is to improve the acceptability of plant-based event reporting schemes, especially voluntary reporting of human errors.

  Further attempts should be made to supplement the operating experience on human error by expert judgement. Methods like ranking and rating, paired comparisons and direct/indirect estimation should be developed purposeful.

- For improving the knowledge on human behaviour under accident conditions, simulators are a useful source of information. But operator's behaviour is not perfectly representative of what it actually is under accident conditions, and there is a necessity to cooperate with specialists of various behavioured sciences for the development of suitable test criteria.

- To diminish the importance of errors during maintenance and testing, procedures should be proved whether they can contribute to confusion and to disadvantageous results of routine acting.

REFERENCES

/Ap88/ Apostolakis, G.E.; Bier, V.M.; Mosleh, A.; A Critique of Recent Models for Human Error Rate Assessment; Reliability Eng. + System Safety 22, 1988, pp. 201-207

/Ba82/ Baron, S., et al.. (1982); A Framework for Modelling Supervisors Control Behavior of Operators of Nuclear Power Plants
in Proceedings of a Workshop on Cognitive Modelling of Nuclear Plant Control Room Operators, NUREG/CR-3114, Oak Ridge National Laboratory, Oak Ridge, TN

/Be80/ Bello, G. C. et al.; The Human Factors in Risk Analyses of Process Plants: The Control Room Operator Model "TESEO". Reliability Engineering, 1 pp 3-14; 1980

/Bl66/ Blanchard, P. C. et al.; Likelihood-of-accomplishment scale for a sample of man-machine activities. Dunlap and Associates, Inc., Santa Monica, CA, USA; 1966

/Co84/ Comer, K.K.; Seaver, D.A.; Stillwell, W.G.; Goddy, C.D.; Generating Human Reliability Estimates Using Expert Judgement, Part 1; NUREG-CR-3688, 1984

/Do88/ Dougherty, E. M.; Fragola, J. R.; Human Reliability Analysis: a system engineering approach with nuclear power plant applications; J. Wiley and Sons, Inc.; 1988

/Do90/ Dougherty, E.M.; On Taking Human Performance Seriously in Risk Analysis; Reliability Engineering and System Safety 29; 1990

/Em84a/ Embrey, D. E. et al.; SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement; NUREG/CR-3518, Vol.1 Summary ; DOE-BNL, Upton, New York 11973; 1984

/Em84b/ Embrey, D. E. et al.; SLIM-MAUD; An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement; NUREG/CR-3518, Vol.2 DOE-BNL, Upton New York 11973; 1984

/EW87/ Probabilistic Safety Analysis Procedures Guide EWE-2572.01, rev. 1, Electrowatt Eng. Serv., SOZA-KFD, May 1987

/Fl75/ Fleming K. N. et al.
HTGR Accident Initiation and Progression Analysis Status Report, Vol. II; AIPA Risk Assessment Methodology GA/A13617, San Diego, CA 1975

/Ha84a/ Hannaman, G. W. et al.; Human Cognitive Reliability Model for PRA Analysis, draft report NUS-4531, EPRI Project RP2170-3; 1984

/Ha84b/ Hannaman, G. W. et al.; SHARP, Systematic Human Action Reliability Procedure; EPRI-NP-3583, Palo Alto, CA, 1984

/Ha87/ Hannaman, G. W. et al.; Some developments in Human Reliability Analysis Approaches and Tools; intern. post-smirt 9 seminar on accident sequence modelling, Human Actions, System Response, Munich, Germany, 1987

/Hi90/ Hirschberg, Stefan (Ed.); Dependencies, Human Interactions and Uncertainties in Probabilistic Safety Assessment;
Final Report of the NRA Project RAS 470, April 1990

/Hu88/ Humphreys, P.; Human Reliability Assessors Guide; Safety and Reliability Directorate RTS 88/95Q; 1988

/HW91/ Hauptmanns, U., Werner, W.; Engineering Risks, Evaluation and Valuation
Springer Verlag Berlin, Heidelberg, 1991

/IA89a/ Guidelines for Conducting Probabilistic Safety Assessment of Nuclear Power Plants
IAEA Safety Series Report, Draft for Comment, Vienna, 1989

/IA89b/ Models and Data Requirements for Human Reliability Analysis
IAEA Teedoc-499, Vienna, 1989

/IR83/ Interim Reliability Evaluation Program Procedures Guide
NUREG/CR-2728, SAND82-1100, Washington D.C., January 1983

/IP90/ Procedural and Submittal Guidance for Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities
Draft Report for Comment, NUREG-1407, Washington D.C., July 1990

/Iv90/ Iven, F.W.; A Human Reliability Analysis Model Proposal and Application to Evaluate the Effect of Operator Errors on Experimental Breeder Reactor II, Argonne Nat. Lab., RAD; Chicago, Ill. 1990

/Je90/ Jehee, I.N.T.; Seebregts, A.J.; Comparison of Level-1 Probabilistic Safety Analysis Guidelines
Netherlands Energy Research Foundation ECN, Petten, Sept. 1990 (Draft)

/Jo84/ Joksimovich, V.; A review of Plant Specific PRAs; Risk Analysis, 1984; 4 (4); pp 255-266; 1984

/Jo88/ Joksimovich, V., et al.; EDF/EPRI Collaborative Program on Operator Reliability Experiments Proceedings of the International ENS/ANS Conference on thermal reactor safety "Nucsafe 88", Avignon, Oct. 1988

/Ko86/ Kolaczkowski, A.M. et al.
Analysis of Core Damage Frequency from Internal Events: Peach Bottom, Unit 2
NUREG/CR-4550, Oct. 1986

/La91/ I.M. Lanore, M. Champ; Probabilistic Safety Assessment of French PWRs: Importance of Non-Power States. Proceedings of the 'International Syposium on the Use of Probabilistic Safety Assessment for Operational Safety', PSA 91, Vienna, Austria, 3-7 June 1991

/Le84/ Levine, S.; Rasmussen, N. C.; Nuclear Plant PRA: How far has it come? Risk Analysis, 1984 4 (4), pp247-254; 1984

/Me64/ Meister, D.; Methods of predicting human reliability in man-machine systems; Human Factors 6 (6), pp621-646, 1964

/Me82/ Metwally, A.M.M.
Analysis and Modelling of Human Performance in NPPs
Dissertation at Iowa State University; Iowa 1982

/Mo88/ Mosneron; HF-RBE;
Final Report-Part I, page 22, 1988

/Mo91/ F. Mosneron-Dupin, G. Sahiou, R, Lars; Probabalistic Human Reliability Analysis: The Lessons Derived for Plant Operation at EDF. Proceedings of the 'International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA 91, Vienna, Austria, 3-7 June 1991

/Nu89/ Comparison and Application of Quantitative Human Reliability Analysis Methods for the Risk Methods Integration and Evaluation Program (RMIEP); NUREG/CR-4835; 1989

/Nu90/ Probabilistic Risk Assessment about seven US nuclear power plants; NUREG/CR-1150; 1990

/Oc64/ Oconee PRA, Chapter 6, "Human-Reliability Analysis," in Oconee PRA. A Probabilistic Risk Assessment of Oconee Unit 3, Vol. 1, NSAC/60, The Nuclear Safety Analysis Center, Electric Power Research Institute, Palo Alto, CA, and Duke Power Company, Charlotte, NC, June 1964.

/OE89/ Human Reliability in PRA-Use of Operating Experience (Draft)
OECD/CSNI PWG5, TF5

/Pa91/ Palla, Robert L.; El-Bassioni, A.; Higgings, J.; An Assessment of the Risk Significance of Human Errors in Selected PSAs and Operating Events
CSNI Workshop on Special Issues of Level-1-PSA, Cologne, May 27-29, 1991

/Pe81/ Pew, R.W.; Miller, D.C.; Fehrer, C.E.
1981; Evaluation of Control Room Improvements though Analysis of Critical Operator Decision EPRI NP-1982

/Pe83/ PRA Procedures Guide, a Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants
NUREG/CR-2300, Volume 1 and 2, Washington D.C., January 1983

/Ph85/ Phillips, L.D. et al.
A Socio-Technical Approach to Assessing Human Reliability (STAHR);
NUREG/CR-4022; Pressurized Thermal Shock Evaluation of the Calvert Cliffts Unit 1 Nuclear PP; App. C; US NRC Washington DC, 1985

/Ph89/ Phillips, L. D.; STAHR A Socio Technical Approach t Assessing Human Reliability; Influence Diagrams, Belief Nets and Decision Analyses, Oliver, R.; John Wiley + Sons Ltd. 1989

/Pi83/ Pickard, Lowe and Garrick, Inc., "Human Actions Analysis," in Seabrook Station Probabilistic Safety Assessment, Newport Beach, CA, December 1983.

/Po88/ Poucet, A.; Human Factors Reliability Benchmark Exercise (HF-RBE), Final Report-part I; summary of results and conclusions; P.E.R.1482/88; Commission of the European Communities, Joint Research Centre Ispra, 21020 Ispra (Va), Italy, 1988

/Pr91/ Parry, G.W., Singh, A., Spurgin, A., Moieni, P., Beare, A.; An Approach to the Analysis of Operating Crew Responses Using Simulator Exercises for Use in PSAs, OECD/BMU Workshop on 'Special Issues of Level-1 PSA, Köln, 1991, GRS 86

/PS85/ Probabilistic Safety Analysis Procedures Guide
NUREG/CR-2815, BNL-NUREG-51569 rev. 1, Washington D.C., August 1985

/Ra83/ Rasmussen, J.; Skills, rules,knowledge; signals, signs and symbols and other distinctions in human performance models; IEEE Transactions on Systems, Man and Cybernetics, SMC-13, no.3; 1983

/Ra85/ Rasmussen, J.; Trends in Human Reliability Analysis; Ergonomics 1985, Vol.28, No.8 pp1185-95; 1985

/Re91/ Reiman, L.S.: A SLIM-based approach in analyzing operator cognitive actions
OECD/BMU Workshop on 'Special Issues of Level-1-PSA', KÖln, Mai 1991, GRS 86

/Ro87/ Roth,E.M.; Human Interaction with an "intelligent machine"; Int. J. Man-Machine Studies 27; 1987

/Sa81/ Samanta P.K. et al.
Modelling of Multiple Sequential Failures
During Testing, Maintenance and Calibration
NUREG/CR-2211, 1981

/Se83/ Seavers, D. A. and Stillwell, W. G.; Procedures for using Expert Judgement to Estimate Human Error Probabilities in Nuclear Power Plants Operations. NUREG/CR-2743;US-NRC; 1983

/Si84a/ Siegel, A. et al.; Maintenance Personnel Performance Simulation(MAPPS) Model; Summary description, NUREG/CR-3626, Vol.1, USNRC 1984

/Si84b/ Siegel, A. et al.; Maintenance Personnel Performance Simulation(MAPPS) Model: Description of model content structure and sensitivity testing; NUREG/CR-3626, Vol.2, USNRC 1984

/Sa87/ Gavried Salvendes (Ed.); Handbook of Human Factors Johan Wiley & Sons, New York, 1987

/Sp90/ Spurgin, A.J. et Al.; Operator Reliability Experiments Program, Vol. 1,2,3. EPRI NP-6937, 1990

/Sv89/ Svenson, O.; On Expert Judgement in Safety Analysis; Reliability Engineering and System Safety, Vol.25 No.3; 1989

/Sw64/ Swain,A. D.; Some Problems in the Measurement of Human Performance in man-machine systems; Human Factors, Vol.6, pp687-700; 1964

/Sw83/ Swain, A. D., and Guttman, H. E.; Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUGEG/CR-1278, US-NRC; 1983

/Sw87/ Swain, A. D.; Accident Sequence Evaluation Program (ASEP): Human Reliability Analysis Procedure; NUREG/CR-4772; 1987

/Sw89/ Swain, A. D.; Comparative Evaluation of Methods for Human Reliability Analysis; GRS report RS 688 Germany; 1989

/Sw90/ Swain, A.G.; Human Reliability Analysis: Need, Status, Trends and Limitations
Reliability Engineering and System Safety 29, 1990

/Va87/ Vaurio, J.K.
Review and Comments on "Accident Sequence Evaluation Program Human Reliability Analysis Procedure"
NUREG/CR-4772, 1987

/Va91/ Vaurio, J.K. and Vuorio, U.M.;
Human Reliability Assessment in Loviisa 1 PSA, Proc. PSAM, Feb 4-7, 1991, Beverly Hills, California, USA Society for Risk Analysis.

/Ve91/ Vestrucci, P.; Santucci, R.; Calderon, R.; Monte Carlo Simulation of Crew Response to Accident Sequences; Reliability Engineering and System Safety, Vol. 31, No. 2; 1991

/Wh92/ Whitfield, D., Health & Safety Executive, U.K. (personal communication)

/Wo78/ Wortman, D.B.; et al.
The SAINT User's Manual; AMRL-TR-77-62
Wright-Patterson Air Force Base; OH, 1978

/Wo81/ Woods, D.D.; Wise, J.; Hanes, L.
1981; An Evaluation of Nuclear Power Plant Safety Parameter Display Systems; Proceedings of the 24th Annual Meeting of Human Factors Society; Santa Monica, CA

/Wo82/ Woods, D.D.
Operator Decision Behaviour During the Steam Generator Tube Rupture at the Ginna NPP
Research Report 82-1C57-CONRM-R2
Westinghouse R&D, Pittsburg

/Wo87/ Woods, D.D. et al.; Cognitive Environment Simulation; An Artificial Intelligence System for Human Performance Assessment; NUREG/CR-4862; 1987

/Wo90a/ Woods, D.D. et al.; The cognitive Environment Simulation as a Tool for modelling Human Performance and Reliability; NUREG/CR-5213 Vol.1+2; 1990

/Wo90b/ Woods, D.D.; Risk and Human Performance; Measuring the Potential for Disaster; Reliability Engineering and System Safety 29; 1990

/Wr82/ Wreathall, J. W.; Operator Action Tree, An Approach to Quantifying Operator Error Probability During Accident Sequences, NUS-4159, 1982

3 - TIME - DEPENDENT PHENOMENA

3.1 - Introduction

The objective of this chapter is to present an overview of time dependent phenomena in PSA.

A preliminary remark is that although several authors consider time dependencies as a limitation of PSA and a source of uncertainties, there are not many documents presenting developments on this area, and still less documents presenting effective use of time dependent models in PSA. As can be seen in the following paragraphs, the main reason is that the treatment of time dependencies leads generally to excessively complex models. Clearly the treatment of time dependencies is not a current practice in PSA.

This chapter gives an identification of the time dependencies which may affect the results of the PSA's, a review of existing methods and models, discussion on the need of time dependent models in PSA applications and some general conclusions.

3.2 - Time - dependent phenomena in PSA's

The results of PSA's are generally expressed as a risk frequency. In particular the result of a level 1 PSA is always the frequency of core damage. This presentation implies implicitly that the core-melt probability is uniformly distributed during all the life time of the plants (per reactor year). Moreover this core damage frequency is generally calculated by multiplying the frequency of the initiating events (uniformly distributed) by the failure probability of the safety systems (or functions) upon demand, with no account for the duration of the accidental situation.

These assumptions, more or less implicit, are obviously not correct, and several time dependent phenomena may be treated in the probabilistic approach. For instance the following time dependent phenomena can be analysed :

- Time dependent failure rates.

- Time dependent unavailabilities due to test and maintenance.

- Time cependencies in accident sequences
  - Recovery of equipments.
  - Human interventions.
  - Time dependencies of system operating conditions.

- Evolution of knowledge.

These different points are summarized on Table 1 (from Ref 4) and are developed in the following paragraphs.

3.3 - Time dependent failure rates

The failure rate of equipments may depend on time, due to ageing effects, preventive maintenance, etc. These time-dependent phenomena may concern active components such as valves, pumps, or passive components such as pipes or pressure vessel (réf 1).

The impact of component ageing on the plants safety can be evaluated using time dependent component failure models in the PSA. In order to make this possible, component ageing analyses should be performed. The aim of component ageing analysis is to identify the deterioration and the increase of failure occurences of components, to predict the remaining lifetime of components and to find suitable ways to mitigate the ageing effects. The component ageing analyses should be focused on the components that are the most significant for the plant safety. The selection may be based on PSA models and on the evaluation of the risk sensitivity with various importance or sensitivity measures (see for example reference 32). After the components for ageing analyses are selected, the analysis methods for ageing identification are chosen. The suitable methodology depends on the selected components and on the data available.

If the available failure data is sufficient, quantitative or statistical methods may be applied to reveal trends, assess the degree of degradation and evaluate the remaining lifetime of the component. Furthermore, the parameters of time dependent failure model can be estimated from data. An example of simple statistical method to identify trends is the total time on test plots (discussed in reference 27 and 33). Other methods, e.g. estimation of Weibull process parameters from the data are also widely used. The estimation of failure rates and trend testing based on operating experiences in Finnish PWR plants is descibed in reference 34. A review of ageing models is given in reference 35.

More recently some ageing models of failure rates were introduced in a whole PSA in order to calculate the core damage frequency increase due to ageing under a given maintenance program (generally a linear failure rate model) (ref 2). Examples of results are given in Figure 1. The latest version of the FRANTIC - code (réf 6), FRANTAGE, published recently, includes models for ageing analyses to be used in PSAs (ref 31). FRANTAGE includes options for sensitivity analyses, which may be applied especially in optimization of test, inspection and maintenance strategies.

The impact, directly related to the frequency of some initiating events (LOCA, SGTR, ...) may be important. The ageing effects are a possible important source of uncertainty.

Basically there are two types of ageing. The ageing of components, which have a mean time to failure shorter than the plant lifetime may be called short term ageing. This means that the succesive time period between failures tends to decrease in the course of time. For this type of components (e.g. pumps, valves etc...) there are typically a lot of failure data and statistical ageing analyses may be performed. Long term ageing appears in components the lifetime of which is longer than the plant lifetime (e.g. pipes, pressure vessel, etc...) and there are almost no failure data. The evaluation of failure rate or expected remaining lifetime of such components must be based on surveillance and condition monitoring.

The introduction of the ageing phenomena in PSA models is not a current practice. In living PSAs the failure rates are updated periodically and the operating experience feedback can be used in the assessment of ageing. However, the long term ageing is not easily included even in the living PSA models.

3.4 - Time dependent unavailabilities due to test and maintenance

The unavailability of a component or of a stand by system upon demand is dependent on test interval, and on the test arrangements. Testing unavailabilities are generally treated by a mean value in the classical PSA methodology. Some examples of detailed treatment are proposed (réf 4 - 5 - 6 - 7 - 8 - 9 - 10 -11). Historically the most classical tool which treats a detailed modeling of component unavailabilities due to testing is the FRANTIC code (ref 6).

The paper of ref. 11 gives several detailed models for component unavailabilities and for common cause failures resulting from testing, taking into account several parameters (test intervals, test arrangements, latent failures not revealed by test, critical or not critical failures, test introduced failures, etc ...). The models discussed in ref 11 are rather similar to the models in FRANTIC and only some modifications have been made. Detailed component models are given in Table 2. An example of a system unavailability versus time with a detailed model is given in Figure 2.

The complexity of the models which cannot be treated by the classical fault tree codes, and the need for detailed data which are not currently available (for instance test efficiency) make in practice some difficulties for the application of time dependent models.

The usual assumption in PSA models is that the repair time distributions are exponential. In some PSA applications (e.g the optimization of technical specifications) more detailed models are needed. It leads to another type, more complex, of time dependence not typical in classical PSA applications.

The impact of a detailed time dependent treatment of unavailabilities does not appear significant for the overall result of a PSA. The interest of using a detailed model is derived from a need for a more realistic assessment of operation of NPPs and a possible use for optimizing the testing strategy. But due to the amount of work and to the lack of data, this treatment is limited to some specific examples.

3.5 - Time dependencies in accident sequences

3.5.1 - Time dependencies of system operating conditions

- The success criteria of systems may depend on time (two or one train necessary, different possibilities of functional redundancies, ...).

- The operation of systems is time dependent : active redundancy, then one train on stand-by, use of mobile equipments after some delay.

The success criteria and the operation modes may depend on time because of physical phenomena (the decay heat production is a decreasing function of time) or of human interventions.

3.5.2 - Recovery of equipments

Recovery can be considered for initiating events, front line and support systems. If recovery is taken into account, it introduces several time dependencies :

- The failure probability of systems depends on recovery possibilities, especially for long mission times.

- The recovery probability of a whole sequence depends on time available for carrying out a recovery (when there is a delay available for recovery between a system failure and the severe consequences).

- The repair conditions may depend on time, for example an intervention is not possible at the beginning of an accident (pressure, temperature, radiation level, ...) but possible after some hours or some days. The repair rate may be time dependent.

- The delay available for a recovery is time dependent, for instance when the residual heat production decreases, the delay available for recovery of a cooling system increases.

Recovery is generally introduced in current PSA's, for instance recovery of an initiating event, such as the loss of DC or AC power supply.

Time dependency of available delays, of repair time and accident conditions are treated in the French PSA's in several cases, for instance for long term post-LOCA situations. A specific example is given in paragraph 5.5. The example shows that the impact of recovery is obvious either for the aspect of repair of equipment or for human reliability. The recovery probability versus time (including both time available for a recovery and absolute time since the beginning of the accident) is clearly a very important parameter both on level 1, level 2 and level 3 PSA results.

3.5.3 - Human interventions

Human interventions are strongly time dependent, for many reasons, for instance :

- The error probability of human intervention depends on the time available for making a diagnosis, performing an action.
- The error probability depends on absolute time (for example the stress is lower after some hours).
- The available delay for an action depends on time elapsed since the occurrence of initiating event.
- The probability of an action depends on the timing of previous other actions.

Timing of human interventions is treated in most PSA's, by use of time reliability curves or correlation models (HCR model). However recovery by repair of equipment or by human interventions are often considered as a whole recovery factor which makes time dependencies to remain implicit. Some more precise examples are given in the human reliability benchmark exercice (JRC-ISPRA) (réf 12).

The models of human reliability are extensively presented in a specific chapter of this report and are not detailed here.

3.5.4 - Methods used for time dependencies in sequences

The interest of an improved treatment of time dependencies in accident sequences appears as necessary in several recent works. Interesting methods are developed for that purpose such as improved event trees methodology, dynamic event trees, Markov graphs or state graphs, Monte Carlo simulation.

- Improvement of the classical event tree methodology, by including system timing, recovery events or operator actions as top events, needs a more detailed analysis of the sequences, and leads to complex event trees. The quantification, however, is possible by means of classical tools (réf 13 - 14).

- In the same way, a more refined method is the construction of dynamic event trees. This approach allows for event sequence branchings at successive points in the course of time. The probabilities of the branchings depend on the operators decisions and behaviour, and on the physical state of the plant. This methods requires specific tools and a large amount of data concerning human factor and physical process (réf 15 - 16 - 17 - 18 - 19 -20). A dynamic event tree is illustrated in Figure.3.

- Markov graphs (and more generally state graphs) are used in several recent studies. This method is efficient for the treatment of reparaible systems, with stand-by components, and long mission times. By help of suitable simplifications (construction of macro components) the states graphs can be introduced as a part of complete PSA's. Their use, as a complement of "static" fault trees, introduces an important improvement in modeling "dynamic" systems (réf 21 - 22 - 23 - 24 - 25).

- A method able to treat all possible time dependencies is the Monte Carlo simulation method (réf 26). Although various variance reduction methods may be used, this approach remains complex and time consuming. But it is interesting to note that Monte Carlo simulation can be used for any difficult problem, and to check the validity of simplifications.

3.5.5 - An example

To illustrate the treatment of time dependencies in accident sequences, an example is summarized. This example is derived from the French PSA related to the 900 MWe standardized PWR. In case of a large LOCA an assumption was made that the mission time for safety injection and heat removal was one year (time necessary to reach a situation in which the break may be repaired or the core unloaded). The following facts reflect the physical progress of the accident and timely measures to manage and mitigate the consequences.

- The Low Pressure Safety Injection (LPSI) and Containment Spray System (CSS) pumps are not reparable during a first period (15 days) and reparable afterwards.

- The systems configuration (normal/stand-by), and the success criteria change within time.

- The operators can use (after some time) mobile equipments for a backfitting of LPSI and CSS pumps (emergency procedures H4-U3 for French NPPs).

All these time dependencies are treated by means of several chained state graphs. The treatment produces interesting results (for a large LOCA and mission time of one year) :

- without any repair, the conditional core melt probability is nearly 1,

- taking into account repair of pumps, but no emergency strategy, this conditional probability is 5.3 10^{-2},
- with all the recovery possibilities, the conditional core-melt frequency is 1.3 10^{-2}.

This detailed model used in the analysis was very usefull in analysing possible strategies in case of a post-LOCA situation (Ref 30).

3.6 - Evolution of knowledge

The aforementioned time dependent phenomena are of a particular nature, but it is clear that new knowledge may have important effects on PSA results : increased experience feedback leading to more complete and more precise data, new knowledge on physical phenomena derived from recent studies or experiments can directly contribute to the PSA results.

The increased operating experience helps in identification of new failure modes and phenomena and possibly in detecting trends in failure rates. These new phenomena can be modelled based on the new knowledge which increases the completeness. However, the revised failure models usually include more parameters the estimation of which may be rather uncertain.

The effect of improved knowledge on the treatment of time dependencies will lead to a reduction of uncertainties and an increase of completeness. The only way for taking these effects into account is the updating of the studies in the framework of living PSA's.

3.7 - Conclusions

This chapter has presented an overview of the time dependent phenomena which may have an effect on the results of PSA, and of the methods for taking these dependencies into account. With our present state of knowledge, some general conclusions can be drawn :

- Some time dependent phenomena are slow (ageing - improvement of knowledge), those phenomena have not to be modelled in the PSA itself, but can be analysed in the framework of living PSA's by means of trend analysis.

- Other time dependent phenomena may have an effect on the PSA results also in a short term (effect of testing, time dependencies in accident sequencies such as recovery or evolving system mission). For these problems specific tools have been developed, especially the use of state graphs for quantifying the accident sequences.

The interest of these specific models is clearly an increased realism of the plant models and furthermore a increased credibility of the studies. The difficulties are the complexity of the treatment (so the amount of work necessary) and the need for the corresponding data which are more detailed than in classical models and often not available.

The time-dependent models are needed in some rather specific PSA applications. The optimization of test or inpection intervals is the most wellknown example. Other application, such as the optimization of allowed outage times and the optimization of test and maintenance strategies, require often rather complete time dependency models.

So it is impossible to introduce the treatment of time dependencies systematically in a PSA. It is necessary to ensure a reasonable balance between the advantages and the disavantages of the methods, by considering in particular the objectives of the study (for example the effect is different if considering the overall results or a sensitivity study related to a specific problem). The modeling of time dependencies has to be limited to specific points for which, on the contrary, this modeling appears as necessary.

REFERENCES

1 - J. DUFRESNE
"Probabilistic Application of Fracture Mechanics",
5ème Conférence Internationale sur la rupture (ICF 5)
Cannes - April 1991

2 - W.E VESELY
Calculation of The Core Damage Frequency Increase Due to Ageing under a given Maintenance Program,
International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety (PSA '91)
Vienna - 3-7 June 1991

3 - Dr VICKI - M. BIER
Issues in the Estimation of ageing in Event Frequencies,
International Symposium on the Use of Probabilistic Safety, Assessment for Operational Safety (PSA '91)

4 - S. HIRSCHBERG et al.
Dependencies, Human Interaction and Uncertainties in Probabilistic Safety Assessment.
NKA/RAS - 470, April 1990

5 - VAURIO, J.K
Application of a New Reliability Growth Model that Fits Data.
Scandinavian Reliability Engineers Symposium, Otaniemi, finland,
October 14-16, 1986

6 - US NRC The FRANTIC Code Manual.
NUREG 0193 - Mars 1977

7 - T MANKAMO - U.PULKKINEN
Test Interval of Standby Equipment.
VTT 892 - September 1988

8 - T. MANKAMO
Phased Mission Reliability - A New Approach Based on Event
Sequence Modelling,
Scandinavian Relibility Engineering Symposium, Otaniemi, Finland October 14-16, 1986

9 - M. KNOCHENHAUER
Development of a Time Dependent Failure Model for Motor Operated Valves Based on Analysis
of Failure Data and Testing - ABB-Atom. RPC 89-69, 890920

10 - S. BIORE et al.
Defences against CCF and Generation of CCF Data, Pilot Study for
Diesel Generators,
SKI Research Program, To be published

11 - GUNNAR JOHANSON
NKS/SIK-1 Project Report : Time Dependencies in LPSA Models,
CSNI Workshop on Special Issues of Level-1 PSA,
Cologne, 27-29 May, 1991)

12 - HF - RBE
Human Factors Reliability Benchmark Exercise Synthesis Report,
Commission of the European Communitics - JRC ISPRA
August 1989

13 - A.P MACWAN - K.S HSUEH and A.MOSLEH
An Approach to Modeling Operator Behavior in Integrated Dynamic
Accident Sequence Analysis,
International Symposium on the Use of Probabilistic Safety,
Assessment for Operational Safety (PSA '91)

14 - JM. LANORE and JL. CARON
A. ELLIA-HERVY and J. L'HENORET
Interaction between Thermal/hydraulics, Human Factors and System
Analysis for assessing Feed and Bleed Risk Benefits.
ENS/ANS/SNS Int. Topical Meeting on PSA and Risk Management,
Zurich, Aug-Sept. 1987

15 - C. ACOSTA an N. SIU
Event Trees and Dynamic Event Trees Applications to Steam
Generator Tube Rupture Accidents,
International Symposium on the Use of Probabilistic Safety
Assessment for Operational Safety (PSA '91)
June 3-7, 1991 - Vienna, Austria

16 - A. AMENDOLA
"Accident Sequence Dynamic Simulation Versus Event Trees"
in Accident Sequence Modeling : Human Actions, System Response, Intelligent Decision
Support, G. APOSTOLAKIS,
G. MANCINI and P. KAFKA, eds, Elsevier Applied Science, 1988

17 - N. SIU
"Dynamic Accident Sequence Analysis in PRA : A Comment on
human Reliability Analysis - Where Shouldst Thou Turn', "Reliability
Engineering and System Safety 27, 23-51 (1990)

18 - G. APOSTOLAKIS - T.L. CHU
"Time-dependent Accident sequences Including Human Actions",
Nucl. Tech. (64), Feb. 1984 (p. 115)

19 - E. SILVESTRI - S. SERRA - D.F PADDLEFORD
"A Model for the Probability of Core Uncovery in LOOSP Induced
Accidents. As Applied in the PSS for ENEL PWR Standard Power Plant",
ANS/ENS Int. Topical Meeting on Probabilistic Safety Methods and Applications,
San Francisco, Calif. Feb. 1985

20 - A. VILLEMEUR - M. BOUISSOU - A. DUBREUIL-CHAMBARDEL
"Accident Sequences : methods to Compute Probabilities"
ENS/ANS/SNS Int. Topical Meeting on PSA and Risk Management
Zurich, Aug.-Sept. 1987

21 - ENRICO SILVESTRI
Why is the Markov method not used as a standard thecnique in PSA.
CNSI Workshop on Special Issues of Level-1 PSA
Cologne, 27-29 May, 1991

22 - A. DUBREUIL - CHAMBARDEL
Why Markovian Techniques were used in EDF's PSA of PALUEL ?
Probabilistic Safety Assessment and Management (PSAM). Beverly Hills, USA - 4-7 février 1991

23 - B. ARIEN - D. LAMY
Reliability Analyses of large Systems by the Markovian Technique,
Developement of the CAMERA Software,
International Symposium on the Use of Probabilistic Safety
Assessment for Operational Safety (PSA '91)
June 3-7 1991 - Vienna, Austria

24 - J. DEVOOGHT - C. SMIDTS
"Framework for time dependent interaction between operator and
reactor between a transient involving human errors",
ENS/ANS International Topical Meeting on Probabilistic Reliability
and Safety Assessment - Pittsburg 1989

25 - F. DUCAMP - A. ELLIA-HERVY
Risk Assessment for Long-Term Post-Accident Sequences,
ENS/ANS/SNS Int. Topical Meeting on PSA and Risk Management
Zurich, Aug.-Sept. 1987

26 - K. NAKADA et al.
A Method of State Transition Analysis Under System Interactions
An Analysis of a Shutdown Heat Removal System.
"Nuclear Technology" 82, 132-146 (1988)

27 - H. PAMME
Graphical Tools for Detection and Modelling of Time Dependent ageing behaviour in
Component data, CNSI Workshop on Special Issues of Level-1 PSA
Cologne, 27-29 May, 1991

28 - W.E. VESELY
Risk Evaluation of ageing Phenomena : the linear ageing reliability
model and extensions,
NUREG/CR-4769, April 1987

29 - GUESS. F., HOLLANDER, M. PROSCHAN. F.

Testing Exponentiality Versus a Trend Change in Mean Residual Life.
The Annals of Statistics, Vol. 11,
N° 1, S. 1388-1398, 1986

30 - M. BERTRAND - M. CHAMBON - M. DUCAMP (CEA-IPSN)
Improving Cooling after a non-isolatable Rupture in the Primary Circuit.
International Symposium of the Use of Probabilistic Safety
Assessment for Operational Safety (PSA '91)
June 3-7 1991 - Vienna, Austria

31 - GINZBURG, T. FERSON, S. VESELY, W.E
Time-Dependent Evaluations of Risk due to Aging Using FRANTAGE. Aging Research Information Conference, March 24-27, 1992, Rockville, Maryland.

32 - DAVIS, T., SHAFAGI, A. KURTH, R. & LEVERENZ, E.
Importance Ranking based on ageing Considerations of Components included in Probabilistic Risk Assessments. Washington, D.C., U.S Nuclear Regulatory Commission, NUREG/CR-4144. 1985. 66 p.

33 - AKERSTEN, P.E. The bivariate TTT-plot - A Tool for the Study of non-constant Failure Intensities. SRE Symposium '86, OTANIEMI, Finland, 14-16 october 1986. Society of Reliabilyty Engineers, Scandivavian Chapter. Espoo, Technical Research Centre of Finland. 44 p.

34 - JANKALA, K.E. VAURIO, J.K Component Ageing and Reliability Trends in Loviisa Nuclear Power Plant. ENS/ANS International Topical Meeting : Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, April 2-7, 1989.

35 - SIMOLA, K. Probabilistic Methods in Nuclear Power Plant Component ageing Analysis. VTT Publications 94. Tecnical Researcn Centre of Finlan. Espoo 1992.

Table 1

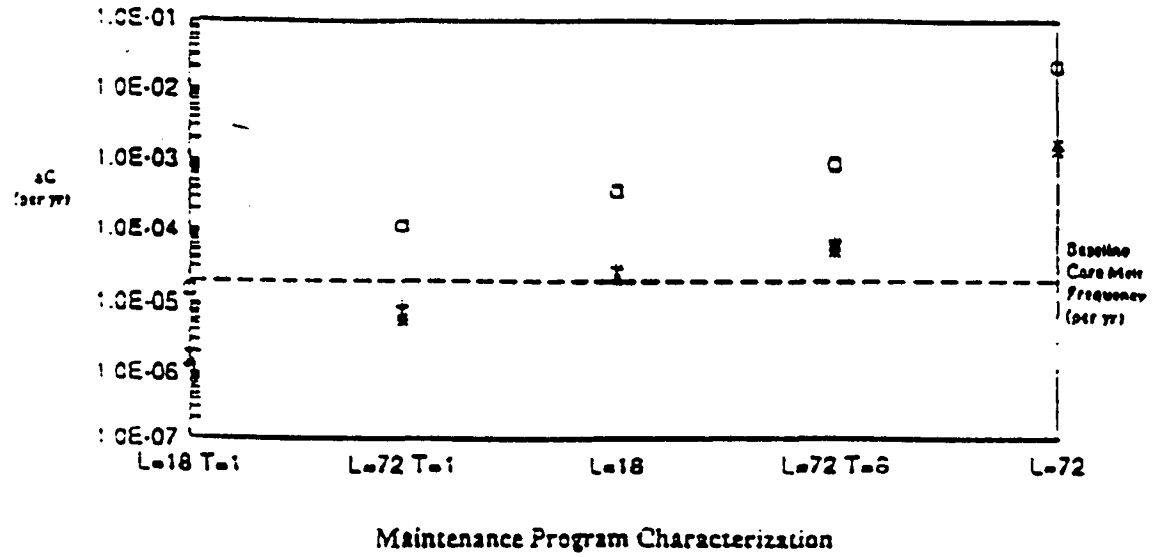
Time dependency categories

Time dependency category	Remarks
Time-dependent failure rates 1. AGEING 2. LEARNING	- affect the component failure probability and initiating event frequency - different for components with short and long life lengths - different ageing mechanisms
Time-dependent unavailabilities 1. TEST INTERVAL DEPENDENCIES 2. TEST ARRANGEMENT DEPENDENCIES 3. LATENT FAILURES NOT REVEALED IN TESTS 4. REPAIR UNAVAILABILITIES	- not always modeled in PSAs - affect also CCF-probabilities - rather complicated models
Time dependencies of accient sequencies 1. TIME-DEPENDENT SUCCESS CRITERIA 2. TIMING OF EMERGENCY SYSTEM OPERATION 3. TIMING OF OPERATOR ACTIONS 4. TIME DEPENDENCY OF OPERATOR ERROR PROBABILITIES 5. TIME-DEPENDENT PHYSICAL PHENOMENA	- affect both level 1 and 2 PSA results - one of the main uncertainties in PSA - different models exist - treatment with sensitivity studies
Increase of statistical evidence	- problem of living PSA - possibility to take several factors into account in PSA failure data

Figure 1

Core Melt Frequency Increase ΔC Versus Maintenance Program Characteristics

Plant A

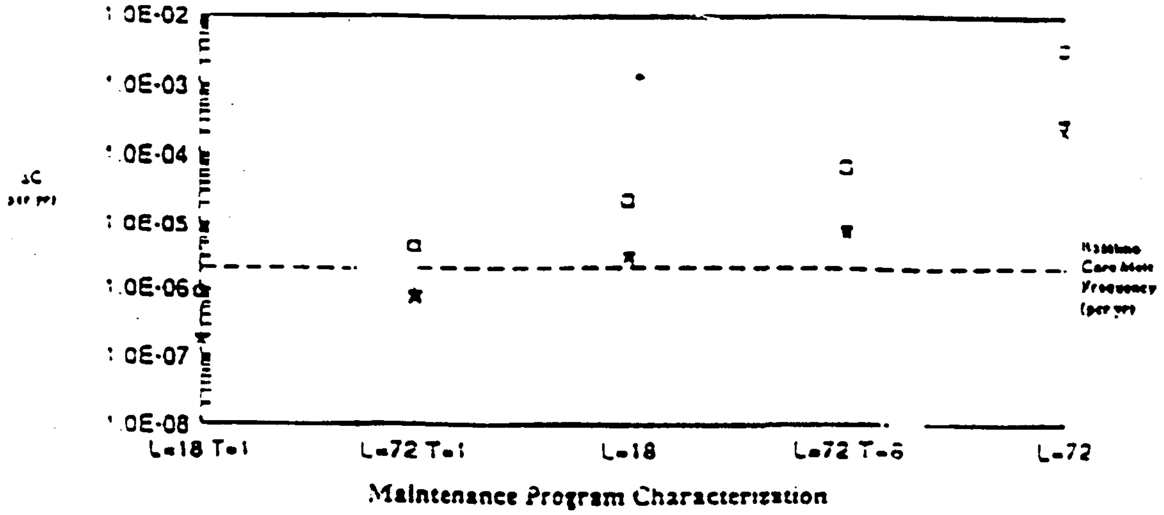


L = Overhaul interval (in months) for all components

T = Surveillance interval (in months) for all components (if intermediate surveillance is performed)

Core Melt Frequency Increase ΔC Versus Maintenance Program Characteristics

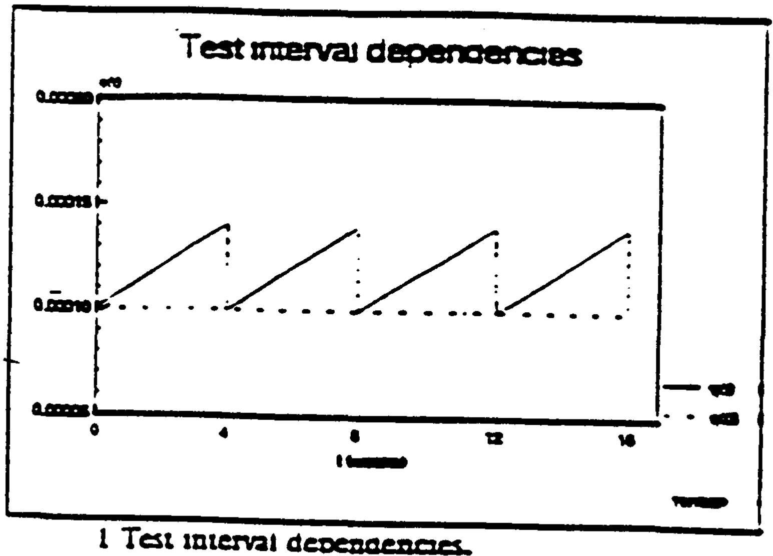
Plant B



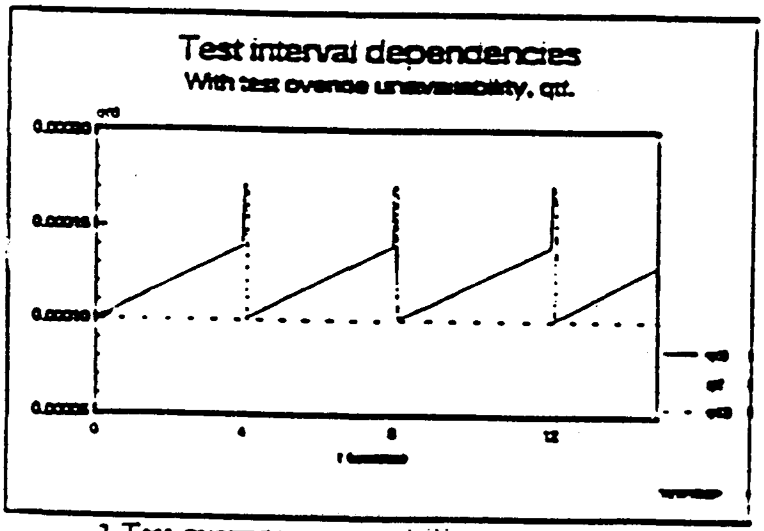
L = Overhaul interval (in months) for all components

T = Surveillance interval (in months) for all components (if intermediate surveillance is performed)

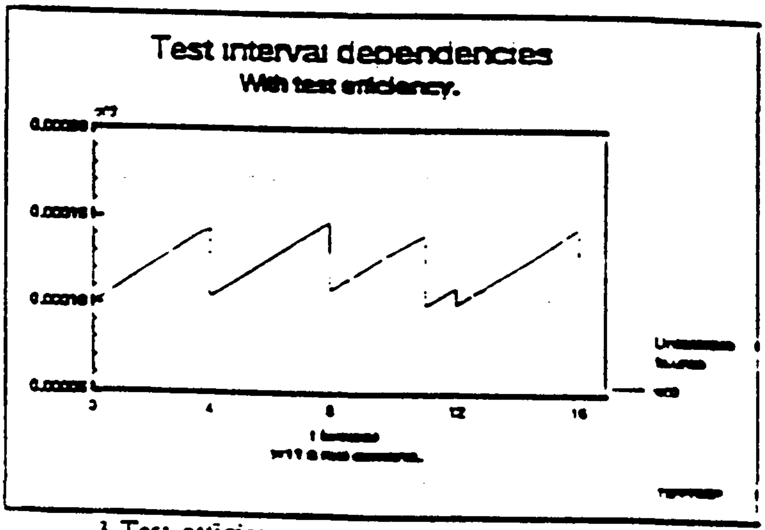
Figure 2



1 Test interval dependencies.

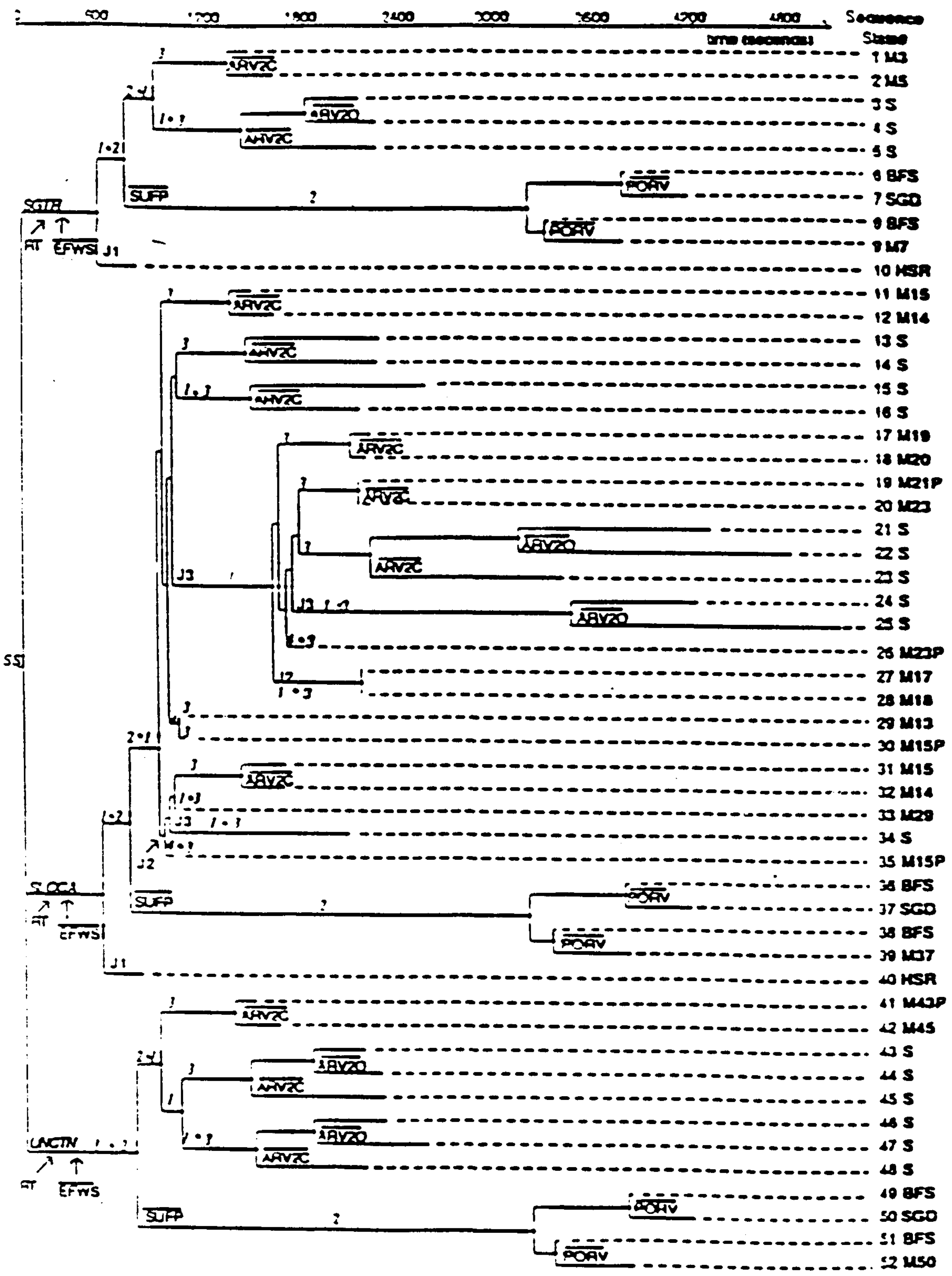


2 Test override unavailability



3 Test efficiency dependencies

Figure 3



*The number of the sequence state refers to the sequence number. The number after letter M refers to the other sequence with which the sequence merges. The letter P after the sequence number refers to the sequence's pruning.

1 - Response to Reactor Trip or Safety Injection
2 - Loss of Secondary Heat Sink
3 - Steam Generator Tube Rupture
4 - Loss of Reactor or Secondary Coolant
BFS - Bleed and Feed cooling successful

J1 - Crew misses step that checks EFWS
J2 - Crew misses the first step that checks SGTR
J3 - Crew misses the first step that checks SGTR
S - Successful depressurization

RT - Reactor Trip
SGTR - SGTR Diagnosis State
SLOCA - SLOCA Diagnosis State
UNCTN - Uncertain Diagnosis State
SGD - Intact SGs Dryout

SGTR Dynamic Event Tree (EFWS Failed)

4 EXTERNAL EVENTS

General Remarks

External events are potential accident initiators produced by natural phenomena or hazardous activities in the vicinity of a nuclear power plant. These events have often the common characteristic to threaten at the same time both the plant structural integrity and system operability. Because of their common cause effect, they might significantly contribute to the estimated risk. The contribution however depends on the nature and strength of the phenomena involved and also on the plant response to possible consequent accidents.

Methods for assessing accident sequences initiated by external events have mainly been developed after the WASH 1400 Reactor Safety Study /1/. The external events contribution to core damage are frequently analyzed in several recent Level 1 PSAs. Because of the large uncertainties in the analysis, the treatment of external events in Level 1 PSA is not as complete nor as definitive as the treatment of internal events. In addition the current methods to deal with the physical phenomena related to the external events have not reached the same maturity as those to internal events, and are still in progress.

Past PRA applications (Zion, Indian Point 2 & 3, Limerick, Seabrook, Oconee and Millstone 3) have regularly dealt with earthquakes as major external initiator of accident sequences. Other external events such as floods, extreme winds, tornadoes, and fires have also been considered in these applications. In the NUREG 1150 report /2/ an extensive analysis has been conducted to assess the frequencies of both the seismic and fire induced accident sequences for the Surry and Peach Bottom plants reflecting State-of-the-Art in the level 1 PSA methodology. Bounding analyses for other events have also been performed in NUREG 1150, using conservative models.

The methods currently used to perform external events analysis in level 1 PSAs are briefly described in the following chapters making references to the available literature. The discussion is focused on seismic events, floods and fires that in past PRAs were more extensively treated than other events /3/.

REFERENCES

1. USNRC, "Reactor Safety and Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (NUREG-75/014). October 1975.

2. USNRC, "Severe Accidents Risks: An Assessment for Five U.S. Nuclear Power Plants", NUREG 1150 Vol. 1, 2 and 3, December 1990.

3. S. Hirschberg, L. Gunsell. Defensive Measures Against External Events and Status of External Event Analysis in Swedish Probabilistic Safety Assessments, Second International Post-SMIRT 10 Seminar "Probabilistic Risk Assessment (PRA) of Nuclear Power Plants for External Events", Irvine, California, August 21-22. 1989.

4.1 Seismic analysis in level 1 PSA

4.1.1 Basic approach

After the publication of the Wash-1400 report /1/ in 1975, the seismic risks have been analyzed in several plant specific PRA applications. Various procedures have also been developed in support of this analysis, and documented in the "PRA Procedures Guide" /2/. They provide methods to identify the seismic hazards at the site, to evaluate the plant response to accidents initiated by seismic events, to assess the accident consequences and to quantify the risk. The most recent state of the art on the seismic analysis has been made and given in the NUREG 1150 report /3/.The procedures have been updated in the "Procedures Used for the External Event Core Damage Frequency Analysis for NUREG 1150".

To determine the core melt frequencies of seismically induced initiating events, the fault trees and event trees worked out for internal events are utilized. The fault and event trees are, however, modified to reflect the unique common cause features of seismic events.

Several steps of analysis have been recognized in the approach. As indicated in ref. /5,6/ they may be grouped as follows:

1) Hazard analysis which determines the expected frequency of the site ground motion due to earthquakes;

2) Fragility analysis which determines the impact of earthquake on specific the plant components, systems and structures of the plant;

3) System analysis which evaluates the impact of failed components, systems and structures on the plant response.

Computation of core melt frequencies and treatment of phenomena and consequences associated with core melt accident are similar to those for internal event analysis. System analysis includes the assessment of the containment response to seismic events that allows, through the use of PRA techniques, to determine frequencies of various release categories. The flowchart shown on fig. 1 outlines the course of seismic PRA up to level 3. The uncertainty analysis is very important in seismic PSA. A number of studies /7,8/ performed in connection with NUREG 1150 studies have shown that uncertainties in the seismic hazard analysis dominate the uncertainties in the overall results.

The fragility analysis is typically regarded as greatest contribution to uncertainties in seismic analysis. Some authors however /5/ think the state of the art has recently advanced well, due to the available test and actual data on the equipment behaviour during earthquakes, and consequently reduced the uncertainties.

4.1.2 Seismic hazard determination

Seismic hazard analysis must include the site specific effects since seismological characteristics and the availability of active fault data and past earthquake records fluctuate site by site /6/. Usually geological investigations are accurately performed and the site ground motion features are properly evaluated /7,10/. Collection of seismic data from the past seismic history is also needed to support the analyses. The purpose is to acquire information and data for understanding, with the help of theoretical studies, how earthquakes are originated and affect the site. In practice the following four steps of analyses are performed:

- identification of the sources of earthquakes (such as faults or other seismogenetic structures);

- evaluation of the historical seismicity in order to assess the frequencies of occurrence of earthquakes of given intensity or magnitude;

- development of attenuation relationships to estimate the intensity of the site ground motion, expressed for instance in terms of peak ground acceleration;

- integration of all available information to generate a seismic hazard curve, i.e. frequency of exceedance as a function of ground motion parameters.

A flowchart for the seismic hazard determination is shown in fig. 2.

Because of insufficient data and information for full understanding of the earthquakes generation and propagation processes, considerable uncertainties are associated with the above analyses, resulting in large uncertainties in the seismic hazard estimates.

One of the largest contributors to the uncertainty in the hazard estimates is the uncertainty in the earthquake generation.

In general the existing geological evidences in the region where a site seismic hazard has to be determined, help identifying tectonic structures potentially capable to generate earthquakes. These evidences are particularly clear in some specific areas such as California, Anatolia, Japan and other high seismicity regions in the world. Even in these areas, however, large uncertainty still exists in the frequency of huge earthquakes. In general the frequency of introplate earthquakes is more uncertain than that of interplate earthquakes.

In areas such as Eastern U.S., Italy and other European countries where geo-tectonic features are less evident, different specific investigations are needed. In particular historical seismic data are used to localize epicenters of historical earthquakes, providing, therefore, good additional information for identifying seismogenetic structures. On the other hand the frequencies of historical earthquakes allow to estimate the frequencies of largest earthquakes through non linear extrapolations with an upper magnitude (or intensity) cut-off value. In this regard data information from the seismic history are also useful to support the assessment of the maximum seismogenetic capacity of identified structures.

The other largest contributor to the uncertainty in the hazard estimate is the uncertainty in the attenuation models /6/, which relates site ground motion parameters (e.g. peak ground acceleration) with the earthquake generation data (e.g. magnitude and epicenter distance) based on historical and instrumental data on the regional seismicity.

Historical seismic data and information, therefore, may contribute to decrease uncertainties of the seismic hazard analysis in regions where they are more consistent and are referred to larger periods of the past seismic history. Different methods have been developed for including the uncertainties in the seismic hazard analysis. In general they need help of expert judgments to postulate hypotheses and assign probabilities in the used models. If different hypotheses are postulated, a family of different hazard curves is produced. Such a family of hazard curves has generally been used in past PRA applications.

Two study programs have been undertaken by the Lawrence Livermore National Laboratory (LLNL) and by the Electrical Power Research Institute (EPRI) in U.S. for developing methods and data bank to estimate the seismic hazard in all locations in the Central and Eastern U.S. area /11,12/. Both methods embody the four aforementioned steps of analysis and rely on expert judgements, but significant differences lie in the expert judgement processes (LLNL solicits judgments from individuals with little interaction among them, whereas EPRI uses teams with a great deal of interaction among the experts). In practical applications the EPRI approach led to a different treatment of the ground motion, which the experts felt less subjective and fairly well defined. The family of the hazard curves produced by the EPRI method has characteristics similar to the LLNL one, but exhibits less uncertainties.

Calculations from both methods demonstrated that a large spread exists in the family of the hazard curves, and the variability is increasingly higher in the low frequency part of the curve.

This fact reflects the difficulties in the estimation of the probabilities of strongest earthquakes, and also poses the issue that very uncertain low probability numbers might be little meaningful when compounded in PRA applications with less uncertain probabilities referred to other events (e.g. internal events). That issue suggests that results of the seismic risk estimates be presented separately from other risk contributors. It could also be argued that the meaningfulness of low probability numbers might not be the same in various regions, due to the different consistency and quality of the available seismic information and data. For instance, because of the brevity of the historical record, probabilities of large earthquakes in U.S. could not be judged much below values of the order of 10^{-3} - 10^{-4}, whereas in some European countries (e.g. Italy), the meaningfulness of the estimated probabilities could be extended down to 10^{-4} - 10^{-5}.

In spite of these difficulties LLNL and EPRI studies represent the most comprehensive effort undertaken to estimate the seismic hazard today. They provide good reference to perform similar studies in other countries. The hazard curves produced by these methods have been used in NUREG 1150 to estimate the core melt frequencies for Surry and Peach Bottom NPPs.

The LLNL and EPRI studies have also provided estimation of uniform hazard spectra for Central and Eastern U.S. sites. The uniform hazard spectra are families of site dependent frequency spectra of the ground motion at given probability values. They were developed from available earthquakes records, and are important to the plant response analysis.

4.1.3 Fragility analysis

The objective of the fragility analysis is to estimate the seismic fragility of plant structures, components and equipments /5,7/.

The seismic fragility is also referred to acceleration capacity of structures, components and equipments located at specific points of the plant. It is defined as the peak ground acceleration for which the seismic loads exceed the ground acceleration capacity of the concerned structures, components and equipments, resulting in their failure. Because there are many sources of variability in the estimation of this acceleration capacity, the seismic fragilities are expressed as fragility functions in which probabilities are assigned to reflect the uncertainties in the fragility estimations. The fragility functions, therefore, represent the probability that structures, components or equipments fail for various seismic loads.

In deriving fragility functions much deliberation must be given to all phenomena which are responsible for the failure of the concerned structure and equipment. The fragility analysis should comprise the development of floor response spectra from the site ground motion taking into account the soil structural interactions and the dynamic property of materials (including those in the non linear field). Theoretical models are useful to determine the single parameters needed in the fragility analysis, but quite often the analyst is forced to use simplified methods and to loose, therefore, the richness of details that could be obtained.

Fragility functions for generic categories of equipment and structures have been developed using information on the plant design, plant responses calculated with simplified methods, experimental data and data obtained from extensive survey of expert judgments. The experimental data were obtained from the results of component's manufactures qualification tests, independent testing failure data and data from generic surveillance programs including equipment performance during past earthquakes. All these data were statistically combined with the expert opinions data in order to produce the fragility curves for each one of the generic categories.

A set of generic fragility data was provided in the Seismic Safety Margins Research Program (SSMRP) by LLNL /13/. Efforts to collect fragility data have been continued especially in the United States (e.g. by Brookhaven National Laboratory) /14/.

Despite the fact that today the state-of-the-art seems to be advanced enough, the fragility analysis remains still subject to large uncertainties that must be recognized in all subsequent analyses. This conclusion means that care must be taken in using numerical fragility estimates. Major difficulties have been met in developing fragility estimates for certain components such as relays, pressure switches, contactors and related equipment that could chatter during large earthquakes. Specific studies /15/ have demonstrated that these components may be important in some PRAs and thus the analysis should become very detailed. It should be noted that some of those chatterings are recovered easily but others are not /6/. When seismic PRA includes the effects of chattering, the possibility of the recovery should definitively be taken into account in the PRA model.

Some past PRAs performed simplified seismic analyses (Zion, Indian Point 2 & 3, Limerick, Seabrook, Oconee, and Millstone3) using generic fragility data provided by Ravindra and Kennedy /16,17/ and documented in the "PRA Procedures Guide" /2/. In these studies fragilities were expressed in terms of median ground acceleration capacity, together with two numerical factors representing the variability and uncertainties of the median value.

The variability of the seismic loads resulted typically from various propagation phenomena of the site ground motion.

The uncertainties in the estimation of the response of structures and equipment resulted mainly from lack of data and experience especially in the field of high acceleration values. The variability of the seismic loads also included the variability of the expected site ground motion spectra. A detailed determination of the building and component seismic response was performed for Zion plant within the frame of the Seismic Safety Margin Research Program (SSMRP) at LLNL in U.S. /13,18/. Estimations were done for peak ground accelerations at various probability intervals of the hazard curve. They formed a valuable basis for assessing uncertainties and assigning variability and correlations in responses.

Also in NUREG 1150 detailed structural analyses were performed to support fragility estimations of all important safety related structures of the examined plants (Surry and Peach Bottom). In addition, an analysis of liquefaction for the underlying soils was also performed. The analyses used earthquakes time histories to determine the vibratory motion in each part of the plant. The peak ground accelerations of real earthquakes records were anchored to site hazard curves to perform the probabilities analysis. The records were derived from western earthquakes in U.S. whose frequency spectral shape, therefore, is typical of those regions. The implications resulted from the use of site dependent uniform hazard spectra, instead of western earthquake records, have not been evaluated in NUREG 1150.

4.1.4 System analysis

The system analysis is the final part of the seismic analysis in level 1 PSA. The frequencies of accident sequences, plant damage states and core melt are calculated on the basis of the hazard analysis outcomes and fragility data. The method is conceptually identical to the traditional method of event tree and fault tree analysis used in all PRAs for internal events except for the necessity of iterating calculations for every level of ground motion intensity. However the details of the analysis could be very different, because correlated common failures are expected during earthquakes (e.g. cascading failures of piping support structures and simultaneous component failures due to correlation of responses) and also because the sequences could involve combination of seismically and non seismically induced failures in various equipments and structures of the plant. In addition data base on human failures does not take into account the possibility of increased error rates during large earthquakes. That could force the analyst to make assumptions that are arbitrary and highly uncertain.

In NUREG 1150 a simplified method was used for the accident analysis of Surry and Peach Bottom plants. This method is based on results of two already mentioned NRC sponsored programs at LLNL /11,13/.

4.1.5 Uncertainties analysis

The probability distributions of individual parameters assessed in the seismic analysis can be together combined in order to yield frequency distributions of accident sequences, plant damage states and total core melt. This process can be performed using various techniques like for internal events.

In NUREG 1150 studies the uncertainty analyses were performed using families of seismic hazard curves (from both LLNL and EPRI) and fragility functions obtained with the help of plant response calculations. Some concern however has to be expressed on the methods described in par. 4.1.3 to perform the response analysis, and in particular on the manner in which calculations correlate the potential damage from earthquakes with the magnitude, frequency content and duration of the motion. In this regard detailed response analysis (including non linear effects) should made use of magnitude dependent spectral shapes to remove excessive conservativism and to evaluate more realistically the seismic response of the plant. In addition, the peak ground accelerations used as input for the response analysis are not good indicators of the damages produced by earthquakes, especially in ductile structures and components, since low magnitude events could have large accelerations at high frequencies, and so a little damage is expected on these structures and components.

4.1.6 Presentation and utilization of results

The mean values of seismic core damage frequencies calculated in PRAs for seven U.S. Nuclear power plants are shown in table 1. They have been published in NUREG/CR/5042, Supplement 1 /19/ and reproduced in NUREG 1150. The seismic contribution (in %) to the total core damage frequency and the dominant earthquake level are also indicated in table 1. In order to understand the impact of uncertainties on the core melt frequencies fig. 3 and 4, reproduced from NUREG 1150, show results of uncertainty analyses. The figures report the core melt frequency ranges calculated for internal events, seismic events (using LLNL and EPRI hazard curves) and fires. Values of mean, median, 5th and 95th percentiles are given in table 2. Fig. 5 shows results of analysis for six PWRs /20/. They are indicative of the contribution of earthquakes, and of other events as well, which is significantly different plant by plant.

A clear conclusion that can be derived from the examination of fig. 3 and 4 is that the contribution of seismic induced core melt frequencies overlaps with distribution of other initiators reflecting its higher uncertainty. In this regard the mean value would better characterize point estimates of the core melt frequencies if needed.

In addition the results address that full range of uncertainties should be taken into account in decision making, engineering insights and understanding of the integrated plant response to seismic events.

References

1. USNRC, "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (NUREG-75/014), October 1975.

2. USNRC, "PRA Procedures Guide", Report NUREG/CR 2300, January 1983.

3. USNRC, "Severe Accidents Risks: An Assessment for Five U.S. Nuclear Power Plants", NUREG 1150 Vol. 1,2 and 3, December 1990.

4. M.P. Bohn and J.A. Lambright, "Procedures for External Event Core Damage Frequency Analysis for NUREG 1150",

Sandia National Laboratories, NUREG/CR-4840, SAND88-3102.

5. R.J. Budnitz, "Recent Developments in Methodology and Applications for Seismic PRA", paper presented at PSA '87, ENS/ANS International Topical Conference on PSA and Risk Management, Zurich (1987).

6. H. Shibata, K.Abe, "Discussion of Seismic Risk Analysis Issues in Japan Raised by Recent research at JAERI", PSA '89 Intl. Topical Mtg.-Probability, Reliability, and Safety Assessment, Pittsburgh, (April 1989).

7. M.K. Ravindra, "Seismic Probabilistic Risk Assessment and its Impact on Margin Studies", Symposium on Current Issue Related to Nuclear Power Plant Structure, Equipment and Piping. North Carolina State University, Raleigh, N.C. December 10-12, 1986.

8. R.C. Bertucio and J.A. Julius, "Analysis of Core Damage Frequency: Surry Unit 1, Sandia National Laboratories, NUREG/CR-4550, Vol. 3, Rev. 1, SAND86-2084, to be published.

9. A.M. Kolaczhowski et al., "Analysis of Core Damage Frequency: Peach Bottom Unit 2, "Sandia National Laboratories, NUREG/CR-4550, Vol. 4, Rev. 1, SAND86-2084, to be published".

10. R. McGuire, "Seismic Ground Motion Hazard at Limerick Generating Station", Report Prepared for NUS Corporation (May 1982).

11. D.L. Bernreuter et al., "Seismic Hazard Characterization of 69 Nuclear Power Plant Sites East of the Rocky Mountains", Lawrence Livermore National Laboratory, NUREG/CR-5250, Vols. 1-8, UCID-21517, January 1989.

12. Seismicity Owners Group (SOG) and EPRI, "Seismic Hazard Methodology for the Central and Eastern United States", EPRI NP-4726, July 1986.

13. G.E. Cummings, "Summary Report on the Seismic Safety Margins Research Program", Lawrence Livermore National Laboratory, NUREG/CR-4431, UCID-20549, January 1986.

14. K.K. Bandyopadhyay, et al., "Seismic Fragility of Nuclear Power Plant Components (Phase II)", NUREG/CR-4659, (1990).

15. R.J. Budnitz, H.E. Lamber, and E.E. Hell, "Relay Chatter and Operator Response After a Large Earthquake: An Improved PRA Methodology with Case Studies", Report NUREG/CR-4910, Future Resources Associates, Inc. Berkeley, California (1987).

16. R.P. Kennedy and M.K. Ravindra, "Seismic Fragilities for Nuclear Power Plant Risk Studies", Nuclear Engineering Design 79 (1984), pp. 47-68.

17. R.D. Campbell, M.K. Ravindra, A. Bhatia and R.C. Murray, "Compilation of Fragility Information from Available Probabilistic Risk Assessment", UCID-20571, Lawrence Livermore National Laboratory (September 1985).

18. M.P. Bohn et al., "Application of the SSMRP Methodology to the Seismic Risk at the Zion Nuclear Power Plant", Lawrence Livermore National Laboratory, NUREG/CR-3428, UCRL-53483.

19 P.G. Prassinos, "Evaluation of External Hazards to Nuclear Power Plants in the United States - Seismic Hazard", Lawrence Livermore National Laboratory, NUREG/CR-5042 Supplement 1, UCLD-21223, April 1988.

20. B.J. Garrick, "Lessons Learned from 21 Nuclear Plant PRAs", Probabilistic Safety Assessment and Risk Management, PSA '87, (September 1987).

Table 1 - Seismic Core Damage Frequencies from published PRAs

Plant	Type	(*) Annual Seismic CDF (mean value)	% of Total CDF	(**) SSE (g)	Dominant Earthquake Level (g)
Zion 1 & 2	PWR	5.6×10^{-6}	3	0.17	> 0.35
Indian Point2	PWR	4.8×10^{-5}	—	0.15	> 0.30
Indian Point3	PWR	2.5×10^{-5}	—	0.15	> 0.30
Limerick	BWR	4.0×10^{-6}	--	0.15	> 0.35
Millstone3	PWR	9.4×10^{-5}	68	0.17	> 0.30
Seabrook	PWR	2.9×10^{-5}	13	0.25	> 0.30
Oconee3	PWR	6.3×10^{-5}	25	0.15	> 0.15

* Core Damage Frequency
** Safe Shutdown Earthquake

Table 2 - Core Damage Frequencies for Surry and Peach Bottom

	5th	Median	95th	Mean
Surry				
LLNL	$3.92\text{x}10^{-7}$	$1.48\text{x}10^{-5}$	$4.38\text{x}10^{-4}$	$1.16\text{x}10^{-4}$
EPRI	$3.00\text{x}10^{-7}$	$6.12\text{x}10^{-6}$	$1.03\text{x}10^{-4}$	$2.50\text{x}10^{-5}$
Fire	$2.2\text{x}10^{-6}$	$8.32\text{x}10^{-6}$	$3.08\text{x}10^{-5}$	$1.13\text{x}10^{-5}$
Internal	$6.8\text{x}10^{-6}$	$2.30\text{x}10^{-6}$	$1.30\text{x}10^{-4}$	$4.10\text{x}10^{-5}$
Peach Bottom				
LLNL	$5.33\text{x}10^{-8}$	$4.41\text{x}10^{-6}$	$2.72\text{x}10^{-4}$	$7.66\text{x}10^{-5}$
EPRI	$2.30\text{x}10^{-8}$	$7.07\text{x}10^{-7}$	$1.27\text{x}10^{-5}$	$3.09\text{x}10^{-6}$
Fire	$1.09\text{x}10^{-6}$	$1.16\text{x}10^{-5}$	$6.37\text{x}10^{-5}$	$1.96\text{x}10^{-5}$
Internal	$3.50\text{x}10^{-7}$	$1.90\text{x}10^{-6}$	$1.30\text{x}10^{-5}$	$4.50\text{x}10^{-6}$

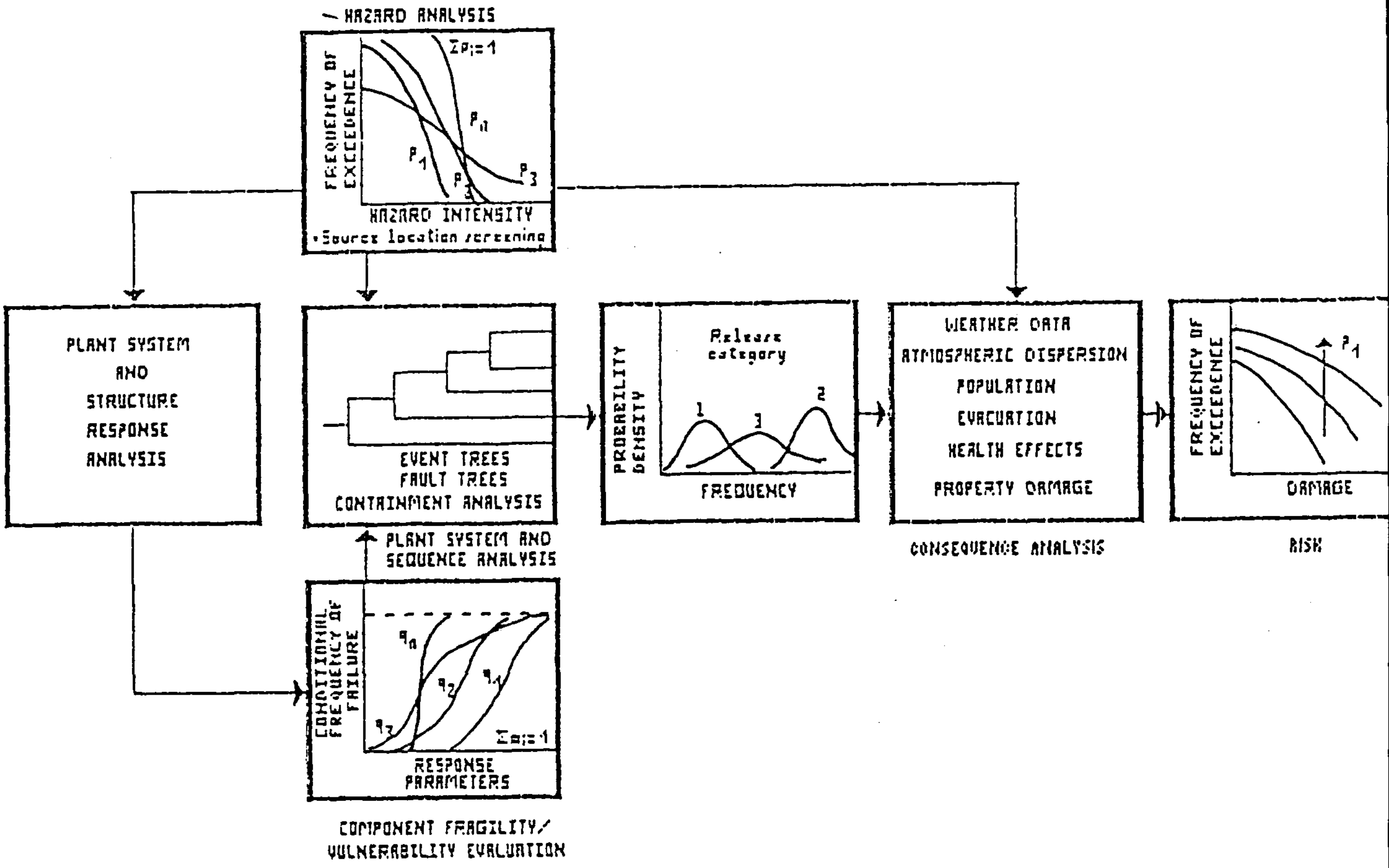
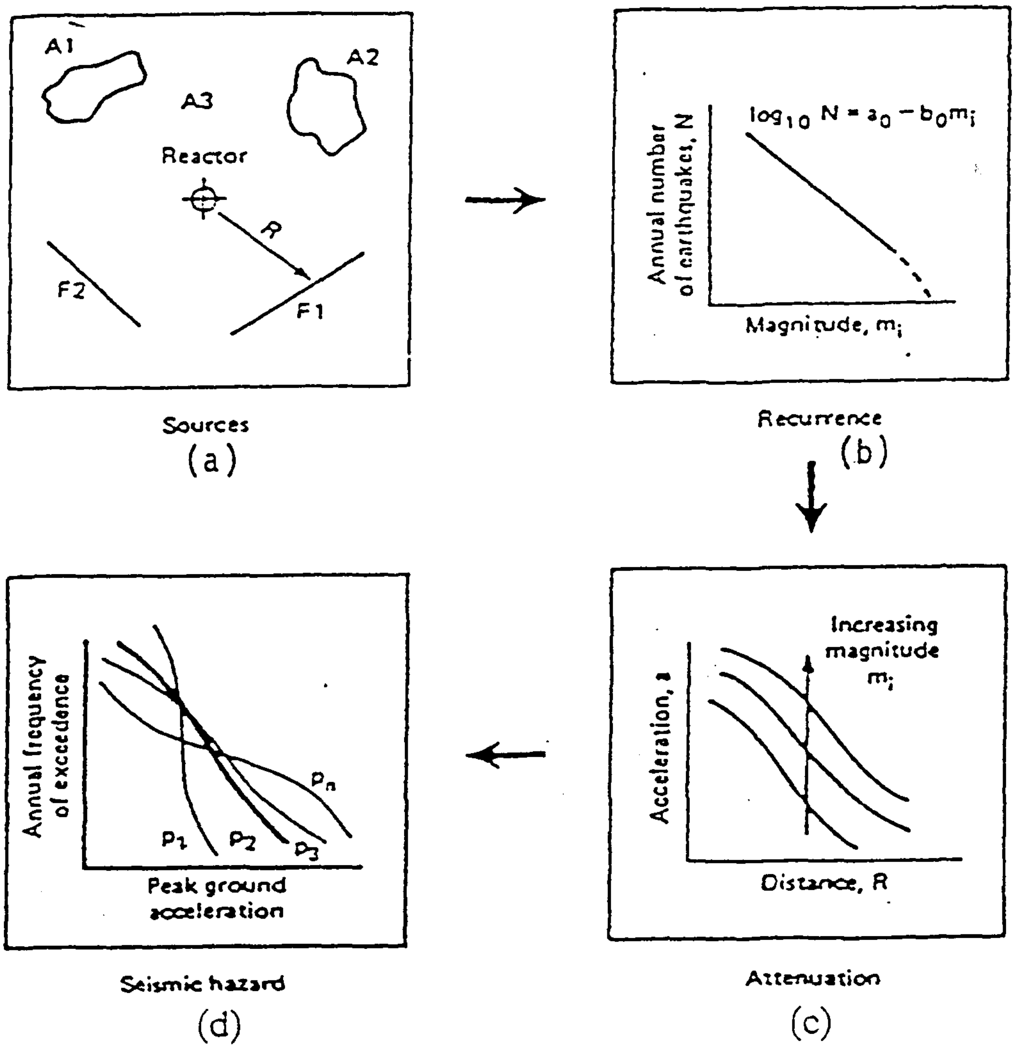


Fig. 1 Seismic Risk Analysis Flow Chart


A1
A2
A3
Reactor
R
F2
F1
Annual number of earthquakes, N
$\log_{10} N = a_0 - b_0 m_i$
Magnitude, m_i
Acceleration, a
Increasing magnitude m_i
Distance, R
Annual frequency of exceedence
P_n
P_1
P_2
P_3
Peak ground acceleration

Sources
(a)

Recurrence
(b)

Attenuation
(c)

Seismic hazard
(d)

Fig. 2 Model for Seismic Hazard Analysis

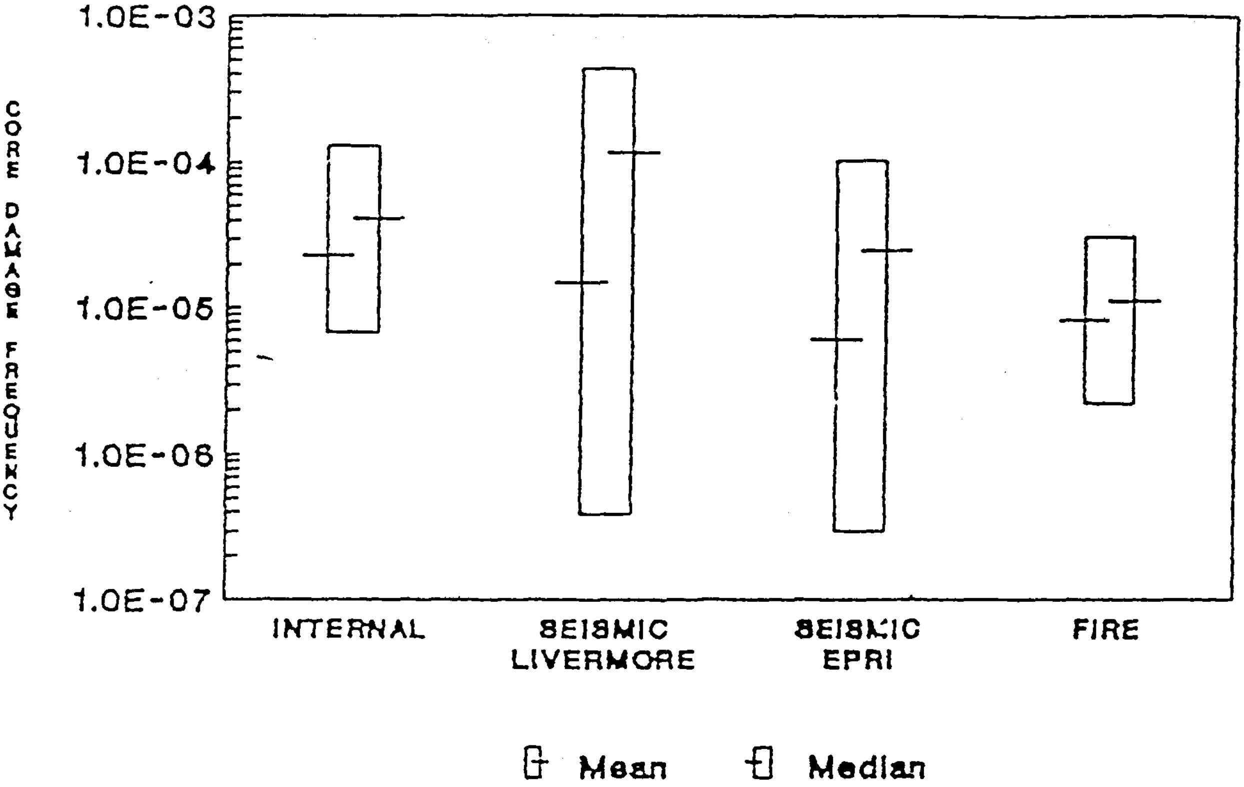


Fig. 3 Surry External Events CDF ranges

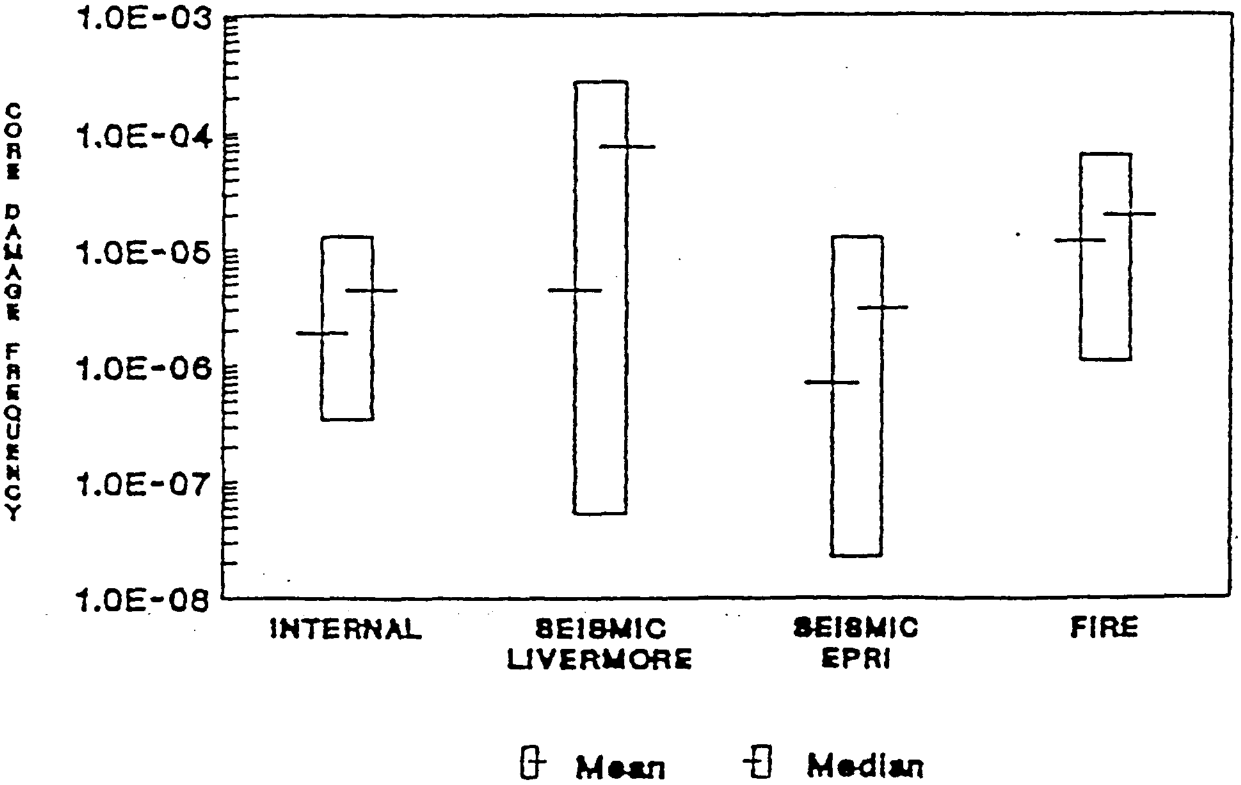


Fig. 4 Peach Bottom External Events CDF ranges

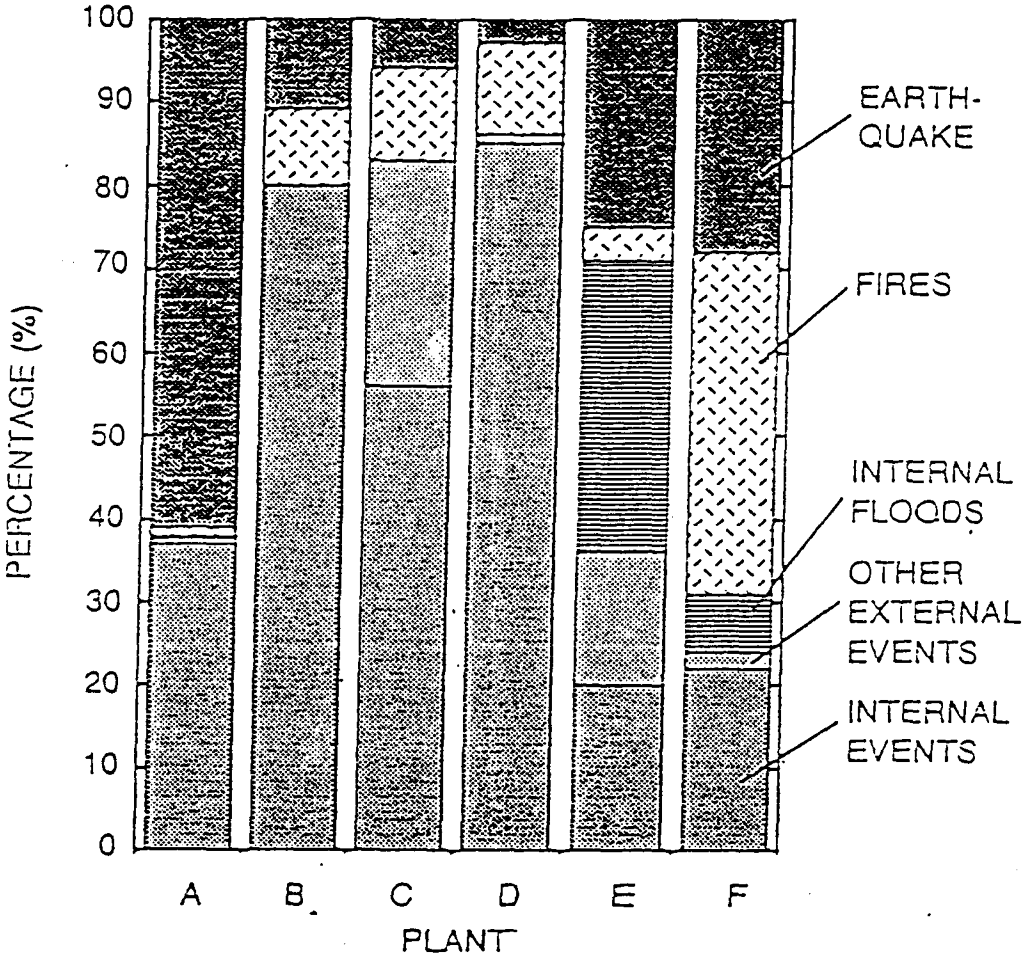


Fig.5 - Contribution of Internal and External Events to Core Damage Frequencies at six PWRs (edited from Garrick's Report)

4.2 Analysis of accidents for external floods

4.2.1 Introduction

External floods are natural abnormal events resulting directly or indirectly from severe atmospheric perturbations. Generally a severe local precipitation is considered as a cause of the flooding itself but it can also be accompanied by other effects such as water run-off from rivers and lakes, or, in coastal and near estuaries sites, wave run-up actions caused by storms, tides, seiches, strong winds and seisms. Dam failures and landslides are indirect causes of possible flooding on sites.

A review and evaluation of what is known about of the risk of core melt accidents caused by external floods is given in the NUREG/CR-5042 report /1/. The review consists of understanding the degree of protection achieved by the plant that has been designed and built to avoid damage from flooding. The basic regulations considered in the review are those that are cited in the NRC's regulatory guidance on flooding (10 CFR 50, Appendix A, General Design Criterion 2; 10 CFR 100 Paragraph 100.10 c, and 10 CFR 100, Appendix A, Section VI c; Regulatory Guides 1.27, 1.59 and 1.102). The guidance also addresses specific issues that are relevant to the flooding analysis, such as the status of the ultimate heat sink, the service water system and the electrical distribution system.

The review of the NUREG/CR-5042 report also examines the available literature on the probabilistic approach to the assessment of the degree of protection achieved in nuclear plants against external flooding. The literature includes not only the few PRAs that have been performed on actual plants in the past, but also information and methods on how to estimate the probabilities of various types of floods, and those of consequent damages potentially leading to core melt.

In this chapter current regulatory requirements to protect nuclear plants against external floods are briefly described and a short discussion is given over the general methodology used in PRAs to assess frequencies of core damages caused by these events.

4.2.2 Basic Regulatory Requirements

In simplified language, the NRC's Regulatory Guidance requires that nuclear reactors are adequately protected against external floods. The applicant is supposed to determine a parameter, so called Design-Basis Flooding Level (DBFL), and to assure that critical safety related components and structures needed for safe shutdown and maintenance of the plant, are protected also in the unlikely event that, if a site flooding occurs, DBFL is exceeded.

The DBFL is defined as a maximum elevation attained by the water during the flood, taking into account all the effects generated by the involved phenomena (winds, storms, tides, etc.). Methods and investigations to define DBLF are, therefore, site specific and require consideration of the full range of possible phenomena. Regulations provide guidance on investigations to be performed, on local and regional base, in the field of the physical and morphological characteristics that may affect the appearance and the evolution of flooding phenomena on the concerned site. Studies and research programmes are also recommended to improve the actual understanding of these phenomena.

Various types of protections (barriers) exist against flooding and are recommended by current regulations. Their functions, of course, will depend on the site and on the local flooding potential from various phenomena. When designing the protections, static and dynamic forces due to flooding effects must be evaluated. Generally, structural and inundation flooding effects are considered separately, since they may harm structures even if there is no inundation and viceversa.

Provided that sufficient warning time is available in each plant and emergency procedures exist for early shutdown, not all safety related equipment need to be protected against flooding.

4.2.3 Assessment of core damage frequencies

Basic approach

The probabilistic approach to assess the frequencies of core damages accidents caused by external floods consists in three parts:

- acquisition of the frequencies of initiating events;
- assessment of the plant systems and components vulnerability to floods that may cause on site flooding levels larger than DBFL;
- assessment of the plant response to flooding induced failures in systems and components and determination of frequencies of accidents potentially capable to provoke core melt.

Such a full approach has never been carried out in the past on any plant. Few flooding PRA studies are available in the literature /2,3,4,5,6/. They include the analysis of the flooding initiating events and only an abbreviated system analysis of the items that are threatened by the events. The methodology, in all steps, makes often use of bounding analysis based on expert judgements when the lack of information on the concerned phenomena does not allow to develop sound models to justify the meaningfulness of the results.

Determination of the flooding frequency

The determination of the frequencies of flooding in nuclear sites is the most difficult part of the accident analysis, since large floods are generally caused by rather infrequent natural phenomena.

Different types of floods, also combined among them, may occur on specific sites. The NUREG/CR-5042 report reviews the current methods for determining the frequencies of these various flooding events and also provides information on the available documentation. The methods, in general, rely on the development of the Probable Maximum Precipitation (PMP) /7/, given that a severe localprecipitation is the controlling event on all the concerned sites. PMP, however, is to be examined in connection with other possible events that might contribute to increase the on site flooding level. For sites on rivers and streams the Probable Maximum Flood (PMF) is commonly used as the major contributor to the on site flooding level /8/. In other river sites, the PMF is determined by upstream dam failures provoked by too much water in the river, ice jams, earthquakes and other natural phenomena. Flooding due to a combination of high tides, wave effects, high wind water levels, surges, seiches and so on, may affect the ocean, near estuaries and lakes sites /10,11/. Finally, ocean sites are affected by the possibility of flooding due to a tsunami.

The frequency value of the flooding events is expressed in number of events per year. Because the flooding are rare events, that value can be realistically evaluated within the range of the available historical records. A period of about 100 years, corresponding to a frequency value of about 0.01%, is the return period generally used if data are consistent. For larger return periods extrapolations are usually done beyond the range that has been considered. If extended much beyond that range, however, calculations become difficult and uncertain. They require analytical models to be combined with data using statistical methods. Expert opinions are often needed to assess the involved phenomena. Since the uncertainties increase very much for the most unlikely events, one must be very careful when assuming very low frequency values. These, in fact, could become of little meaningfulness and be improperly used.

At the present state of the art, it seems that a generally accepted methodology for developing reliable frequency values for the extreme events beyond the range of historical data, does not exist. Several research groups have been committed over the years on this matter, but the studies are continuing especially in the field of the most rare and complex phenomena. The principal difficulty is that extreme events, as large as for instance PMP, can occur only when a number of extremely rare other phenomena occur together. Correlations among them, however, are not well understood. In particular it seems that it is not adequate to assess the probability of a very large rainfall (e.g. hurricane) from the knowledge of short duration extreme rainfall data, without using a sound model of all the involved phenomena. The scarcity of phenomena could make it necessary an appropriate combination of them, since a simultaneous occurrence of two or three events could be less unlikely than the occurrence of an extreme single event.

In case of dam failures, for which the analysis is almost entirely dependent on dam construction and features, the frequency of events that would produce the maximum flood downstream reactor sites is function of extreme conditions that are difficult to find in the literature. Even if calculations for a modern and well engineered dam produced a very low value (about 10^{-6} per year) /12/, data for dams that are available in the literature do not justify values smaller than 10^{-3}.

In any case, for all the little known events, bounding calculations allow to quantify more defensible frequency values. Conservative models and hypotheses, that are judged to be acceptable by the experts, are used to increase the reliability of results. There are also a number of methodologies available for quantifying the values in a formal sense. A good example is a NRC sponsored study /13/ in which a formal mathematical approach is suggested for determining not only the flood frequencies, but also other related parameters. The approach, however, does not avoid the uncertainties due to the lack of data and correlations among the involved phenomena.

System analysis

The system analysis is to quantify the core damage probability given a flooding event large enough to cause a damage on the plant.

The analysis is to work out event trees that incorporate the response of relevant safety equipment involved in flooding initiated sequences. Flooding fragility data, expressed in terms of conditional probabilities for specific safety functions failures at various flood levels, would be obtained through the vulnerability analysis of the plant safety systems and components. The functional event trees would allow to make a systematic study of the system response to the initiating events so that, through combinations of failures, various paths leading to core damage could be identified and quantified in terms of probability. Fragility data, however, cannot be easily obtained because there is no realistic world data base, nor theoretical models exist for understanding the system and component behavior during exceptional inundations. Expert judgements could be used in place of theoretical calculations, and a bounding approach with conservative assumptions could give support to probabilistic estimations.

A bounding analysis, as performed in some existing PRAs /2,3,4,5,6/, proceeds from the assumption that some inadequate warning time exists for a postulated flood. A list of equipment and structures that could be either inundated or threatened by the flood, can be then identified. The analysis should demonstrate, in a convincing bounding way, that in case of the total loss of all such threatened equipment and structures, there is still enough capacity to achieve safe plant shutdown conditions. In a probabilistic language it means that the remaining combinations of failures leading to potential core melt, are of sufficient low probability, taking into account the frequency of the initiating events. The demonstration could be supported giving credit to specific safety functions performed by all possible alternative means, as appropriate, or using sound engineering judgements to assure that structural threats to building foundations would not necessarily compromise the equipment dependent on the structure.

Based on the discussion made above, it may be concluded that the methods to determine the conditional 'probability of core melt upon external flooding do exist and are in line with approaches followed in PRAs for other events. Unfortunately the few limited applications made of these approaches do not allow to state that a general consolidated methodology is available

Presentation of results

In the PRA literature, the external floods analyses are not frequent. Table 1 reports the values of the flooding frequencies and estimates of the core damage frequencies obtained in PRAs for 14 US nuclear plants. Table 1 also indicates the type of site and the flooding of concern for each of these plants. In general the results show that the core damage frequencies are insignificant or very low values. It must be pointed out, however, that the analyses have been performed, in mot cases, by using only qualitative and semiquantitative arguments. Care should however be exercised when comparing these results with each others, since different methodologies and data bases are often used in the analyses.

References

1. C.Y.Kimura, R.J. Budnitz, "Evaluation of External Hazards to Nuclear Power Plants in the United States" NUREG/CR-5042, UCID-21233, December 1987.

2. W.R. Cramond, D.M. Ericson, Jr., and G.A. Sanders, Shutdown Decay Heat Removal Analysis of a Babcock and Wilcox PWR Case Study" NUREG/CR-4713, March 1987.

3. W.R. Cramond, D.M. Ericson, Jr., and G.A. Sanders, "Shutdown Decay Heat Removal Analysis of Westinghouse 2-Loop PWR-Case Study", NUREG/CR-4458, SAND86-2496, March 1987.

4. S.W. Hatch, D.M. Ericson, Jr., and G.A. Sanders, "ShutdownDecay Heat Removal Analysis of a General Electric BWR3/Mark I - Case Study", NUREG/CR-4448, SAND85-2373 March, 1987.

5. G.A. Sanders, D.M. Ericson, Dr., and W.R.Cramond, "Shutdown Decay Heat Removal Analysis of a Combustion Engineering 2-Loop PWR - Case Study", NUREG/CR-4710, 1987.

6. G.A. Sanders, D.M. Ericson, Jr., and W.R. Cramond, "Shutdown Decay Heat Removal Analysis of a Westinghouse 3 - Loop PWR Case Study", NUREG/CR-4762 March, 1987.

7. National Weather Service, U.S. National Oceanographic and Atmospheric Administration, "Seasonal Variation in the Probable Maximum Precipitation East of the 105th Meridian for Areas from 10 to 1000 Square Miles and Durations of 6,12,24 and 48 Hours", Hydrometeorological Report N° 33 (1956).

8 Work Group on Probable Maximum Flood Risk Assessment, under the direction of the Hydrology Subcommittee of the Interagency Advisory Committee on Water Data, "Feasibility of Assigning a Probability to the Probable Maximum Flood", Office of Water Data Coordination (1986).

9. U.S. Army Corps of Engineers, "Engineering and Design - Policies and Procedures Pertaining to Determination of Spillway Capacities and Freeboard Allowances for Dams", Engineering Circular Number EC 1110-2-27, Change I (19 Feb. 1986).

10. V.A. Myers, "Joint Probability Method of Tide Frequency Analysis", Environmental Science Services Administration, U.S. Dept. of Commerce, Technical Memorandum WBTM Hydro11 (1970).

11. F.P. Ho, R.W. Schwerdt, and H.V.Goodyear, "Some Climatological Characteristics of Hurricanes and Tropical Storms, Gulf and East Coasts of the United States", National Weather Service, U .S. National Oceanographic

and Atmospheric Administration, Technical Report NWS 15 (1975).

12. Electric Power Research Institute/Nuclear Safety Analysis Center and Duke Power Company, "Oconee PRA, A Probabilistic Risk Assessment, of Oconee Unit 3", in 4 volumes (1984).

13. L.E. Borgman, "Feasibility of Quantitative Assessment of Available Margins Inherent in Flood Protection of Nuclear Plants", U.S. Army Engineering Waterways Experiment Station, NUREG/CR-2879 (1983).

Table 1 CDF of Accidents due to External Events

Plant	Site type	Flooding level	Flood of concern	Flood frequency (per year)	Core Melt frequency (per year)
Zion	Lake	——	Rising lake level with wave run up	Insignificant	Insignificant
Indian Point 1&2	River	13,1 ft	Water overflow	3×10^{-3}	Extremely small
Limerick	Normal	-----	Local precipitation	Negligible	Negligible
Millstone 3	Ocean	-----	Tide and local precipitation	Insignificant	Insignificant
Oconee 3	Downstream dam	-----	Dam failure	2.3×10^{-5}	2.3×10^{-5}
Point Beach	Lake	a) +8,42 ft b) + 16 ft	Rising lake level Rising lake level with wave run up	1×10^{-10} $2 X 10^{-8}$	NA NA
Turkey Point	Ocean	a) $>$ 18 ft b) $>$ 20 ft c) $>$ 19 ft	Hurricane storm surge " " " " " "	2×10^{-4} 6×10^{-5} 1×10^{-4}	2×10^{-4} (*) 1×10^{-5} (**)
St Lucie	Ocean	a) + 19 ft b) + 22 ft	Hurricane storm surge Hurricane storm surge with wave run up	2×10^{-7} 2×10^{-6}	9×10^{-8} 2×10^{-6}
Quad City	River	----	Water overflow	$< 7 \times 10^{-7}$	NA
Arkansas Nuclear One 1	River Reservoir	+ 361 ft	Water overflow	$< 7 \times 10^{-6}$	NA

(*) Without off site power recovery
(**) With off site power recovery

4.3 Accident analysis for internal floods

4.3.1 Introduction

Internal floods are typically caused by the failures or incorrect operations of plant system components such as piping, tanks or vessels containing water. The occurence of these events may threaten the operation of plant safety systems and initiate accident sequences potentially leading to core melt.

Indeed the evaluation of the plant systems response to internal floods is performed in a similar manner as in the internal events analysis. The only major difference resides in the potential to provoke common cause effects that is a particular feature belonging to all external events. For this reason, while performing PRAs, internal floods like internal fires, are usually included in external events category.

Although in the past some significant floods have occurred in LWR plants /2/ only a few examples exist in the PRA literature where these events were extensively treated. One of the best known analysis is included in the PRA for the Limerick Power Station /3/. This analysis concluded concervatively, mainly through bounding analyses, that contribution to risk of internal floods is small. Similar studies conducted for Surry and Peach Bottom Power Stations in the NUREG 1150 report /4/ obtained the same results.

4.3.2 Methods of flood analysis

The determination of flood induced initiating events is typically made by manyfold iterative screening process. It is usual that the mapping of flood source locations are confined to compartments containing significant amounts of water sources or grossing water pipes. However the electrical and instrument rooms furnished with sprinkler facilities pertain to the mapping scope as well. The identification of the flood spreading routes are an essential part of the flood analysis, too.

The screening of the compartments is usually made based on factors such as the existence of flood sources, flood sensitivity of the equipments, location of the equipments and the rising of the water level in the room. The consequences resulted from the loss of equipment are an important aspect in the screening ie. the question is, does the failure of components result in a plant transient or an obligation to shut the plant down.

Only flood events resulting in both plant transient and a failure or partial failure of safety related system are regarded as a flood initiating event. This is important in order to avoid double counting, of initiating events because part of flood events, such that do not cause equipment failures, pertain to the internal initiating events.

In general terms the internal flood analysis consists of three major steps as follows:

- Determination of the internal flood events frequencies (hazard analysis)

- Determination of failure probabilities attributable to internal floods for each key component or system in the plant (fragility analysis).

- Analysis of flood induced accidents and estimation of core melt probabilities (plant response analysis).

Procedure and recommendations to perform the internal floods analysis in PRAs are discussed and well documented in the NUREG/CR 2300 report /1/.

<u>Determination of flood frequencies</u>

The internal flood hazard analysis is to provide a quantitative estimate of flood frequency in relevant plant areas. The following definitions are generally used to identify the flood severity:

1. <u>Small</u>: when water floods into valve pits instrument housing and small component locations (hundreds of gallons).

2. <u>Moderate</u>: when flooding water covers the floor of typical pump rooms with a few feet layer (several thousands of gallons).

3. <u>Large</u>: when flooding water covers the floor of large rooms with a few feet layer or deeply submerges typical pump rooms (ten of thousands of gallons).

4. <u>Very large</u>: when flooding water comes from the rupture of circulating water or service water piping (hundreds of thousand of gallons).

To some extent the flood analysis method is consistent with the fire hazard analysis. In fact it firstly requires to identify those important plant areas where the existence of flooding conditions have a great impact on the operability of key safety equipment and components. The locations where floods are most likely to start (source locations) must also be identified and the possibility that the flooding will propagate from one location to another should be evaluated as well. In the internal flood hazard analysis specific sources of flooding can easily be detected and enumerated and flood propagation is very likely to occur. This aspect must be taken into account in the screening methods to determine the relative importance (ranking) of each location at postulated floods conditions. In this regard a fault tree may be developed on the assumption that the postulated flood results in a failure of various systems or sub-systems located in different rooms or compartments. This allows to rank the locations in terms of the impact that the failures have on both initiation of accident sequences and mitigation of generic initiating events.

After the important impact locations have been determined it is necessary to identify the flooding source locations and evaluate their potential to propagate to important impact locations selected by the screening analysis. This analysis, that is plant specific, implies to know how much water is available and where are the major water sources, such as tanks and systems that supply, circulate and process the water.

When source locations have been identified, the frequency of various flood conditions at the selected important impact locations may be estimated using data from the Operating Experience /2/. Data are statistically combined and Bayesian procedures are used to express the uncertainties associated with the most severe events and the floods propagation.
Furthermore it should be considered the possibility to terminate floods through mitigating and recovery actions e.g. shutting down pumps and closing isolation valves.

Fragility analysis

The fragility analysis for internal floods is to estimate the conditional probability of failure for relevant equipment and components. Methods to develop fragility data for flooding conditions are, in principle, similar to those applied to other external events. This entails the review of the operating experience and experimental tests, as well as the results from theoretical calculations.

Indeed the methods above have not reached a high level of maturity in PRA applications, especially for the most rare events. To some extent they are mostly used in the seismic fragility analysis (see chapt. 1), and sometimes also for estimating the fragility of structures subjected to extreme winds and wind generated missiles. In context of floods they would imply calculations of structural loads and evaluations of system integrity accounting for the unique characteristics of the flood impact. This includes wave run-up, missile striking, sliding, hydrostatic loading, leakages, and, for the less severe floods, the loss of electrical isolation in cabinet and cable trays and also the blockage of cooling water intakes by water transportted trash. At present however no example is known to exist in regard to the application of these methos to floods.

Due to the lack of experience and information on the actual systems failure mechanism resulted from floods, bounding assumptions with the help of expert judgements can be made. A conservative approach is to assume that components and equipments located in critical areas are failed if flood propagates into that area.

Plant response analysis

The objective of the plant response analysis is to estimate the frequencies of core melt accidents initiated by flooding in important impact locations as identified by the flood hazard analysis. This phase of the flood accident analysis uses the event tree and fault tree methods currently used for all internal events. Once a transient or an accident sequence has started the response of the involved system, equipment and component should be evaluated accounting for the common cause failures and system dependencies attributable to floods.

4.3.3 Concluding remarks

In the flood accident analysis for the Limerick Power Generating Station a deep investigation was performed to identify all relevant areas that could be affected by internal floods. These areas are the turbine enclosure, the diesel generator enclosure, the reactor enclosure, the control system enclosure and the spray pond pump building. A rough bounding analysis was carried out for each of the aforementioned areas reflecting the worst case of the flooding effect. More refined analyses were conducted only when significant risk potential assessed by the screening analysis was judged to exist.

The results of analysis which to the large extent was a bounding analysis, indicated that the core melt frequency of transients and small LOCAs induced by flooding is moderate (about 4 percent of the core melt frequency of all initiating events belonging to the same category).

This study concluded that internal flooding has a negligible effect on the overall core melt frequency and risk at the Limerick Power Generating Station.

The general conclusion that may be derived from all available application is that internal floods are usually not significant contributors to core damage probabilities, provided that some protection measures have been taken. The measures, at preventive level, are addressed to plant layout and pipes design. At mitigative level the protection measures concerning the floor, walls and ceiling penetrations seals are related to adequate design and design standards. It is also important to prevent by adequate lay-out design the floods from spreading between redundant safety systems. Flooding alarms and floor and equipment drains are to prevent accumulation of flood water in flooding sensitive areas. Particular care should be devoted to protect electric equipment that could be damaged by floods. Detailed protection measures against internal floods in a specific plant must be evaluated on the basis of national regulations and accounting for accident analysis results /5,6/.

References

1. USNRC "PRA Procedures Guide", NUREG/CR-2300, January 1983

2. Verna B.J., "Nuclear Power Experience", 1982

3. NUS Corporation: "Severe Accidents Risk Assessment, Limerick Generating Station", prepared for Philadelphia Electic Company, April 1983

4. USNRC "Severe Accident Risk: An Assessment for Five" U.S. Nuclear Power Plants, NUREG 1150 Vol. 1, 2 and 3, December 1990

5. American Nuclear Society, "Standards for Determining Design Basis Flooding at Power Reactor Sites", ANSI N-170-1976

6. URNRC "Flood Protection for Nuclear Power Plants", Regulatory Guide 1.102, Revision 1, 1976

7. Probabilistic Safety Analysis Procedures Guide, NUREG/CR-2815 Vol. 2, Rev. 1, Sections 8-12 (1985)

4.4 Fire risk analysis

4.4.1 General

Probabilistic risk assessments (PRA) have shown that fires have a significant impact on the safety of several nuclear power plants. The differences between plants, however, are significant which implies that the insights received from the fire analysis of specific plant cannot directly be transferred to another plant.

The fire analysis pertains to levels I and II of PSA and are usually regarded as a supplementary analysis of level I like other external events analyses.

It is foreseen that in the future the fire analyses are supposed to be made for each nuclear power plant due to the significant contribution of the fires to the core damage frequency.

4.4.2 Methods of fire analyses

The purpose of the fire analyses is to evaluate the contribution of fire events to the core damage frequency and to the failure frequency of containment isolation as well as amount of the release of radioactive material to the environment. The fire analysis methods can be divided into four quite independent parts such as

- fire hazard analysis for evaluating the critical plant compartments and frequencies of fires
- analysis of fire growth and effects of suppression activities for evaluating the behavior of fires in the critical compartments
- system analysis for evaluating the frequency of fires leading to serious accident sequences that can result in core damage
- analyses of the frequency of loss of containment isolation capability and source term of radioactive releases to the environment.

Fire hazard analysis

Fire hazard analysis is usually initiated by surveying compartments. Approximate "importances" are assigned for compartments using as main criteria the equipment, fire load and the extinguishing arrangements. The compartments where fires do not cause a significant impact on reactor safety are excluded from further analysis.

Some examples of fire hazard analysis methods are outlined below in few details.

The number of safety related equipments and systems is evaluated in the method of Callucci /2/ to estimate the impact of the fire damaged safety systems on the loss of safety functions. The results of level I PSA are worthwhile in evaluating on how many redundancies the fire is affecting. Some compartments can be excluded by failure analysis.

The compartments which contain equipment exposed to the damage of fire are identified in the method of Kazarian and Apostolakis /3/. Supposing the loss of function of these equipment PSA models are used to assess whether these events lead to the initiating events, LOCA or transient. It has to be kept in mind that in context of almost all fires, the reactor scram is made. If the consequence is LOCA or a transient, several safety systems are challenged in managing the situation.

If the fire causes an initiating event, the next question is, whether the fire can result in failures preventing the functioning of safety features such as

- residual heat removal
- control of reactivity
- the control of reactor cooling system and the maintenance of the reactor coolant inventory.

Because the reactor scram is usually very reliable, the consideration is mainly focused on the residual heat removal and other cooling functions. The most critical fires can prevent both the residual heat removal and the reactor cooling but a part of fires affects only one of these functions and their contribution to the total risk could be small.

All compartments are not definitely considered in this method. However, if the possibility of the spread of fire from one room to another is substantial, more exact methods ought to be used. One possibility is to put the location indication of components to the fault tree and to search the minimal cut sets based on the location of components. This procedure is possible within several PSA computer codes today.

The above mentioned two methods can be supplemented by additional studies. Some methods classify the rooms based on the fire loads and ignition sources located in the rooms and give the weighting factors for the rooms. In addition the extinguishing possibilities, properties of the neighboring rooms, ventilation etc. can be taken into consideration (Berry et al) /10/.

The methods outlined above require sometimes much resources and at least level I (and II) PSA.

Fire frequencies

The fire frequencies are assigned for quantitative reliability and risk assessments after identification of rooms sensitive to fire. The fire statistics for nuclear power plants are scarce including mainly U.S. plants /1/.

Analyses for fire events and fire frequencies are published also for non-nuclear power plants and insurance companies maintain statistics for industrial fires. In spite of the differences between conventional and nuclear industry, it is worthwile to acquire the fire frequencies from various sources for comparison.

Many different factors are taken into account in the statistical analyses of fires such as

- place of fire
- circumstances in catching fire
- reason for fire
- extent and duration of fire
- function of extinquishing equipment.

The identification of factors above is of importance in evaluating whether the fire can occur in a specific place. In this evaluation the results obtained in the screening of rooms (fire loads and their location, the procedures in this room etc.) are utilized. It is, however, worthwile to notice that much subjective engineering judgement is always associated with evaluation of this sort and to confess the uncertainties pertaining to the evaluation. The uncertainty caused by subjective evaluation methods can be analyzed by existing inference procedure based on Bayesian method /5-6/.

Apostolakis, /7/, has studied fire frequencies and gives the frequencies per year and room. The estimates are based on Bayesian method and U.S. experiences. The fire frequencies of Apostolakis are in table 1.

Table 1. Fire frequencies by Apostolakis

	Frequency of fire 1/a			
Location	5 % Lower limit	Median	95 % Upper limit	Mean
Control room	$3.1\cdot10^{-4}$	$3.0\cdot10^{-3}$	$1.2\cdot10^{-2}$	$4.1\cdot10^{-3}$
Cable spreading room	$1.4\cdot10^{-3}$	$6.2\cdot10^{-3}$	$1.7\cdot10^{-2}$	$7.2\cdot10^{-3}$
Diesel generator	$1.1\cdot10^{-2}$	$1.8\cdot10^{-2}$	$3.0\cdot10^{-2}$	$1.9\cdot10^{-2}$
Containment	$6.2\cdot10^{-3}$	$1.4\cdot10^{-2}$	$2.8\cdot10^{-2}$	$1.6\cdot10^{-2}$
Turbine building	$1.7\cdot10^{-2}$	$3.0\cdot10^{-2}$	$5.0\cdot10^{-2}$	$3.2\cdot10^{-2}$
Auxiliary building	$1.9\cdot10^{-2}$	$3.3\cdot10^{-2}$	$5.3\cdot10^{-2}$	$3.4\cdot10^{-2}$

In the severe accident study for Limerick the room specific fire frequencies were assigned based on the above statistics and are given in table 2 /8/.

Table 2. Fire frequencies used in Limerick PSA

Location	fire frequency 1/a
Control room	0.0018
Auxiliary equipment room, relays	0.0035
Cable spreading room	0.0018
Reactor building	0.016
Turbine building	0.012

Fire risk analysis was carried out also in Oconee PSA. In this context the fire frequency for auxiliary building, 2.3 x 10^{-2}/a, was received. This number was used for evaluating cable damages etc. /9/.

Seabrook PSA /11/, contains quite an extensive fire risk analysis as well. The fire frequencies used are given in table 3.

Table 3. Fire frequencies of Seabrook PSA

	Fire frequency (1/a)			
Location	5 % Lower limit	Median	95 % Upper limit	Mean
Control room	$1.3 \cdot 10^{-1}$	$3.2 \cdot 10^{-4}$	$1.5 \cdot 10^{-2}$	$4.9 \cdot 10^{-3}$
Cable spreading room	$7.0 \cdot 10^{-1}$	$7.0 \cdot 10^{-4}$	$2.2 \cdot 10^{-2}$	$6.7 \cdot 10^{-3}$
Auxiliary building	$5.6 \cdot 10^{-3}$	$3.5 \cdot 10^{-2}$	$1.3 \cdot 10^{-2}$	$4.8 \cdot 10^{-2}$
Turbine building	$1.0 \cdot 10^{-4}$	$1.0 \cdot 10^{-2}$	$7.0 \cdot 10^{-2}$	$1.6 \cdot 10^{-2}$
Cooling pump (1/Demand)	$1.9 \cdot 10^{-6}$	$9.0 \cdot 10^{-4}$	$4.4 \cdot 10^{-2}$	$7.4 \cdot 10^{-3}$
Diesel generator (1/Demand)	$1.0 \cdot 10^{-5}$	$3.2 \cdot 10^{-4}$	$3.5 \cdot 10^{-3}$	$7.4 \cdot 10^{-4}$

The fire frequencies used in Millstone PSA are given in table 4.

Table 4. Fire frequencies of Millstone PSA

	Fire frequency (1/a)			
Location	5 % Lower limit	Median	95 % Upper limit	Mean
Control room	$6.2\cdot10^{-4}$	$2.5\cdot10^{-3}$	$9.7\cdot10^{-3}$	$4.0\cdot10^{-3}$
Cable spreading room	$1.9\cdot10^{-3}$	$5.4\cdot10^{-3}$	$1.5\cdot10^{-2}$	$6.6\cdot10^{-3}$
Auxiliary building	$2.0\cdot10^{-2}$	$3.3\cdot10^{-2}$	$5.5\cdot10^{-2}$	$3.5\cdot10^{-2}$
Diesel generator	$1.9\cdot10^{-2}$	$3.2\cdot10^{-2}$	$5.3\cdot10^{-2}$	$3.4\cdot10^{-2}$
Containment				$1.5\cdot10^{-2}$

The fire frequencies in different tables above differ quite much from each other because the special features of the plants are taken into account. The frequencies are actually based on the same basic material.

Fire initiators and models for fire event sequences and insights received from recent PSA studies.

All fires leading to either transients (e.g. reactor scrams) or to other accident initiators (e.g. LOCA) are regarded as initiating events. In addition it is presumed that safety systems are needed in the management of transients. Fires not jeopardizing the plant safety are excluded. The fires are very often so called common cause initiators causing a transient and affecting the function of various safety systems. The nature of such events is very plant specific and no generally accepted list can be made in advance.

Not all fires lead to event sequences jeopardizing nuclear safety even if they occur in important rooms. This is caused on one hand because the most fires are small and on the other hand due to the function of extinquishing systems. The purpose of the room specific analyses is especially to clarify which kind of fires could develop dangerous.

Below typical fire initiators analyzed in the context of some PSAs are discussed.

The loss of cooling accidents caused by fires are one of the fire initiator categories. The Limerick PSA regarded two such events: LOCAs result from direct fire impact on the pipelines and interface LOCA caused by unintentionally opened valves in decay heat removal system due to fire. The first type of event is regarded highly unlikely. The latter one supposes that several valves are opened erroneously and the control and power cables are located in different rooms which makes the probability of the event small /8/.

Seabrook PSA deals with the LOCA events caused by fire. The events, however, are different from those in Limerick PSA because Seabrook is PWR plant (Limerick BWR). In PWR plants the LOCAs are caused by either by premature opening of PORVs or other isolation valves in primary circuit. In addition the burning of the seal of the main coolant pumps results in small LOCA caused by premature opening of PORV is a significant event. The possibility of LOCA caused by fire is considered also in Millstone 3 PSA. According to the analysis the events like this are possible if the fire causes short-circuit in the cables of the isolation valves of the decay heat removal system. Further the failure of PORVs have been found in case of fire /11/.

A small LOCA caused by fire is regarded in Oconee PSA. This is possible if the function of PORVs is prevented. Another LOCA possibility is found as a consequence of pump seal fire /9/. It is important to understand that the previously described LOCA events are indirectly caused by fires: the cable fire leads to the transient but preventing at the same time the function of PORVs which causes a LOCA difficult to manage. A LOCA may be caused by the leak through the systems associated with the primary circuit or as a consequence of seal fire of the main cooling pump. The leaks trough associated systems (interfacing system LOCA) can be difficult to manage, because those are not taken into consideration in training and design.

The transients resulted from fires are another important accident initiator category. These are regarded in all PSAs mentioned before.

Four transient types resulted from fires /8/ are regarded in Limerick PSA such as

- inadvertent closure of main steam isolation valve or loss of feed water
- inadvertent opening of safety valves
- turbine trip
- manual scram.

The cause for the events mentioned above is almost without exception a cable damage due to fire in a room considered.

In the Limerick PSA the events are analyzed room by room and in this context different fire ignition mechanisms are separately taken into account. In Seabrook (PWR) PSA several transient resulted from fires are taken into account. Some of the most important fire initiators lead to the loss of component cooling function which can be a consequence of fire of cable spreading room, due to fire in control room, or due to fire in component cooling pum room.

The loss of onsite power can be caused by fire. It can be caused by cable fire (several different rooms) or by fire in control room. The loss of offsite power can be brought about by the fire of turbine building. In some cases the loss of power is further followed by the loss of PORV function. The fire in cable tunnel can directly cause the reactor scram. Several different fires can cause the loss of service water as well.

The space orientated approach of Millstone PSA /12/ is very clear. Each fire in certain compartment is regarded as an fire initiator. The initiators are divided into three categories

- fire initiators not leading to an accident initiating event

- fire initiators causing initiating events that do not affect safety systems
- fire initiators causing initiating events that affect safety systems and cooling down systems.

The initiators analyzed lead to accident sequences much like those of Seabrook PSA /11/.

In Oconee PSA the initiators are analyzed by the methods of same type as in Millstone PSA. The adequate analysis of cable damages of motor operated valves is one highlight of Oconee PSA /9/.

The fire initiators of different PSA studies discussed above seem to lead to very similar event scenarios but through different routes. Even though few plants have similar layouts, their function in the transient situation is quite similar. It is, however, incorrect to apply a surrogate PSA study for substituting the PSA study of a specific plant. In all PSAs outlined above there is heavy reliance on the conventional fault tree/event tree modelling. This is quite natural solution because the fault and event trees of level I PSA can be utilized.

The event trees for the most important fire initiators are presented in Limerick PSA. Some typical fire event trees are presented here (Fig. 1-3).

The event tree related to PORV failures is presented in Seabrook PSA. The accident sequences are specified according to the time the LOCA takes place in different scenarios. In addition the logical scheme related to accident sequences due to cable fire are presented (Fig. 4-5). Other models are not presented because those conform with the other level 1 models.

In the Millstone PSA no logical models of fire event sequences are presented. In the Oconee PSA an event tree for cable-shaft fire is given (Fig. 6).

Principles of system analyses

The probabilities of fire event sequences are usually evaluated by fault and event trees. SETS program has been favoured in PSA studies including fire risk analyses. In SETS the fires are interpreted as CCFs.

The fire risk analysis can be made as well by several other programs where the dependence between fire and component is included in the location information of the component. The components in different rooms can be postulated unavailable, when the impact of fire will be taken into account. In general the reliability programs are customized and user-friendly, but different kind of dependency analyses require however experience of reliability engineering /3-4/.

A little bit different approach is introduced in the FIRENET program developed in UK. In this code the rooms and their interconnections are described by a special network. The location of control and other cables is given separately in input information. When additionally the fire frequencies and fire spreading frequencies of different rooms are given, the probabilities of different event sequences can be computed /13/.

4.4.3 Fire development analyses

The fire in a NPP is very complex phenomenon and it cannot be analyzed in great detail. A fire in a simple room can to certain extent be described in quantitative way. The fire development in a room is well discussed in ref. /14/.

The growth period of the fire starts from the ignition after which the temperature keeps rising. In the course of time the growth rate of temperature rise is accelerating and ends up to a flashover. The flashover means that all flammable surfaces catch fire in the whole room. For cellulose based materials this happens in about 500°C. After flashover the temperature is rising rapidly but reaches soon a quasi steady-state, which is determined by the air flow into the room.

During the fully developed fire the temperature and concentrations of gases are almost equal everywhere in the room and the behaviour of the fire can be discribed by a well stirred chemical reactor. The fire continues until all fuel is consumed. During the decay period before the temperature is decreasing. The fire prevention and mitigation measures are possible during the growth period before flashover. After flashover all the contents of the room are lost, and the extinguishing measures has to be concentrated on the limitation of fire spreading. For this reason one of the most important task of the fire simulation is to predict the flashover time of the fire.

For the analysis of room fire various numerical simulation programs are developed. The numerical simulation of room fires can be divided into three major categories:

A. Deterministic models
B. Stochastic models
C. Empirical models

Deterministic models (A) are based on equations the solutions of which can be used for predicting the temporal development of fire. Given the room dimensions and fire load, the gas temperature, the heating of wall structures and the production of exhaust gases can be calculated as a function of time.

The stochastic models (B) do not try to predict the temporal progress of fire. Instead the probability of ignition of targets outside the fire zone is predicted. The state of stochastic models is less developed than the other type of models. Some simulation codes exist for limited purposes.

The empirical models (C) try to simplify the development of room fire using crude model temporal curves. A good example of this is a standard fire curve ISO 834, where the temperature is supposed to grow in logaritmic way as a function of time. Another well-known type is a hydrocarbon-fire-curve. These are used for the evaluation of thermal load on structures. They cannot take into account the effect of room dimensions.

Determinisctic models can be divided into three categories:

A_1. Field models

A_2. System models (lumped parameter models)

A_3. Zone models

In the field models (A_1) the mathematical field equations including initial values and boundary conditions are written for the variables describing the fire in the room.

Their solutions are functions of the space and time. A hydrodynamic part of the equations of the field models are well known, but the turbulent flow, burning reactions and some boundary conditions are poorly known. The fires are described in field models by mass and energy source terms, the temporal behaviour of which are given based on the experiments. From these data the temperatures and flows are calculated. The field models give good results for practical purposes, if the source terms are chosen by care /43/. The complexity of input preparations and the long CPU of calculations are the biggest drawbacks of the field models. The computer time has often been so long that the potential user of results cannot afford to use these models. The field models, however, are in the long run the most promising direction for the future of fire simulation. This is due to their sound physical basis. The costs of program use decrease quickly due to handy input/output routines, as well as due to fast development of calculation speeds of computers.

The system models (A_2) describe large complex buildings, such as power plants, by the method of lumped parameters. The rooms and process components are described by time dependent variables of cells, which are constants inside a cell. These cells are nodes of the network. They are connected to each other by branches. Balance equations for them are written down and solved for the whole system. The equations are based on mass and energy balances. The solutions describe the flows in the network. The system model can not describe the fire as a such. The fire development is taken as a source term either from experiments or is computed by other models. Several system model codes are available and these can be successfully applied for nuclear power plants.

The worst drawback of these models is the labour intensive application. Preparation of the input takes plenty of time. It is worth of mentioning as a rough estimate that the evaluation of the inputs for a small nuclear power unit takes not less than one man-year. Main frame computers were traditionally needed. However, the work stations and bigger PCs can solve many of the simpler problems if a PC version of the code is available.

The zone models (A_3) try to find short cut in the simulation of fires for small systems (one or few rooms). Only the most important variables are taken into account and the others are not considered. The early zone models were either

Post flashover zone models or
Pre-flashover zone models, but nowadays

most of the models combile both features into a full fire zone models. Post flashover zone models assume that the flashover has already occurred. The earliest is the one zone model, where the fire room is regarded as a well stirred chemical reactor. The temperature and the concentrations of cases are constant in the whole room, but their temporal development is calculated based on energy and mass balances. The burning rate is restricted by the flow of oxygen into the room. These models apply well for the prediction of the production of exhaust gases and the fire resistance of structures. The programs run well on personal computers.

The simulation of the pre-flasover zone model is initiated at the moment of the ignition of the first fire compartment. The aim is to describe the development of the fire in the growth period. The increase of the burning rate is restricted by flammable material. Often it is assumed that the fire is spreading along the surfaces by a constant speed until the moment of flashover. The most important use of these zone models is to predict the time for flashover. Several simulation codes are currently used extensively /44/.

4.4.4 Numerical fire simulation codes

Numerical simulation codes available are compiled in Appendix. It is not exhaustive, because limited information is available of codes under development, and only few of them are commercially available. The programs are described in more details in the respective reference and user manuals. A recent compilation by Friedman /35/ gives a short overview on the plethora of fire development codes. It includes 24 documented codes for fire development and smoke spread.

Some promising results are obtained for NPP by applying the simulation models. The fire can be described fairly well in single or few rooms by field models. The costs of simulation, however, are so high that several analyses for one plant are out of question. The simulation of bigger systems e.q. a containment fire is still very expensive.

The whole plant without restrictions can be described by a system model, but the costs of input preparation increase rapidly when the size of system increases. To obtain adequate source terms for the fire is problematic. The verification of predictions by either system of field models are still rudimentary and is available for only one or two rooms systems. The results obtained in HDR-project show that the qualitative descriptions of system models are adequate for several variables.

The simulation costs in using zone models are reasonable, but the models are so far quite limited. The compartments of nuclear power plant are connected to each other which means that the multiroom models are needed. The distribution of fire load is often so complex (e.g. crossing cables) that the models can not describe them in many details. Only in few cases the simulation are validated by well planned experiments.

As a general conclusion is that all numerical simulation codes are still incomplete and much work is needed to bring them onto an ideal consolidated level. Fortunately, in context of PSA studies also less qualitative information is often enough and approximate results together with conservative assumptions can be significant for decision making. Second, the efforts to validate different codes for large space fire simulation have improved and also will improve the performance of the codes for quantitative predictions of fire development.

References

1. PRA Procedures Guide. NUREG/CR-2300. U.S. Nuclear Regulatory Commission, Washington, D.C. (1983).

2. Callucci, R.H.V., 1980. "A Methodology for Evaluating the Probability for Fire Loss of Nuclear Power Plant Safety Functions." Ph.D. thesis submitted to the Rensselaer Polytechnic Institute, May 1980.

3. Kazarians, M., and G.E. Apostolakis, 1981. Fire Risk Analysis for Nuclear Power Plants. UCLA-ENC-8102, may 1981.

4. Worrell, R.B. SETS Reference Manual. NUREG/CR-4212, SAND83-2675. U.S. Nuclear Regulatory Commission, Washington, D.C. (1985).

5. Pulkkinen, U., Huovinen, T., Kuhakoski, K. Combination of several data sources. In Probabilistic Safety Assessment and Risk Management PSA'87, Volume I. Verlag TüV Rheinland GmbH, Köln. (1987).

6. Mosleh, A. On the Use of Uncertain Data in Common Cause Failure Analysis. In Probabilistic Safety Assessment and Risk Management PSA'87, Volume I. Verlag TüV Rheinland GmbH, Köln (1987).

7. Apostolakis, G., Kazarians, M. The Frequency of Fires in Light Water Reactor Compartments, in Thermal reactor safe-

ty, Knoxville, Tennessee, Apr. 7-11, 1980, Report CONF-800403, NTIS. (1980).

8. Severe Accident Risk Assessment, Limerick Generating Station, Report no. 4161. Philadelphia Electric Company, NUS Corporation, Philadelphia. (1983).

9. A Probabilistic Risk Assessment of Oconee Unit 3. Vols. 1-4. NSAC-60. Palo Alto, Electric Power Research Institute. (1984).

10. Berry D.L., Minor E.E. Nuclear Power Plant Fire Protection - Fire Hazard Analysis. NUREG/CR-0654, 1979.

11. Seabrook Station Probabilistic risk Assessment. Pickard, Lowe and Garrick Inc. Irvine, Washington, D.C. (1983).

12. Millstone Unit 3 Probabilistic Safety Study. (1983).

13. Hall, S.F., Scattergood, W.M. FIRENET - A Program for Performing Probabilistic Risk Assessment of Fires in Buildings. SRD R 299. UKAEA, Culcheth. (1984).

14. S. Kumar. Mathematical Modelling of Natural Convection in Fire - A State-of-the-Art Review of the Field Modelling of Variable Density Turbulent Flow, Fire and Materials 7, 1-24 (1983).

15. K.T. Yang and J.C. Chang. UNDSAFET-I. A computer code for buoyant turbulent flow in an enclosure with thermal radiation. University of Notre Dame Technical Report TR-79002-78-3 (1978).

16. V.K. Liu and K.T. Yang. UNDSAFE-II. A computer code for buoyant turbulent flow in an enclosure with thermal radiation. University of Notre Dame Technical Report TR-79002-78-3 (1978).

17. M.J. Thurgood. COBRA-TF: A thermal hydraulic code for transient analysis of nuclear reactor components, Vol. 4: User's manual for containment analysis (COBRA-NC), Report NUREG/CR-3262, Febr. 1983.

18. D.B. Spalding. A General-purpose computer program for multi-dimension one- and two-phase flow, Mathematics and computers in Simulation, North Holland (IMACSI), Vol. XXIII, pp. 267-276 (1981).

19. J.W. Bolstad, F.R. Krause, P.K. Tang, R.W. Andrae, R.A. Martin, W.S. Gregory. FIRAC - A Computer Code to Predict Fire Accident Effects in Nuclear Facilities, in Fire Dynamics and Heat. Transfer, The 21st National Heat Transfer Conference, Seattle, Washington, July 24-28, 1983, s. 125-132.

20. H.E. Mitler. The physical basis for the Harvard Computer Fire Code, Home Fire Project Technical Report No. 34, Harvard University, Cambridge, Mas., (1978), 91 s.

21. H.E. Mitler and H.W. Emmons. Documentation for CFC V, The Fifth Harvard Computer Fire Code, NBS-GCR-81-344, National Bureau of Standards, Washington D.C., (1981), 180 p.

22. H.W. Emmons, C.D. MacArthur, R. Pape. The Status of fire modelling in the United States 1978, Proc, of the 4th Joint Panel Meeting, The U.J.N.R. Panel on fire Research & Safety, 5-9 Febr. 1979, Tokyo, p. 135-160.

23. H.E. Mitler. Comparison of several compartment fire models: an interim report, NBSIR 85-3233, National Bureau of Standards, Washington, D.C., (1985), 34 p.

24. J.A. Rockett and M. Morita. The NBS/Harvard Mark VI Multi-Room Fire Simulation, NBSIR 85-3281, National Bureau of Standards, Washington, D.C., (1986), 24 p.

25. L.Y. Cooper, D.W. Stroup. Calculating Safe Egress Time (ASET) - A Computer Program and User's Guide. NBSIR 82-2578; National Bureau of Standards, Washington, D.C., (1982), 131 p.

26. W.D. Walton, S.R. Baer, W.W. Jones. User's guide for FAST, NBSIR 85-3284, National Bureau of Standards, Washington, D.C., (1985), 31 p.

27. W.W. Jones. A Multicompartment Model for the Spread of Fire, Smoke and Toxic Gases, Fire Safety J. 9, 55-79 (1985).

28. S. Bengtson, B. Hägglund. A Smoke Filling Simulation Model and its Engineering Applications, Fire Technology 22, 92-103 (1986).

29. B. Hägglund. Simulating Fires in Natural and Forced Ventilated Enclosures, Försvarets Forksningsanstalt, FOA rapport C 20637-2.4 (1986), 42 p.

30. M. Curtat, NAT: Prediction of heat flux on structural members or building elements in case of a compartment fire, 6 p.

31. X.E. Bodard and M.R. Curtat, The CIFI Computer Code: Air and Smoke Movement during a Fire in a Building with Ventilation Ducts Network Equipment, 7 p.

32. G. Chung, N. Siu, G. Apostolakis. Improvements in compartment fire modelling and simulation of experiments, Nucl. Technol. (USA) 69, 14-26 (1985).

33. R. Dobbernack, U. Schneider. Wärmebilanzrechnungen in Brandräum unter Berücksichtigung der Mehrzonenmodellbildung (Teil III), Institut für Baustoffe, Massivbau und Brandschutz, Technische Universität Braunschweig, Heft 59, Braunschweig (1983), 96 p. (in German).

34. R. Huhtanen, Numerical Fire Modelling of a Turbine Hall, Fire Safety Science - Proceedings of the Second International Symposium, Tokyo 1988, Hemisphere New York 1989, pl 771-779.

35. R. Friedman, Survey of Computer for Fire and Smoke, Factory Mutual Research, Norwood (1990), 50 p.

36. J. B. Gahm, Computer Fire Code VI, NBS-GCR 83-451, National Bureau of Standards, Washington, D.C., 1983, 2. Vols.

37. B. Karlsson, User's Guide to DISLAYV, Department of Fire Safety Engineering, Lund University, Lund 1988.

38. V. Ho, N. Siu, G. Apostolakis, COMPBRN-III - A Computer Code for Modeling Compartment Fires, UCLA-ENG-8524, NUREC/CR-4566 (1985).

39. U. Max, Zur Berechnung der Ausbreitung von Feuer und Rauch in Komplexen Debäuden, Arbeitsbericht PHDR5.157/91 Kernforselungszeutrum Karlsruhe 1990, 151 p.

40. T. Tanaka, K. Nakamura, Refinement of a multiroom fire spread model, in: Proceedings of the 1987 ASME/ISME Thermal Engineering Joint Conference, eds. P. J. Marto and I. Tanasawa, p. 319-326.

41. G.P. Forney, L.Y. Cooper, A Plan for the Development of the Generic Framework and Associated Computer Software for a Consolidated Compartment Fire Model Computer Code, NBSIR 86-3500, NIST, Gaithersburg MD, 1987.

42. NIST Handbook 146 "HAZARD I Fire Assessment Method, 1989.

43. O. Keski-Rahkonen, E. Eloranta, R. Huhtanen, Use of numerical simulation computer codes to fire problems in nuclear power plants in Finland, Nuclear Engineering and Design 125 (1991) 377-382.

44. T. Hallberg, S. Hirschberg, M. Pedersén, D. Tannenberg (AB Asea-Atom Västerås, Sweden) and O. Åkerlund (Studsvik Energiteknik Ab, Nyköping, Sweden). Fire Risk Analysis: Status of Computer Codes for Simulation of Compartment Fires. SRE-Symposium, Otaniemi, Finland, 14-16 Oktober 1986.

Table 5. NUMERICAL FIRE SIMULATION CODES (STAND 1986)

Nr	Name of code	Development place and developer	Type of code	Main function of program	Remarks
1.	JASMINE	FIRE RESEARCH STATION, UK, G. Cox, S. Kumar	Field model	Fire development and smoke movement	3D /14/
2.	UNDSAFE	UNIVERSITY OF NOTRE DAME, USA, K. Satoh, K.T. Yang, J.R. Lloyd	Field model	Fire development and smoke spread	2D, 3D 1977, /15-16/
3.	COBRA-NC		Field/system model	Fire development in the containment of a NPP	1983, /17/
4.	PHOENICS	CHAM LTD, UK, D.B. Spalding	Field model	General 1- and 2-phase flow	1981, /18/
5.	RALOC	GESELLSCHAFT FÜR REAKTORSICHERHEIT, FRG, H. JAHN	System model	Flow in system: Three gases and water as a liquid and vapor	Different program for fire as source form, 1985
6.	FIRAC	LOS ALAMOS NATIONAL LABORATORY, USA	System model	Flows in compartments and in most important equipment	Fire is described by a zone code FIRIN, 1983, /19/
7.	HARVARD V	HARVARD UNIVERSITY, NATIONAL BUREAU OF STANDARDS, USA, H.W. Emmons, H. Mitler	Full fire zone model	Fire development and smoke spread in a room	Single compartment 1976, /20-23/

8. HARVARD VI	HARVARD UNIVERSITY, NATIONAL BUREAU OF STANDARDS J.A. Rocket, M. Morita	Full fire zone model	Fire development and smoke spread in rooms	up to 10 compartments /21-24, 36/
9. ASET	NATIONAL BUREAU OF STANDARDS, USA, L.Y. Cooper, D. W. Stroup	Pre-flashover zone model	Safe egress time	1980, /25/
10. FAST	NATIONAL BUREAU OF STANDARDS, USA, W.W. Jones	Full fire zone model	Smoke spread in rooms	Multiroom, 1984 /23, 26-27/
11. RFIRES	ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, USA, R. Pape	Zone model	Simulation of furniture fire in a room	Burning rate as input, 1976, /23/
12. DISLAYV	FÖRSVARETS FORSKNINGSANSTALT, Sweden, B.M. Hägglund	Pre-flashover zone model	Smoke filling of and extraction from a room	1986, /28-29, 37/
13. NAT	CENTRE SCIENTIFIQUE ET TECHNIQUE DU BATIMENT, (CSTB), FRANCE, M. Curtat	Full fire/ empirical zone model	Heat transfer into structures	One-zone model 1986, /30/
14. FISBA	CSTB, FRANCE M. CURTAT, X. Bodart, P. FROMY, A. BEYHOM	As 13	Fire development in a room	One room
15. CIFI	CSTB, FRANCE X. BODART, M. CURTAT	As 13	Fire development and smoke spread	Multiroom, multi-floor, 1987, /31/
16. COMPBRN III +	UNIVERSITY OF CALIFORNIA, Los Angeles, USA, V. Ho, N.O. Siu, G. Apostolakis	Full fire zone model		/32, 38/

17.	DOB	TECHNISCHE UNIVERSITÄT BRAUNSCHWEIG, FRG, R. Dobbernack	Full fire zone model	Fire development in a room	1 - 10 rooms, heat transfer by Monte Carlo, method, 1983, /33/ NPP validation
18.	MRFC	GESAMTHOCHSCHULE KASSEL, FRG, U. Schneider, U. MAX	Full fire zone model	Fire development in a room	NPP validation, /39/
19.	KAMELEON FIRE E-3D	SINTEF, NORWAY	FIELD MODEL	TRANSIENTS CALCULATION OF POOL FIRES	3D
20.	FLOW-3D		FIELD MODEL		
21.	BRI 2	BRI, JAPAN, T. TANAKA K. NAKAMURA	FULL FIRE ZONE MODEL	FIRE DEVELOPMENT AND SMOKE SPREAD	MULTIFLOOR-MULTIROOM CODE /40/
22.	CCFM.VENTS	NIST, USA, L. Y. COOPER G. P. FORNEY	FULL FIRE ZONE MODEL	FIRE DEVELOPMENT AND SMOKE SPREAD	TWO-ZONE CODE WELL DOCUMENTED /41/
23.	HAZARD I	NIST, USA, R. W. BUKOWSKI R. D. PEACOCK, W. W. JONES, C. L. FORNEY	INCLUDES FAST (Nr. 10) AND RISK ASSESSMENT ROUTINES	FIRE DEVELOPMENT, EGRESS TIME	RISK ASSESSMENT FOR A HOUSE /42/

5 UNCERTAINTY ANALYSIS

5.1 Introduction

The results of level 1 PSA are exposed to various uncertainties which have sometimes been considered to limit the value and the usefulness of PSA. In spite of the fact that the uncertainties related to the probabilistic approach are inherent to the method and cause some difficulties to the analysis, it is possible to evaluate the uncertainties in a rational way. This property is not a weakness but a strength of the PSA-methodology. Thus far the other methods for dealing with uncertainty and risk have not been developed to similar maturity and consistency as PSA. If the uncertainty issues are treated rigorously and stated clearly, the uncertainty analysis is beneficial in supporting the credibility of the results and in prioritizing further analyses and research.

The basic types of uncertainty are usually divided into two categories:

- statistical uncertainty due to stochastic variability of the quantity of interest and scarce data base
- modelling uncertainty due to incomplete knowledge of correct success criteria and inability to deal with all phenomena or accident scenarios in the model.

The uncertainties of PSA originate from several sources. The specification of the problem to be solved by the PSA may be inexact and may lead to an incomplete picture of the plant and an inadequate PSA scope and procedure. The conceptual model for the description of the relevant mechanisms and processes may be insufficient. The logical or mathematical models as well as the values of the model parameters (probability models, fault trees, event trees etc.) used in the description of the process may be improper representations of the plant.

The approximations and truncations used in the numerical solutions of the model may cause undetected errors in the results. In the case of very large fault trees this error may be substantial.

The scope of the uncertainty studies is partly dependent on the type of analysis and the objective of the PSA. Two major categories of PSAs are briefly defined as follows:

- The first type of analysis, a-posteriori analysis, is normally based on plant specific operating experience and it is used for safety assessments of operating plants.
- The second type of analysis, a-priori analysis, refers to new design projects or new plants without operating history where a generic data base is used to provide the basic information for the analysis.

In every case the objective of uncertainty analyses is to identify the uncertain assumptions behind the PSA models and data and to evaluate the impact of uncertainties on the result of PSA and the decisions made by the aid of PSA. Further, uncertainty analyses may be performed to enable meaningful comparisons of PSA results for different system designs, strategies or whole nuclear power stations. The results of uncertainty analyses may also be essential in evaluating the compliance of PSA results with safety goals.

5.2 Uncertainties of PSA

5.2.1 Statistical data uncertainties

The statistical or data uncertainties originate from the lack of proper, plant-specific, statistical information or operational experience on the issues under analysis. Further, the information available to the analysts may not be applicable or may not be consistent with the details of the fault trees or component failure models.

The data often come from several sources and the analysts have to decide whether to pool the data together or not. If the data are pooled the uncertainty or confidence regions of the parameters are apparently smaller but, if these parameter values are used to describe several components in system reliability analyses, the uncertainty of system reliability is larger due to the failure rate dependencies introduced by pooling.

Some of the most important contributors of the PSA models are sometimes based on the smallest statistical evidence. Good examples of this are LOCA frequencies, CCF probabilities and human error probabilities. Often the value of these parameters depends on plant specific factors and thus the data from generic sources may not be applicable.

5.2.2 Modelling uncertainties

The modelling uncertainties may have an impact on the risk estimates through the initiating events, event tree models, systems success criteria and fault tree models, as well as through the human error and component failure models.

The dependencies between initiating events, system functions and associated success criteria result in underlying modelling uncertainties in event trees. In the case of common cause initiators this problem is familiar; for example it may not be known with certainty how many redundant trains are needed to satisfy a system function in case a specific initiator occurs and how many redundant trains are unavailable due to the initiator. Furthermore the models for systems interactions in phased accident sequences include uncertainties (e.g. it may not be known whether common cause failures have effect in each phase of the accident sequence).

The modelling uncertainties of the fault trees are rather similar to those of event trees. Most uncertainties are connected to the models due to system interactions, electrical systems and time dependent phenomena.

Modelling uncertainties concerning the basic events are connected to inadequate descriptions of quantities, events and actions such as

- component failures

- component recovery
- component interactions
- human interactions.

Models for component failures may also be inadequate to account for the failure mechanisms under analysis, and the repair or recovery models may be based on incorrect assumptions. Examples are the time dependent vs. time independent component wear-in and ageing failure models, the reliability models of components in external phenomena such as floods, fires or extreme weather conditions. Similar types of uncertainty originate from some common cause failure models e.g. parametric models that give almost no credit to additional redundancies due to a poor underlying structure of the models. The models of human error are still rather poor, and their structure does not necessarily correspond to the complex real phenomena.

The special modelling uncertainties concerning the boundary conditions of PSA and incompleteness are discussed in their own paragraph below.

Issues related to the boundary conditions of PSA

The objective of the PSA determines its scope. All PSAs are not equally extensive. Some phenomena are intentionally excluded from the scope of a PSA and thus they should not be considered as a modelling uncertainty.

In order to avoid the improper interpretation of the incompletenes issue the scope of a PSA should be defined explicitly and clearly. The clear definition also makes further extensions of the analyses possible. Further, unconstructive criticism can be avoided.

Another aspect of modelling uncertainty is the excessive conservatism sometimes used in PSA models e.g. FSAR success criteria of system functions result in an intentional overestimation of risks. On the other hand, some passive components (e.g. pipes and vessels) may not be included in the explicit models because of their high reliability compared to active components.

5.2.3 Incompleteness

In principle the incompleteness is one of the most important uncertainty issues because it tends to cause underestimation on the total risk. If a PSA is "incomplete" (within its scope), then all phenomena or accident possibilities are not included in the models and some might remain as serious, but unseen, danger.

The causes of incompleteness are methodological, economical and technical. The methodological causes are due to the weaknesses of the hazard identification methods. The methods used may be improper for identification of risks of the system under analysis or may be unable to reveal disturbances caused by certain factors. For example FMEA does not apply well to identification of human errors in operation of a nuclear power plant.

The practical causes for the identification of incompleteness originate from insufficient resources available to the analysis. The problem of analysis resource allocation thus has to be solved in management of the risk analysis.

The technical causes of incompletenesses are due to the complexity of the systems and phenomena to be analyzed. The complexity may be both internal or external. The external complexity arises from the interactions between the technical system and its environment. Possibilities for identifying all the effects of external phenomena are always limited.

Lack of completeness is typically connected to the identification of initiating events, to the construction of the accident sequence models and event trees and to the construction of fault trees. The component failure models may also be incomplete.

Typical incompleteness of the initiating event analysis is:

- incomplete identification of initiating events
    * e.g. initiating events resulting from nitrogen and compressed air systems

- incomplete categorization of initiating events
    - * e.g. inadequate definition of loss of coolant accident categories
- inadequate treatment of dependencies between initiating events and systems
    - * e.g. main coolant pump seal LOCA and simultaneous loss of ECCS due to loss of cooling of pump bearings induced by loss of service water.

The incomplete treatment of initiating events may originate from analysts' inadequate knowledge of the plant. The approach in which the initiating events are taken directly from other PSAs or generic lists may lead to the mis-identification of plant specific features.

Possible lack of completeness in the event tree analyses include

- incompletenesses due to the modelling principles
- incomplete identification of systems interactions and operator interactions in the event trees
- incomplete evaluation of influence of the plant state and operating conditions and the variability of physical parameters of a given plant state on success criteria and the availability of the emergency functions.

The modelling principle used in the event tree analyses may give rise to incomplete models of some phenomena. For example, the approach where very large fault trees and small event trees are used may lead more easily to inadequate models of the accidents, since the small event trees may not describe in details the accident sequences. Large event trees and small fault trees may lead more easily to ignorance of the details in the emergency system models. This issue is also very important in the review of PSAs.

The safety functions are often performed by several systems which are interconnected and dependent on each other. The dependencies have a very large impact on the final results of PSAs and thus careful analysis of them is important.

The state of the plant before and after an initiating event affects the course of the accident. Depending on the plant state the success criteria of the emergency systems may vary remarkably. If these factors are not taken into account the results of the analyses may be misleading.

Incompleteness of the fault tree models is interconnected with that of the event tree models discussed earlier. The basic causes of incompleteness in the fault tree models are

- inadequate identification of basic events
- inadequate and inexact definition of basic events
- poor implicit or explicit modelling of common cause failures and human errors
- poor modelling of several failure modes of components
- inadequate modelling of logical loops.

The inadequate identification of basic events in the fault tree includes for example the incomplete treatment of the human error events, mis-calibrations and common cause failures.

The above type of incompleteness is also related to the definition of the basic events. If the basic events for some component type are not clearly specified, it is not easy to include them into the fault tree. In the specification of the basic events, methods like FMEA are of great advantage.

CCF events may be included in the fault tree models both in explicit and implicit ways. In the implicit approach, the CCFs are not modelled as basic events in the fault tree. Depending on the approach it is possible to miss some CCF possibilities. The same problem also occurs in the case of human errors.

Some system failure mechanisms may contain complicated looped dependencies and the failures may happen in cascades. For example control of AC systems needs DC power which requires power supply from AC system. This kind of dependency causes loop-like structures into the fault trees, and the respective models are difficult to construct.

The problem becomes more difficult if the components have several failure modes.

5.3 Methods and principles of uncertainty analysis

Mature methods are available for the analysis of parametric and data uncertainties. In contrast, very few methods for analysing modelling uncertainty seem to be available. In the following we discuss the methods for each uncertainty category.

5.3.1 Analysis methods for data uncertainties

The treatment of the parametric or statistical uncertainties has been a part of PSAs since WASH-1400 study was published. The approach in which the parameter uncertainties are propagated through the models is well known. Problems arise with the determination of the probability distributions for uncertain parameters.

In the Bayesian approach the uncertainty distribution of the parameter is obtained by combining the prior distribution with the statistical evidence by applying the Bayes Theorem. The statistical evidence is described with the likelihood function, which is based on the sampling model (e.g. the sampling model describing the numbers of failures in certain time period is the Poisson distribution). The prior distribution is either non-informative or based on expert judgement or earlier empirical observations. In the Bayesian approach the probability may be interpreted as a subjective degree of belief, and the subjectivity of the assumptions in the prior distributions is admitted.

In the frequentist approach all distributions should be based on empirical observations since the probability is interpreted as a objective property of nature. Further, the statistical confidence on the estimates or the values of unknown parameters is interpreted as the uncertainty distribution.

Often the Bayesian and the frequentist approaches have been seen as totally contradicting views. However, there are statistical methods which lie between these two approaches. Many so called empirical Bayesian methods are examples of this (see for example, Jänkälä and Vaurio, 1987 and Vaurio, 1987). The basic difference of these two views is the interpretation of probability, which usually has no remarkable impacts on the practical use of PSA. The philosophical discussions on the interpretation of probability can be found in Apostolakis et al (1988).

Often the uncertainty distributions needed in PSAs cannot be determined on the basis of actual operational experience but only as expert opinions. Since the expert opinions are always subjective or some kind of concensus distribution formed from experts' distributions, the frequentistic interpretation of probability is not sufficient. Expert judgements have been applied for example in NUREG-1150 and some of the results concerning the probability of check valve failure have been published (see Ortiz et al, 1989). The nature and the problems of expert judgements are discussed e.g. in NUREG/CR-4962 (1987) and Clarotti and Lindley (1988).

Despite continuing efforts, the plant specific reliability data bases with parametric uncertainty intervals for use in PSA are still missing in many countries. Good examples of data bases are found from Sweden, where a plant specific reliability data book is updated regularly (see Pörn, 1990, 1991), from the Loviisa nuclear power plant in Finland (see Jänkälä et Vaurio, 1987), and in the French data collection programme 'SRDF'.

Often the data used in PSAs is taken directly from PSAs of similar plants, or from plant specific operational experiences on adhoc base. In USA, there are several compilations of reliability data based on the licensee event reports (see NUREG/CR-1205, -1331, -1363, -1740, -2886, -3831). IAEA has also compiled a data base (see IAEA-TECDOC-508).

The most uncertain reliability parameters in PSAs are without doubt the common cause failure probabilities and human error probabilities. The methodology for evaluation of the uncertainty distributions of CCF-parameters is available, but the interpretation of operating experience, which has a strong effect on the uncertainty distributions, needs to be considered carefully. In addition, the treatment of correlations between different CCF parameters is still an unresolved issue in parametric methods. For human error probabilities the problem is still worse, because in almost every case one has to lean on expert judgements.

The grouping of the components in the statistical data analysis causes dependence of the parameters of component failure models. If this dependence is not taken into account in the propagation of uncertainties, the result will be incorrect. This so called "state of knowledge" dependence is very important also in the common cause failure analysis. There are several ways of handling failure rate coupling phenomena in PSA quantification. The complete coupling approach assumes that the failure rates of all similar components have a common (random) value. This implies broader uncertainty intervals and also larger core melt frequencies due to the dependency of failure rates. The other extreme approach is based on the assumption that the failure rates of similar components are independently (randomly) sampled from a common distribution. This leads to narrower uncertainty intervals and possibly to the underestimation of the core melt frequency. Other possibilities are intermediates between the above two extreme cases, and they may be more realistic. The coupling models have been discussed by several authors, for example Apostolakis and Kaplan (1981), Virolainen (1984, 1985), Kleppman and Wutchig (1986) and quite recently Vaurio (1991).

The sampling models and the dependency structures built into them should be taken into account in the coupling considerations. For example, if the operational experience evidence for a group of components is pooled, then these components should be treated as completely coupled in the PSA calculations. This dependency can also be modelled explicitly as is done in the Bayesian model of the Swedish reliability data book (see Pörn, 1990).

Expert judgement in uncertainty analysis

Expert judgements are used to assess the probabilities and frequencies of events and their uncertainties in the cases of scarce data as well as some phenomena difficult to understand. In level 1 PSA expert judgements are frequently used in human error analyses and in seismic hazard analyses.

In human error analysis made by means of expert judgments the uncertainty bounds are usually based on some anchor points i.e. known error probabilities received from simulator exercise or operating experience and on common statistical methods. In case of seismic hazard analysis the uncertainty bounds are derived by giving weighting factors to each of the hazard curves estimated by separate experts. These weighting factors are also expert judgements and highlight the variations between the estimates provided by different experts. Expert judgements are used also to assess the probabilities and uncertainty of phenomena during severe accident progress in containment; such as steam explosions, direct containment heating and hydrogen burns which are difficult to estimate by analysis or by experiments.

5.3.2 Analysis methods for uncertainty propagation

Monte Carlo simulation

One of the most usual methods for propagation of the parameter uncertainties is the direct Monte Carlo simulation. The approach is straightforward; first the parameters are sampled from their uncertainty distribution and then the PSA calculations are performed with the sampled parameter values. After repeating the calculations several times the distribution of the quantity of interest is constructed. The procedure requires rather large sample sizes (appr. 5,000-20,000) and the computation time may be long. However, the development of algorithms and the efficiency of computers has been fast and nowadays the computational problems are not a remarkable restriction. Satisfactory results can be obtained by PCs as was demonstrated for example in the Nordic reference study on uncertainty analysis (see Hirschberg et al, 1989).

The Monte Carlo sampling algorithms are usually realised by utilizing standard efficient sampling techniques. Recent PSA codes on PCs are usually equipped with a Monte Carlo simulation algorithm. As an example we mention the codes STUK PSA (Niemelä, 1990)and RISKSPECTRUM (see Berg, 1990).

In order to make the Monte Carlo simulation more efficient approaches based on so called Latin Hypercube Sampling (LHS) have been developed and applied. An example of this methods is the computer code TEMAC, which has been applied in NUREG-1150 (see Iman and Shortencarrier 1984, 1986).

In the LHS method the range of each input parameter X_i, i = 1,...,k, is divided, to n non-overlapping intervals, which have the same probability. One value is selected from each interval at random with respect to the conditional probability distribution in the interval. The n values thus obtained for X_1 are paired in a random manner with the n values of X_2. These pairs are combined in a random manner with the respective values of X_3 and so on, until n k-tuplets are formed. The sample obtained this way is called Latin hypercube sample. It is convenient to think of the LHS, or a random sample of size n, as forming an n,k matrix of inputs where the i^{th} row contains the specific values of each of the k input parameters to be used on the i^{th} run of the computer model. It is clear from the above that the model has to be evaluated n times, and thus the computational cost grows linearly with the number of discretization intervals (n) of the input parameters.

It is also possible to apply discretization of the input parameters in the usual Monte Carlo simulation. This may be useful when the input distributions are complex.

Discrete probability distribution method (DPD)

The analytical evaluation of the uncertainty of an output variable is feasible or possible only in some very simple special cases. However, if the probability distributions are discretized it is possible to give analytical expressions for the uncertainty distributions of the output variables. In the DPD method (DPD = discrete probability distribution) the distributions of the input variables are described with a discrete distribution (x_1, p_1;...;x_n, p_n) in such a way that the moments of the original distribution are equal to those of the discretized distribution. Since the function describing the core melt frequency is usually a polynomial or other simple function of the input parameters, it is possible to determine the discrete distribution for the core melt frequency rather simply. The problem is that the number of calculations increases rapidly when the number of discretization intervals and the number of input variables increases (Ahmed et al, 1982).

The DPD method has been applied in many PSAs made by Pickard, Lowe and Garrick Inc. As an example we mention the Seabrook Station PSA (1983). The method is applied in the computer code BEST.

Variance propagation

In principle the moments of any output variables (if exist) can be determined as a function of the moments of the input variables. Exact expressions can be calculated only in the case of simple structures, i.e. when the structure is a simple series and parallel structure and when the input parameters follow some specific distribution (gamma or beta distribution). In the case of more complex functions one has to apply some approximation, e.g. a Taylor series approximation. The properties of approximation techniques have been studied by Dinsmore (1986). This approach has not been very popular in PSAs. Principles based on methods similar to variance propagation have been applied in evaluation of uncertainty importance measures e.g. in the Loviisa PSA (Andsten, Vaurio 1989). The same problem is also discussed by Iman and Hora (1990).

5.3.3 Analysis methods for modelling uncertainties

The identification of modelling uncertainties is equivalent to the identification of uncertain assumptions in the PSA models. The uncertain assumptions may be identified by careful review of the models. The review is possible only when the documentation of the models is adequate.

After identification of uncertain modelling assumptions their significance should be evaluated. It is, in principle, possible to perform sensitivity analyses with respect to the uncertain assumptions, but in practice the number of these sensitivity analyses may be too large. The significance of the uncertain assumptions must then be evaluated on the basis of engineering or expert judgements, informed by limited sensitivity studies.

An example of uncertain modelling assumption in the TVO PSA is discussed by Virolainen (1991). The success criterion 1/12 for safety relief valves was used in PSA model. However this success criterion may be non-conservative. If the success criterion were converted into 5/12, this change would result in a significant increase in the core melt probability such that the total core damage probability, 3.5 x 10^{-5}/a, increases as high as to 5.4 x 10^{-5}/a. By assigning subjective probabilities to alternative success criteria this kind of modelling uncertainty could have been propagated through the PSA model analogously to parameter uncertainty (see Chibber et al, 1991).

It should be noted that the scope of probabilistic uncertainty analysis is limited to the uncertainties satisfying the following conditions:

- there is a well defined set of alternatives
- it is unknown which of the alternatives is true.

One approach to the evaluation of the model uncertainties is based on qualitative review of the PSA-models. This approach was adopted in the PRA of the Finnish nuclear power plant TVO 1-2 (Holmberg and Himanen, 1991). In this study the uncertainties were first identified and classified following the hierarchy of the PSA models. The highest level in the hierarchy was the initiating events, the second level was event trees, then the fault trees and the lowest level was the basic events in the fault trees.

The uncertainties were identified by interviewing the PSA analysts and studying the PSA reports (such as failure mode and effects analyses and event tree descriptions). Also the plants' Final Safety Analysis Reports (FSAR) were used. In this context also the PSAs made for similar plants (e.g. the Forsmark 1/2 PSA) are used for comparison of the modelling assumptions. The identified uncertainties were documented on a specific model form, which contains the name of the submodel considered, the participants of the uncertainty analysis, references to the PSA models and methods applied, and the list of assumptions behind the modelling issue. Further, the significance of the uncertainties in the assumptions was evaluated and documented on the model form.

Holmberg and Himanen (1991) compare also the qualitative and quantitative uncertainty analyses, since these two approaches have different objectives and principles. The comparison is summarized in Table 1.

The issues considered in Table 1 are relevant with respect to all kinds of uncertainties, not only the modelling uncertainties. For example, the uncertainty in failure model parameters can also be analysed qualitatively. In any practical case the uncertainty analysis should include qualitative considerations, which are often neglected.

5.3.4 Analysis of incompleteness

The degree of completeness of a PSA can hardly be quantified. The only possibility to treat the uncertainty due to incompletenesses is to minimise it. The incompletenesses can be minimised by careful review of the PSA models. In this review the plant specific event reports are extremely useful; they can be used in comparison between the occurences and their models. The operating experience from other plants (similar and different) is also useful. The analysis of operating experiences can be made in the form of so called precursor studies.

Table 1. Comparison of qualitative and quantitative uncertainty analyses

	QUALITATIVE STUDY	QUANTITATIVE STUDY
Goals	Identification Description	Assessment of importance Demonstration of impact
Treatments	Check lists Comparison between uncertainties	Sensitivity studies Uncertainty propagation
Description of uncertainties	Verbal Classification (large/ small, over-/under-estimation, etc.)	Numerical Importance measures Probability distributions
Benefits (+)	+ Flexible to cope with all kinds of uncertainties	+ Provides means for comparisons - difficult to treat modelling uncertainties
Drawback (-)	- uncertainties from various sources - no uncertainty statement for PSA result	

5.4 Use of uncertain PSA results in decision making

The results of level 1 PSA can be applied in various decision making situations. The most usual decisions are connected to selection of alternative designs, optimization of maintenance routines and surveillance testing schemes and optimization of safety related technical specifications. In many cases the decisions are made without considering the impact of uncertainties in the results on the decision.

Often the level 1 PSA results have been only one ingredient within the basically deterministic decision making procedure. In many cases the safety decision making is also based on a simple evaluation of PSA results providing insights into

- balance between accident sequences
- compliance between results and informal safety objectives
- probability of core melt, if exceptionally high.

When pursuing a consistent, unambiguous decision making procedure by the aid of PSA the clear interpretation and documentation of the results of uncertainty analyses is essential. The core melt uncertainty distribution is not enough. The identification of the most important contributors to the uncertainty is one of the objectives of uncertainty analysis. For this purpose some measures for uncertainty importance have been developed (see for example Iman and Hora, 1990 and Andsten & Vaurio, 1989). We have to admit, however, that the uncertainty importance measures have not been applied very often in level 1 PSA, and that there is still a need for further research.

The documentation of uncertainty analysis should include all the assumptions and reasoning behind the states of knowledge of quantifications with respect to parameter and model uncertainties and an evaluation of the effects of these assumptions on the final result (see Holmberg and Himanen, 1991 and NKA project RAS-450, 1990). In this respect a careful uncertainty analysis is also a part of PSA review.

If the uncertainties included in the different decision alternatives have equal impacts on the results, the need to take them into account is not quite decisive. However, in many cases the uncertainties included in the competing alternatives differ both in quality and in quantity. The decisions can be difficult, if in one decision alternative the most important uncertainties are connected to modelling assumptions and in the other alternative the uncertainties are connected to the values of the model parameters.

The first step in the comparison of decision alternatives is the identification of the uncertainties of each alternative. In this step the analysts should question every modelling assumption and identify and classify the uncertainties involved. After this basically qualitative step the analysts should rank the uncertainties included in the decisions alternatives. The ranking of alternatives requires various sensitivity analyses in which the uncertain assumptions of parameter values are varied in order to find the dominating factors.

The application of sensitivity analyses is essential in finding the preferred decision alternatives and often no further analyses are necessary. If the most important decision criterion is the core melt frequency, it may be interesting to find the parameter values or combination of assumptions where the preference order of the alternatives changes. The order of alternatives may be very sensitive to the assumptions and in this case the decisions cannot be made solely on the basis of PSA calculations and further uncertainty analyses are needed. The nature and the amount of the sensitivity studies needed are highly case dependent.

The parameter (and sometimes modelling) uncertainties may be described with probability distributions and it is possible to analyse the impact of these uncertainties on the final results by applying the methods discussed earlier. If the resulting uncertainty distributions are ordered stochastically (see Figure 1), the best decision alternative is easily found (the best alternative has also the smallest expected core melt frequency). In practice the alternatives rarely dominate each other and deeper decision analysis is needed.

The core melt frequency is not the only decision criterion. In practice the safety decisions are often made without analytical deliberation, using common sense and engineering judgement. These decisions, however, typically contain an implicit evaluation of some important factors such as, cost, benefit and damage. The decision e.g. on a plant backfit is typically preceeded by optimizing the combination of the aforementioned factors, not necessarily by consistent analytical method but by judgement. So, in almost all cases the safety decision is also based on other factors than safety indicators. This makes the decision making complex. Usually one has to take into account the source term, and the possible consequences of the accidents as well as the economical operation of the plant. This leads to a multi-criteria decision problem in which the conflicting decision criteria have to be balanced with respect to each other. First, one has to identify the decision criteria and divide them into subcriteria. Furthermore, the weights of each criterion have to be assessed by making trade-off analyses, which are often very difficult.

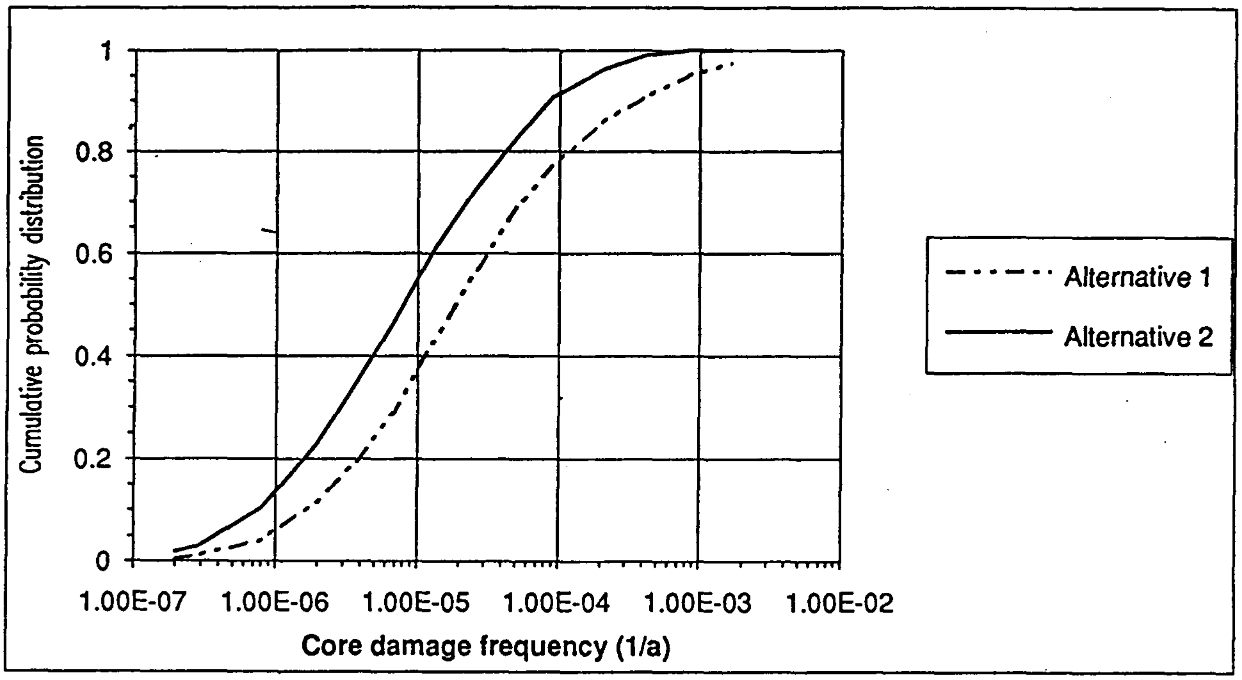


Figure 1. Stochastic dominance of core melt frequency distributions: the distribution of the alternative 1 is stochastically larger

The applications of decisions theoretic methods in safety related decisions are not very widely discussed in the literature and only a few examples are reported (Nelson and Kastenberg 1986). Often the results of multi-criteria decision analyses are sensitive to the assumptions and small changes in trade-off principles may lead to large changes in the optimality of the alternatives (Sinkko K., 1991). Evidently the decision analyses in their present form are laborious to use as practical every day tools and further research and experience on their application are needed (see Appendix 1).

References

1. Ahmed et. al., A Method for Propagating Uncertainty in Probabilistic Risk Assessment, Nuclear Technology Vol. 59, Nov. 1982.

2. Analysis of Core Damage Frequency: Internal Events Methodology. (1990) NUREG/CR-4550, Vol. 1, Rev. 1. U.S. Regulatory Commission, Washington, DC, January 1990.

3. Andsten, R. and Vaurio, J.K. (1989): Reliability Importance Measures and their Calculation, Research Report, IVO-A-01/89, Imatran Voima Oy.

4. Apostolakis, G.E., Farmer, F.R, van Otterloo, R.W. (eds.) 1988. Reliability Engineering & System Safety, Vol. 23 No. 4.

5. Apostolakis, G., Kaplan, S., Pittfalls in Risk Calculations, Reliability Engineering, 2, 135, 1981.

6. Berg, U. (1990) Realisation of True Living PSA: A Challenging Software Development Task. Second TUV-Workshop on Living PSA Application, Hamburg 7-8 May 1990.

7. Chibber, S., Apostolakis, G., Okrent, D. (1991) On the Quantification of Model Uncertainty. Proceedings of the International conference on Probabilistic Safety Assessment and Management (PSAM), Beverly Hills, CA, U.S.A. pp. 1483-1488. February, 1991.

8. Clarotti, C.A., Lindley, D.V. (eds.)(1986), Accelerated Life Testing and Experts' Opinions in Reliability. Proceedings of the International School of Physics "Enrico Fermi", 1988.

9. Clarotti, C., Spizzichio, F., Volta, G., Latest Advances in Bayesian Statistics and their Impact on Reliability and Probabilistic Risk Assessment, Proch. PSA'87, Zürich. European Nuclear Society.

10. Component Reliability Data for Use in Probabilistic Safety Assessment. IAEA-TECDOC-478. A Technical Document Issued by the International Atomic Energy Agency, Vienna, 1988.

11. Dinsmore, S., Approximation Errors During Variance Propagation, SRE Symposium'86, Otaniemi, Finland, October 14-16, 1986.

12. Garrick, B. John, Power Plant Availability Decision Making Under-Uncertainty, 34th Annual Technical Conference American Society for Quality Control, Atlanta, Gerogia, May 20-22. 1980.

13. Hirschberg, S., Jacobsson, P., Pulkkinen, U., Pörn, K. (1989). Nordic Reference Study on Uncertainty and Sensitivity Analysis. PSA'89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pensylvania, U.S.A., April 2-7, 1989.

14. Holmberg, J., Himanen, r. (1991) Uncertainty study in probabilistic risk assessment for TVO I/II nuclear power plant. CSNI Workshop on Special Issues of Level-1 PSA. Cologne, Germany, 27th-29th May 1991.

15. Iman, R.L., Helton, J.C. (1985) A comparison of Uncertainty and Sensitivity Analysis Techniques for Computer Models. NUREG-CR-3904, SAND 84-1461. Sandia National Laboratories, Albaquerque, NM. U.S.A. March, 1985.

16. Iman, R.L. and Hora, S.C. (1990) A Robust Measure of Uncertainty Importance for Use in Fault Tree System Analysis. Risk Analysis, Vol. 10, No. 3, pp. 401-206.

17. Iman, R.L. and Shortencarrier, M.J. (1984), Fortran 77 Program and User's Guide for the Generation of the Latin Hypercube and Random Samples for the Use with Computer Models, NUREG/CR-3624, Sand 83-2365, Sandia National Laboratories, NM, March 1984.

18. Iman, R.L., Shortencarrier, M.J. (1986) A User's Guide for the Top Event Matrix Analysis Code (TEMAC), NUREG/CR-4598, SAND 86-0960, Sandia National Laboratories, Albaquerque, NM, August 1986.

19. Jänkälä, K.E., Vaurio, J.K., Component Aging and Reliability Trends in Loviisa Nuclear Power Plant, Proc. PSA'89, April 2-7, 1989, Pittsburgh, Pennsylvania, USA. American Nuclear Society.

20. Jänkälä, K.E., Vaurio J.K., Empirical Bayes Data Analysis for Plant Specific Safety Assessment, Proc. PSA'87, August 30 to September 4, 1987, Zürich Switzerland. European Nuclear Society.

21. Kleppman, W.G. and Wutchig, R., A Model for Coupling of Failure Rates in a Redundant System. Nuclear Eng. Des. Vol. 94 (1986), pp. 167-175.

22. Nelson, P.F., Kastenberg, W.E., An Extended Value Impact Approach for Nuclear Regulatory Decision Making. Nuclear Engineering and Design 93 (1986) 311-317.

23. Niemelä, I., Demonstration of the Properties of the Finnish STUK PSA-Code *Program-Demonstration* Second TüV-Workshop on Living PSA Application, Hamburg 7-8 May 1990.

24. NKA project RAS-450, "Optimization of Technical Specifications by Use of Probabilistic Methods", edited by K. Laakso, Nordic liaison committee for atomic energy, 1990.

25. NUREG/CR-1205. Data Summaries of Licensee Events Reports of Pumps at U.S. Commercial Nuclear Power Plants EG & Idaho, Inc., January 1982.

26. NUREG/CR-1331. Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at US Commercial Nuclear Power Plants, EG & G Idaho, Feb., 1980.

27. NUREG/CR-1363. Data Summaries of Licensee Event Reports of Valves at US Commercial Nuclear Power Plants, EG & G Idaho, Inc., October 1982.

28. NUREG/CR-1740. Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at US Commercial Nuclear Power Plants, EG & G Idaho, Inc., July, 1984.

29. NUREG/CR-2886. In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report, the Pump Component, Oak Ridge National Lab, December 1982.

30. NUREG/CR-3831. In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report, Diesel Generators, Batteries, Chargers and Inverters. Oak Ridge National Lab, January 1985.

31. NUREG/CR-4962. Methods for the Elicitation and Use of Expert Opinion in Risk Assessment, Pickard, Lowe and Garrick, Inc., August, 1987.

32. Ortiz, N.R., Wheeler, T.A., Keeney, R.L. and Meyer, M.A., Use of Expert Judgement in NUREG-1150, PSA'89, Pittsburgh PA, April, 1989.

33. PRA Procedures Guide. (1983) NUREG-CR/2300, U.S. Regulatory Commission, Washington, DC, January 1983.

34. Pörn, K. (1990) On Empirical Bayesian Inference Applied to Poisson Probability Models. Linköping University, Linköping.

35. Pörn, K. (1991) Some New Features of Methodology and Applications of the Updated Swedish Reliability Data Book. IAEA Technical Committee Meeting on "Probabilistic Safety Assess-

ment Requirements for Use in Safety Management", 16-20 September 1991, Stockholm, Sweden, Studsvik Report No. NS-91/79.

36. Sinkko, K., Decision Analysis and Rational Countermeasures in Radiation Protection, STUK-B- VALO 70, Finnish Centre for Radiation and Nuclear Safety, September 1991.

37. Severe Accident Risks: An Assessment for Five U.S. Nuclear Power, NUREG-1150, Vol. 2, U.S. Nuclear Regulatory Commission, Washington, DC, June 1989.

38. Seabrook Station Probabilistic Safety Assessment (1983) Pickard, Lowe and Garrick, Inc. Rev. 2.

39. Vaurio, J.K. (1987), On Analytic Empirical Bayes Estimation of Failure Rates, Risk Analysis 7 (1987) 329-338).

40. Vaurio, J.K. (1991) Failure Rate Coupling Effects in Uncertainty Analysis of Redundant Systems. Reliability Engineering and System Safety. 35. (1992) 183-193.

41. Virolainen, R., On Common Cause Failures, Statistical Dependence and Calculation of Uncertainty; Disagreement in Interpretation of Data, Nuclear Engineering and Design 77 (1984) 103-108.

42. Virolainen, R. and Buslik, A., On Common Cause Failure Methods Dealing with Dependent Failures: a Comparative Application to US Diesel Generation Data Based on Licensee Event Reports, International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications 24-28 February 1985, San Francisco.

43. Virolainen, R.K., Regulatory Review of PSA Studies made for Operating Finnish Nuclear Power Plants and Its Implications For Regulatory Decision Making and Living PSA, Proceedings of International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA'91, IAEA, Vienna, 3-7 June 1991.

An example of the use of multicriteria decision analysis (Sinkko K., 1991)

Table I. Protection problem I. Doses are given in manSv.

	States		
	No release	Inert gases	Particles
No actions	0	10	20
Sheltering	0	5	10
Evacuation	0	0.5	1
		Probabilities	
	0.8	0.15	0.05

Example

There has been a severe accident at a nuclear power plant and the environmental effects caused by it are still unknown at the moment of decision. The probability is 0.8 that the situation will be brought under control and there will be no release. The accident will cause an inert gas release at a probability of 0.15 and, respectively, the probability for other radioactive nuclide release is 0.05. The decision maker must choose between three countermeasures to protect the population of a certain area: evacuation, sheltering indoors, and the zero option, i.e. taking no action at all. The population of the area is 1000 persons. The decision maker has estimated that only the attribute "health detriment caused by radiation" is essential and can be measured as a dose. In this stylized example the dose distribution is not taken into account. The mean doses of the area have been estimated for different options and are shown in Decision Table I.

In this example the purpose is not to illustrate the interactive interview, typical to the analysis, between the decision maker and the analyst, e.g. Keeney[8]. The purpose is only to indicate the structure of the analysis.

Let us assume, without checking it out, that the decision maker is rational and the conditions for utility analysis exist. For example, in a simple money game the decision maker should not think that tossing a five-mark coin is luckier than tossing a one-mark coin. It is also necessary to ensure that the decision maker has understood the contents of the attribute. For example, in this case the attribute "health detriment" has meaning only for the stochastic health effects, and not, e.g. any psychological effects.

The shape of the utility function can be assessed with the following reference experiment[3,7]. There are two options, A and B:

Option A: The dose is 0 manSv with probability 0.5 or, otherwise, the dose is 20 manSv with probability 0.5.
Option B: The dose is 10 manSv for certain.

The decision maker has to choose between these two options. When assessing the value of the utility function at a fixed point, the value of option B is changed until the options are indifferent for the decision maker. The other possibility is to offer the decision maker the following choice:

Option A: The dose is 0 manSv with probability p or, otherwise, the dose is 20 manSv with probability 1 – p.
Option B: The dose is 10 manSv for certain.

The question is: what is the value of p such that the decision maker is indifferent between options

A and B. The decision maker in the example chooses a value of about $p \approx 0.4$. Because the origin and the scale of the utility function can be chosen freely, it can be set u(0 manSv) = 1 and u(20 manSv) = 0. Hence

u(10 manSv)
= 0.4 x u(0 manSv) + 0.6 x u(20 manSv)
= 0.4 x 1 + 0.6 x 0
= 0.4.

Similarly, the value of the utility function at point s = 5 manSv can be found by asking the decision maker to state his preferences between the bets:

Option A: The dose is 0 manSv with probability p or, otherwise, the dose is 10 manSv with probability 1 – p.
Option B: The dose is 5 manSv for certain.

If the probability chosen by the decision maker is p = 0.4 when the options are indifferent, we get

u(5 manSv)
= 0.4 x u(0 manSv) + 0.6 x u(10 manSv)
= 0.4 x 1 + 0.6 x 0.4
= 0.64.

The procedure is continued until all the utility values of the doses shown in the table I are defined:

u(0 manSv)	=	1.00	u(5 manSv)	=	0.64
u(0.5 manSv)	=	0.96	u(10 manSv)	=	0.40
u(1 manSv)	=	0.93	u(20 manSv)	=	0.00

The utility function of the decision maker is convex and implies an attitude apt to taking risks. The attitude toward risk results in a threat of defeat connected to the decision[5]. The decision maker is asked questions until the analyst is satisfied that the utility curve well represents the preferences of the decision maker and there is no inconsistency between the values of the function. The expected utility $E = \sum_i p_i u(x_i)$ can now be calculated for different countermeasures:

No actions:
E = 0.8 x u(0) + 0.15 x u(10) + 0.05 x u(20) = 0.86

Sheltering:
E = 0.8 x u(0) + 0.15 x u(5) + 0.05 x u(10) = 0.92

Evacuation:
E = 0.8 x u(0) + 0.15 x u(0.5) + 0.05 x u(1) = 0.99

Because the values of the utility function defined by the reference experiment are not accurate – they are not assumed to be accurate in actual practice – the expected utility must be checked before a decision of finding out how sensitive the ordering of the actions is to the values used in the calculations. Thus the lower limit on the expected utility of the evacuation and the upper limits of no-action and sheltering indoors must be found. This is done by asking the decision maker the following bets:

Option A: The dose is 0 manSv with probability 0.5 or, otherwise, the dose is 20 manSv with probability 0.5.
Option B: The dose is 10 manSv for certain.

If the decision maker prefers option A to B, then

u(10) < 0.5 x u(0) + 0.5 x u(20) = 0.50

Accordingly, it is estimated that

u(5) < 0.70
u(1) > 0.89
u(0.5) > 0.95

The lower and upper limits on the expected utility (E) can now be calculated for different actions:

E(no actions) = 0.86 < 0.88
E(sheltering) = 0.92 < 0.93
E(evacuation) = 0.99 ≥ 0.99

The lower limit on the expected utility of evacuation is higher than the upper limits of sheltering and no-action. Thus the decision maker should prefer evacuation to the other two actions, whatever the numerical values of the utilities within the limits.

If we want to know at what dose level the evacuation should be implemented, the calculations tell us that the decision maker must favour evacuation no matter how small the dose is. This conclusion may look illogical but is due to the fact that the value structure which the decision maker attaches to the doses cannot change essentially when the dose decreases, assuming he is rational. The analysis in itself is not faulty, but the cause for inconsistency can be traced to excluding important objectives from the analysis (such as financial costs and safety issues involved in the actions).

When there is more than one attribute, the utility independence of the attributes should be verified before launching the utility analysis. Attribute X is utility independent of attribute Y if the preferences between lotteries with varying levels of X, and a common, fixed level of Y are independent of that fixed level of Y. If X is utility independent of Y, it follows that X is also preferentially independent of Y[3].

For example, let us consider the dose attribute S and the costs attribute C. Let us mark the least preferred values of the attributes as s_0 and c_0 and the most preferred ones as s* and c*. Let us also assume that the costs attribute is on the most preferred level, i.e. c* = 0. There are two options to be chosen, one corresponds to lottery $< p, s_0; (1 - p),s^* >$ and the other leads to the fixed value of S, marked as s'. Let p' be the probability when the options are indifferent to the decision maker. If probability p' is the same when $c = c_0$, then attribute S is utility independent of attribute C.

In general, if attributes $X_1,X_2,\ldots,X_q$ are mutually utility independent, the utility function can be written in the multiplicative form:

$$1 + ku(x_1,\ldots,x_q) = \Pi_i(1 + ku_i(x_i)), \qquad (5.1)$$

where $u_i(x_i) = u(x_1{}^0,\ldots,x_i,\ldots,x_q{}^0)$ and $u(x_1,\ldots,x_q)$ has been scaled so that $u(x_1{}^0,\ldots,x_q{}^0) = 0$. If the attributes are additively independent, it means that the utility function is additive

$$u(x_1,\ldots,x_q) = \Sigma_i u_i(x_i),$$

where $u_i(x_i) = u(x_1{}^0,\ldots,x_i,\ldots,x_q{}^0)$. Consider two attributes X and Y. Attributes are additively independent, if for all $x,x' \in X$ and $y,y' \in Y$

$$<0.5,(x,y);0.5,(x',y')> \sim <0.5,(x,y');0.5,(x',y)>.$$

For the present we limit ourselves to the case of two attributes, X and Y. The function $u(x,y_0)$ is effectively a utility function over X alone and $u(x_0,y)$ over Y. Functions u(x) and u(y) can be assessed by reference experiment in the same way as the utility function in the protection example. The decision maker do not need to consider trade-offs between the values of the attributes when assessing the functions. He is only required to assess single-dimensional utility functions. However, before the assessments it is necessary to fix the origin and the unit of measurement by choosing $u(x_0,y_0) = 0$, and $u(x_1,y_0) = 1$ and $u(x_0,y_1) = 1$ where it is advisable to take x_0 and y_0 as some mid-range values and where x_1 is more prefered than x_0 and y_1 is chosen so that $u(x_1,y_0)$ is indifferent to $u(x_0,y_1)$. In other words, after the unit of measurement of X has been chosen $u(x_1,y_0) = 1$, the decision-maker is asked to assess y_1 so that $(x_1,y_0) \sim (x_0,y_1)$. Concerning the decision maker this requires trade-offs between the attributes, but no considerations of uncertainties.

To determine the constant k, the decision maker is asked to define the points x_2,y_2 and x_3,y_3 so that $(x_2,y_2) \sim (x_3,y_3)$. Providing that $u(x_2,y_0) \times u(x_0,y_2) \neq u(x_3,y_0) \times u(x_0,y_3)$, k can be calculated using the expression $u(x_2,y_2) = u(x_3,y_3)$.

When there are more than two attributes, the following theorem provides a useful method for the analysis[8]. Let it be that $X = X_1 \times X_2 \times \ldots \times X_n$, $n \geq 3$. If, for some X_1, $\{X_1,X_j\}$ is preferentially independent of $\underline{X}_{1j}$ for all $j \neq 1$ and X_2 is utility independent of $\overline{X}_2$ ($\overline{X}_2 = X_1 \times X_3 \times \ldots \times X_n$), then

$$u(x) = \Sigma_i k_i u_i(x_i), \quad \text{if } \Sigma_i k_i = 1, \text{ or}$$

$$1 + ku(x) = \Pi_i(1 + kk_i u_i(x_i)), \quad \text{if } \Sigma_i k_i \neq 1,$$

Table II. Protection problem II. Doses given in manSv and costs as marks (FIM, manSv).

	States		
	No release	Inert gases	Particles
No actions	(0,0)	(0,10)	(0,20)
Sheltering	(50 000,0)	(50 000,5)	(50 000,10)
Evacuation	(400 000,0)	(400 000,0.5)	(400 000,1)
		Probabilities	
	0.8	0.15	0.05

where the utility functions u(x) and $u_i(x_i)$ are scaled from zero to one, k_i are scaling constants, $0 < k_i < 1$, and $k > -1$.

Example

We shall continue the protection example I and assume now that the decision maker has estimated only the attributes "health detriment" S and "the costs of the actions" C as important when making a decision. When estimating the costs, direct and indirect costs are taken into account. If no actions are taken costs are assumed to be meaningless. The expenses of sheltering indoors are 50 FIM/person and the evacuation 400 FIM/person. The decision table now has the form as shown in Table II.

To check the utility independence the decision maker is offered the following two choices:

Option A: The dose is 0 manSv with probability 0.4 or, otherwise, the dose is 20 manSv with probability 0.6.
Option B: The dose is 10 manSv for certain.

The costs are at first fixed at 0 FIM. Earlier in protection example I it was verified that the options are indifferent for the decision maker when the value of p is 0.4. Let us now fix the costs to 400 000 FIM. The decision maker in the example feels that the options are indifferent as long as the costs are fixed. Thus attribute S is utility independent of cost attribute C. To make sure that the valuations of the decisison maker are consistent, it is necessary to ask the lotteries with different values of probability p. The costs should not be fixed only to the smallest or the largest value. Correspondingly, the costs are verified to be utility independent of the dose with the following options:

Option A: The costs are 0 FIM with probability 0.4 or, otherwise, the costs are 400 000 FIM with probability 0.6.
Option B: The costs are 200 000 FIM for certain.

The dose is first fixed to 0 manSv and then to 20 manSv. The options are indifferent on both dose values for the decision maker in this example. Thus the attributes are mutually utility independent.

Let us now choose u(2 000 000,20) = 0 and u(0,20) = 1. After this the decision maker is asked to identify s such that (2 000 000,s) is indifferent with (0,20), i.e. how much the decision maker is ready to decrease the dose with 2 000 000 FIM. The answer is 20 manSv, i.e., when s = 0. If we want to calculate the constant k (expression 5.1), after assessing the utility functions, the following indifference is indentified:

(100 000,2) ~ (200 000,1)

Thus the decision maker is ready to invest 100 000 FIM in order to decrease the dose 1 manSv. Generally, the decision maker of the example is ready to invest 100 000 FIM to avoid one manSv on all values of the dose, provided that the consequences of the radiation exposure are stochastic.

The attributes are additively independent if the following lotteries are indifferent for the decision maker:

$< 0.5, (200\,000,2);0.5,(100\,000,1) > \sim$
$< 0.5 ,(200\,000,1);0.5,(100\,000,2) >$.

The constant k is then zero and the utility function can be written as:

$$u(c,s) = u(c,s_0) + u(c_0,s).$$

The single-attribute utility functions are assessed by the reference lotteries, as was done in protection example I. If there are many points, it is practical to use functional representation. In this case we can write the single-attribute utility function as:

$$u(x) = a(e^{bx} + c).$$

By fitting this function to the points determined with the reference experiment we get

$$u(c,s_0) = 1.8(\exp(-4.1\ 10^{-7}c) - 0.444)$$
$$u(c_0,s) = 1.8(\exp(-0.041s) - 0.444).$$

The values of the single-attribute utility functions in different points can now be calculated with these functions. The utilities are:

$u_s(0\ \text{manSv}) = 1.00 \quad u_s(5\ \text{manSv}) = 0.64$
$u_s(0.5\ \text{manSv}) = 0.96 \quad u_s(10\ \text{manSv}) = 0.40$
$u_s(1\ \text{manSv}) = 0.93 \quad u_s(20\ \text{manSv}) = 0.00$

$u_c(400\,000) = 0.73 \quad u_c(50\,000) = 0.96.$

The utilities calculated with the functions deviate a little from the utilities determined earlier with the reference experiment. The difference is meaningless, however. If the values are calculated only by the utility function, it must be checked whether the calculated values correspond to the preferences of the decision maker. For example, when the calculated utility $u_s(0.5\ \text{manSv}) = 0.96$, we ask the decision maker the following bet:

Option A: The dose is 0 manSv with probability 0.4 or, otherwise, the dose is 1 manSv with probability 0.6.
Option B: The dose is 0.5 manSv for certain.

Which bet would the decision maker choose? If the options are indifferent for him, it meets the consistency demands, because the utility for both the options is 0.96.

The utilities for different actions can now be presented in a decision table (Table III).

The expected utility E for different actions can now be calculated. Before the decision is made, it must be checked how sensitive the expected utility is in order to arrange the actions in preference order. For this we must find the upper and lower limits of the utilities of single-attribute utility functions. This is accomplished by the reference experiment shown in protection example I. The values are:

$u_s(0.5\ \text{manSv}) > 0.97 \quad u_s(10\ \text{manSv}) > 0.30$
$u_s(1\ \text{manSv}) < 0.96 \quad u_s(10\ \text{manSv}) < 0.50$
$u_s(5\ \text{manSv}) > 0.58$

$u_c(400\,000) < 0.79 \quad u_c(50\,000) > 0.93.$

Thus the expected utility E and its upper and lower limits for different actions are:

E(No actions) $= 1.86 < 1.88$
E(Sheltering) $= 1.88 > 1.83$
E(Evacuation) $= 1.72 < 1.78$

The expected utility of sheltering indoors has the highest value of the countermeasures, but is by no means truly the most preferred action. The other possibility is noaction, which has almost as good an expected utility as sheltering. According to the demands for consistency the decision maker

Table III.Calculated utilities for protection problem II.

	States		
	No release	Inert gases	Particles
No actions	2.00	1.40	1.00
Sheltering	1.96	1.60	1.36
Evacuation	1.73	1.69	1.66
		Probabilities	
	0.8	0.15	0.05

should choose sheltering indoors. The fact that these two actions have almost as good expected utilities points to an alternative action that would be a combination of noaction and sheltering indoors. This kind of combination of actions, with a better expected utility than sheltering indoors, can be constructed so that sheltering is decreased where costs are high and the averted dose small. Evacuation is a truly excluded action.